UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE MATEMÁTICA

Leonardo Guarnieri Justino

VALORES ABSOLUTOS E VALORAÇÕES

Florianópolis

2018

Leonardo Guarnieri Justino
Orientador: Prof. Dr. Daniel Gonçalves

VALORES ABSOLUTOS E VALORAÇÕES

Trabalho de Conclusão de Curso apresentado na Universidade Federal de Santa Catarina como requisito para a obtenção do grau de Bacharel em Matemática

Florianópolis
2018

RESUMO

Esse trabalho tem como objetivo apresentar uma introdução à teoria de valorações em corpos, bem como sua relação com algumas outras teorias da matemática. O trabalho foi pensado com alunos da graduação em mente, significando que conceitos incomuns na graduação serão abordados na medida do necessário para o entendimento do leitor não habituado com os mesmos.

Palavras-chave: Valoração, Valores absolutos, Corpos

SUMÁRIO

1 INTRODUÇÃO

Esse trabalho tem como tema estudar o conceito de valoração em corpos. Por se tratar de uma monografia de TCC, e portanto poder eventualmente ser lido por um aluno de graduação em matemática, ou área relacionada, será dada uma abordagem o mais auto-contida o possível para ele. Nessa abordagem, assumiremos conhecimento do leitor em teoria de anéis e grupos, bem como nos conceitos introdutórios de análise. Conceitos de álgebra linear ajudarão na intuição, mas não são, de fato, mais pré-requisitos.

Escolhemos ter esses conteúdos como pré-requisito pois os mesmos são normalmente obrigatórios em cursos de graduação, mas outros conteúdos relevantes, tais como topologia, grupos ordenados e módulos, serão introduzidos ao leitor conforme necessário.

Como dito, começaremos com uma introdução a topologia na qual apresentaremos o conteúdo necessário ao leitor. Em seguida, iniciaremos o estudo de valor absoluto em um corpo, seguindo a definição de normas em um espaço vetorial. Será apresentado uma classe de valores absolutos com uma propriedade que não é análoga à de normas, e que será nosso alvo de estudo, junto com suas generalizações. As propriedades métricas e topológicas que se pode obter serão estudadas logo em seguida.

Buscando generalizar o que foi estudado, definiremos um grupo abeliano ordenado, e após estudarmos algumas das propriedades que surgem, iremos usá-los como ferramenta na generalização que buscamos. Após isso, algumas caracterizações serão provadas, relacionando o nosso objeto principal de estudo com divisibilidades e corpos projetivos.

Finalmente, iremos ver como valorações nos ajudam a entender polinômios com coeficientes em um domínio de integridade, e usaremos o que vimos para definir e estudar brevemente os anéis de Prüfer. Após isso, veremos que outros estudos podem ser feitos na área, bem como mencionaremos generalizações que foram usadas fora da área.

A referência principal desse trabalho será o livro Valuation Theory de Otto Endler [1], e essa será referida como “referência principal” ou apenas como “referência”.

2 NOÇÕES DE TOPOLOGIA

Com o intuito de deixar esse trabalho o mais acessível possível para alunos de graduação, iremos dar algumas noções topológicas conforme for necessário saber para nossos fins, começando pela definição de espaço topológico. O leitor interessado pode consultar [2].

Definição 1. *Seja X um conjunto não vazio. Uma* topologia *em X é uma família τ de subconjuntos de X com as seguintes propriedades:*

1) $\emptyset, X \in \tau$

2) $A, B \in \tau \implies A \cap B \in \tau$

3) $T \subseteq \tau \implies \bigcup\limits_{U \in T} U \in \tau$

O par (X, τ) é dito um espaço topológico *e os elementos de τ são chamados de abertos. Se $x \in X$ e $U \in \tau$ são tais que $x \in U$, então U é dita ser uma* vizinhança aberta de x.

Observação 2. *Note que a propriedade 2 é suficiente para mostrar que uma interseção finita de abertos é, novamente, um aberto. Um esboço de como mostrar isso é notar que $A_1 \cap A_2 \cap ... \cap A_n = A_1 \cap (A_2 \cap ... \cap A_n)$, aplicar indução supondo que a interseção dos $n-1$ abertos é um aberto e aplicar a definição para mostrar que a interseção de A_1 com esse aberto ainda é um aberto.*

Exemplo 3. *Dado um conjunto X não vazio, a família de todos os subconjuntos de X é uma topologia para X, chamada de* topologia discreta sobre X. *De fato, $\emptyset$ e X são subconjuntos de X, a interseção de dois subconjuntos de X é um subconjunto de X e a união de quaisquer subconjuntos de X é um subconjunto de X.*

Exemplo 4. *Dado um conjunto X não vazio, $\tau = \{\emptyset, X\}$ é uma topologia para X, chamada de* topologia caótica sobre X. *De fato, por construção, $\emptyset, X \in \tau$. Dados dois elementos de τ, ou ambos são X, nesse caso a interseção é $X \in \tau$, ou um deles é $\emptyset$, e nesse caso a interseção é $\emptyset \in \tau$.*

Exemplo 5. *Seja (M, d) um espaço métrico. Da análise, definimos um aberto dele como sendo um conjunto U tal que para qualquer $x \in U$, existe $r \in \mathbb{R}_+^* := \{s \in \mathbb{R}; s > 0\}$ tal que $B_r(x) \subseteq U$. É conhecido que o conjunto de todas as bolas de M tem as propriedades da definição acima, logo, é um espaço topológico sobre M.*

Por algum tempo, o último exemplo será o único tipo de espaço topológico que trabalharemos, mas quando falarmos de valorações de

Krull, precisaremos de espaços topológicos que não vem de um espaço métrico. É interessante dar um nome para os espaços métricos compreendidos no último exemplo.

Definição 6. *Um espaço topológico (X, τ) é dito* metrizável *se existe alguma métrica d sobre X tal que τ é o conjunto dos abertos dessa métrica. Nesse caso, dizemos que τ é a* topologia induzida por d.

Em topologias metrizáveis, sabemos da definição que dado um aberto e um ponto dele, existe uma bola centrada nesse ponto que está contida no aberto. Esse noção se estende para espaços topológicos via bases, das quais falaremos adiante. Por hora, iremos provar um resultado semelhante que nos ajudará adiante.

