Universidade de Aveiro Departamento de Matemática
2009

OLGA NOBRE LIMA **ANÉIS DE VALUAÇÃO E VALUAÇÕES**

Universidade de Aveiro Departamento de Matemática
2009

OLGA NOBRE LIMA

ANÉIS DE VALUAÇÃO E VALUAÇÕES

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática e Aplicações, realizada sob a orientação científica da Dra. Ana Helena Alves de Malta Roque, Professora Auxiliar no Departamento de Matemática da Universidade de Aveiro.

Aos meus pais, José Maria e Ondina e aos meus irmãos Odelisa, Cíntia, Wilson e Tiago.

o júri

presidente

Prof. Doutor Paulo José Fernandes Almeida
professor auxiliar no Departamento de Matemática da Universidade de Aveiro

Prof. Doutor Gonçalo Gutierres da Conceição
professor auxiliar do Departamento de Matemática da Faculdade de Ciências e Tecnologias da Universidade de Coimbra.

Prof. Doutora Ana Helena Alves de Malta Roque
professora auxiliar no Departamento de Matemática da Universidade de Aveiro

agradecimentos

À minha orientadora, Prof. Dra. Ana Helena Alves de Malta Roque, pelo acompanhamento, pelas exigências, pelas sugestões e comentários, pelo apoio que me deu na execução desta dissertação.

Aos meus familiares e amigos, pelo estímulo, pelo apoio incondicional desde os primeiros momentos e sobretudo pelo carinho e amizade.

palavras-chave

Anéis, Valuação, Anel de Valuação, Valuação discreta, Anel de Valuação Discreta.

resumo

Esta dissertação consiste no estudo dos Anéis de Valuação e Valuações. Inicialmente fez-se um estudo sobre os tipos de anéis e algumas das suas propriedades. De seguida apresentam-se algumas propriedades dos Anéis de Valuação e a caracterização dos Anéis de Valuação Discreta. As Valuações surgem no final com a identificação dos dois tipos de valuações e com caracterização das valuações no conjunto dos números racionais.

keywords Rings, Valuation, Valuation Ring, Discrete Valuation, Discrete Valuation Ring.

abstract This thesis consists of study the Valuation Rings and Valuations. Initially we carried out a study on the types of rings and some of its properties. Then we present some properties of the Valuation Rings and characterization of the Discrete Valuation Rings. The Valuations appear at the end with the identification of two types of valuations and characterization of valuations in the set of rational numbers.

Introdução

A Teoria das Valuações teve início em 1912 pelo matemático húngaro Josef Kürschák (1864-1933) com a formulação dos axiomas de uma valuação. Tendo como suporte de estudo o livro de Kurt Hensel (1861-1941), a principal motivação de Kürschák era construir uma base sólida para o estudo da Teoria dos Números p-ádicos de Hensel.

Nas décadas seguintes houve um rápido desenvolvimento da Teoria das Valuações, evidenciada principalmente pela descoberta de que grande parte da teoria dos números algébricos poderia ser melhor compreendida usando os conceitos e métodos da teoria das valuações. Esse desenvolvimento deve-se às contribuições de matemáticos como Helmuth Hasse (1898-1979), Alexander Ostrowski (1893-1986), Wolfgang Krull (1899-1971), etc. A Teoria das Valuações acabou por ser aplicada em disciplinas como Geometria Algébrica e Análise Funcional.

Os anéis de valuação discreta surgem em Geometria Algébrica no estudo de propriedades locais de curvas planas, por exemplo, na caracterização da multiplicidade de um ponto numa curva plana.

O presente trabalho que se destina à defesa da dissertação para a obtenção do mestrado em matemática e aplicações, subordinado ao tema "Anéis de Valuação e Valuações"está estruturado do seguinte modo:

No Capítulo 1 - Preliminares - apresentamos os tipos de anéis com os respectivos exemplos e identificamos algumas propriedades necessárias para a elaboração dos capítulos seguintes.

O Capítulo 2 - Anéis de Valuação - destina-se ao estudo de anéis de valuação e algumas

das suas propriedades e à caracterização de anéis de valuação discreta;

No Capítulo 3 - Valuações - tratam-se de valuações em geral com a identificação dos dois tipos de valuações (arquimedianas e não-arquimedianas), com especial ênfase nas não-arquimedianas. Caracterizam-se as valuações no conjunto dos números racionais - $\mathbb{Q}$. Para além disso, mostramos que é condição necessária e suficiente para que uma valuação não-arquimediana seja discreta que o anel de valuação definido à sua custa seja anel de valuação discreta.

Conteúdo

Capítulo 1

Preliminares

Apresentam-se neste capítulo alguns conceitos que estão na base do desenvolvimento desta dissertação, designadamente os conceitos da Teoria dos Anéis, Teoria dos Corpos, Relações de Ordem e Grupos Ordenados. Pressupõe-se conhecidos a revisão básica da Teoria dos Grupos (definições e propriedades específicas), as propriedades da topologia usual em $\mathbb{R}$ e o Princípio de Zorn.

1.1 Anéis

Definição 1.1. *Chama-se* **anel** *a uma sequência* $(A, +, -, \cdot, 0)$ *onde* A *é um conjunto,* $+$ *e* $\cdot$ *são as duas operações binárias em* A*,* $-$ *é a operação unária em* A *tal que* $a + (-a) = (-a) + a = 0$*, para qualquer* $a \in A$*,* 0 *um elemento de* A *tais que* $(A, +, 0)$ *é um grupo abeliano,* $\cdot$ *é associativa e distributiva em relação à* $+$*. As operações* $+$ *e* $\cdot$ *são usualmente designadas por adição e multiplicação respectivamente. Designemos* $(A, +, -, \cdot, 0)$ *por* A*. Se a multiplicação for comutativa, diz-se que* A *é um* ***anel comutativo****. Se* A *é um anel e* $1 \in A$ *tal que para qualquer* $a \in A \quad a1 = 1a = a$*, diz-se que* A *é um* ***anel com identidade*** *e denota-se por* $(A, +, -, \cdot, 0, 1)$*.*

Exemplos. O anel dos números inteiros é dado por $(\mathbb{Z}, +, -, \cdot, 0, 1)$; O anel dos números reais é $(\mathbb{R}, +, -, \cdot, 0, 1)$; $(\mathbb{Q}, +, -, \cdot, 0, 1)$ é o anel dos números racionais; A sequência

$(\mathbb{Z}_k, +, -, \cdot, 0, 1)$ é um anel, onde $k \in \mathbb{Z}$ e $\mathbb{Z}_k$ é o conjunto formado pelos restos da divisão inteira por k, ou seja, $\mathbb{Z}_k = \{0, 1, 2, ..., k-1\}$. As operações de adição e multiplicação são definidas da seguinte forma: $a + b$ e $a \cdot b$ correspondem ao resto da divisão inteira por k da adição e multiplicação dos números inteiros a e b.

Definição 1.2. *Seja A um anel e $a \in A\backslash\{0\}$. a é um* **divisor de zero** *se existe $b \in A\backslash\{0\}$ tal que $ab = ba = 0$.*

Nota 1. *Num anel A sem divisores de zero tem-se que para quaisquer $a, b \in A$ tais que $ab = 0$ então $a = 0$ ou $b = 0$.*

Definição 1.3. *Seja A um anel comutativo com identidade e $a \in A$. a é* **invertível** *se existe $b \in A$ tais que $ab = ba = 1$.*

Proposição 1.4. *Num anel comutativo A, dois elementos a e b são invertíveis se e só se ab é invertível.*

Prova:($\Rightarrow$) Se a e b são invertíveis em A, então existem c, $d \in A$ tais que $ac = bd = 1$. Uma vez que A é comutativo, $(ac)(bd) = (ab)(cd) = 1$ e portanto ab é invertível.

($\Leftarrow$) Se ab é invertível, existe $c \in A$ tal que $(ab)c = 1$. Mas pela comutatividade de A, $(ab)c = a(bc) = b(ac) = 1$ e portanto a e b também são invertíveis. □

Definição 1.5. *Um anel comutativo com identidade $1 \neq 0$ e sem divisores de zero chama-se* **domínio de integridade**.

Defina-se recursivamente num anel A, a potência de um elemento $a \in A$:

$$a^0 = 1 \text{ e } a^{n+1} = a^n a,\ n = 0, 1, 2, ...$$

Teorema 1.6 (Binómio de Newton)**.** *Seja A um anel comutativo com identidade, n um inteiro positivo e x, $y \in A$. Então $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$*

Prova: Por indução sobre n, quando $n = 0$, $(x + y)^0 = 1 = \binom{0}{0} x^0 y^0$.
Hipótese indução: $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$ para qualquer $n \geq 1$. Pretende-se mostrar

que $(x+y)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} x^i y^{n+1-i}$.

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i} = x\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i} + y\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i} \\
&= x^{n+1} + \sum_{i=0}^{n-1}\binom{n}{i}x^{i+1}y^{n-i} + \sum_{i=1}^{n}\binom{n}{i}x^i y^{n+1-i} + y^{n+1} \\
&= x^{n+1} + \sum_{i=1}^{n}\binom{n}{i-1}x^i y^{n+1-i} + \sum_{i=1}^{n}\binom{n}{i}x^i y^{n+1-i} + y^{n+1} \\
&= x^{n+1} + \sum_{i=1}^{n}\left[\binom{n}{i-1} + \binom{n}{i}\right]x^i y^{n+1-i} + y^{n+1} \\
&= x^{n+1} + \sum_{i=1}^{n}\binom{n+1}{i}x^i y^{n+1-i} + y^{n+1} = \sum_{i=0}^{n+1}\binom{n+1}{i}x^i y^{n+1-i}
\end{aligned}$$

A quarta deve-se ao facto de $\sum_{k=0}^{n-1} a_k = \sum_{k=1}^{n} a_{k-1}$ e $\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$ justifica a sexta igualdade. □

Definição 1.7. *Sejam A_1, A_2 dois anéis. Uma função $f : A_1 \longrightarrow A_2$ é um* **homomorfismo de anéis** *quando:*

(i) $f(-a) = -f(a)$, *para qualquer* $a \in A_1$;

(ii) $f(a+b) = f(a) + f(b)$, *para qualquer* $a,\ b \in A_1$;

(iii) $f(ab) = f(a)f(b)$, *para qualquer* $a,\ b \in A_1$;

(iv) $f(0) = 0$.

No caso em que A_1 e A_2 possuem identidade , tem-se que

(v) $f(1) = 1$.

Definição 1.8. *Chama-se* **característica** *de um anel A com identidade, ao menor inteiro positivo n tal que*

$$n \cdot 1 = \underbrace{1 + 1 + ...1}_{n\ \ vezes} = 0$$

Se tal n não existir, diz-se que A tem **característica infinita**.

Exemplos. O anel dos números reais tem característica infinita e o anel $\mathbb{Z}_k$ com $k \in \mathbb{Z}$ tem característica k.

1.1.1 Subanéis e Ideais

Definição 1.9. *Seja A um anel e S um subconjunto de A tal que $0 \in S$. S é* **subanel** *de A se for fechado para as operações de adição, simétrico e multiplicação em A.*

Exemplos. $(\mathbb{Z}, +, -, \cdot, 0)$ é um subanel de $(\mathbb{Q}, +, -, \cdot, 0)$ e este, por sua vez, é um subanel de $(\mathbb{R}, +, -, \cdot, 0)$;

Sendo p um primo e $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z}, p \nmid n\}$, tem-se que $(\mathbb{Z}_{(p)}, +, -, \cdot, 0, 1)$ é um subanel de $(\mathbb{Q}, +, -, \cdot, 0, 1)$: Tomando $\frac{m}{n}$, $\frac{m'}{n'} \in \mathbb{Z}_{(p)}$, $\frac{m}{n} + \frac{m'}{n'} = \frac{mn'+nm'}{nn'} \in \mathbb{Z}_{(p)}$, porque uma vez que p é primo, $p \nmid nn'$; $\frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{nn'} \in \mathbb{Z}_{(p)}$, pela mesma razão abordada no caso da adição; $-\frac{m}{n} = \frac{-m}{n} \in \mathbb{Z}_{(p)}$, porque $p \nmid n$; A identidade de $\mathbb{Z}_{(p)}$ é $1 = \frac{1}{1}$ e zero de $\mathbb{Z}_{(p)}$ é $0 = \frac{0}{1}$ e pertencem a $\mathbb{Z}_{(p)}$, porque $p \nmid 1$. Tem-se então que $\mathbb{Z}_{(p)}$ é fechado para as operações usuais de $\mathbb{Q}$.

Definição 1.10. *Seja A um anel e $I = (I, +, -, \cdot, 0)$ um subconjunto de A. Diz-se que I é um* **ideal** *de A se:*

- *$(I, +, -, 0)$ é um subgrupo de A;*
- *$ai \in I$ e $ia \in I$, para quaisquer $a \in A$ e $i \in I$.*

Proposição 1.11. *A intersecção de ideais de um anel A é um ideal de A.*

Prova: Seja $\{A_i : i \in I\}$ a família de ideais de A. Então $\cap_{i\in I} A_i \subseteq A$ e para quaisquer a, $b \in \cap_{i\in I} A_i$, tem-se que a, $b \in A_i$ para qualquer $i \in I$. Logo, $a - b \in A_i$ para qualquer $i \in I$, porque A_i é um ideal de A. Consequentemente, $a - b \in \cap_{i\in I} A_i$. Sejam agora $a \in A$ e $k \in \cap_{i\in I} A_i$. Então para qualquer $i \in I$, $k \in A_i$ e portanto, $\{ak, ka\} \subset A_i$, porque A_i é ideal. Logo $\{ak, ka\} \subset \cap_{i\in I} A_i$. □

Definição 1.12. *Seja X um subconjunto do anel A. Seja $\{A_i : i \in I\}$ a família de todos os ideais de A que contêm X. Então $\cap_{i\in I} A_i$ é chamado* **ideal gerado por** *X e denota-se por (X). Se $X = \{x_1, x_2, ..., x_n\}$ então (X) é denotado por $(x_1, x_2, ..., x_n)$ e diz-se que o ideal é finitamente gerado. Um ideal (x) gerado por um único elemento é chamado* **ideal principal**. *Um anel onde todo o ideal é principal chama-se* **anel de ideais principais**.

Ao domínio de integridade onde todo o ideal é principal chama-se **domínio de ideais principais**.

Exemplo. O anel $(\mathbb{Z}, +, -, \cdot, 0, 1)$ é um anel de ideais principais . Seja J um ideal de $\mathbb{Z}$. Se $J = \{0\}$ então $J = (0)$. Suponha-se que $J \neq \{0\}$. Então se $x \in J$ então $-x \in J$ porque $(J, +)$ é um grupo. Assim, podemos dizer que existe pelo menos um inteiro positivo em J. Seja q o menor inteiro positivo em J. Considere-se $x \in J$ e divida-se x por q, ou seja, $x = \theta q + r$ onde $\theta \in \mathbb{Z}$ e $0 \leq r < q$. Assim, $r = x - \theta q \in J$ porque $(J, +)$ é um grupo. Mas isto é impossível porque o menor inteiro pertencente em J é q. Logo, conclui-se que $r = 0$, $x = \theta q$ e portanto $x \in (q)$. Se $a \in (q)$, então $a = \alpha q$ para $\alpha \in \mathbb{Z}$. Como J é um ideal, tem-se que $a \in J$. Logo, J é principal.

Proposição 1.13. *Seja A um anel comutativo com identidade e $a \in A$. Então o ideal gerado por a é dado por $(a) = \{ra : r \in A\}$.*

Prova: Uma vez que (a) é a intersecção de todos os ideais que contêm a, basta mostrar que $I = \{ra : r \in A\}$ é um ideal que contém a e que $I \subseteq J$ para qualquer ideal J que contém a.

Para r, $s \in A$ tem-se que $ra - sa = (r - s)a \in I$, porque A é anel; Se $x \in A$ e $y \in I$, então $y = ra$ com $r \in A$. Logo, $yx = xy = x(ra) = (xr)a \in I$. Uma vez que A tem identidade, $1 \cdot a = a \in I$.

Se J é um ideal que contém a, então J contém ra para qualquer $r \in A$. Conclui-se assim que $I \subseteq J$. □

Definição 1.14. *Sejam I e J dois ideais de um anel A. O* **produto** *de I por J é dado por*

$$IJ = \bigcup_{n \in \mathbb{N}} \{\sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J, n \in \mathbb{N}^*\}.$$

Proposição 1.15. *Sejam A um anel, I e J dois ideais de A. Então IJ é um ideal de A.*

Prova: Sejam x, $y \in IJ$. Então, $x = \sum_{i=1}^{n} a_i b_i$ e $y = \sum_{j=1}^{m} c_j d_j$, com a_i, $c_j \in I$, b_i,

$d_j \in J$, para quaisquer i e j.

$$x - y = \sum_{i=1}^{n} a_i b_i - \sum_{j=1}^{m} c_j d_j = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} (-c_j) d_j = \sum_{k=1}^{n+m} p_k q_k$$

onde

$$p_k = \begin{cases} a_k, & k = 1, ..., n \\ -c_{k-n}, & k = n+1, ..., n+m \end{cases} \text{ e } q_k = \begin{cases} b_k, & k = 1, ..., n \\ d_{k-n}, & k = n+1, ..., n+m \end{cases}$$

Logo, $x - y \in IJ$. Para $r \in A$ e $x \in IJ$, tem-se que $rx = r \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (ra_i) b_i \in IJ$ e $xr = (\sum_{i=1}^{n} a_i b_i) r = \sum_{i=1}^{n} a_i (b_i r) \in IJ$ porque I e J são ideais.

□

Defina-se recursivamente, a potência de um ideal I num anel A:

$$I^1 = I \text{ e } I^{n+1} = I^n I,\ n = 1, 2, ...$$

Proposição 1.16. *Sejam A um anel comutativo com identidade e $a \in A$. Então $(a^n) = (a)^n$, para $n \in \mathbb{N}$.*

Prova: Por indução sobre n, quando $n = 1$ verifica-se facilmente que $(a^1) = (a)^1$. Para a hipótese indução temos que $(a^n) = (a)^n$ para $n \in \mathbb{N}$. Pretende-se provar que $(a^{n+1}) = (a)^{n+1}$. Se $x \in (a^{n+1})$ então, pela Proposição 1.13, tem-se que $x = ra^{n+1}$ com $r \in A$.

$$x = (ra^n)a \in (a^n)(a) = (a)^n(a) = (a)^{n+1}.$$

Se $x \in (a)^{n+1} = (a^n)(a)$, vem que $x = \sum_{i=1}^{n} (a_i a^n)(b_i a) = (\sum_{i=1}^{n} a_i b_i) a^{n+1}$, pela comutatividade de A, com a_i, $b_i \in A$. Logo $x \in (a^{n+1})$. □

Definição 1.17. *Um ideal P de um anel A é* **primo** *se $P \neq A$ e para quaisquer dois ideais de A, I e J, se $IJ \subset P$ então $I \subset P$ ou $J \subset P$.*

Teorema 1.18. *Seja P um ideal de um anel A tal que $P \neq A$. Se para quaisquer a, $b \in A$*

$$ab \in P \Rightarrow a \in P \quad \vee \quad b \in P$$

então P é primo. Se A é comutativo com identidade, o recíproco é verdadeiro.

Prova: Sejam I, J dois ideais de A tais que $IJ \subset P$. Suponha-se que $I \not\subset P$ e seja $i \in I \setminus P$. Para qualquer $j \in J$, $ij \in IJ \subset P$, donde $i \in P$ ou $j \in P$. Como $i \notin P$ então $j \in P$ para qualquer $i \in J$, porque P é ideal. Logo, $J \subset P$ e portanto P é primo.

Se P é um ideal de A tal que $ab \in P$ com a, $b \in A$ então $(ab) \subset P$, pela definição de um ideal finitamente gerado. Uma vez que A é comutativo com identidade, então $(a)(b) \subset (ab)$, donde $(a)(b) \subset P$. Como P é primo, $(a) \subset P$ ou $(b) \subset P$, isto é, $a \in P$ ou $b \in P$. □

Definição 1.19. *Sejam a, b elementos de um anel comutativo A. Diz-se que a* **divide** *b se existe $x \in A$ tal que $ax = b$ e denota-se por $a|b$.*

Definição 1.20. *Seja A um anel comutativo com identidade. Um elemento $p \in A$ é* **primo** *se*

(i) p é não nulo e não invertível;

(ii) $p|ab \Rightarrow p|a$ ou $p|b$, para quaisquer a, $b \in A$;

Proposição 1.21. *Seja A um anel comutativo com identidade e $p \in A$. Então p é primo se e só se (p) é um ideal primo.*

Prova: ($\Rightarrow$) Sejam x, $y \in A$ tais que $xy \in (p)$. Então $p|xy$ e como p é primo, tem-se que $p|x$ ou $p|y$, onde $x \in (p)$ ou $y \in (p)$.

($\Leftarrow$) Por hipótese, (p) é primo. Suponha-se que $p|ab$ para a, $b \in A$. Então $ab \in (p) \Rightarrow a \in (p)$ ou $b \in (p) \Rightarrow p|a$ ou $p|b$. □

Exemplo. Os ideais primos de $\mathbb{Z}$ são da forma $(p) = p\mathbb{Z}$ onde p é primo. Como vimos anteriormente, todo o ideal I de $\mathbb{Z}$ é principal e pela Proposição 1.21 I é gerado por um primo p.

Definição 1.22. *Um ideal M de um anel A diz-se* **maximal** *se $M \neq A$ e para qualquer ideal N tal que $M \subset N \subset A$ se tem $N = M$ ou $N = A$.*

Teorema 1.23. *Seja A um anel não nulo com identidade. Então existem sempre ideais maximais em A e todo o ideal de A está contido em algum ideal maximal de A.*

Prova: Como A é não nulo, existe um ideal J tal que $J \neq A$. Considerem-se J um ideal de A tal que $J \neq A$ e $\mathcal{S}$ o conjunto de todos os ideais próprios de A que contêm J. Note-se que $\mathcal{S} \neq \emptyset$ porque $J \in \mathcal{S}$. Considere-se em $\mathcal{S}$ a relação usual de inclusão de conjuntos ($B_1 \leq B_2 \Leftrightarrow B_1 \subset B_2$). A inclusão é uma relação de ordem parcial (Ver 1.3). Seja $\mathcal{C} = \{C_i : i \in I\}$ uma cadeia de elementos de $\mathcal{S}$ e seja $C = \cup_{i \in I} C_i$. Prove-se que C é um ideal de A: para a, $b \in C$ tem-se que, para algum i, $j \in I$, $a \in C_i$ e $b \in C_j$. Como $\mathcal{C}$ é uma cadeia, vem que $C_i \subset C_j$ ou $C_j \subset C_i$. Supondo que $C_j \subset C_i$, então a, $b \in C_i$ e uma vez que C_i é ideal, temos que $a - b \in C_i$ e $ra \in C_i$ para qualquer $r \in A$. Mas como $C_i \subset C$ então C é um ideal.

Por definição de $\mathcal{S}$, $J \subset C_i$ para qualquer $i \in I$, logo $J \subset \cup C_i = C$. Uma vez que $C_i \in \mathcal{S}$, então $C_i \neq A$ para qualquer $i \in I$. Consequentemente, $1 \notin C_i$ para qualquer $i \in I$ e portanto $1 \notin \cup C_i = C$. Logo, $C \neq A$ e $C \in \mathcal{S}$. Assim, C é um majorante da cadeia $\mathcal{C}$ em $\mathcal{S}$. Tendo as hipóteses do Lema de Zorn satisfeitas, então existe em $\mathcal{S}$ um elemento maximal (Ver 1.3) que coincide com o ideal maximal de A que contem J, por definição de $\mathcal{S}$. □

Teorema 1.24. *Se A é um anel comutativo tal que $A^2 = A$ (em particular, se A possui identidade) então todo o ideal maximal M é primo.*

Prova: Suponha-se que $ab \in M$ tal que $a \notin M$ e $b \notin M$. Então cada um dos ideais $M + (a)$ e $M + (b)$ contém M. Mas, uma vez que M é maximal, tem-se que $M + (a) = M + (b) = A$. Sendo A comutativo com identidade e $ab \in M$, tem-se que $(a)(b) \subset (ab) \subset M$. Como por hipótese, $A = A^2$, vem que $(M + (a))(M + (b)) = M^2 + (a)M + M(b) + (a)(b) \subset M$. Mas, como M é maximal, isto contradiz o facto de que $M \neq A$. Portanto, $a \in M$ ou $b \in M$. □

Definição 1.25. *Um* **anel local** *é um anel comutativo com identidade e com um único ideal maximal.*

Exemplo. O anel $(\mathbb{Z}_{(p)}, +, -, \cdot, 0, 1)$ é local e o seu ideal maximal é $M = (p)$.

Teorema 1.26. *Se A é um anel comutativo com identidade então as seguintes condições são equivalentes:*

(i) *A é um anel local;*

(ii) *Os elementos não invertíveis de A formam um ideal de A.*

(iii) *O conjunto de todos os elementos não invertíveis de A formam um ideal maximal de A.*

Prova:$(i) \Rightarrow (ii)$ Suponha-se que os elementos não invertíveis de A não formam um ideal em A. Então o anel A não possui ideais maximais porque os invertíveis formam o ideal impróprio A. Logo A não é local.

$(ii) \Rightarrow (iii)$ Seja M o conjunto de todos os elementos não invertíveis de A. Por *(ii)* M é um ideal. Vejamos que M é maximal. Suponha-se que existe um ideal N em A tal que $M \subset N \subset A$. Se $M \neq N$, então N possui pelo menos um elemento invertível de A e portanto $N = A$. Logo, M é maximal.

$(iii) \Rightarrow (i)$ Por *(iii)*, M é maximal. Quanto à unicidade de M, suponha-se que existe um outro ideal maximal N em A. Por definição de ideal maximal, N não contém nenhum elemento invertível e portanto, $N \subseteq M$. Mas como N também é maximal então $M \subseteq N$ e consequentemente $M = N$. Logo A é um anel local. □

Definição 1.27. *Um anel A satisfaz a* **condição de cadeia ascendente** *sobre ideais se para toda a cadeia $I_1 \subseteq I_2 \subseteq ... \subseteq I_n ...$ de ideais de A existe $n \in \mathbb{N}$ tal que $I_i = I_n$, $\forall i \geq n$.*

Definição 1.28. *Um anel A é de* **Noether** *se A satisfaz a condição da cadeia ascendente sobre ideais.*

Proposição 1.29. *Se A é um anel de ideais principais então A é de Noether.*

Prova: Seja $(a_1) \subset (a_2) \subset \ldots$ uma cadeia de ideais em A e $I = \cup_{i \geq 1}(a_i)$. Vejamos que I é um ideal de A. Se $x, y \in I$ então $x \in (a_i)$ e $y \in (a_j)$, onde $i \geq j$ ou $j \geq i$. Supondo que $i \geq j$, vem que $(a_j) \subset (a_i)$ e portanto, $x, y \in (a_i)$. Como (a_i) é ideal, $x - y \in (a_i) \subset I$ e para $r \in A$, $rx \in (a_i) \subset I$ e $xr \in (a_i) \subset I$. Portanto, I é um ideal de A. Por hipótese, I é principal, isto é, $I = (a)$ para $a \in A$. Uma vez que $a \in I = \cup_{i \geq 1}(a_i)$, $a \in (a_n)$ para algum $n \in \mathbb{N}^*$. Logo, $(a) \subset (a_n)$. Assim, para qualquer $j \geq n$, $(a) \subset (a_n) \subset (a_j) \subset I = (a)$ e consequentemente, $(a_j) = (a_n)$. Portanto, A é de Noether. □

Proposição 1.30. *Seja A um domínio de integridade local de Noether com um único ideal maximal principal $M \neq \{0\}$. Então $\bigcap_{n=0}^{\infty} M^n = 0$.*

Prova: Como $M = (p)$, para $p \in A$ e $M \neq \{0\}$ então $p \neq 0$. Pela Proposição 1.16, $M^n = (p)^n = (p^n)$. Seja $a \in \bigcap_{n=0}^{\infty} M^n$. Então $a \in M^n$, para qualquer n, e $a = b_n p^n$ para algum $b_n \in A$. Da mesma forma, $a = b_{n+1}p^{n+1}$, ou seja, $b_n p^n = b_{n+1}p^{n+1}$. Assim, $p^n(b_n - b_{n+1}p) = 0$. Uma vez que A é domínio de integridade, não existem divisores de zero e portanto, $p^n = 0$ ou $b_n - b_{n+1}p = 0$. Como $p \neq 0$, vem que $b_n = b_{n+1}p$, o que implica que $(b_n) \subseteq (b_{n+1})$, para qualquer n. Sendo A um anel de Noether, existe $N \geq 0$ tal que $(b_N) = (b_{N+1})$. Logo, $b_N = b_{N+1}p = cpb_N$ para algum $c \in A$. Assim, $b_N(1 - cp) = 0$. Como A não possui divisores de zero, $b_N = 0$ ou $1 - cp = 0$. Uma vez que M é maximal, p é não invertível e portanto $1 \neq cp$. Assim $b_N = 0$ o que implica que $a = 0$. □

1.1.2 Anéis Quociente

Seja A um anel comutativo e I um ideal de A. Defina-se a seguinte relação entre dois elementos de A, a e b:

$$a \sim b \Leftrightarrow a - b \in I.$$

Sejam $a, b, c \in A$ arbitrários:

- *Reflexiva*: $a \sim a$ porque $a - a = 0 \in I$
- *Simétrica*: $a \sim b \Leftrightarrow a - b \in I \Leftrightarrow b - a \in I \Leftrightarrow b \sim a$
- *Transitiva*: $a \sim b \quad e \quad b \sim c \Leftrightarrow a - b \in I \quad e \quad b - c \in I \Rightarrow (a - b) + (b - c) \in I \Leftrightarrow a + (-b + b) - c \in I \Leftrightarrow a - c \in I \Leftrightarrow a \sim c$.

Ou seja, $\sim$ é uma relação de equivalência.

Sejam $a, a', b, b' \in A$ tais que $a \sim a'$ e $b \sim b'$, ou seja, $a - a' \in I$ e $b - b' \in I$. Tendo em conta as operações usuais de um anel, prove-se a compatibilidade dessas operações no conjunto das classes de equivalência de A:

- *Simétrico*: $a \sim a' \Leftrightarrow a - a' \in I \Leftrightarrow -(a - a') \in I \Leftrightarrow (-a) - (-a') \in I \Leftrightarrow -a \sim -a'$;

- *Soma*: $(a-a')+(b-b') \in I \Leftrightarrow (a+b)-(a'+b') \in I \Leftrightarrow a+b \sim a'+b'$
- *Produto*: $(a-a')b+(b-b')a' \in I \Leftrightarrow ab-a'b+ba'-b'a' \in I \Leftrightarrow ab-b'a' \in I$
  $\Leftrightarrow ab \sim a'b'$

Considere-se $A/_\sim = \{[a]_\sim : a \in A\}$ o conjunto de todas as classes de equivalência em A, onde

$$\begin{aligned}[a]_\sim &= \{b \in A : b \sim a\} = \{b \in A : b-a \in I\} \\ &= \{b \in A : b = a+i, i \in I\} = \{a+i : i \in I\} \\ &= a+I.\end{aligned}$$

Assim o conjunto $A/_\sim$ passa a ser denotado por A/I e assume a estrutura de um anel, onde o simétrico de um elemento $a+I \in A/I$ é $(-a)+I$ e as operações da soma e da multiplicação são definidas da seguinte forma:

$$\begin{aligned} + : A/I \times A/I &\longrightarrow A/I \\ (a+I, b+I) &\mapsto (a+b)+I \end{aligned} \qquad \begin{aligned} \bullet : A/I \times A/I &\longrightarrow A/I \\ (a+I, b+I) &\mapsto ab+I \end{aligned}$$

O anel anterior designa-se por **Anel Quociente** onde $0+I$ e $1+I$ são o zero e a identidade de A/I respectivamente.