Teorema 7. *Seja X um espaço topológico e $U \subseteq X$. Então U é aberto se, e somente se, para todo $x \in U$ existe uma vizinhança aberta U_x de x tal que $U_x \subseteq U$.*

Demonstração. Suponha que U seja aberto. Então para cada $x \in U$, tome $U_x = U$. Claramente, U_x é aberto e $x \in U_x \subseteq U$. Reciprocamente, se temos U_x para cada x como na hipótese, de $\{x\} \subseteq U_x \subseteq U$ temos

$$U = \bigcup_{x \in U} \{x\} \subseteq \bigcup_{x \in U} U_x \subseteq U.$$

Sabemos da definição de espaço topológico que união qualquer de abertos é aberto, logo $U = \bigcup\limits_{x \in U} U_x$ é aberto.

■

Assim como em espaços métricos, estamos interessados em saber quando uma sequência é convergente e uma função é contínua. Para chegar a essas definições, note que $d(x, y) < \varepsilon$ é o mesmo que $y \in B_\varepsilon(x)$. Substituindo essa bola por um aberto que contém x como elemento, obtemos a definição para espaços topológicos. Veremos mais adiante, quando falarmos em bases, que essa definição coincide com a definição usual para espaços métricos. Abaixo, daremos essas definições formalmente.

Definição 8. *Seja (X, τ) um espaço topológico e $(x_n)_{n \in \mathbb{N}}$ uma sequência de elementos de X. Dado um elemento $x \in X$, dizemos que a sequência $(x_n)_{n \in \mathbb{N}}$* converge para x *se para toda vizinhança aberta U de x, existe $n_0 \in \mathbb{N}$ tal que para $n \geq n_0$ temos $x_n \in U$. Denotaremos isso por $x_n \xrightarrow{n \to \infty} x$*

Note que não definimos os sentido de $\lim_{n\to\infty} x_n = x$. Evitaremos usar o símbolo de igualdade nesse caso, pois diferente do que acontece com espaços métricos, em um espaço topológico, uma mesma sequência pode convergir para vários elementos distintos.

Exemplo 9. *Considere X um conjunto com ao menos dois elementos e τ a topologia caótica em X. Seja $(x_n)_{n\in\mathbb{N}}$ qualquer sequência de de X e $x \in X$ qualquer. Dado uma vizinhança aberta U de x, temos $x \in U \in \{\emptyset, X\}$, logo $U = X$. Então, tomando $n_0 = 0$, se $n \geq n_0$ temos $x_n \in X = U$, logo qualquer $(x_n)_{n\in\mathbb{N}}$ converge para qualquer x.*

Mais abaixo, quando virmos espaços topológicos de Hausdorff, mostraremos que neles toda sequência que converge para algum elemento converge para um único elemento. Lá, definiremos o sentido de $\lim_{n\to\infty} x_n = x$ da maneira evidente. Agora, mudando para continuidade, a motivação é análoga ao que foi feito antes.

Definição 10. *Sejam X e Y espaços topológicos e $F : X \to Y$ uma função. Dado $x \in X$, diremos que f é* contínua em X *se para toda vizinhança aberta V de $F(x)$ em Y, existe uma vizinhança aberta U de x em X tal que $f(U) := \{f(x); x \in U\} \subseteq V$, isto é, para qualquer $x' \in U$ temos $f(x') \in V$. Se f for contínua em todo ponto de seu domínio, diremos que f é* contínua.

A seguinte caracterização é usada frequentemente:

Teorema 11. *Sejam X e Y espaços topológicos e $f : X \to Y$ uma função. Então f é contínua se, e somente se, para todo aberto V de Y temos que $f^{-1}(V) := \{x \in X; f(x) \in V\}$ é aberto. Em outras palavras, funções contínuas são, precisamente, as funções que levam apenas (mas não necessariamente todos) os abertos em abertos.*

Demonstração. Suponha f contínua. Então, dado um aberto V de Y, considere $U = f^{-1}(V)$. Para cada $x \in U$, temos $f(x) \in V$ e como f é contínua, ela é contínua em x e logo existe uma vizinhança aberta U_x de x tal que $f(U_x) \subseteq V$. Tome $x' \in U_x$. Temos $f(x') \in f(U) \subseteq V$ e logo $x' \in f^{-1}(V) = U$. Disso, concluímos $U_x \subseteq U$. Do teorema 7, U é aberto. Reciprocamente, suponha que $f^{-1}(V)$ é aberto para todo aberto V de Y. Então, dado $x \in X$ e V vizinhança aberta de $f(x)$ em Y, tome $U = f^{-1}(V)$. Da hipótese temos que U é aberto, de $f(x) \in V$ temos que $x \in U$ e dado $x' \in U$ temos que $f(x') \in V$, provando a continuidade de f em x. Como x foi qualquer, concluímos que f é contínua.

■

Agora introduziremos o conceito de base de um espaço topológico, que é similar ao conceito de bolas de um espaço métrico.

Definição 12. *Seja X um conjunto. Uma coleção $\beta \neq \emptyset$ de subconjuntos de X é dita uma* base de X *se $\bigcup \beta = X$ e se dados $B_1, B_2 \in \beta$ e $x \in B_1 \cap B_2$, existe $B \in \beta$ tal que $x \in B \subseteq B_1 \cap B_2$.*

Exemplo 13. *Se X é um conjunto qualquer, então $\{X\}$ é base de X, bem como a coleção de todos os subconjuntos de X.*

Exemplo 14. *Se (M, d) é um espaço métrico, então o conjunto β de todas as bolas do espaço métrico é uma base de M.*

Teorema 15. *Seja $X \neq \emptyset$ um conjunto e β uma base de X. Defina uma coleção τ de subconjuntos de X da seguinte forma: $U \in \tau$ se, e somente se, para todo $x \in U$, existe $B \in \beta$ tal que $x \in B \subseteq U$. Então τ é uma topologia em X com $\beta \subseteq \tau$ e além disso, se τ' é uma topologia de X para a qual $\beta \subseteq \tau'$, então $\tau \subseteq \tau'$ (isto é, τ é a menor topologia de X que contém β).*

Demonstração. Por vacuidade, $\emptyset \in \tau$. Além disso, tome $x \in X$ e note que como β é base, existe $B \in \beta$ tal que $x \in B$. Então, $B \subseteq X$, mostrando que $X \in \tau$.

Agora, tome $U, V \in \tau$. Dado $x \in U \cap V$, existem $B_U, B_V \in \beta$ tais que $x \in B_U \subseteq U$ e $x \in B_V \subseteq V$. Tome $B \in \beta$ tal que $x \in B \subseteq B_U \cap B_V$, que existe pois β é base, e observe que $x \in B \subseteq B_U \cap B_V \subseteq U \cap V$, logo $U \cap V \in \tau$. Finalmente, considere $T \subseteq \tau$ e note que dado $x \in \bigcup T$, existe $U_0 \in T$ tal que $x \in U_0$. Tome $B \in \beta$ tal que $x \in B \subseteq U_0$ e conclua que $x \in B \subseteq \bigcup_{U \in T} U$, provando que τ é topologia.