Dado um anel A e um ideal I de A, os ideais do anel quociente A/I são todos os ideais da forma J/I em que J é um ideal de A que contém I, isto é, formam o conjunto

$$\{J/I : I \subseteq J \text{ e } J \text{ é ideal de A}\}.$$

Sejam x, $y \in J/I$ e $z \in A/I$. Então $x = a+I$, $y = b+I$ e $z = c+I$, com $\{a,b\} \subset J$ e $c \in A$. Como J é um ideal em A, tem-se que

$$x-y = (a-b)+I \in J/I;$$

$$rx = (ca)+I \in J/I \text{ e } xr = (ac)+I \in J/I.$$

Portanto, J/I é um ideal de A/I.

Nota 2. *Seja K um anel e I um ideal de K. Designe-se o conjunto de todos os ideais de K por $\tau(K)$ e o conjunto de todos os ideais de K que contém I por $\tau_I(K)$.*

Proposição 1.31. *Sejam A um anel e I um ideal de A. Existe uma correspondência bijectiva entre o conjunto de todos os ideais de A que contém I e o conjunto de todos os ideais de A/I, dada por*

$$\alpha : \tau_I(A) \longrightarrow \tau(A/I)$$
$$J \mapsto J/I$$

Prova: Sejam J, $K \in \tau_I(A)$ tais que $\alpha(J) = \alpha(K)$. Então,

$$J/I = K/I \Leftrightarrow \{a + I : a \in J\} = \{b + I : b \in K\} \Leftrightarrow J \subseteq K \text{ e } K \subseteq J \Leftrightarrow J = K.$$

Logo, α está bem definida e é injectiva.

$\alpha(\tau_I(A)) = \{\alpha(J) : I \subseteq J \text{ e } J \text{ é ideal de A}\} = \{J/I : I \subseteq J \text{ e } J \text{ é ideal de A}\} = \tau(A/I)$. Portanto, α é sobrejectiva. □

1.2 Corpos

Definição 1.32. *Um* **corpo** *é domínio de integridade onde todos os elementos não nulos são invertíveis.*

Exemplos. As sequências $(\mathbb{Q}, +, -, \cdot, \{\}^{-1}, 0, 1)$ e $(\mathbb{R}, +, -, \cdot, ^{-1}, 0, 1)$ são corpos. Para p primo, $(\mathbb{Z}_p, +, -, \cdot, ^{-1}, 0, 1)$ é um corpo.

Definição 1.33. *Sejam K_1 e K_2 corpos. Uma aplicação $\psi : K_1 \to K_2$ é um* **homomorfismo de corpos** *se ψ for um homomorfismo de anéis com identidade tal que para qualquer $a \in \mathbb{K}_1 \setminus \{0\}$, se tem que:*

$$\psi(a^{-1}) = \psi(a)^{-1}.$$

1.2.1 Corpo das Fracções e Localização

Considere-se A, um anel comutativo e sem divisores de zero. Um subconjunto não vazio S de A diz-se ***multiplicativo*** se para quaisquer $a, b \in S$ se tem que $ab \in S$.

Dado S um subconjunto multiplicativo de A tal que $0 \notin S$. A relação definida em $A \times S$ por

$$(a, s) \sim (a', s') \Leftrightarrow as' - sa' = 0$$

é uma relação de equivalência:

Sejam $(a, s), (a', s'), (a'', s'') \in A \times S$ arbitrários.

- *Reflexiva*: Como $as - sa = 0$ tem-se que $(a, s) \sim (a, s)$.
- *Simétrica*: $(a, s) \sim (a', s') \Leftrightarrow as' - sa' = 0 \Leftrightarrow -(as' - sa') = 0 \Leftrightarrow sa' - as' = 0 \Leftrightarrow a's - s'a = 0 \Leftrightarrow (a', s') \sim (a, s)$
- *Transitiva*: $(a, s) \sim (a', s')$ e $(a's') \sim (a'', s'') \Leftrightarrow as' - sa' = 0$ e $a's'' - s'a'' = 0$ $\Leftrightarrow as' = sa' \quad$ e $\quad a's'' = s'a''$

$$\begin{aligned} a's'' - s'a'' = 0 \Leftrightarrow sa's'' - ss'a'' = 0, \quad s \neq 0 \\ \Leftrightarrow as's'' - ss'a'' = 0 \Leftrightarrow as'' - sa'' = 0, \quad s' \neq 0 \\ \Leftrightarrow (a, s) \sim (a'', s'') \end{aligned}$$

E portanto, $\sim$ é uma relação de equivalência.

Nota 3. *O conjunto de todas as classes de equivalência em $A \times S$ denota-se por $S^{-1}A$. Denote-se cada classe de equivalência $[(a, s)]_\sim \in S^{-1}A$ pelo seu representante (a, s).*

Teorema 1.34. *Seja S um subconjunto multiplicativo do anel comutativo sem divisores de zero A. Considerem-se $\sim$ e $S^{-1}A$ como acima:*

(i) $S^{-1}A$ é um anel comutativo com identidade onde a adição e a multiplicação entre dois elementos de $S^{-1}A$ são definidas por

$$(a, s) + (a', s') = (as' + sa', ss')$$

$$(a,s)\cdot(a',s') = (aa', ss');$$

(ii) Se $A \neq \{0\}$ é um anel sem divisores de zero e $0 \notin S$ então $S^{-1}A$ é um domínio de integridade;

(iii) Se $A \neq \{0\}$ é um anel sem divisores de zero e S o conjunto de todos os elementos não nulos de A então $S^{-1}A$ é um corpo.

Prova: *(i)* As operações da soma e da multiplicação estão bem definidas. Sejam $(a,s),(a',s'),(a'',s''),(a''',s''') \in S^{-1}A$ tais que $(a,s) \sim (a'',s'')$ e $(a',s') \sim (a''',s''')$, ou seja, $as'' - sa'' = 0$ e $a's''' - s'a''' = 0$.

Soma: pretende-se provar que $(a,s) + (a',s') \sim (a'',s'') + (a''',s''')$, o que significa mostrar que $(as' + sa')s''s''' = ss'(a''s''' + s''a''')$.

$$\begin{aligned}(as' + sa')s''s''' &= as's''s''' + sa's''s''' = as''s's''' + sa's'''s'' \\ &= sa''s's''' + ss'a'''s'' = ss'(a''s''' + a'''s'').\end{aligned}$$

Multiplicação: pretende-se provar que $(a,s)\cdot(a',s') \sim (a'',s'')\cdot(a''',s''')$ o que significa mostrar que $aa's''s''' = ss'a''a'''$.

$$aa's''s''' = as''a's''' = sa''s'a''' = ss'a''a'''.$$

E portanto, as duas operações estão bem definidas.

$S^{-1}A$ é um anel comutativo com identidade:

- $(S^{-1}A, +)$ é um grupo abeliano, onde o elemento neutro é $(0,s)$ e o inverso de um elemento (a,s) é dado por $(-a,s)$.

- $(S^{-1}A, \cdot)$ é um semigrupo comutativo.

- $S^{-1}A$ tem como identidade (b,b), para $b \in A \setminus \{0\}$:

$$(b,b)\cdot(a,s) = (a,s)\cdot(b,b) = (a,s)$$

(ii) Por *(i)*, $S^{-1}A$ é um anel comutativo com identidade. Falta provar que $S^{-1}A$ não tem divisores de zero.

$$(a,s)\cdot(a',s') = (0,r) \Leftrightarrow (aa', ss') = (0,r)$$
$$\Leftrightarrow aa'r = 0 \Leftrightarrow aa' = 0, \text{ porque } r \neq 0$$
$$\Leftrightarrow a = 0 \vee a' = 0, \text{ porque em } A \text{ não existem divisores de zero}$$
$$\Leftrightarrow (a,s) = (0,r) \vee (a',s') = (0,r).$$

(iii) $S = A \setminus \{0\}$ e por *(ii)*, $S^{-1}A$ é um domínio de integridade. Seja $(a,s) \in S^{-1}A \setminus \{(0,r)\}$. Então $a \neq 0$ e

$$(a,s)^{-1} = (s,a) :$$
$$(a,s)(s,a) = (s,a)(a,s) = (as,as).$$

□

Ao corpo da alínea *(iii)* chama-se ***Corpo das Fracções*** de A.

Note-se que A é subanel do seu corpo das fracções $S^{-1}A$ via o homomorfismo:

$$h : A \longrightarrow S^{-1}A$$
$$a \mapsto [(ab,b)]_{\sim}$$

para $b \neq 0$.

Seja A um anel comutativo com identidade e P um ideal primo de A. Então $S = A \setminus P$ é multiplicativo: tendo $a, b \in S \Rightarrow \{a,b\} \nsubseteq P \Rightarrow ab \notin P \Rightarrow ab \in S$. Ao anel da alínea *(ii)* com $S = A \setminus P$ chama-se ***Localização*** de A em P e denota-se por A_P.

Exemplo. O anel $(\mathbb{Z}_{(p)}, +, -, \cdot, 0, 1)$ é a localização do anel $(\mathbb{Z}, +, -, \cdot, 0, 1)$ em $M = (p)$.

Proposição 1.35. *Seja $\mathbb{K}$ um corpo de característica infinita. Então a aplicação ϕ de $\mathbb{Z}$ em $\mathbb{K}$ tal que $\phi(n) = n \cdot 1$, é um homomorfismo de anéis injectivo. Para além disso, $\mathbb{Q}$ é subcorpo de $\mathbb{K}$.*

Prova: Sejam $m, n \in \mathbb{Z}$ arbitrários. $\psi(m+n) = (m+n)\cdot 1 = m\cdot 1 + n\cdot 1 = \psi(m) + \psi(n)$; $\psi(mn) = (mn)\cdot 1 = (m\cdot 1)(n\cdot 1) = \psi(m)\psi(n)$; $\psi(1) = 1\cdot 1 = 1$; $\psi(0) = 0\cdot 1 = 0$, o que

vem provar que ψ é um homomorfismo de anéis. Suponha-se que $\psi(m) = \psi(n)$. Então, $m \cdot 1 = n \cdot 1 \Leftrightarrow m \cdot 1 - n \cdot 1 \Leftrightarrow (m-n) \cdot 1 = 0 \Leftrightarrow m - n = 0$, porque, por hipótese, $\mathbb{K}$ tem característica infinita. E portanto $m = n$, o que permite concluir que ψ é injectiva.

Considere-se agora m e $n \neq 0$ dois inteiros e $f : \mathbb{Q} \hookrightarrow \mathbb{K}$ tal que $f(\frac{m}{n}) = (m \cdot 1)(n \cdot 1)^{-1}$. Prove-se que f está bem definida e é um homomorfismo de corpos injectivo: sejam m_1, m_2, n_1, $n_2 \in \mathbb{Z}$, com $n_1 \neq 0$ e $n_2 \neq 0$.

a) Suponha-se que $f(\frac{m_1}{n_1}) = f(\frac{m_2}{n_2})$. Então, tem-se que:

$$\begin{aligned} & (m_1 \cdot 1)(n_1 \cdot 1)^{-1} = (m_2 \cdot 1)(n_2 \cdot 1)^{-1} \\ \Leftrightarrow \quad & (m_1 \cdot 1)(n_1 \cdot 1)^{-1} - (m_2 \cdot 1)(n_2 \cdot 1)^{-1} = 0 \\ \Leftrightarrow \quad & (m_1 n_2) \cdot 1 - (m_2 n_1) \cdot 1 = 0 \Leftrightarrow (m_1 n_2 - m_2 n_1) \cdot 1 = 0 \\ \Leftrightarrow \quad & m_1 n_2 - m_2 n_1 = 0 \Leftrightarrow \frac{m_1}{n_1} = \frac{m_2}{n_2} \end{aligned}$$

Logo, f está bem definida e é injectiva.

b) $f(\frac{m_1}{n_1} + \frac{m_2}{n_2}) = f(\frac{m_1 n_2 + m_2 n_1}{n_1 n_2}) = [(m_1 n_2 + m_2 n_1) \cdot 1]((n_1 n_2) \cdot 1)^{-1}$
$= [(m_1 \cdot 1)(n_2 \cdot 1) + (m_2 \cdot 1)(n_1 \cdot 1)](n_1 \cdot 1)^{-1}(n_2 \cdot 1)^{-1}$
$= (m_1 \cdot 1)(n_1 \cdot 1)^{-1} + (m_2 \cdot 1)(n_2 \cdot 1)^{-1} = f(\frac{m_1}{n_1}) + f(\frac{m_2}{n_2})$;

c) $f(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}) = f(\frac{m_1 m_2}{n_1 n_2}) = ((m_1 m_2) \cdot 1)((n_1 n_2) \cdot 1)^{-1}$
$= (m_1 \cdot 1)(m_2 \cdot 1)(n_1 \cdot 1)^{-1}(n_2 \cdot 1)^{-1} = [(m_1 \cdot 1)(n_1 \cdot 1)^{-1}][(m_2 \cdot 1)(n_2 \cdot 1)^{-1}]$
$= f(\frac{m_1}{n_1}) f(\frac{m_2}{n_2})$

E portanto, f é um homomorfismo de anéis. □

1.2.2 Anéis dos Polinómios com Coeficientes num Corpo

Seja $\mathbb{K}$ um corpo e $\mathbb{K}[x]$ o conjunto de todas as sequências finitas de elementos de $\mathbb{K}$ representadas por $(a_i)_{i \in \mathbb{N}_0} = (a_0, a_1, a_2, ..., a_k)$, para $k \in \mathbb{N}_0$. Defina-se neste conjunto as operações de adição e multiplicação entre dois elementos de $\mathbb{K}[x]$, $(a_i)_{i \in \mathbb{N}_0}$ e $(b_j)_{j \in \mathbb{N}_0}$, respectivamente:

$$(a_i)_{i \in \mathbb{N}_0} + (b_j)_{j \in \mathbb{N}_0} = (a_n + b_n)_{n \in \mathbb{N}_0}$$

$$(a_i)_{i\in\mathbb{N}_0}(b_j)_{j\in\mathbb{N}_0} = (c_n)_{n\in\mathbb{N}_0}$$

onde

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}, \text{ para qualquer } n \in \mathbb{N}_0$$

O conjunto $\mathbb{K}[x]$ com estas operações é um anel e chama-se ***Anel dos Polinómios*** em x com coeficientes em $\mathbb{K}$. Aos elementos de $\mathbb{K}[x]$ chamam-se polinómios em x. O zero de $\mathbb{K}[x]$ é o polinómio nulo (0)=(0,0,0,...) e a identidade de $\mathbb{K}[x]$ é (1,0,0,0,...). O simétrico do polinómio $(a_i)_{i\in\mathbb{N}_0}$ é $(-a_i)_{i\in\mathbb{N}_0}$.

Considerando o conjunto de todas as sucessões de elementos de $\mathbb{K}$ e adoptando nesse conjunto as operações definidas em $\mathbb{K}[x]$, obtém-se o ***anel das séries de potências formais*** e denota-se por $\mathbb{K}\big[[x]\big]$.