Agora, considere $U \in \beta$ e note que dado $x \in U$, temos $x \in U \subseteq U$, logo $U \in \tau$.

Se τ' é topologia em X tal que $\beta \subseteq \tau'$, tome $U \in \tau$ qualquer e para cada $x \in U$, fixe $B_x \in \beta$ com $x \in B_x \subseteq U$. Temos $B_x \in \beta \subseteq \tau'$, logo, de τ' ser topologia, $U = \bigcup_{x \in U} B_x \in \tau'$, provando $\tau \subseteq \tau'$.

■

Exemplo 16. *A base $\{X\}$ gera a topologia caótica. De fato, se U é um aberto não-vazio da topologia gerada, temos que para $x \in U$ escolhido arbitrariamente, $x \in X \subseteq U$. Como $U \subseteq X$, concluímos $X = U$.*

Exemplo 17. *Já a base formada por todos os subconjuntos de X gera a topologia discreta. De fato, dado $U \subseteq X$, para $x \in X$ tome $B = \{x\}$. Temos $x \in B \subseteq U$, logo U é aberto.*

Exemplo 18. *Se (M, d) é espaço métrico e β é a base das bolas do espaço, a topologia gerada por β é a topologia induzida de d.*

Diversos conceitos da topologia que são dados em função de abertos podem ser dados em função dos elementos de uma base. Como exemplo, mostraremos isso para limite de sequências e para continuidade.

Teorema 19. *Seja (X, τ) o espaço topológico gerado por uma base β de X. Dada uma sequencia $s = (x_i)_{i \in \mathbb{N}}$ de elementos de X e um elemento $x \in X$, a sequencia s converge para x se, e somente se, para todo $B \in \beta$ com $x \in B$, existe $n_0 \in \mathbb{N}$ tal que se $n \geq n_0$, então $x_n \in B$.*

Demonstração. Como todo elemento de β é aberto, se s converge para x, aplicamos a definição de convergência para obter o resultado que queremos. Reciprocamente, dado $U \in \tau$ com $x \in U$, tome $B \in \beta$ tal que $x \in B \subseteq U$. Temos que da hipótese, existe $n_0 \in \mathbb{N}$ tal que se $n \geq n_0$, então $x_n \in B \subseteq U$, concluindo a demonstração.

■

Teorema 20. *Sejam (X, τ) e (Y, ν) os espaços topológicos gerados, respectivamente, pelas bases $\beta \subseteq \tau$ e $\gamma \subseteq \nu$. Então uma função $f : X \to Y$ é contínua em um ponto $x \in X$ se, e somente se, para todo $C \in \gamma$ com $f(x) \in C$, existe $B \in \beta$ com $x \in B$ tal que $f(B) \subseteq C$, isto é, para todo $y \in B$, $f(y) \in C$.*

Demonstração. Novamente, como elementos de β são abertos de X e elementos de γ são abertos de Y, assumindo a continuidade de f, o resultado que queremos provar é imediato. Reciprocamente, considere $V \in \nu$ com $f(x) \in V$. Então existe $C \in \gamma$ tal que $f(x) \in C \subseteq V$. Da hipótese, existe $B \in \beta \subseteq \tau$ tal que para todo $y \in B$, $f(y) \in C \subseteq V$, provando a continuidade da função.

■

Como podemos ver até o momento, a noção abstrata de topologia nos dá uma teoria já rica. Ainda assim, é necessário pedir mais coisas para que os espaços topológicos se comportem mais próximos da intuição métrica que temos (por exemplo, toda sequencia convergente ter um único limite). Há várias formas de se fazer isso, como por exemplo com os Axiomas de Separação, mas veremos aqui apenas o axioma conhecido como T2 (ou Hausdorff).

Definição 21. *Um espaço topológico (X, τ) é dito ser um* espaço de Hausdorff *quando dados $x, y \in X$ com $x \neq y$, existem abertos $U_x, U_y \in \tau$ tais que $x \in U_x$, $y \in U_y$ e $U_x \cap U_y = \emptyset$.*

Nem todos os espaços que trabalharemos serão metrizáveis, mas normalmente, estes serão Hausdorff. Mostraremos que em um espaço Hausdorff, o limite é único sempre que existir.

Teorema 22. *Seja (X, τ) um espaço topológico Hausdorff. Se $s = (x_i)_{i \in \mathbb{N}}$ é uma sequência de elementos de X e $x, y \in X$ são tais que s converge para x e s converge para y, então $x = y$.*

Demonstração. Suponha por absurdo que $x \neq y$. Então, pela propriedade Hausdorff, existem $U_x, U_y \in \tau$ tais que $x \in U_x$, $y \in U_y$ e $U_x \cap U_y = \emptyset$. Da definição de convergência, existem $n_1, n_2 \in \mathbb{N}$ tais que se $n \geq n_1$ e $m \geq n_2$, então $x_n \in U_x$ e $x_m \in U_y$. Tome $n = \max(n_1, n_2)$. Temos $n \geq n_1$ e $n \geq n_2$, logo $n \in U_x$ e $n \in U_y$. Mas isso contradiz $U_x \cap U_y = \emptyset$. Por absurdo, $x = y$. ∎

Observação 23. *Se o caso acima ocorrer, definiremos $\lim_{n \to \infty} x_n := x = y$.*

Por último, faremos uma outra construção nos moldes do que foi feito em bases. Essa construção não é usual em introduções, mas um caso muito particular dela será usado quando estudarmos valorações de Krull. Essa construção será repetida lá no caso que nos interessa, e portanto o leitor não interessado poderá ir diretamente à próxima sessão. Por esse motivo, usaremos um conceito que só iremos definir (em um caso particular) mais à frente, assumindo que o leitor interessado já conhece o mesmo.