Proposição 1.36. *Seja $f = (a_i)_{i\in\mathbb{N}}$ em $\mathbb{K}\big[[x]\big]$. Então f é invertível se e só se $a_0 \neq 0$.*

Prova: Seja $f = (a_i)_{i\in\mathbb{N}}$ tal que $a_0 \neq 0$ e seja $g = (b_i)_{i\in\mathbb{N}}$. Pela definição do produto entre dois polinómios, $fg = (c_i)_{i\in\mathbb{N}}$ onde $c_i = \sum_{k=0}^{i} a_k b_{i-k}$, para $i \in \mathbb{N}$. Logo $(c_i)_{i\in\mathbb{N}} = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, ...) = (1, 0, 0, ...)$ se e só se $c_0 = a_0b_0 = 1$ e $c_i = 0$ para $i \geq 1$. Donde $b_0 = {a_0}^{-1}$ e $\sum_{k=0}^{i} a_k b_{i-k} = a_0b_i + \sum_{k=1}^{i} a_k b_{i-k} = 0$, para $i \geq 1$. Assim os coeficientes de g são da forma $b_i = -b_0 \sum_{k=1}^{i} a_k b_{i-k}$ para $i \geq 1$. □

Proposição 1.37. *$\mathbb{K}\big[[x]\big]$ é um anel local.*

Prova: Vejamos que $\mathbb{K}\big[[x]\big]$ possui um único ideal maximal. Uma vez que $\mathbb{K}\big[[x]\big]$ é comutativo e com identidade, tem-se que para $x \in \mathbb{K}\big[[x]\big]$,

$$(x) = \{xf : f \in \mathbb{K}\big[[x]\big]\}.$$

Consequentemente, qualquer elemento $xf \in (x)$ possui o termo constante não nulo e pela proposição anterior, xf é não invertível. Tomando $f \in \mathbb{K}\big[[x]\big]$ não invertível, então $f = (a_i)_{i\in\mathbb{N}}$ com $a_0 = 0$. Seja $g = (b_i)_{i\in\mathbb{N}}$ com $b_i = a_{i+1}$. Então $xg = f$ e portanto, $f \in (x)$. Conclui-se então que (x) é o conjunto dos elementos não invertíveis de $\mathbb{K}\big[[x]\big]$. Como $1 \notin (x)$ então $(x) \neq \mathbb{K}\big[[x]\big]$. Assim, todo o ideal próprio de $\mathbb{K}\big[[x]\big]$ consiste em elementos

não invertíveis de $\mathbb{K}\big[[x]\big]$ e está contido em (x). De forma análoga à demonstração do Teorema 1.26, tem-se que (x) é maximal e é único. □

Ao conjunto formado pelos elementos da forma $(a_r, a_{r+1}, a_{r+2}, ...)$ onde $r \in \mathbb{Z}$ e $a_r \neq 0$ com as duas operações definidas em $\mathbb{K}[x]$ chama-se ***corpo das séries formais de Laurent*** e denota-se por $\mathbb{K}\big((x)\big)$. Observe-se que $f \in \mathbb{K}\big((x)\big)$, não nulo, pode ser escrito como $f = a_r x^r g$ onde $g \in \mathbb{K}\big[[x]\big]$, ou seja,

$$f = (0, 0, 0, ..., a_r, 0, 0, ...)(1, b_1, b_2, ...).$$

O termo constante de g é $b_0 = 1 \neq 0$. Logo, pela Proposição 1.36, g é invertível. Seja $h \in \mathbb{K}\big[[x]\big]$ o inverso de g. Assim, $f^{-1} = a_r^{-1} x^{-r} h$.

1.3 Relações de Ordem e Grupos Ordenados

Definição 1.38. *Seja A um conjunto não vazio. Uma* **relação de ordem parcial** *em A, é um subconjunto R de $A \times A$ tal que, para quaisquer a, b, $c \in A$, se tem que:*

1. $(a, a) \in R$; *(Reflexiva)*

2. *Se $(a, b) \in R$ e $(b, a) \in R$ então $a = b$;* *(Anti-simétrica ou lata)*

3. *Se $(a, b) \in R$ e $(b, c) \in R$ então $(a, c) \in R$.* *(Transitiva)*

R é uma **relação de ordem total** *se for uma relação de ordem parcial e para além disso, quaisquer dois elementos de A são comparáveis, ou seja,*

4. $(a, b) \in R$ *ou* $(b, a) \in R$, *para quaisquer* a, $b \in A$.

Nota 4. *Costuma notar-se uma relação por $\leq$ e $a < b$ significa $a \leq b$ e $a \neq b$.*

Definição 1.39. $(G, +, -, 0, \leq)$ *chama-se* **grupo ordenado** *(***grupo parcialmente ordenado***) se $(G, +, -, 0)$ é um grupo e $\leq$ é a relação de ordem parcial em G. A relação*

$\leq$ *é compatível com a adição em* G*, ou seja, se* $a \leq b$ *então* $x + a \leq x + b$ *para qualquer* $x \in G$*.*

Se $\leq$ *é uma relação de ordem total,* $(G, +, -, 0, \leq)$ *chama-se* **grupo totalmente ordenado** *(***grupo linearmente ordenado***).*

Exemplos. $(\mathbb{R}, +, -, 0, \leq)$ e $(\mathbb{R}^+, \cdot, ^{-1}, 1, \leq)$ são grupos ordenados.

Observação 1. $(\mathbb{R}, +, -, 0, \leq)$ *e* $(\mathbb{R}^+, \cdot, ^{-1}, 1, \leq)$ *são isomorfos.*

As funções $\varphi = \exp$ e $\psi = 1/\exp$ são isomorfismos entre $(\mathbb{R}, +, -, 0, \leq)$ e $(\mathbb{R}^+, \cdot, ^{-1}, 1, \leq)$, onde φ preserva a ordem e ψ inverte a ordem. Para além disso, φ e ψ são homeomorfismos.

Para $\varphi = \exp$, tem-se que:

i. Sejam x, $y \in \mathbb{R}$: $\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$, o que significa que φ é um homomorfismo de grupos;

ii. Sejam x, $y \in \mathbb{R}$ tal que $\varphi(x) = \varphi(y)$. Então $e^x = e^y \Leftrightarrow e^x e^{-y} = 1 \Leftrightarrow e^{x-y} = 1 \Leftrightarrow x - y = 0 \Leftrightarrow x = y$, ou seja, φ é injectiva;

iii. Seja y um real positivo. Pelas propriedades da função exponencial e da sua inversa, existe $x = \log(y)$ tal que $y = e^x$. Portanto, φ é sobrejectiva.

Sejam x, $y \in \mathbb{R}$ tal que $x \leq y$. Então $e^x e^{-y} = e^{x-y} \leq 1 \Rightarrow e^x \leq e^y$. Logo, φ preserva a ordem.

A função exponencial é contínua e invertível. A sua inversa é a função do logaritmo (log) que por sua vez também é contínua. Assim, φ é um homeomorfismo.

Para $\psi = 1/\exp$ tem-se que:

i. Sejam x, $y \in \mathbb{R}$: $\psi(x + y) = e^{-(x+y)} = e^{-x-y} = e^{-x} e^{-y} = \psi(x)\psi(y)$, o que significa que ψ é um homomorfismo de grupos;

ii. Sejam x, $y \in \mathbb{R}$ tal que $\psi(x) = \psi(y)$. Então tem-se que $e^x = e^y \Leftrightarrow x = y$, ou seja, ψ é injectiva;

iii. Seja y um real positivo. Então existe $x = -\log(y)$ tal que $y = e^{-1}$. Portanto, ψ é sobrejectiva.

Sejam x, $y \in \mathbb{R}$ tal que $x \leq y$. Então $e^x \leq e^y$, donde se conclui que $e^{-x} \geq e^{-y}$. Logo, ψ inverte a ordem.

Tal como a função exp, a função $1/\exp$ é contínua e invertível cuja função inversa é $-\log$ e é contínua, ou seja, $1/\exp$ é um homeomorfismo.

Definição 1.40. *Seja B um subconjunto não vazio de um conjunto parcialmente ordenado $(A, \leq)$. $M \in A$ é* **majorante** *de B se para qualquer $x \in B$, $x \leq M$; $m \in A$ é* **minorante** *de B se para qualquer $x \in B$, $m \leq x$; $i \in A$ é* **ínfimo** *de B se i é minorante de B e se $i' \leq x$ então $i' \leq i$, para qualquer $x \in B$; $a \in A$ é* **elemento maximal** *em A se para qualquer $c \in A$, se $a \leq c$ então $a = c$; $b \in B$ é* **elemento mínimo** *de B se para qualquer $x \in B$ se tem que $b \leq x$; B chama-se* **cadeia** *se $(B, \leq)$ é totalmente ordenado; A é um conjunto* **bem ordenado** *se todo o subconjunto não vazio de A possui um elemento mínimo.*

[**Lema De Zorn**] *Se A é um conjunto não vazio parcialmente ordenado tal que toda a cadeia possui um majorante em A, então A contém um elemento maximal.*

Definição 1.41. *Considere-se em $\mathbb{R}$ a topologia usual em τ. Um subconjunto C de $\mathbb{R}$ diz-se* **discreto** *se a topologia induzida em C por τ for a discreta, ou seja, C é subgrupo de $\mathbb{R}$ e para qualquer $a \in C$, existe um $\epsilon > 0$ tal que $]a - \epsilon, a + \epsilon[\cap C = \{a\}$.*

Proposição 1.42. *Tendo em conta a topologia usual em $\mathbb{R}$, os subgrupos de $(\mathbb{R}, +, -, 0, \leq)$ discretos se e só se são subgrupos cíclicos.*

Prova: ($\Rightarrow$) Seja G um subgrupo discreto de $(\mathbb{R}, +, -, 0, \leq)$. Então $0 \in G$ porque G é subgrupo. Se $G = \{0\}$ então G é gerado por um único elemento que é o próprio zero. Assume-se então que $G \neq \{0\}$. Uma vez que G é discreto então existe uma vizinhança de zero, V_0, tal que $G \cap V_0 = \{0\}$. Como $G \neq \{0\}$, existe um elemento $a \neq 0$ tal que $a \in G$ e consequentemente, pelas propriedades de um subgrupo, $\{a, -a\} \subset G$. Suponha-se que

$a > 0$ e seja $A = \{a \in G : a > 0\}$. Como $A \neq \emptyset$ é um subconjunto de $\mathbb{R}$ com minorante então A tem ínfimo. Seja i o ínfimo de A. Se $i = 0$, existe uma sucessão $(a_n)_{n\in\mathbb{N}}$, com $\{a_n\} \subset A$ para todo $n \in \mathbb{N}$ tal que $(a_n)_{n\in\mathbb{N}}$ tende para i e portanto, para qualquer $\epsilon > 0$ tem-se que $B_\epsilon(0) \cap A \neq \emptyset$. A vizinhança V_0 que intersecta G no ponto zero é tal que $V_0 \cap A = \emptyset$ porque $0 \notin A$. Obtém-se assim uma contradição, ou seja, $i \neq 0$.

Tomando a sucessão $(a_n)_{n\in\mathbb{N}}$ e considerando a sucessão $(b_n)_{n\in\mathbb{N}} := (a_{n+1} - a_n)_{n\in\mathbb{N}}$, onde $b_n \in G$ para todo n, tem-se que $(b_n)_{n\in\mathbb{N}}$ tende para zero. Como $V_0 \cap G = \{0\}$, então a partir de uma certa ordem, n_0, tem-se que $a_{n+1} - a_n = 0 \Leftrightarrow a_{n+1} = a_n$, ou seja, a sucessão $(a_n)_{n\in\mathbb{N}}$ toma o valor da constante i, para todo $n \geq n_0$. Então $i \in A \subset G$ e portanto, $i \in G$. Desta forma conclui-se que $\{n \cdot i : n \in \mathbb{Z}\} \subseteq G$. Vejamos que $\{n \cdot 1 : n \in \mathbb{Z}\} = G$. Suponha-se que existe um $g \in G$ tal que $g \notin \{n \cdot i : n \in \mathbb{Z}\}$. Então $g = n \cdot i + \alpha$ com $0 < \alpha < i$. Assim, $\alpha \in A$ e $\alpha < i$, o que é um absurdo por que i é ínfimo de A. Portanto, $G = \{n \cdot i : n \in \mathbb{Z}\}$, ou seja, i é gerador de G.

($\Leftarrow$) Se S é um subgrupo cíclico de $\mathbb{R}$, então $S = \{nk : n \in \mathbb{Z}\}$ onde k é o menor real positivo em S. Assim, para qualquer $x = nk \in S$ e para $\epsilon < k$, tem-se que $]x - \epsilon, x + \epsilon[\cap S = \{x\}$. E portanto, S é um subgrupo discreto de $\mathbb{R}$. □

Proposição 1.43. *Os subgrupos discretos não nulos de* $(\mathbb{R}^+, \cdot, ^{-1}, 1, \leq)$ *são isomorfos a* $(\mathbb{Z}, +, -, 0, \leq)$.

Prova: Tendo em conta o isomorfismo entre $(\mathbb{R}, +, -, 0)$ e $(\mathbb{R}^+, \cdot, ^{-1}, 1)$, basta mostrar que existe um isomorfismo entre os subgrupos discretos de $(\mathbb{R}, +, -, 0)$ e $(\mathbb{Z}, +, -, 0)$. Pela proposição anterior, os subgrupos discretos de $(\mathbb{R}, +, -, 0)$ são cíclicos.

Se S é um subgrupo cíclico de $(\mathbb{R}, +, -, 0)$ então a aplicação $\alpha : \mathbb{Z} \to S$ dada por $n \mapsto nk$ é um isomorfismo:

i. Sejam n, $m \in \mathbb{Z}$. Então $\alpha(n + m) = (n + m)k = nk + mk = \alpha(n) + \alpha(m)$, o que significa que α é um homomorfismo de grupos;

ii. Sejam n, $m \in \mathbb{Z}$ tais que $\alpha(n) = \alpha(m)$. Tem-se que $nk = mk \Leftrightarrow (n - m)k = 0 \Leftrightarrow n = m$. Portanto, α está bem definida e é injectiva;

iii. $\alpha(\mathbb{Z}) = \{\alpha(n) : n \in \mathbb{Z}\} = \{nk : n \in \mathbb{Z}\} = S$. Logo, α é sobrejectiva. $\square$

Capítulo 2

Anéis de Valuação

Estudam-se neste capítulo algumas propriedades dos anéis de valuação e caracterizam-se os anéis de valuação discreta.

2.1 Anéis de Valuação

Definição 2.1. *Seja V um subanel de um corpo $\mathbb{K}$. V chama-se* **anel de valuação** *se para qualquer $\alpha \in \mathbb{K}$, ou $\alpha \in V$ ou $\alpha^{-1} \in V$.*

Exemplos.

1. Qualquer corpo é um anel de valuação;

2. Seja $\mathbb{K} = \mathbb{Q}$ e $V = \mathbb{Z}_{(p)}$ com $\mathbb{Z}_{(p)}$ a localização de $\mathbb{Z}$ em (p). Vejamos que $\mathbb{Z}_{(p)}$ é um anel de valuação de $\mathbb{Q}$. Como vimos anteriormente, $\mathbb{Z}_{(p)}$ é um subanel de $\mathbb{Q}$. Seja $\alpha \in \mathbb{Q}$. Se $\alpha = 0$, $\alpha \in \mathbb{Z}_{(p)}$, porque este é subanel de $\mathbb{Z}$. Se $\alpha \neq 0$, então $\alpha = \frac{r}{s}$ com $\{r, s\} \subset \mathbb{Z} \setminus \{0\}$, ou seja, $r = p^i k_1$ e $s = p^j k_2$ com $i, j \geq 0$, $p \nmid k_1$ e $p \nmid k_2$. Assim, $\alpha = p^{i-j}\frac{k_1}{k_2}$. Se $i \geq j \Rightarrow i - j \geq 0 \Rightarrow \alpha \in V$. Se $i < j \Rightarrow i - j < 0 \Rightarrow \alpha^{-1} \in V$. Portanto, V é um anel de valuação.

3. Considere-se o corpo das séries formais de Laurent - $\mathbb{K}\big((x)\big)$. Um elemento não nulo de $\mathbb{K}\big((x)\big)$ escreve-se da forma $f = \sum_{i=r}^{\infty} a_i x^i$ com $a_i \in \mathbb{K}$, $r \in \mathbb{Z}$ e $a_r \neq 0$. Considere-se $V = \mathbb{K}\big[[x]\big]$ o anel das séries de potências formais sobre $\mathbb{K}$. V é um anel de valuação.

i. V é subanel de $\mathbb{K}$:

Considerando $f,\ g \in V$, vem que $f = (a_0, a_1, a_2, ...)$ e $g = (b_0, b_1, b_2, ...)$, onde $a_i,\ b_i \in \mathbb{K}$ para todo $i \geq 0$. Atendendo às operações definidas em V: $f + g = (a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...) \in V$ porque $\mathbb{K}$ é fechado para a soma; $fg = (a_0, a_1, a_2, ...)(b_0, b_1, b_2, ...) = (c_0, c_1, c_2, ...)$ onde $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ com $k = 0, 1, 2...$, logo $fg \in V$; $-f = (-a_0, -a_1, -a_2, ...) \in V$; $(1, 0, 0, ...) \in V$; $(0, 0, 0, ...) \in V$.

ii. V é um anel de valuação:

Seja $f \in \mathbb{K}\big((x)\big) \setminus \{0\}$. $f = (a_r, a_{r+1}, a_{r+2}, ...)$ onde $r \in \mathbb{Z}$, $a_i \in \mathbb{K}$ e $a_r \neq 0$. Se $r \geq 0$ então $f \in \mathbb{K}\big[[x]\big]$. Se $r < 0$, tem-se que $f = a_r x^r g$ onde $g = (b_0, b_1, b_2, ...) \in \mathbb{K}\big[[x]\big]$ com $b_0 = 1$ e $b_i = a_{r+i} a_r^{-1}$ para $i > 0$. Pela Proposição 1.36, g é invertível e portanto,

$$f^{-1} = a_r^{-1} x^{-r} g^{-1} = (c_{-r}, c_{1-r}, c_{2-r}, ...) \in \mathbb{K}\big[[x]\big].$$

Propriedades de Anéis de Valuação

Seja V um anel de valuação num corpo $\mathbb{K}$.