Considere $(R, \cdot, \leq)$ um monoide comutativo dirigido (para baixo), isto é, um monoide comutativo parcialmente ordenado tal que dados $x, y \in R$, existe $z \in R$ tal que $z \leq x$ e $z \leq y$. Suponha também que R admite mínimo 0, que $R \neq \{0\}$ e que dados $x, y \in R$ tais que $x < y$, existe $x' \in R$ tal que $x' > 0$ e $x + x' \leq y$. Dado um conjunto M, seja $d : M \times M \to R$ uma função satisfazendo propriedades análogas às de espaço métrico, isto é:

1) $d(x, y) = 0 \Leftrightarrow x = y$
2) $d(x, y) = d(y, x)$
3) $d(x, z) \leq d(x, y) + d(y, z)$

Em M, podemos definir uma base τ da seguinte forma: Dados $x \in M$ e $r \in R^* = R \setminus \{0\}$, defina a bola de centro x e raio r como o conjunto $B_r(x) = \{y \in M; d(x, y) < r\}$ e $\beta = \{B_r(x); x \in M \text{ e } r \in R^*\}$. Temos de imediato a seguinte propriedade:

Teorema 24. *Nas notações acima, dado $r \in R^*$ e dados $x, y \in M$ tal que $d(x, y) < r$, existe $s \in R^*$ tal que $B_s(y) \subseteq B_r(x)$.*

Demonstração. De fato, tome s tal que $d(x,y)+s \leq r$, como na definição de M. Se $z \in B_s(y)$, então $d(z,x) \leq d(z,y)+d(y,x) < s+d(y,x) \leq r$, logo $B_s(y) \subseteq B_r(x)$.

■

Note que β é de fato uma base, pois dado $x \in M$, $d(x,x)=0$, portanto qualquer $r \in R^*$ é tal que $x \in B_r(x)$ e temos $\bigcup_{x\in M} B_r(x) = M$. Além disso, se $B_r(x), B_s(y) \in \beta$, considere $z \in B_r(x) \cap B_s(y)$ e tome $t, t_x, t_y \in R^*$ tais que:

(1) $B_{t_x}(z) \subseteq B_r(x)$ e $B_{t_y}(z) \subseteq B_s(y)$ (existem, do teorema acima).

(2) $t \leq t_x$ e $t \leq t_y$ (existe, pois M é dirigido.)

Temos que $B_t(z) \subseteq B_{t_x}(z) \subseteq B_r(x)$ e $B_t(z) \subseteq B_{t_y}(z) \subseteq B_s(y)$. Provamos que $z \in B_t(z) \subseteq B_r(x) \cap B_s(y)$. Tome τ como sendo a topologia gerada por β.

Já vimos caracterizações da noções de limite de sequência e continuidade para topologias geradas por bases, mas nesse caso particular, nossa topologia assume caracterizações ainda mais parecidas com as de um espaço metrizável, onde as bases precisam ser centradas no ponto em questão:

Teorema 25. *Nas notações acima, $U \in \tau$ se, e somente se, para todo $x \in U$, existe $r \in R^*$ tal que $B_r(x) \subseteq U$.*

Demonstração. Se U é um aberto, então dado $x \in U$, existe $B_s(y) \in \beta$ tal que $x \in B_s(y) \subseteq U$. Tome $r \in R$ tal que $B_r(x) \subseteq B_s(y)$, e obtemos a bola centrada em x desejada. Reciprocamente, suponha que tal r sempre exista. Então, dado $x \in U$, a bola $B_r(x)$ é um elemento de β e $x \in B_r(x) \subseteq U$, provando que U é aberto. ■

Teorema 26. *Nas notações acima, (M,τ) é Hausdorff e $\lim\limits_{n\to\infty} x_n = x$ se, e somente se, para todo $\varepsilon \in R^*$, existe $n_0 \in \mathbb{N}$ tal que para $n \geq n_0$, $d(x_n,x) < \varepsilon$*

Demonstração. Considere $x,y \in M$ com $x \neq y$ e note que $d(x,y) > 0$. Separaremos em dois casos: suponha inicialmente que existe $s \in R^*$ tal que $s < d(x,y)$. Então podemos tomar $r \in R^*$ tal que $s + r \leq d(x,y)$. Então, $x \in B_r(x)$, $y \in B_s(y)$ e se supormos $z \in B_r(x) \cap B_s(y)$, temos $d(x,y) \leq d(x,z) + d(z,y) < r+s \leq d(x,y)$, o que é uma contradição, logo $B_r(x) \cap B_r(y) = \emptyset$.

Agora, suponha que não exista $s \in S^*$ tal que $s < d(x,y)$. Considere $r = d(x,y)$ e note que $x \in B_r(x)$ e $y \in B_r(y)$. Agora suponha por absurdo que exista $z \in B_r(x) \cap B_r(y)$. Então como $r > 0$, $d(x,y) \leq d(x,z) + d(z,y) < r + r < r = d(x,y)$, o que é uma contradição e logo $B_r(x) \cap B_r(y) = \emptyset$. Como para cada $x, y \in M$ com $x \neq y$ um dos dois casos acontece, concluímos que (M, τ) é Hausdorff.

Finalmente, suponha que $\lim_{n\to\infty} x_n = x$. Então dado $\varepsilon \in R^*$, $B_\varepsilon(x)$ é uma vizinhança aberta de x. Da convergência, existe $n_0 \in \mathbb{N}$ tal que se $n \geq n_0$, então $x_n \in B_\varepsilon(x)$. Mas então, $d(x_n, x) < \varepsilon$, e encontramos o valor desejado. Por outro lado, se tal n_0 existe para qualquer ε, podemos tomar um $B_r(y) \in \beta$ com $x \in B_r(y)$ e lembrar que existe $\varepsilon \in \mathbb{R}^*$ tal que $B_\varepsilon(x) \subseteq B_r(y)$. Então, tomando n_0 adequado, temos que se $n \geq n_0$, então $d(x_n, x) < \varepsilon$ e então, $x_n \in B_\varepsilon(x) \subseteq B_r(y)$ e $\lim_{n\to\infty} x_n = x$.

■

Teorema 27. *Nas notações acima, se $N \neq \emptyset$ é um conjunto, $(S, +, \leq)$ é monoide dirigido nas mesmas hipóteses de R e $d' : N \times N \to S$ é uma função com as propriedades de espaço métrico, então uma função $f : M \to N$ é contínua em $x \in M$ se, e somente se, para todo $\varepsilon \in S^*$, existe $\delta \in R^*$ tal que se para qualquer $y \in M$, vale que $d(x,y) < \delta \implies d'(f(x), f(y)) < \varepsilon$.*

Demonstração. Seja $B'_s(y)$ a bola de N com centro $y \in N$ e raio $s \in S^*$ e β' é o conjunto das bolas de (N, d'). Suponha f contínua e tome $x \in M$, $\varepsilon \in S^*$. Então $f(x) \in B'_\varepsilon(f(x)) \in \beta'$, logo existe $B_r(x') \in \beta$ tal que $f(B_r(x')) \subseteq B'_\varepsilon(f(x))$. Tome $\delta \in R^*$ tal que $B_\delta(x) \subseteq B_r(x')$ e note que se $d(x,y) < \delta$, então $y \in B_\delta(x)$ e logo $f(y) \in B'_\varepsilon(f(x))$, isto é, $d'(f(y), f(x)) < \varepsilon$. Suponha agora a hipótese da recíproca. Temos que dado $B'_r(y) \in \beta'$ com $f(x) \in B'_r(y)$, podemos tomar $\varepsilon \in S^*$ tal que $B'_\varepsilon(f(x)) \subseteq B'_r(y)$. Então, pulando passos análogos aos que já foram feitos algumas vezes, existe $\delta \in R^*$ tal que se $d(z,x) < \delta$, então $d'(f(z), f(x)) < \varepsilon$. ■

3 VALORES ABSOLUTOS

Definição 28. *Seja* $\mathbb{K}$ *um corpo. Uma função* $|\cdot|:\mathbb{K}\to\mathbb{R}$ *é dita um* valor absoluto *em* $\mathbb{K}$ *se valem, para todos* $x,y\in\mathbb{K}$*:*

1) $|x|\geq 0$ *e* $|x|=0$ *se, e somente se,* $x=0$.

2) $|x+y|\leq |x|+|y|$

3) $|xy|=|x||y|$

Além disso, se $|x+y|\leq \max(|x|,|y|)$*,* $|\cdot|$ *é dita* não-arquimediana *e caso contrário é dita* arquimediana. *O par ordenado* $(\mathbb{K},|\cdot|)$ *será dito um* corpo com valor absoluto.

Observação 29. *Note que se uma função* $|\cdot|:\mathbb{K}\to\mathbb{R}_+$ *satisfaz* $|x+y|\leq\max(|x|,|y|)$*, então, de* $\max(a,b)\leq\max(a,b)+\min(a,b)=a+b$ *para* $a,b\in\mathbb{R}_+$*, temos* $|x+y|\leq|x|+|y|$*. Com isso, concluímos que se queremos mostrar que uma função é um valor absoluto não-arquimediano, não precisamos mostrar 2., já que ela é consequência da propriedade extra que temos que mostrar.*

Exemplo 30. *Defina* $|0|=0$ *e* $|x|=1$ *para* $x\neq 0$*. Então* $|\cdot|$ *é um valor absoluto não-arquimediano sobre* $\mathbb{K}$*, denominado* valor absoluto trivial.

Exemplo 31. *Considere* $\mathbb{K}$ *subcorpo de* $\mathbb{C}$*. Como já conhecido, a função* $|\cdot|$ *usual tem as propriedades da definição acima, e é um valor absoluto arquimediano.*

Teorema 32. *Sejam* $a,b,c,d\in\mathbb{Z}^*$ *e fixe* p_0 *primo positivo. Para* $k\in\mathbb{Z}^*$*, defina* n_k *como o maior inteiro tal que* $p_0^{n_k}|k$*, isto é,* n_k *é o expoente de* p_0 *na decomposição de* k *em fatores primos. Se* $\frac{a}{b}=\frac{c}{d}$*, então* $n_a-n_b=n_c-n_d$ *e a função* $v_{p_0}:\mathbb{Q}\to\mathbb{Z}$ *com* $v_{p_0}(\frac{a}{b})=n_a-n_b$ *está bem definida.*

Demonstração. Seja $\mathcal{P}$ o conjunto de todos os primos positivos e escreva

$$a=u_a\prod_{p\in\mathcal{P}}p^{\alpha_p},\ b=u_b\prod_{p\in\mathcal{P}}p^{\beta_p},\ c=u_c\prod_{p\in\mathcal{P}}p^{\gamma_p},\ d=u_d\prod_{p\in\mathcal{P}}p^{\delta_p},$$

em que cada produto tem uma quantidade finita de fatores diferentes de 1 e $u_i\in\{-1,1\}$ para $i\in\{a,b,c,d\}$. De $\frac{a}{b}=\frac{c}{d}$, obtemos que $ad=cb$, isto é, $\prod_{p\in\mathcal{P}}p^{\alpha_p+\delta_p}=\prod_{p\in\mathcal{P}}p^{\gamma_p+\beta_p}$. Da unicidade da fatoração em primos, sai que para qualquer $p\in\mathcal{P}$, $\alpha_p+\delta_p=\gamma_p+\beta_p$ e portanto $\alpha_p-\beta_p=\gamma_p-\delta_p$. Em particular, para $p=p_0$, $n_a-n_b=\alpha_{p_0}-\beta_{p_0}=$

$\gamma_{p_0} - \delta_{p_0} = n_c - n_d$. Isso mostra que v_{p_0} está bem definida.

∎

Observação 33. *A demonstração do teorema acima também nos revela uma versão do Teorema Fundamental da Aritmética para números racionais. Dado $x = \frac{a}{b} \in \mathbb{Q}^*$, como temos uma quantidade finita de primos que aparecem na decomposição de a ou de b, temos uma quantidade finita de primos p tal que $v_p(x) \neq 1$. Escrevendo a e b como na demonstração, note:*

$$x = \frac{a}{b} = \frac{u_a \prod\limits_{p \in \mathcal{P}} p^{\alpha_p}}{u_b \prod\limits_{p \in \mathcal{P}} p^{\beta_p}} = \frac{u_a}{u_b} \cdot \prod_{p \in \mathcal{P}} p^{\alpha_p - \beta_p} = \frac{u_a}{u_b} \cdot \prod_{p \in \mathcal{P}} p^{v_p(x)}$$

Notando que $\frac{u_a}{u_b} \in \{-1, 1\}$, acabamos de escrever x como o produto de um inversível por um produto de potências de primos positivos, porem os expoentes aqui não estão restritos a $\mathbb{N}$ e sim a $\mathbb{Z}$. Para a unicidade, note que o inversível será -1 se $x < 0$ e 1 se $x > 0$, logo este será único. Suponha $x = u \prod\limits_{p \in \mathcal{P}} p^{\lambda_p}$ onde $u = \frac{u_a}{u_b}$ e $\lambda_p \in \mathbb{Z}$ com uma quantidade finita de $p \in \mathcal{P}$ tais que $\lambda_p \neq 0$. Defina $\zeta_p = \min(\lambda_p, 0)$ e $\eta_p = -\max(\lambda_p, 0)$ e observe que $\lambda_p = \zeta_p - \eta_p$, logo $x = u \prod\limits_{p \in \mathcal{P}} \frac{p^{\zeta_p}}{p^{\eta_p}}$. Mas então, fazendo $m = u \prod\limits_{p \in \mathcal{P}} p^{\zeta_p}$ e $n = \prod\limits_{p \in \mathcal{P}} p^{\eta_p}$, $x = \frac{m}{n}$ e por v_p estar bem definida para todo p, $\lambda_p = \zeta_p - \eta_p = v_p(\frac{m}{n}) = v_p(x)$.