0. V **é um domínio de integridade**.

   Como $\mathbb{K}$ é comutativo e não possui divisores de zero, então V adopta essas duas propriedades de $\mathbb{K}$ e portanto V é um domínio de integridade.

1. $\mathbb{K}$ **é corpo das fracções de** V.

   O corpo das fracções de V é o conjunto de todas as classes de equivalência em $D = V \times V \setminus \{0\}$, denotado por D/R onde R é a relação de equivalência definida em D da seguinte forma:

   $$(a, b), (c, d) \in D : \qquad (a, b) R (c, d) \Leftrightarrow ad = bc$$

   Tome-se a aplicação $\varphi : D/R \longrightarrow \mathbb{K}$ definida por $\varphi([(a, b)]_R) = ab^{-1}$.

   (a) φ está bem definida e é injectiva:

Para $[(a,b)]_R, [(c,d)]_R \in D/R$ temos que $[(a,b)]_R = [(c,d)]_R \Leftrightarrow (a,b)R(c,d) \Leftrightarrow ad = bc \Leftrightarrow add^{-1}b^{-1} = bcd^{-1}b^{-1} \Leftrightarrow ab^{-1} = cd^{-1} \Leftrightarrow \varphi([(a,b)]_R) = \varphi([(c,d)]_R)$.

(b) φ é sobrejectiva:

Tomando $k \in \mathbb{K}$, para $t = [(k,1)]_R$ tem-se que $\varphi(t) = k$.

(c) φ é um homomorfismo:

Sejam $[(a,b)]_R, [(c,d)]_R \in D/R$. Então, pelas propriedades das operações em V, tem-se que
$\varphi([(a,b)]_R + [(c,d)]_R) = \varphi([(ad+bc,bd)]_R) = (ad+bc)(bd)^{-1} = ad(bd)^{-1} + bc(bd)^{-1} = ab^{-1} + cd^{-1} = \varphi([(a,b)]_R) + \varphi([(c,d)]_R)$; $\varphi([(a,b)]_R[(c,d)]_R) = \varphi([(ac,bd)]_R) = (ac)(bd)^{-1} = (ab^{-1})(cd^{-1}) = \varphi([(a,b)]_R)\varphi([(c,d)]_R)$;
$\varphi(-[(a,b)]_R) = \varphi([(-a,b)]_R) = (-a)b^{-1} = -(ab^{-1}) = -\varphi([(a,b)]_R)$; $\varphi([a,b]_R^{-1}) = \varphi([b,a]_R) = ba^{-1} = (ab^{-1})^{-1} = \varphi([(a,b)]_R^{-1}$; $\varphi([(0,1)]_R) = 0.1^{-1} = 0$; $\varphi([(1,1)]_R) = 1.1^{-1} = 1$.

Portanto $D/R \cong \mathbb{K}$, ou seja, $\mathbb{K}$ é corpo das fracções de V.

2. **Qualquer subanel de $\mathbb{K}$ que contém V é um anel de valuação**.

Seja W um subanel arbitrário de $\mathbb{K}$ que contém V e seja $\alpha \in \mathbb{K} \setminus \{0\}$. Como V é anel de valuação, tem-se que $\alpha \in V \subseteq W$ ou $\alpha^{-1} \in V \subseteq W$.

3. V **é um anel local**.

Como V é um anel comutativo com identidade, pelo Teorema 1.26, basta mostrar que os elementos não invertíveis de V formam um ideal. Seja $I = \{u : u \text{ não invertível em } V\}$.

(a) Sejam $a, b \in I$ (a e b não são invertíveis em V). De imediato se tem que $-a \in I$ e $0 \in I$. Como V é anel de valuação, então $a/b \in V$ ou $b/a \in V$. Usando a Proposição 1.4 tem-se que se $a/b \in V \Rightarrow a - b = b(a/b - 1) \in I$ e se $b/a \in V \Rightarrow a - b = a(1 - b/a) \in I$.

(b) Sejam $r \in V$, $a \in I$. Como a é não invertível, pela Proposição 1.4, ra é não invertível, isto é, $ra \in I$.

Portanto, I é um ideal de V.

4. **Os ideais de V são totalmente ordenados por inclusão**.

   Sejam I e J dois ideais de V e suponhamos que $I \nsubseteq J$. Tome-se $a \in I \setminus J$ e considere-se $b \in J$. Se $b = 0 \Rightarrow b \in I$ porque I é ideal. Se $b \neq 0$, então $b/a \in V$ porque V é anel de valuação. Se não, $a/b \in V$ e como $a = (a/b)b \in J$, tem-se uma contradição. Então $b = a(b/a) \in I$ e portanto, $J \subset I$.

5. **Seja W um domínio de integridade cujo corpo das fracções é $\mathbb{K}$. Se os ideais de W são totalmente ordenados por inclusão então W é um anel de valuação**.

   Seja $\alpha \in \mathbb{K}$. Se $\alpha = 0 \Rightarrow \alpha \in W$, porque W é um anel. Se $\alpha \neq 0$ então $\alpha = a/b$ com $\{a, b\} \subset W \setminus \{0\}$, porque $\mathbb{K}$ é o corpo das fracções de W. Por hipótese, os ideais de W são totalmente ordenados por inclusão. Em particular, considerando os ideais principais (a) e (b), tem-se que ou $(a) \subseteq (b)$ ou $(b) \subseteq (a)$. Se $(a) \subseteq (b) \Rightarrow a = kb \Rightarrow a/b = k$, com $k \in W$. Analogamente, se $(b) \subseteq (a) \Rightarrow b/a \in W$.

6. **Se P é um ideal primo de V, então V_P é um anel de valuação**.

   Vejamos que se $\mathbb{K}$ é corpo das fracções de V então $\mathbb{K}$ é corpo das fracções de V_P. Sejam $S = V \setminus P$ e $D = V_P \times V_P \setminus \{0\}$ onde $V_P = \{(a, b) : a \in V, b \in S\}$. Defina-se em D a seguinte relação de equivalência:

$$((a, b), (c, d))R((a', b'), (c', d')) \Leftrightarrow adb'c' = bca'd'$$

   R é uma relação de equivalência:

   Sejam $((a, b), (c, d)), ((a', b'), (c', d')), ((a'', b''), (c'', d'')) \in D$ arbitrários.

   - *Reflexiva*: Como $adbc = bcad$ tem-se que $((a, b), (c, d))R((a, b), (c, d))$.

- *Simétrica*: $((a,b),(c,d))R((a',b'),(c',d')) \Leftrightarrow adb'c' = bca'd' \Leftrightarrow bca'd' = adb'c' \Rightarrow a'd'bc = b'c'ad \Rightarrow ((a',b'),(c',d'))R((a,b),(c,d))$.
- *Transitiva*: Se $((a,b),(c,d))R((a',b'),(c',d'))$ e $((a',b'),(c',d'))R((a'',b''),(c'',d''))$ então $adb'c' = bca'd'$ e $a'd'b''c'' = b'c'a''d''$.

$$\begin{aligned} a'd'b''c'' = b'c'a''d'' &\Leftrightarrow bca'd'b''c'' = bcb'c'a''d'', bc \neq 0 \\ &\Leftrightarrow adb'c'b''c'' = bcb'c'a''d'' \Leftrightarrow adb''c'' = bca''d'', b'c' \neq 0 \\ &\Leftrightarrow ((a,b),(c,d))R((a'',b''),(c'',d'')) \end{aligned}$$

E portanto, R é uma relação de equivalência. Denote-se por D/R o conjunto de todas as classes de equivalência em D. Tome-se $\psi : D/R \longrightarrow \mathbb{K}$ definida por $\psi([((a,b),(c,d))]_R) = ad(bc)^{-1}$. Sejam $[((a,b),(c,d))]_R$, $[((a',b'),(c',d'))]_R \in D/R$.

(a) ψ está bem definida e é injectiva:

$[((a,b),(c,d))]_R = [((a',b'),(c',d'))]_R \Leftrightarrow ((a,b),(c,d))R((a',b'),(c',d')) \Leftrightarrow adb'c' = bca'd' \Leftrightarrow adb'c'(bc)^{-1}(b'c')^{-1} = bca'd'(bc)^{-1}(b'c')^{-1} \Leftrightarrow ad(bc)^{-1} = a'd'(b'c')^{-1} \Leftrightarrow \psi([((a,b),(c,d))]_R) = \psi([((a',b'),(c',d'))]_R)$.

(b) ψ é sobrejectiva:

Tomando $k \in \mathbb{K}$, para $t = [(k,1),(1,1)]_R$ tem-se que $\psi(t) = k$.

(c) ψ é um homomorfismo:

$\psi([((a,b),(c,d))]_R + [((a',b'),(c',d'))]_R) = \psi([(ac'db' + bd'ca', bd'db'),(cc',dd')]_R) = ((ac'db' + bd'ca')dd'(bd'db'cc')^{-1} = ad(bc)^{-1} + a'd'(b'c')^{-1} = \psi([((a,b),(c,d))]_R) + \psi([((a',b'),(c',d'))]_R)$;
$\psi([((a,b),(c,d))]_R \cdot [((a',b'),(c',d'))]_R) = \psi([(aa',bb'),(cc',dd')]_R)$
$= (aa'dd')(bb'cc')^{-1} = ad(bc)^{-1}a'd'(b'c')^{-1} = \psi([((a,b),(c,d))]_R)\cdot\psi([((a',b'),(c',d'))]_R)$;
Portanto $D/R \cong \mathbb{K}$, ou seja, $\mathbb{K}$ é corpo das fracções de V_P. Logo, pela Propriedade 4, os ideais de V são totalmente ordenados por inclusão e o mesmo se verifica com

os ideais de V_P. Assim, pela Propriedade 5, V_P é um anel de valuação.

Considere-se $\mathbb{K}$ um corpo e A um anel de valuação em $\mathbb{K}$. Tome-se $\mathbb{K}^*$ e A^* os conjuntos dos elementos invertíveis de $\mathbb{K}$ e de A respectivamente. Note-se que $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. Pelas propriedades de corpo e de anel respectivamente, tem-se que $\mathbb{K}^*$ e A^* munidos com a operação produto são grupos comutativos. Ainda mais, $(A^*, \cdot)$ é um subgrupo normal de $(\mathbb{K}^*, \cdot)$.

Considere-se o grupo quociente $\mathbb{K}^*/A^*$. Notemos cada elemento $aA^* \in \mathbb{K}^*/A^*$ denota-se por $[a]$.

Proposição 2.2. *$(\mathbb{K}^*/A^*, \cdot, [1], \leq)$ é um grupo ordenado para a ordem definida por*

$$[a] \leq [b] \Leftrightarrow ba^{-1} \in A$$

Prova:

- $\leq$ está bem definida em $\mathbb{K}^*/A^*$.

Sejam a, a_1, b, $b_1 \in \mathbb{K}^*$. Se $[a] = [a_1]$, $[b] = [b_1]$ e $[a] \leq [b]$ então temos que $aa_1^{-1} \in A^*$, $bb_1^{-1} \in A^*$ e $ba^{-1} \in A$, donde $b_1b^{-1} \in A^*$. Pretende-se provar que $[a_1] \leq [b_1]$, ou seja, $b_1a_1^{-1} \in A$. $b_1a_1^{-1} = (b_1b)(ba^{-1})(aa_1^{-1}) \in A$.

- $\leq$ é uma relação de ordem total em $\mathbb{K}^*/A^*$.

Sejam a, b, $c \in \mathbb{K}^*$ arbitrários. $[a] \leq [a]$ porque uma vez que A é um anel, $1 = aa^{-1} \in A$; Se $[a] \leq [b]$ e $[b] \leq [a]$ então $ba^{-1} \in A$ e $ab^{-1} \in A$. Logo, ba^{-1}, $ab^{-1} \in A^*$, ou seja, $b \in [a]$ e $a \in [b]$, o que implica que $[a] = [b]$; Se $[a] \leq [b] \leq][c]$, então $ba^{-1} \in A$ e $cb^{-1} \in A$. Logo, $cb^{-1}ba^{-1} = ca^{-1} \in A$, isto é, $[a] \leq [c]$. Portanto, $\leq$ é uma relação de equivalência.

$\leq$ é uma relação de ordem total, ou seja, para qualquer a, $b \in \mathbb{K}^*$, $[a] \leq [b]$ ou $[b] \leq [a]$. Por definição da relação $\leq$, se $[a] \not\leq [b] \Rightarrow ba^{-1} \notin A$ e como A é anel de valuação, tem-se que $ab^{-1} \in A \Leftrightarrow [b] \leq [a]$.

- $\leq$ é compatível com a operação do produto.

Tendo $a,\ b \in \mathbb{K}^*$, se $[a] \leq [b]$ então $ba^{-1} \in A$ e para qualquer $c \in \mathbb{K}^*$, $(bc)(ac)^{-1} = bcc^{-1}a^{-1} = ba^{-1} \in A$. Portanto, $[ac] \leq [bc]$. □

Considere-se o homomorfismo canónico:

$$\begin{aligned} v : \mathbb{K}^* &\longrightarrow \mathbb{K}^*/A^* \\ a &\mapsto [a] = aA^* \end{aligned}$$

Proposição 2.3. *A aplicação v satisfaz as seguintes condições: $v(ab) = v(a)v(b)$ e $v(a+b) \geq \min\{v(a), v(b)\}$. Tem-se ainda que $A = \{x \in \mathbb{K}^* : [1] \leq v(x)\} \cup \{0\}$.*

Prova: Sejam $a,\ b \in \mathbb{K}^*$. Por definição de v e do produto de duas classes laterais, $v(ab) = [ab] = abA^* = aA^*bA^* = [a][b] = v(a)v(b)$; $v(a+b) \geq \min\{v(a), v(b)\}$, ou seja, $[a+b] \geq [a]$ ou $[a+b] \geq [b]$. Se $[a] \not\leq [a+b] \Rightarrow \frac{a+b}{a} = 1 + \frac{b}{a} \notin A \Rightarrow \frac{b}{a} \notin A \Rightarrow \frac{a}{b} \in A \Rightarrow \frac{a}{b} + 1 \in A \Rightarrow \frac{a+b}{b} \in A \Leftrightarrow [b] \leq [a+b]$.

Repare-se que

$$\begin{aligned} \{x \in \mathbb{K}^* : [1] \leq v(x)\} \cup \{0\} &= \{x \in \mathbb{K}^* : [1] \leq [x]\} \cup \{0\} \\ &= \{x \in \mathbb{K}^* : x \in A\} \cup \{0\} \\ &= A \end{aligned}$$

2.2 Anéis de Valuação Discreta

Definição 2.4. *Seja $\mathbb{K}$ um corpo. Uma* **valuação discreta** *em $\mathbb{K}$ é uma aplicação sobrejectiva $v : \mathbb{K} \setminus \{0\} \to \mathbb{Z}$ tal que para quaisquer $a,\ b \in \mathbb{K}$, as seguintes condições são verificadas:*

(i) $v(ab) = v(a) + v(b)$;

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

Proposição 2.5. *Seja v uma valuação discreta em $\mathbb{K}$ e $U = \{a \in \mathbb{K} : v(a) \geq 0\}$. Então,*

a) $v(1) = v(-1) = 0$;

b) Se a, $a^{-1} \in \mathbb{K} \setminus \{0\}$ *então* $v(a^{-1}) = -v(a)$;

c) Se $a \in U$, *então* $a^{-1} \in U$ *se e só se* $v(a) = 0$.

Prova:

a) Uma vez que $1 = 1 \cdot 1$, tem-se que $v(1) = 2v(1) \Rightarrow v(1) = 0$. De um modo análogo se tem que $1 = (-1)(-1)$ e portanto, $0 = v(1) = 2v(-1) \Rightarrow v(-1) = 0$.

b) Pela alínea anterior, tem-se que $0 = v(1) = v(aa^{-1}) = v(a) + v(a^{-1}) \Rightarrow v(a^{-1}) = -v(a)$. A terceira igualdade deve-se à condição (i) da definição da valuação discreta.

c) ($\Rightarrow$) Se $a^{-1} \in U$, da alínea anterior, vem que $v(a) + v(a^{-1}) = 0$. Como a, $a^{-1} \in U$ então $v(a)$, $v(a^{-1}) \geq 0$ e portanto $v(a) = v(a^{-1}) = 0$.
($\Leftarrow$) Tome-se $a \in U$ tal que $v(a) = 0$. Pela alínea anterior, $v(a^{-1}) = -v(a) = 0$ e portanto $a^{-1} \in U$. □

Proposição 2.6. *Se* v *é uma valuação discreta em* $\mathbb{K}$ *então, tomando o conjunto* U *da Proposição 2.5, tem-se que* $V = U \cup \{0\}$ *é um anel de valuação com o ideal maximal* $M = \{a \in \mathbb{K} : v(a) \geq 1\} \cup \{0\}$.

Prova:

- V é um anel.

Como $\mathbb{K}$ é um corpo e $V \subseteq \mathbb{K}$, basta mostrar que V contem as duas constantes do corpo (0 e 1) e é fechado para as operações que conferem a $\mathbb{K}$ a estrutura de um anel. $0 \in V$, por definição do conjunto V; Como $v(1) = 0 \Rightarrow 1 \in V$, pela Proposição 2.5; Tendo $a, b \in V$, vem que por definição de V, $a, b \in \mathbb{K}$ e $v(a), v(b) \geq 0$. $ab \in V$ porque $v(ab) = v(a) + v(b) \geq 0$; $a + b \in V$ porque $v(a + b) \geq min(v(a), v(b)) \geq 0$; $-a \in V$ porque $v(-a) = v(-1) + v(a)$ e pela Proposição 2.5, $v(-1) = 0$. Logo, $v(-a) = 0 + v(a) \geq 0$.

- V é um anel de valuação.

Tome-se $a \in \mathbb{K} \setminus \{0\}$ tal que $a \notin V$. Então $v(a) < 0$ e por $b)$ da Proposição 2.5, $v(a^{-1}) = -v(a) > 0$ e portanto, $a^{-1} \in V$.

- M é o ideal dos não invertíveis em V e é maximal em V.

Por $c)$ da Proposição 2.5, vem que M é o conjunto de todos os elementos não invertíveis em V. Sendo V um anel de valuação, V é anel local e portanto, M forma o único ideal maximal de V, pelo Teorema 1.26. □

Definição 2.7. *Um anel de valuação V definido à custa de uma valuação discreta v tal como na Proposição 2.6 chama-se* **Anel de Valuação Discreta**.

Proposição 2.8. *Seja V um anel de valuação discreta e $t \in V$ tal que $v(t) = 1$. Então t gera o ideal maximal M de V, isto é, $M = (t)$.*

Prova: A existência de t é garantida pela sobrejectividade da valuação discreta v. Por *c)* da Proposição 2.5, t é não invertível e por isso, $(t) \neq V$. V é um anel de valuação e, em particular, é um anel local. Logo o ideal maximal M é único e portanto, $(t) \subseteq M$. Tomando $a \in M$, tem-se que $v(a) \geq 1$. Pretende-se mostrar que $a \in (t)$:

$$v(at^{-1}) = v(a) - v(t) \geq 1 - 1 = 0 \Rightarrow at^{-1} \in V \Rightarrow a \in Vt \subseteq (t).$$

Portanto, $M = (t)$. □

Proposição 2.9. *Seja V um anel de valuação discreta e $t \in V$ tal que $v(t) = 1$. Então qualquer elemento não nulo em $\mathbb{K}$ escreve-se de forma única como ut^n onde u é invertível em V e $n \in \mathbb{Z}$.*

Prova: Seja $a \in \mathbb{K} \setminus \{0\}$ e suponhamos que $v(a) = n$. Note-se que $v(at^{-n}) = v(a) - v(t^n) = n - n = 0 \Rightarrow at^{-n}$ é invertível em V, por $c)$ da Proposição 2.5. Logo $a = ut^n$, com u invertível em V. Suponha-se que $a = ut^n$ e $a = wt^m$ com u e w invertíveis em V e $n, m \in \mathbb{Z}$. Por aplicação da valuação v ao elemento a, tem-se que $v(u) + v(t^n) = v(w) + v(t^m) \Rightarrow n = m \Rightarrow u = w$, porque $v(u) = v(w) = 0$ e $v(t) = 1$. □

Proposição 2.10. *Se V é um anel de valuação discreta então V é um anel de ideais principais.*

Prova: Seja I um ideal de V. Se $I = \{0\}$ então $I = (0)$. Se $I \neq \{0\}$, existe $a \in I$ tal que $v(a) = n$, para $n \in \mathbb{N}$. Assim, o conjunto $\mathcal{C} = \{n \in \mathbb{N} : \exists a \in I \text{ tal que } v(a) = n\}$ é não vazio. Uma vez que $\mathcal{C} \subseteq \mathbb{N}$ e $\mathbb{N}$ é um conjunto bem ordenado, então $\mathcal{C}$ possui um elemento mínimo, digamos n_0. Então existe $a \in I$ tal que $n_0 = v(a)$. Pela Proposição 2.9, $a = ut^{n_0}$ com u invertível em V e portanto, $t^{n_0} = u^{-1}a \in I$, ou seja, $(t^{n_0}) \subseteq I$.

Seja agora $b \in I$ com $v(b) = k$. Pela minimalidade de n_0, $k \geq n_0$ e então $b = wt^k$, com w invertível em V. Assim, $b = wt^{n_0+p}$ onde $p \geq 0$. Logo, $b = wt^p t^{n_0} \Rightarrow b \in (t^{n_0})$. Portanto, $I = (t^{n_0})$. □

Teorema 2.11. *São equivalentes as seguintes afirmações:*

1. *A é um anel de valuação discreta;*

2. *A é um domínio de ideais principais local em que o único ideal maximal é não nulo;*

3. *A é um domínio local de Noether em que o único ideal maximal é não nulo e principal.*

Prova:

(*1⇒2*) Sendo A um anel de valuação, A é um domínio de integridade e pela Propriedade 3, A é local e o único ideal maximal é não nulo. Pela Proposição 2.10, A é um anel de ideais principais.

(*2⇒3*) Por hipótese, A é um domínio de ideais principais. Logo, pela Proposição 1.29, A é de Noether e sendo A local, o único ideal maximal é também principal.

(*3⇒2*) Seja M o ideal maximal de A. Por hipótese, M é principal, ou seja, $M = (p)$ com $p \in A$. Vejamos que todo o ideal de A é principal. Seja I um ideal de A. Se $I = \{0\}$ então $I = (0)$. Se $I \neq \{0\}$ então $I \subseteq M$ porque M é o único ideal maximal de A. Mas pela Proposição 1.30, $\bigcap_{n=0}^{\infty} M^n = 0$. Logo, $I \nsubseteq \bigcap_{n=0}^{\infty} M^n$ e portanto, existe $n \in \mathbb{N}$ tal que $I \subseteq M^n$ e $I \nsubseteq M^{n+1}$. Escolha-se $a \in I \setminus M^{n+1}$. Como $M^n = (p)^n = (p^n)$, temos que $a = up^n$ com $u \notin M$ (porque $a \notin M^{n+1}$). Mas então u é invertível em A (pelo Teorema

1.26) e portanto, $p^n = u^{-1}a \in I$. Assim provámos que $I \subseteq M^n = (p^n) \subseteq I$, ou seja, I é principal.

(*2* $\Rightarrow$ *1*) Por hipótese, o único ideal maximal de A é principal, $M = (t)$ para $t \in A$. Pela Proposição 1.30, $\bigcap_{n=0}^{\infty} M^n = 0$. Seja $a \in A \setminus \{0\}$. Então $(a) \subseteq M$ e como $\bigcap_{n=0}^{\infty} M^n = 0$ então, de modo análogo à demonstração *3*$\Rightarrow$*2*, existe um n tal que $(a) \subseteq (t^n)$ mas $(a) \nsubseteq (t)^{n+1}$. Logo, a escreve-se de forma única como $a = ut^n$ com $u \notin M$, ou seja, u é invertível. Verifique-se esta unicidade: suponha-se que $a = ut^n$ e $a = wt^m$ para u, $w \notin M$ e m, $n \in \mathbb{Z}$. Se $n > m$ tem-se que $n = m + k$ para $k \in \mathbb{N}$ e $ut^{m+k} = wt^m \Leftrightarrow t^m(ut^k - w) = 0$. Uma vez que A é um domínio de integridade, não existem divisores de zero e portanto, $t^m = 0$ ou $ut^k - w = 0$. Mas $t \neq 0$ porque $M = (t)$. Logo, $t^k = u^{-1}w$ é invertível, o que é um absurdo. Se $n = m$, tem-se que $t^n(u - w) = 0$ e conclui-se pela mesma razão acima que $u = v$.

Sendo A um domínio de integridade, A possui um corpo da fracções $\mathbb{K}$. Seja $\beta \in \mathbb{K}\setminus\{0\}$. Então $\beta = \frac{a}{b}$ com a, $b \in A \setminus \{0\}$, ou seja, $a = ut^n$ e $b = wt^m$ para u e w invertíveis em A e n, $m \geq 0$, como provado acima. Logo, $\beta = uw^{-1}t^{n-m}$. Vejamos que β se escreve de forma única como $\beta = pt^k$ com p invertível em A e $k \in \mathbb{Z}$. Se $\beta = qt^l$ com q invertível em A e $l \in \mathbb{Z}$ então $pt^k - qt^l = 0$. Se $k > l$ então $k = l + r$ com $r > 0$ e $pt^k - qt^l = t^l(pt^r - q) = 0 \Leftrightarrow t^r = p^{-1}q$, porque não existem divisores de zero em A. Assim, t^r é invertível em A, o que é um absurdo. Se $k = l$ então $t^l(p - q) = 0$ e pela mesma razão referida acima, $p = q$.

Defina-se $v : \mathbb{K} \setminus \{0\} \longrightarrow \mathbb{Z}$ da seguinte forma:

$$v(pt^k) = k.$$

Sejam x, $y \in \mathbb{K} \setminus \{0\}$. Então $x = pt^k$ e $y = qt^l$ com p e q invertíveis em A e k, $l \in \mathbb{Z}$. Por definição de v, $v(x) = k$ e $v(y) = l$.

- v está bem definida. $x = y \Rightarrow pt^k - qt^l = 0 \Rightarrow k = l$, pela demonstração da unicidade de escrita de um elemento não nulo de $\mathbb{K}$.

- v é sobrejectiva. Para $z \in \mathbb{Z}$, existe $t^z \in \mathbb{K} \setminus \{0\}$ tal que $v(t^z) = z$.

- v uma valuação discreta.$v(xy) = v(pqt^{k+l}) = k + l$ porque pq é invertível em A; Se $k \geq l$ então $k = l + r$, com $r \geq 0$. Logo, $v(x+y) = v(t^l(pt^r - q)) = v(t^l) + v(pt^r - q)$. Uma vez que $x + y \neq 0$ então $pt^r - q \neq 0$. Para além disso, $pt^r - q \in A$ e por isso, escreve-se de forma única como rt^s com r invertível em A e $s \geq 0$. Assim, $v(x + y) = k + s \geq \min\{k, l\}$.

Verifique-se que $A = \{x \in \mathbb{K} : v(x) \geq 0\} \cup \{0\}$. Se $a \in A$, então $a = ut^n$ com u invertível em A e $n \geq 0$. Portanto, $v(a) = n \geq 0$. Seja $b \in \{x \in \mathbb{K} : v(x) \geq 0\}$. Se $b = 0 \Rightarrow b \in A$. Se $b \neq 0 \Rightarrow b = pt^k$ com p invertível em A e $k \in \mathbb{Z}$. Mas como $v(b) \geq 0$ então $k \geq 0$ e por isso, $b \in A$. □

Exemplos.

Retomando os exemplos de anéis de valuação anteriormente exibidos, verifique-se que também são anéis de valuação discreta.

1. Seja $\mathbb{K} = \mathbb{Q}$ e $V = \{\frac{m}{n} \in \mathbb{Q} : \quad p \nmid n, \quad m, n \in \mathbb{Z}\}$, com p um primo.

Uma vez que V é um anel de valuação, em particular é um domínio de integridade e é local. O ideal maximal é $M = (p)$. Vamos provar que V é um domínio de ideais principais. Seja I um ideal de V. Se $I = \{0\}$ então $I = (0)$. Se $I \neq \{0\}$, pelo Teorema 1.23, tem-se que $I \subseteq M$. Seja $a \in I$, não nulo. Então $a = kp$ com $k \in V$. Se $p \nmid k$, tem-se que $k \notin M$ e $a = kp$ com a maior potência de p em I que divide a igual a 1. Mas se $p|k$, então $k = lp$ com $l \in V$. Deste modo, ficamos com $a = lp^2$. Continuando sucessivamente com o estudo da divisibilidade de l por p, de forma análoga, conclui-se que existe uma maior potência de p em I que divide a, ou seja, $a = up^r$ onde $p \nmid u$.

Seja m o menor expoente positivo tal que $p^m \in I$. Vejamos que $I = (p^m)$. Se $p^m \in I$ então $(p^m) \subseteq I$. Seja $b \in I$. Se $b \notin (p^m)$, existe um potência positiva em I, $n < m$ tal que $p^n|b$. Mas isto é um absurdo porque m é o menor expoente positivo de p em I. Logo, $I = (p^m)$.

Assim, pelo teorema anterior, V é um anel de valuação discreta.

2. Seja $\mathbb{K}$ um corpo. Considere-se o corpo das séries formais de Laurent - $\mathbb{K}\big((x)\big)$ e o anel das séries de potências formais - $\mathbb{K}\big[[x]\big]$.

De forma análoga ao exemplo anterior, prova-se que $\mathbb{K}\big[[x]\big]$ é um anel de valuação discreta.

Capítulo 3

Valuações

Nesta secção, é feito um estudo sobre os tipos de valuações definidas em $(\mathbb{R}_0^+, \cdot, ^{-1}, 1, \leq)$. Foram identificados os dois tipos de valuações - arquimedianas e não-arquimendianas e caracterizam-se as valuações em $\mathbb{Q}$.

Definição 3.1. *Uma* **valuação** *num corpo* $\mathbb{K}$ *é uma função* $\phi : (\mathbb{K}, +, -, \cdot, 0, 1) \longrightarrow (\mathbb{R}_0^+, \cdot, ^{-1}, 1, \leq)$ *que satisfaz as seguintes condições para quaisquer* x,$y \in \mathbb{K}$*:*

1. $\phi(x) = 0$ *se e só se* $x = 0$*;*

2. $\phi(xy) = \phi(x)\phi(y)$*;*

3. *Existe um* $C \in \mathbb{R}^+$ *tal que* $\phi(x + y) \leq C \max\{\phi(x), \phi(y)\}$.

À menor constante C que satisfaz a terceira condição da Definição de valuação dá-se o nome de **norma da valuação** ϕ.

Observe-se que C é maior ou igual a 1: $\phi(1) = \phi(1+0) \leq C \max\{\phi(1), \phi(0)\} = C\phi(1)$. Por *1* da definição anterior, $\phi(1) > 0$ e portanto, $C \geq 1$.