Lema 34. *Seja $p_0 \in \mathcal{P}$, $v = v_{p_0}$ e $x, y \in \mathbb{Z}^*$. Então $v(x+y) \geq \min(v(x), v(y))$.*

Demonstração. De fato, escreva

$$x = u{p_0}^{v(x)} \prod_{p \in \mathcal{P} \setminus \{p_0\}} p^{v_p(x)}$$

$$y = u'{p_0}^{v(y)} \prod_{p \in \mathcal{P} \setminus \{p_0\}} p^{v_p(y)}$$

com $u, u' \in \{-1, 1\}$ e note que como $x, y \in \mathbb{Z}^*$, $v(x) \geq 0$ e $v(y) \geq 0$.

Suponha inicialmente que $v(x) \leq v(y)$. Então podemos colocar

$p_0^{v(x)}$ em evidência para obter

$$x+y={p_0}^{v(x)}\left(u\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(x)}+u'{p_0}^{v(y)-v(x)}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(y)}\right),$$

e como $v(x)\leq v(y)$, $v(x)\geq 0$ e $v(y)\geq 0$, obtemos

$$u\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(x)}+u'{p_0}^{v(y)-v(x)}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(y)}\in\mathbb{Z}^*.$$

Agora, pelo Teorema Fundamental da Aritmética, existem $u''\in\{-1,1\}$ e
$\lambda_p\in\mathbb{N}$ tais que

$$u\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(x)}+u'{p_0}^{v(y)-v(x)}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(y)}=u''p_0^{\lambda_{p_0}}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{\lambda_p}$$

e disso podemos concluir

$$x+y=p_0^{v(x)}\left(u''p_0^{\lambda_{p_0}}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{\lambda_p}\right)=u''p_0^{v(x)+\lambda_{p_0}}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{\lambda_p}$$

e portanto $v(x+y)=v(x)+\lambda_{p_0}\geq v(x)=\min(v(x),v(y))$. Caso $v(y)<v(x)$, temos $v(x+y)=v(y+x)\geq\min(v(y),v(x))=\min(v(x),v(y))$. ■

Teorema 35. *Sejam $x,y\in\mathbb{Q}^*$ e $p_0\in\mathcal{P}$. Então para $v=v_{p_0}$ valem:*
a. $v(xy)=v(x)+v(y)$
b. $v(x+y)\geq\min(v(x),v(y))$

Demonstração. Similarmente ao Lema 34, escreva

$$x=u\prod_{p\in\mathcal{P}}p^{v_p(x)}=u{p_0}^{v(x)}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(x)}$$
$$y=u'\prod_{p\in\mathcal{P}}p^{v_p(y)}=u'{p_0}^{v(y)}\prod_{p\in\mathcal{P}\backslash\{p_0\}}p^{v_p(y)}$$

com $u,u'\in\{-1,1\}$.

a. $xy=u\prod_{p\in\mathcal{P}}p^{v_p(x)}\cdot u'\prod_{p\in\mathcal{P}}p^{v_p(y)}=uu'\prod_{p\in\mathcal{P}}p^{v_p(x)+v_p(y)}$, e como temos que $uu' \in \{-1,1\}$, concluímos que $v(xy) = v(x) + v(y)$

b. Escreva, para $a, b, c, d \in \mathbb{Z}$ apropriados, $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Então, usando o item anterior e o lema 34,

$$v(x+y) = v\left(\frac{ad+bc}{bd}\right) = v(ad+bc) + v\left(\frac{1}{bd}\right) \geq \min(v(ad), v(bc)) + v\left(\frac{1}{bd}\right) =$$
$$= \min\left(v(ad) + v\left(\frac{1}{bd}\right), v(bc) + v\left(\frac{1}{bd}\right)\right) = \min\left(v\left(\frac{ad}{bd}\right), \left(\frac{bc}{bd}\right)\right) =$$
$$= \min\left(v\left(\frac{a}{b}\right), \left(\frac{c}{d}\right)\right) = \min(v(x), v(y)).$$

■

Observação 36. *A função v_{p_0} (e qualquer outra v_p para p primo) definida acima não é um valor absoluto em $\mathbb{Q}$, mas posteriormente, quando definirmos uma valoração, veremos que esse teorema quase prova v_p será uma valoração em $\mathbb{Q}$ para todo $p \in \mathcal{P}$. Iremos provar a parte que falta quando tal definição for dada. O exemplo abaixo mostra um caso particular da relação entre valorações e valores absolutos não-arquimedianos.*

Exemplo 37. *Dado um primo $p \in \mathcal{P}$, defina uma função $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ por $|0|_p = 0$ e para $x \neq 0$, $|x|_p = \frac{1}{p^{v_p(x)}}$, onde v_p foi definida no teorema 35. Mostraremos que essa função é um valor absoluto não-arquimediano. De fato, sejam $x, y \in \mathbb{Q}$. Então:*

1) Para $x = 0$, $|x|_p = 0$ e para $x \neq 0$, $|x|_p > 0$.

2) Se $x = 0$, temos $|x+y|_p = |y|_p \leq |y|_p = \max(|x|_p, |y|_p)$. Se $y = 0$, temos $|x+y|_p = |x|_p \leq |x|_p = \max(|x|_p, |y|_p)$. Se $x, y \in \mathbb{Q}^*$, o teorema 35 garante que $v_p(x+y) \geq \min(v_p(x), v_p(y))$. Concluímos que

$$|x+y|_p = \frac{1}{p^{v_p(x+y)}} \leq \frac{1}{p^{\min(v_p(x), v_p(y))}} = \max\left(\frac{1}{p^{v_p(x)}}, \frac{1}{p^{v_p(y)}}\right) = \max(|x|_p, |y|_p).$$

3) Se $x = 0$ ou $y = 0$, $|xy|_p = |0|_p = 0 = |x|_p|y|_p$. Caso $x, y \in \mathbb{Q}^*$, o teorema 35 garante $v_p(xy) = v_p(x) + v_p(y)$ e logo

$$|xy|_p = \frac{1}{p^{v_p(xy)}} = \frac{1}{p^{v_p(x)+v_p(y)}} = \frac{1}{p^{v_p(x)} \cdot p^{v_p(y)}} = \frac{1}{p^{v_p(x)}} \cdot \frac{1}{p^{v_p(y)}} = |x|_p|y|_p.$$

Temos que $|\cdot|_p$ é valor absoluto não-arquimediano, denominado valor absoluto p-ádico (em $\mathbb{Q}$).

Daqui em diante, dado um corpo com valor absoluto $(\mathbb{K}, |\cdot|)$, usaremos apenas $\mathbb{K}$ no lugar de $(\mathbb{K}, |\cdot|)$ quando o valor absoluto ficar claro no contexto.

Abaixo, seguem quatro propriedades essenciais de valores absolutos. Com exceção da propriedade 3., elas serão provadas no contexto de Valorações de Krull, mais para frente. No caso da propriedade 3., esta é relacionada com a continuidade do valor absoluto, no sentido que veremos em breve, o que pode ser justificado notando que ela essencialmente diz que quando x e y estão próximos, então $|x|$ e $|y|$ também o estão. Observe que as três primeiras propriedades já são conhecidas para o caso do valor absoluto usual de $\mathbb{C}$.

Teorema 38. *Seja $\mathbb{K}$ um corpo e $|\cdot|$ um valor absoluto em $\mathbb{K}$. Então*

1) Para toda raiz da unidade $u \in \mathbb{K}$, $|u| = 1$. Em particular, $|1| = 1$.
2) $|x^{-1}| = |x|^{-1}$ e $|-x| = |x|$.
3) $||x| - |y|| \leq |x - y|$.
4) Se $|\cdot|$ é não-arquimediana e $x, y \in \mathbb{K}$ são tais que $|x| \neq |y|$, então $|x + y| = \max(|x|, |y|)$.

Demonstração. 1) Primeiro, note que $u \neq 0$, pois 0 não é raiz da unidade, logo $|u| \neq 0$. Seja n tal que $u^n = 1_{\mathbb{K}}$. Então $|1_{\mathbb{K}}||u|^n = |1_{\mathbb{K}}||u^n| = |1_{\mathbb{K}}u^n| = |u^n| = |1_{\mathbb{K}}| = |1_{\mathbb{K}}| \cdot 1$. Como $1_{\mathbb{K}} \neq 0$, temos $|1_{\mathbb{K}}| \neq 0$, e como $\mathbb{R}$ é corpo (e portanto domínio de integridade) temos $|u|^n = 1$. Mas $|u|^n \in \mathbb{R}$, e como 1 é a única raiz positiva da unidade de $\mathbb{R}$ temos $|u| = 1$. Como $1_{\mathbb{K}}$ é raiz da unidade em $\mathbb{K}$, temos $|1_{\mathbb{K}}| = 1$.

2) De fato, $|x^{-1}||x| = |x^{-1}x| = |1_{\mathbb{K}}| = 1$. Ainda, $-1_{\mathbb{K}}$ é raiz da unidade, logo $|-1_{\mathbb{K}}| = 1$ e $|-x| = |-1_{\mathbb{K}} \cdot x| = |-1_{\mathbb{K}}||x| = 1|x| = |x|$.

3) Caso $|x| \geq |y|$, temos $|x| = |x - y + y| \leq |x - y| + |y|$, logo $||x| - |y|| = |x| - |y| = |x - y + y| - |y| \leq |x - y| + |y| - |y| = |x - y|$. Caso $|x| < |y|$, temos $|y| \geq |x|$, e portanto $||x| - |y|| = |y| - |x| \leq |y - x| = |x - y|$.

4) Suponha inicialmente que $|x| > |y|$. Então, $|x| = |x + y - y| \leq \max(|x + y|, |-y|) = \max(|x + y|, |y|)$. Mas temos $|x + y| \geq |y|$, pois caso contrário teríamos $|x| \leq |y| < |x|$, o que é uma contradição. Então concluímos $\max(|x|, |y|) = |x| \leq \max(|x + y|, |y|) = |x + y| \leq \max(|x|, |y|)$. Caso $|x| < |y|$, temos $|y| > |x|$ e portanto $|x + y| = |y + x| = \max(|y|, |x|) = \max(|x|, |y|)$.

■

Teorema 39. *Seja $|\cdot|$ um valor absoluto sobre $\mathbb{K}$. Definindo $d(x, y) = |x - y|$, com $x, y \in \mathbb{K}$, temos que d é uma métrica sobre $\mathbb{K}$, e portanto* *induz uma topologia sobre $\mathbb{K}$ que tem as bolas abertas do espaço métrico $(\mathbb{K}, d)$ como base.*

Demonstração. Verificaremos as propriedades de espaço métrico. Para isso, considere $x, y, z \in \mathbb{K}$ quaisquer.

1) $d(x, y) = |x - y| \geq 0$.
2) $d(x, y) = 0 \Leftrightarrow |x - y| = 0 \Leftrightarrow x - y = 0 \Leftrightarrow x = y$.
3) $d(x, z) = |x - z| = |x - y + y - z| \leq |x - y| + |y - z| = d(x, y) + d(y, z)$.

O fato que esse valor absoluto gera uma topologia vem do fato de que toda métrica gera uma topologia e esta é da forma que descrevemos. ■

A métrica definida acima é natural, no sentido de que sua definição é essencialmente a mesma dada para espaços métricos normados. Assim como nesse caso, tal métrica tem uma boa compatibilidade com a estrutura considerada: As operações de corpo são contínuas, assim como a função inverso, e como mencionado antes, o valor absoluto é uma função contínua. O enunciado formal disso é dado abaixo, bem como sua demonstração. Após isso, outro resultado útil será dado sobre a continuidade uniforme de certas restrições da função inverso e com isso poderemos, por exemplo, provar que determinadas sequências são de Cauchy, com o objetivo de construir completamentos. Os cálculos serão similares nos dois casos.