Observação 2. *Seja* $v : \mathbb{K} \setminus \{0\} \to \mathbb{Z}$ *uma valuação discreta e* $\phi : \mathbb{K} \to (\mathbb{R}_0^+, \cdot, ^{-1}, 1, \leq)$ *uma valuação. É possível, obter* v *a partir de* ϕ *e vice-versa, a partir de isomorfismos entre* $(\mathbb{R}, +, -, 0, \leq)$ *e* $(\mathbb{R}^+, \cdot, ^{-1}, 1, \leq)$.

Considerando o isomorfismo $(1/\exp)$ entre $(\mathbb{R}, +, -, 0, \leq)$ e $(\mathbb{R}^+, \cdot, ^{-1}, 1, \leq)$, tem-se que

$$\psi(x) = \begin{cases} 0 \text{ se e só se } x = 0 \\ e^{-v(x)} \text{ para } x \in \mathbb{K} \setminus 0 \end{cases}$$

satisfaz as condições de uma valuação. Sejam x, $y \in \mathbb{K} \setminus \{0\}$. Então por *(i)* e *(ii)* da Definição 2.4, $\psi(xy) = e^{-v(xy)} = \psi(x)\psi(y)$ e $\psi(x+y) = e^{-v(x+y)} \leq e^{-\min\{v(x),v(y)\}} = e^{\max\{-v(x),-v(y)\}} = \max\{\psi(x), \psi(y)\}$.

Por outro lado, $-\log$ é um isomorfismo entre $(\mathbb{R}^+, \cdot, ^{-1}, 1, \leq)$ e $(\mathbb{R}, +, -, 0, \leq)$. Para $x \in \mathbb{K} \setminus \{0\}$, tem-se que $u(x) = -\log(\phi(x))$ satisfaz as condições semelhantes as de uma valuação discreta. Sejam x, $y \in \mathbb{K} \setminus \{0\}$. Então por *2* e *3* da Definição 3.1, $v(xy) = -\log(\phi(xy)) = -\log(\phi(x)\phi(y)) = -\log(\phi(x)) - \log(\phi(y)) = v(x) + v(y)$ e $v(x+y) = -\log(\phi(x+y)) \geq -\log(C\max\{\phi(x), \phi(y)) = -\log C - \log(\max\{\phi(x), \phi(y)\}) = -\log C + \min\{-\log(\phi(x)), -\log(\phi(x))\} = -\log C + \min\{v(x), v(y)\}$.

Proposição 3.2. *Seja ϕ uma valuação em $\mathbb{K}$. Então:*

A. $\phi(1) = 1$*;*

B. $\phi(-1) = 1$*;*

C. Para qualquer $x \in \mathbb{K}$, $\phi(-x) = \phi(x)$*;*

D. Para qualquer $x \in \mathbb{K} \setminus \{0\}$, $\phi(x^{-1}) = \phi(x)^{-1}$*;*

E. Se a norma de ϕ for igual a C então $x \mapsto \phi(x)^r$ define uma valuação com norma C^r em $\mathbb{K}$ para cada $r \in \mathbb{R}^+$;

F. Se S é um subcorpo de $\mathbb{K}$, então a restrição de ϕ a S, $\phi\big|_S$, é uma valuação em S.

Prova:

A. $\phi(1) = \phi(1.1) = \phi(1)\phi(1)$, por *2* da definição de valuação. Como $\phi(1) > 0$ então $\phi(1) = 1$.

B. Note-se que, por A e pela definição de valuação, $1 = \phi(1) = \phi((-1)(-1)) = \phi(-1)\phi(-1) \Rightarrow \phi(-1) = 1$.

C. $\phi(-x) = \phi(-1)\phi(x) = \phi(x)$, por *2* da definição de valuação e por B.

D. Seja $x \in \mathbb{K} \setminus \{0\}$. Tendo $1 = xx^{-1}$, então $1 = \phi(1) = \phi(x)\phi(x^{-1})$, donde $\phi(x^{-1}) = \phi(x)^{-1}$.

E. Sejam x,$y \in \mathbb{K}$ arbitrários: $\phi(x)^r = 0 \Leftrightarrow \phi(x) = 0 \Leftrightarrow x = 0$ porque ϕ é uma valuação em $\mathbb{K}$; $\phi(xy)^r = (\phi(x)\phi(y))^r = \phi(x)^r\phi(y)^r$; $\phi(x+y)^r \leq (C\max\{\phi(x), \phi(y)\})^r$ $= C^r \max\{\phi(x)^r, \phi(y)^r\}$. Portanto ϕ^r é uma valuação.

F. Note-se que para qualquer x em S, $\phi\big|_S(x) = \phi(x)$. De imediato, tem-se que $\phi\big|_S$ é uma valuação em S. □

A norma de uma valuação permite distinguir dois tipos de valuação, como se segue na seguinte definição.

Definição 3.3. *Uma valuação ϕ com norma igual a 1 chama-se* ***não-arquimediana*** *e uma valuação com norma maior que 1 chama-se* ***arquimediana****.*

Proposição 3.4. *Uma valuação não-arquimediana ϕ satisfaz a desigualdade ultramétrica:*

$$\phi(\sum_{i=1}^{n} x_i) \leq \max\{\phi(x_i), i = 1, 2, ..., n\}$$

Prova: Sendo ϕ uma valuação não-arquimediana, tem-se que, por *3* da Definição de valuação, $\phi(x+y) \leq \max\{\phi(x), \phi(y)\}$, para quaisquer x e y em $\mathbb{K}$. Por indução no número de parcelas, para $n = 1$ verifica-se a desigualdade ultramétrica de forma natural. Suponha-se que para um n fixo se tem a relação $\phi(\sum_{i=1}^{n} x_i) \leq \max\{\phi(x_i), i = 1, 2, ..., n\}$ e prove-se que também se verifica para $n+1$:

$$\begin{aligned}
\phi(\sum_{i=1}^{n+1} x_i) = \phi(\sum_{i=1}^{n} x_i + x_{n+1}) &\leq \max\{\phi(\sum_{i=1}^{n} x_i), \phi(x_{n+1})\} \\
&\leq \max\{\max\{\phi(x_i), i = 1, 2, ..., n\}, \phi(x_{n+1})\} \\
&\leq \max\{\phi(x_i), i = 1, 2, ..., n+1\}
\end{aligned}$$

□

Se ϕ é não-arquimediana e $\phi(x_1) \neq \phi(x_2)$, a desigualdade ultramétrica pode ser

fortalecida pela igualdade $\phi(x_1 + x_2) = \max\{\phi(x_1), \phi(x_2)\}$ da seguinte maneira:

$$\begin{aligned}\phi(x_1) = \phi(x_1 + x_2 - x_2) &\leq \max\{\phi(x_1 + x_2), \phi(-x_2)\} \\ &= \max\{\phi(x_1 + x_2), \phi(x_2)\} \leq \max\{\max\{\phi(x_1), \phi(x_2)\}, \phi(x_2)\} \\ &\leq \max\{\phi(x_1), \phi(x_2)\} = \phi(x_1), \quad \text{supondo que } \phi(x_1) > \phi(x_2)\end{aligned}$$

As duas primeiras desigualdades devem-se ao facto de ϕ ser uma valuação não-arquimediana e a segunda igualdade justifica-se pela propriedade C da Proposição 3.2. Este resultado é análogo quando se assume que $\phi(x_2) > \phi(x_1)$. Logo, $\phi(x_1) = \phi(x_1 + x_2)$.

Exemplos.

1. Um exemplo de uma valuação não-arquimediana num corpo $\mathbb{K}$ é a *valuação trivial* em $\mathbb{K}$:

$$\phi(x) = \begin{cases} 1 & , \quad x \in \mathbb{K} \setminus \{0\} \\ 0 & , \quad x = 0 \end{cases}$$

De facto, ϕ é uma valuação porque $\phi(x) = 0$ se e só se $x = 0$ e, tendo x, $y \in \mathbb{K} \setminus \{0\}$ tem-se que $\phi(xy) = 1 = \phi(x)\phi(y)$ e $1 = \phi(x + y) \leq \max\{\phi(x), \phi(y)\} = 1$.

2. Dados v uma valuação discreta e $1/\exp$ um isomorfismo entre $(\mathbb{R}, +, 0, \leq)$ e $(\mathbb{R}^+, \cdot, 1, \leq)$, pela Observação 2, tem-se que ψ é uma valuação não-arquimediana.

3. Se $\sigma : \mathbb{K} \longrightarrow \mathbb{C}$ é um homomorfismo de anéis, então ϕ_σ definida por $\phi_\sigma(x) = |\sigma(x)|$ é uma valuação arquimediana. Sejam x, $y \in \mathbb{K}$ arbitrários.

$$\phi_\sigma(x) = 0 \Leftrightarrow |\sigma(x)| = 0 \Leftrightarrow \sigma(x) = 0 \Leftrightarrow x = 0;$$

$$\phi_\sigma(xy) = |\sigma(xy)| = |\sigma(x)\sigma(y)| = |\sigma(x)||\sigma(y)| = \phi_\sigma(x)\phi_\sigma(y) \text{ e}$$

$$\begin{aligned}\phi_\sigma(x + y) = |\sigma(x + y)| = |\sigma(x) + \sigma(y)| &\leq |\sigma(x)| + |\sigma(y)| \\ = \phi_\sigma(x) + \phi_\sigma(y) &\leq 2\max\{\phi_\sigma(x), \phi_\sigma(y)\}\end{aligned}$$

O primeiro caso justifica-se pelo facto de um homomorfismo entre dois corpos ser sempre injectivo.

Lema 3.5. *Seja ϕ uma valuação num corpo $\mathbb{K}$ tal que $\phi(x+y) \leq 2^k \max\{\phi(x), \phi(y)\}$ para todo x,$y \in \mathbb{K}$, $k > 1$. Então,*

$$\phi(\sum_{i=1}^{2^m} x_i) \leq 2^{km} \max\{\phi(x_i), i = 1, 2, ..., 2^m\}. \tag{3.1}$$

Em particular, para $l \in \mathbb{Z}$,

$$\phi(\sum_{i=1}^{l} x_i) \leq 2^k l^k \max\{\phi(x_i), i = 1, 2, ..., l\} \tag{3.2}$$

e

$$\phi(l.1) \leq 2^k l^k \tag{3.3}$$

Prova: Para $m = 1$ tem-se que $\phi(\sum_{i=1}^{2} x_i) = \phi(x_1 + x_2) \leq 2^{1k} \max\{\phi(x_1), \phi(x_2)\}$ como na hipótese do teorema. Para $m = 2$ tem-se que $\phi(\sum_{i=1}^{2^2} x_i) = \phi(x_1 + x_2 + x_3 + x_4) \leq 2^k \max\{\phi(x_1 + x_2), \phi(x_3 + x_4)\} \leq 2^{2k} \max\{\phi(x_i), i = 1, 2, 3, 4\}$. Suponha-se que para qualquer $m \geq 1$, $\phi(\sum_{i=1}^{2^m} x_i) \leq 2^{km} \max\{\phi(x_i), i = 1, 2, ..., 2^m\}$. Pretende-se mostrar que $\phi(\sum_{i=1}^{2^{m+1}} x_i) \leq 2^{k(m+1)} \max\{\phi(x_i), i = 1, 2, ..., 2^{m+1}\}$.

$$\begin{aligned}
&\phi(\sum_{i=1}^{2^{m+1}} x_i) = \phi(\sum_{i=1}^{2^m} x_i + \sum_{i=2^m+1}^{2^{m+1}} x_i) \leq 2^k \max\{\phi(\sum_{i=1}^{2^m} x_i), \phi(\sum_{i=2^m+1}^{2^{m+1}} x_i)\} \\
&\leq 2^k 2^{km} \max\{\phi(x_i), \quad i = 1, 2, ..., 2^{m+1}\}, \text{ porque } 2^{m+1} - 2^m = 2^m) \text{ e por 3.1} \\
&= 2^{k(m+1)} \max\{\phi(x_i), \quad i = 1, 2, ..., 2^{m+1}\}
\end{aligned}$$

Para a segunda parte do enunciado, $\phi(\sum_{i=1}^{l} x_i) = \phi(\sum_{i=1}^{2^m} x_i)$ onde $x_i = 0$ para $i > l$ e sendo l um número inteiro positivo, $2^{m-1} \leq l < 2^m$. Então,

$$\begin{aligned}
\phi(\sum_{i=1}^{l} x_i) &\leq 2^{km} \max\{\phi(x_i), i = 1, 2, ..., l\} \\
&= 2^k (2^{m-1})^k \max\{\phi(x_i), i = 1, 2, ..., l\} \\
&\leq (2l)^k \max\{\phi(x_i), i = 1, 2, ..., l\}
\end{aligned}$$

□

Existe uma relação simples entre a norma de uma valuação e a desigualdade triangular.

Proposição 3.6. *Uma valuação num corpo $\mathbb{K}$ satisfaz a desigualdade triangular se e só se a sua norma não excede 2.*

Prova: É claro que uma valuação que satisfaz a desigualdade triangular tem norma no máximo igual a 2:

$$\phi(x_1 + x_2) \leq \phi(x_1) + \phi(x_2) \leq 2\max\{\phi(x_1), \phi(x_2)\}.$$

Reciprocamente, suponha-se que a valuação ϕ em $\mathbb{K}$ tem norma $C \leq 2$. Pelo Lema 3.5, $\phi(\sum_{i=1}^{2^m} x_i) \leq 2^m \max\{\phi(x_i), i = 1, 2, ..., 2^m\}$, para $k = 1$ e tomando $x_i = 0$ para $i = l+1, l+2, ..., 2^m$, tem-se que a soma dos l termos pode ser limitado da seguinte forma: $\phi(\sum_{i=1}^{l} x_i) \leq 2l \max\{\phi(x_i), i = 1, 2, ..., l\}$, por 3.2. Em particular, por 3.3 tem-se que $\phi(l.1) \leq 2l$. Observe-se que

$$\begin{aligned}
\phi(x+y)^n &= \phi((x+y)^n), \text{ pela alínea } \textit{2} \text{ da Definição 3.1} \\
&= \phi(\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}), \text{ pelo Teorema do Binómio de Newton} \\
&\leq 2(n+1)\max\{\phi(\binom{n}{i} x^i y^{n-i})\}, \text{ por 3.2} \\
&\leq 2(n+1)\max\{2\binom{n}{i}\phi(x^i)\phi(y^{n-i})\}, \text{ por 3.3} \\
&= 4(n+1)\max\{\binom{n}{i}\phi(x)^i\phi(y)^{n-i}\} \leq 4(n+1)\sum_{i=0}^{n}\binom{n}{i}\phi(x)^i\phi(y)^{n-i} \\
&= 4(n+1)[\phi(x)+\phi(y)]^n
\end{aligned}$$

A desigualdade obtida, $\phi(x+y) \leq \sqrt[n]{4(n+1)}[\phi(x)+\phi(y)]$, implica que ϕ satisfaz a desigualdade triangular quando n tender para o infinito. □

Lema 3.7. *Qualquer valuação possui uma potência de expoente natural que satisfaz a desigualdade triangular.*

Prova: Seja ϕ uma valuação de norma C. Se $C \leq 2$, pelo Proposição 3.6, ϕ satisfaz a desigualdade triangular. Se $C > 2$, existe $k > 1$ tal que $C \leq 2^k$ e segue-se que $\phi(x+y) \leq 2^k \max\{\phi(x), \phi(y)\}$. Então, com justificações análogas aos que foram usadas

na prova da Proposição 3.6, para $n \in \mathbb{N}$, tem-se que

$$\begin{aligned}
\phi(x+y)^{kn} &= \phi(\sum_{i=0}^{kn} \binom{kn}{i} x^i y^{kn-i}) \leq 2^k (kn+1)^k \max\{\phi(\binom{kn}{i} x^i y^{kn-i})\} \\
&= 2^k (kn+1)^k \max\{\phi((\binom{kn}{i}.1) x^i y^{kn-i})\} \\
&\leq 2^k (kn+1)^k \max\{2^k \binom{kn}{i} \phi(x^i)\phi(y^{kn-i})\} \\
&\leq 2^k (kn+1)^k 2^k (\binom{kn}{p}^k \max\{\phi(x)^i \phi(y)^{kn-i}\} \text{ para } p = \lfloor kn/2 \rfloor \\
&= \left[4(kn+1)\binom{kn}{p}\right]^k \max\{\phi(x), \phi(y)\}^{kn}
\end{aligned}$$

onde $p = \lfloor kn/2 \rfloor$ designa a parte inteira do número $kn/2$.

A desigualdade obtida, $\phi(x+y)^{kn} \leq \left[4(kn+1)\binom{kn}{p}\right]^k \max\{\phi(x), \phi(y)\}^{kn}$ reduz-se à desigualdade $\phi(x+y)^k \leq \sqrt[n]{\left[4(kn+1)\binom{kn}{p}\right]^k} \max\{\phi(x)^k, \phi(y)^k\}$. Isto implica que ϕ^k satisfaz a desigualdade triangular. □

Um argumento semelhante ao que foi dado na prova da Proposição 3.6 mostra que é possível decidir se uma valuação é ou não não-arquimediana através do estudo da sua aplicação nos múltiplos do elemento invertível.

Proposição 3.8. *Uma valuação num corpo $\mathbb{K}$ é não-arquimediana se e só se é limitada no subconjunto de $\mathbb{K}$, $\{n \cdot 1 : \quad n \in \mathbb{Z}\}$.*

Prova: É claro que se ϕ é não-arquimediana, a partir da desigualdade ultramétrica ($\phi(\sum x_i) \leq \max\{\phi(x_i)\}$), se tem que $\phi(\pm n \cdot 1) = \phi(1 \pm 1 \pm ... \pm 1) \leq \phi(1) = 1$.
Reciprocamente, se ϕ é uma valuação limitada por M no conjunto $\{n \cdot 1 : \quad n \in \mathbb{Z}\}$ e

satisfaz a desigualdade triangular, vem que

$$\begin{aligned}
\phi(x+y)^n &= \phi(\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i}), \text{ pelo Teorema do Binómio de Newton} \\
&\leq \sum_{i=0}^{n}\phi(\binom{n}{i})\phi(x)^i\phi(y)^{n-i}, \text{ pela desigualdade triangular} \\
&= \sum_{i=0}^{n}\phi(\binom{n}{i}\cdot 1)\phi(x)^i\phi(y)^{n-i} \leq M\sum_{i=0}^{n}\phi(x)^i\phi(y)^{n-i} \\
&= M(n+1)\max\{\phi(x),\phi(y)\}^n
\end{aligned}$$

Tomando a n-ésima raíz de ambas os membros da desigualdade $\phi(x+y)^n \leq M(n+1)\max\{\phi(x),\phi(y)\}^n$ e fazendo n tender para o infinito, tem-se que ϕ é não-arquimediana, isto é, $\phi(x+y) \leq \max\{\phi(x),\phi(y)\}$. □

Proposição 3.9. *Uma valuação num corpo de característica positiva é não-arquimediana.*

Prova: Seja ϕ uma valuação num corpo $\mathbb{K}$ de característica positiva n. Pela Proposição 3.8, basta provar que ϕ é limitada no conjunto $\{k\cdot 1: \quad k\in\mathbb{Z}\}$. Mas $k\cdot 1 = (qn+r)\cdot 1 = (qn)\cdot 1 + r\cdot 1 = r\cdot 1$ com $q\in\mathbb{Z}$ e $0\leq|r|<n$, porque n é a característica de $\mathbb{K}$. Assim, $\phi(k\cdot 1) = \phi(r\cdot 1) \in \{\phi(x) : x\in\{0,1,2,...,n-1\}\}$. Portanto, ϕ é limitada em $\{k\cdot 1: \quad k\in\mathbb{Z}\}$. □

O Teorema que se segue caracteriza todas as valuações não-triviais em $\mathbb{Q}$.

Teorema 3.10 (Ostrowski)**.** *Toda a valuação não-trivial no corpo dos números racionais $\mathbb{Q}$, ou é igual a uma valuação p-ádica ϕ_p dada por $\phi_p(x) = c^{ord_p(x)}$ com $c\in]0,1[$ para algum primo p, ou é igual a uma potência de um valor absoluto em $\mathbb{Q}$ dada por $\phi_\infty(x) = |x|^\alpha$ com $\alpha > 0$.*

Prova: Seja ϕ uma valuação não-trivial. Se ϕ é não-arquimediana em $\mathbb{Q}$ então ϕ é limitada por 1 em $\mathbb{Z}$, como provado na Proposição 3.8. O conjunto $P = \{x\in\mathbb{Z} : \phi(x) < 1\}$ é um ideal primo de $\mathbb{Z}$. Sejam x, $y\in\mathbb{Z}$ tais que $\phi(x)<1$ e $\phi(y)<1$. Como ϕ é não-arquimediana, $\phi(x-y) = \phi(x+(-y)) \leq \max\{\phi(x),\phi(y)\} < 1 \Rightarrow x-y\in P$; Sejam $x\in P$

e $a \in \mathbb{Z}$. $\phi(xa) = \phi(x)\phi(a) < 1 \Rightarrow xa \in P$. De modo análogo se prova que $ax \in P$ e portanto P é um ideal de $\mathbb{Z}$.

Prove-se de seguida que, P é primo: sejam a, $b \in \mathbb{Z}$ tais que $ab \in P$. Então $\phi(ab) = \phi(a)\phi(b) < 1 \Rightarrow \phi(a) < 1$ ou $\phi(b) < 1$, ou seja, $a \in P$ ou $b \in P$. Uma vez que ϕ é não-trivial, $P \neq \{0\}$ e portanto, P é um ideal primo em $\mathbb{Z}$.

Como vimos anteriormente, $P = p\mathbb{Z}$ para algum primo p. Como todos os elementos de $\mathbb{Z} \setminus p\mathbb{Z}$ têm valuação 1 ($x \in \mathbb{Z} \setminus p\mathbb{Z} \Rightarrow \phi(x) \geq 1 \Rightarrow \phi(x) = 1$ porque ϕ é limitada por 1 em $\mathbb{Z}$), a valuação assume valor 1 em todas as fracções $u = \frac{a}{b}$ com $p \nmid ab$ (a, $b \in \mathbb{Z} \setminus p\mathbb{Z}$, $\phi(\frac{a}{b}) = \phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = 1 \cdot 1 = 1$).

Escrevendo um $x \in \mathbb{Q} \setminus \{0\}$ como $x = up^k$ com $u = \frac{a}{b}$ tal que $p \nmid ab$ e designando k por $ord_p(x)$ define-se a seguinte valuação:

$$\phi(x) = c^{ord_p(x)}$$

com $c = \phi(p) \in]0, 1[$.

Suponha-se agora que ϕ é uma valuação arquimediana em $\mathbb{Q}$. Assume-se que ϕ satisfaz a desigualdade triangular e que $\phi(k) \leq |k|$ onde $k \in \mathbb{Z}$. Dados dois inteiros m, $n > 1$, pode-se escrever todas as potências de m na base n como $m^t = \sum_{i=0}^{s} a_i n^i$ com $a_i \in \{0, 1, ..., n-1\}$ e $a_s \neq 0$. Existe um $k \geq 1$ tal que $n^{k-1} \leq m^t < n^k$, ou seja, $k - 1 \leq \frac{\log(m^t)}{\log(n)} < k$. O número de parcelas do somatório anterior é $k = \lfloor \frac{\log(m^t)}{\log(n)} \rfloor + 1$ e portanto, obtém-se que $s = k-1$ e $\frac{s}{t} \leq \frac{\log(m)}{\log(n)}$. Como por hipótese $\phi(k) \leq |k|$, tem-se que $\phi(a_i) < n$, para qualquer $i = 0, 1, ..., n-1$. A desigualdade triangular implica que

$$\phi(m^t) = \phi(\sum_{i=0}^{s} a_i n^i) \leq \sum_{i=0}^{s} \phi(a_i)\phi(n^i) < n \sum_{i=0}^{s} \phi(n^i) \leq n(s+1) \max\{1, \phi(n)^s\}$$

Logo, tomando a t-ésima raíz de ambos os membros da desigualdade anterior e deixando t tender para o infinito, tem-se que $\phi(m) \leq \sqrt[t]{(s+1)n} \max\{1, \phi(n)\}^{\frac{s}{t}} \leq \max\{1, \phi(n)\}^{\frac{\log(m)}{\log(n)}}$. Isto implica que $\phi(n)$ é maior do que 1 porque caso contrário, ϕ seria limitada em $\mathbb{Z}$ e consequentemente não-arquimediana.

$$\phi(m) \leq \phi(n)^{\frac{\log(m)}{\log(n)}} \Leftrightarrow \phi(m)^{1/\log(m)} \leq \phi(n)^{1/\log(n)}$$

De facto, a desigualdade anterior reduz-se a uma igualdade quando m e n trocam de papel. Tomando $a = \phi(n)^{1/\log(n)}$, a é maior do que 1 e portanto não depende do valor de $n > 1$ e nem de $\phi(n) = |n|^{\log(a)}$, para qualquer $n \in \mathbb{Z}$. Isto implica que $\phi(x) = |x|^{\alpha}$ define uma valuação, para qualquer $x \in \mathbb{Q}$ com $\alpha = \log(a) > 0$.

Se ϕ não satisfaz a desigualdade triangular, pelo Lema 3.7, existe $k \in \mathbb{N}$ tal que ϕ^k satisfaz a desigualdade triangular e obtém-se assim a valuação $\phi(x) = |x|^{\frac{\alpha}{k}}$. □

Para qualquer valuação não-arquimediana ϕ num corpo $\mathbb{K}$, o conjunto $A_\phi = \{x \in \mathbb{K} : \phi(x) \leq 1\}$ é um subanel de $\mathbb{K}$. A_ϕ é designado por ***anel de valuação de*** ϕ. O anel de valuação A_ϕ é um anel local onde o ideal maximal é o conjunto $m_\phi = \{x \in \mathbb{K} : \phi(x) < 1\}$.

Nota 5. *Seja $y \in \mathbb{K}$ tal que $y \notin A_\phi$. Então $\phi(y) > 1$ e pela Proposição 3.2, $\phi(y^{-1}) = \phi(y)^{-1} < 1$, isto é, $y^{-1} \in A_\phi$. Provámos que A_ϕ é um anel de valuação. Portanto, pela Propriedade 1 dos anéis de valuação, $\mathbb{K}$ é corpo das fracções de A_ϕ.*

Definição 3.11. *Diz-se que uma valuação $\phi : \mathbb{K} \to \mathbb{R}_{\geq 0}$ é* **discreta** *se $\phi[\mathbb{K} \setminus \{0\}]$ é um subgrupo discreto de $(\mathbb{R}^+, \cdot, ^{-1}, 1)$ para a topologia usual em $\mathbb{R}$.*

Proposição 3.12. *Seja $\phi : \mathbb{K} \longrightarrow \mathbb{R}_{\geq 0}$ uma valuação. Então $\phi(\mathbb{K} \setminus \{0\})$ é um subgrupo de $(\mathbb{R}^+, \cdot, ^{-1}, 1)$.*

Prova: $\phi[\mathbb{K} \setminus \{0\}] = \{\phi(x) : x \in \mathbb{K} \setminus \{0\}\}$ e temos que $\phi[\mathbb{K} \setminus \{0\}] \subseteq \mathbb{R}^+$. Logo, é suficiente mostrar que $\phi[\mathbb{K} \setminus \{0\}]$ é fechado para as operações que conferem a $(\mathbb{R}^+, \cdot, ^{-1}, 1)$ a estrutura de um grupo. Sejam r, $s \in \phi[\mathbb{K} \setminus \{0\}]$ arbitrários, então r e s correspondem às imagens por ϕ de x e y em $\mathbb{K} \setminus \{0\}$ respectivamente. Portanto, $rs = \phi(x)\phi(y) = \phi(xy) \in \phi[\mathbb{K} \setminus \{0\}]$ porque $xy \geq 0$. □

Proposição 3.13. *Seja $\phi : \mathbb{K} \longrightarrow \mathbb{R}_{\geq 0}$ uma valuação arquimediana. Então ϕ não é discreta.*

Prova: Uma vez que ϕ é arquimediana, pela Proposição 3.9, $\mathbb{K}$ tem característica infinita e consequentemente, pela Proposição 1.35, $\mathbb{Q}$ é um subcorpo de $\mathbb{K}$. A restrição da

valuação ϕ em $\mathbb{Q}$ continua a ser uma valuação arquimediana e, pelo Teorema de Ostrowski, $\phi\big|_{\mathbb{Q}}(\mathbb{Q} \setminus \{0\}) = \{|x|^\alpha : \quad \alpha > 0\}$. Dado $r \in \mathbb{R}_{\geq 0}$, existe uma sucessão $(x_n)_{n\in\mathbb{N}}$ em $\mathbb{Q}$ tal que $(|x_n|^\alpha)_{n\in\mathbb{N}}$ tende para r. Mas $(|x_n|^\alpha)_{n\in\mathbb{N}}$ tende para r se e só se $(|x_n|)_{n\in\mathbb{N}}$ tende para $r^{1/\alpha}$. Como $\mathbb{Q}$ é denso em $\mathbb{R}$ então $\phi[\mathbb{K} \setminus \{0\}]$ contém um subgrupo denso e portanto, ϕ não é discreta. □

Teorema 3.14. *Seja ϕ uma valuação não-arquimediana não-trivial num corpo $\mathbb{K}$ e A_ϕ o anel de valuação de ϕ. Então ϕ é discreta se e só se A_ϕ é um anel de valuação discreta.*

Prova: Suponha-se que A_ϕ é um anel de valuação discreta e π o gerador do ideal maximal. Pela Nota 5, $\mathbb{K}$ é o corpo das fracções de A_ϕ. Assim, tomando $x \in \mathbb{K} \setminus \{0\}$, x escreve-se de forma única como $x = u\pi^k$, com u invertível em A_ϕ. Logo, $u \notin m_\phi$, $\phi(u) = 1$ e $\phi(x) = \phi(\pi)^k$. Portanto, pela Proposição 1.42 e pela Proposição 3.12, $\phi[\mathbb{K} \setminus \{0\}]$ é um subgrupo discreto de $(\mathbb{R}^+, \cdot, ^{-1}, 1)$ gerado por $\phi(\pi)$.

Suponhamos que ϕ é uma valuação discreta. Atendendo ao isomorfismo $(-\log)$ entre $(\mathbb{R}^+, \cdot, ^{-1}, 1)$ e $(\mathbb{R}, +, -, 0)$ e ao isomorfismo entre os subgrupos discretos de $(\mathbb{R}^+, \cdot, ^{-1}, 1)$ e $(\mathbb{Z}, +, -, 0)$ (Proposição 1.43), temos que

$$A_\phi = \{x \in \mathbb{K} : \phi(x) \leq 1\} = \{x \in \mathbb{K} : (\xi \circ \phi)(x) \geq 0\} \cup \{0\}$$

onde ξ é um isomorfismo que inverte a ordem entre $(\mathbb{R}^+, \cdot, ^{-1}, 1)$ e $(\mathbb{Z}, +, -, 0)$ e consiste na composição entre os dois isomorfismos referidos acima. Portanto, A_ϕ é um anel de valuação discreta. □

Bibliografia

[1] Hungerford, T. W., *Algebra*, Springer-Verlag, 1974.

[2] Ash, R. B., *A Course In Commutative Algebra* , Copyrigth, 2003.
[$http://www.math.uiuc.edu/\ r-ash/ComAlg.html$]

[3] Stevenhagen, P., *VOORTGEZETTE GETALTHEORIE* , Thomas Stieltjes Instituut, 2002. [$http://websites.math.leidenuniv.nl/algebra/localfields.pdf$]

[4] Roquette, P., *History of Valuation Theory*, Heidelberg, 2003.
[$http://www.rzuser.uni-heidelberg.de/\ ci3/hist_val.pdf$]

[5] Sigler, L. E., *Algebra*, Springer-Verlag, 1976.

[6] Azevedo, A. J. C. B. d', *Estruturas Algébricas [Texto policopiado]*, A. d'Azevedo, 2001.

[7] Kempf, G. R., *Algebraic Structures*, Vieweg, 1995.

[8] Ferreira, J.C., *Introdução à Análise Matemática*, 9ª Edição, Fundação Calouste Gulbenkian, 2008.