Teorema 40. *Seja $|\cdot|$ um valor absoluto sobre $\mathbb{K}$ e d a métrica induzida. Então dado $b \in \mathbb{R}_+^*$, a função $f_b : \{x \in \mathbb{K}; |x| \geq b\} \to \mathbb{K}$ definida por $f_b(x) = x^{-1}$ é uniformemente contínua.*

Demonstração. Seja $D_b = \{x \in \mathbb{K}; |x| \geq b\}$. Para $\varepsilon > 0$, tome $\delta = \min\left(\frac{b}{2}, \frac{\varepsilon b^2}{1+\varepsilon b}\right)$. Sendo $\delta \leq \frac{\varepsilon b^2}{1+\varepsilon b}$,

$$\begin{aligned}
&\delta + \delta\varepsilon b = \delta(1 + \varepsilon b) \leq \varepsilon b^2 \implies \\
&\delta \leq \varepsilon b^2 - \delta\varepsilon b = \varepsilon b(b - \delta) \implies \\
&\frac{\delta}{b - \delta} \leq \varepsilon b
\end{aligned}$$

Então, se $|x - y| < \delta$, provaremos uma série de afirmações.

$$y \in D_b \implies |y| \geq b \implies |y| - \delta \geq b - \delta \implies \frac{1}{|y| - \delta} \leq \frac{1}{b - \delta} \implies \frac{\delta}{|y| - \delta} \leq \frac{\delta}{b - \delta} \leq \varepsilon b$$

Mas de $b \leq |y|$ segue $\varepsilon b \leq \varepsilon|y|$ e portanto $\frac{\delta}{|y|-\delta} \leq \varepsilon b \leq \varepsilon|y|$. Logo,

$$|y| = |y - x + x| \leq |y - x| + |x| < \delta + |x| \implies |x| > |y| - \delta$$

e como $b > 0$, temos que $|y| \geq b > \frac{b}{2} \geq \delta \implies |y| - \delta > 0$ e $\left|\frac{1}{x}\right| < \frac{1}{|y|-\delta}$. Finalmente,

$$\left|\frac{1}{x} - \frac{1}{y}\right| = \left|\frac{y}{x} - 1\right| \left|\frac{1}{y}\right| = \left|\frac{y-x}{x}\right| \left|\frac{1}{y}\right| < \frac{\delta}{|y| - \delta} \cdot \frac{1}{|y|} \leq \varepsilon|y| \frac{1}{|y|} = \varepsilon.$$

Concluímos que f_b é uniformemente contínua.

■

Corolário 41. *A função $f : \mathbb{K}^* \to \mathbb{K}^*$ definida por $f(x) = x^{-1}$ é localmente uniformemente contínua, isto é, dado $x \in \mathbb{K}^*$, existe um aberto U de $\mathbb{K}^*$ (com a topologia induzida) tal que $x \in U$ e $f|_U$ é uniformemente contínua.*

Demonstração. Seja $b = \frac{|x|}{2}$ e $U = B_{\frac{|x|}{2}}(x)$. Note que de $0 \notin U$, $U = \mathbb{R}^* \cap U$ e portanto U é aberto de $\mathbb{R}^*$, $x \in U$ e dado $y \in U$, temos $|x| - |y| \leq |x - y| < \frac{|x|}{2}$ e portanto $|y| > |x| - \frac{|x|}{2} = \frac{|x|}{2}$, isto é, $y \in D_b$. Então, $U \subseteq D_b$ e como f_b é uniformemente contínua em D_b, $f|_U$ também o é.

■

Os seguintes resultados serão úteis mais à frente:

Teorema 42. *Seja $\mathbb{K}$ um corpo e $|\cdot|$ um valor absoluto sobre $\mathbb{K}$. Dada uma sequência $(x_n)_{n\in\mathbb{N}}$ de elementos de $\mathbb{K}$, $\lim_{n\to\infty} x_n = 0 \Leftrightarrow \lim_{n\to\infty} |x_n| = 0$.*

Demonstração. As equivalências abaixo são consequência imediata das definições de limite de sequências em seus respectivos espaços métricos:

$$\lim_{n\to\infty} x_n = 0 \Leftrightarrow \forall\varepsilon > 0, \exists N \in \mathbb{N}; \forall n \in \mathbb{N}, n \geq N,\ |x_n - 0| < \varepsilon \Leftrightarrow \lim_{n\to\infty} |x_n| = 0.$$

■

Teorema 43. *Sejam X, Y espaços métricos e $f : X \to Y$ uma função localmente uniformemente contínua. Então f é contínua.*

Demonstração. De fato, considere $x \in X$. Então existe um aberto U de X tal que $x \in U$ e $f|_U$ é uniformemente contínua. Dado $\varepsilon > 0$, existe $\delta' > 0$ tal que $\forall y, z \in U$, $d(y,z) < \delta' \implies d(f(y), f(z)) < \varepsilon$ e além disso, como $x \in U$ e U é aberto, existe $r \in \mathbb{R}_+^*$ tal que $B_r(x) \subseteq U$. Tome $\delta = \min(\delta', r) > 0$ e note que se $y \in X$ é tal que $d(x,y) < \delta$, então $x, y \in B_r(x) \subseteq U$ e $d(x,y) < \delta'$, logo $d(f(x), f(y)) < \varepsilon$, provando a continuidade de f em x. Como x foi arbitrário, f é contínua.

∎

Teorema 44. *Seja $|\cdot|$ um valor absoluto sobre $\mathbb{K}$ e τ a topologia induzida. Então $(\mathbb{K}, +, \cdot, \tau)$ é um corpo topológico, isto é, as operações de subtração e multiplicação de $\mathbb{K}$ são contínuas, bem como a função inverso (usando a topologia produto em $\mathbb{K}^2$). Além disso, a função $|\cdot|$ é contínua.*

Demonstração. Como τ é metrizável, trabalharemos com a continuidade no espaço métrico que à induz. Agora sejam $x_0, y_0 \in \mathbb{K}$ quaisquer. Dado $\varepsilon > 0$, tome $\delta = \frac{\varepsilon}{2}$. Então, se $x, y \in \mathbb{K}$ são tais que $|x - x_0| < \delta$ e $|y - y_0| < \delta$, então

$$|(x-y)-(x_0-y_0)| = |(x-x_0)+(y_0-y)| \leq |x-x_0|+|y_0-y| < \delta+\delta = \varepsilon,$$

o que mostra que a subtração é contínua. Para a multiplicação, podemos tomar $\delta = \min\left(\sqrt{\frac{\varepsilon}{3}}, \frac{\varepsilon}{3|x_0|}, \frac{\varepsilon}{3|y_0|}\right)$. Nesse caso, se $x, y \in \mathbb{K}$ são tais que $|x - x_0| < \delta$ e $|y - y_0| < \delta$, então

$$\begin{aligned}
|xy - x_0y_0| &= |xy - xy_0 + xy_0 - x_0y_0| \leq |xy - xy_0| + |xy_0 - x_0y_0| = \\
&= |x||y - y_0| + |x - x_0||y_0| = |x - x_0 + x_0||y - y_0| + |x - x_0||y_0| \leq \\
&\leq |x - x_0||y - y_0| + |x_0||y - y_0| + |x - x_0||y_0| < \\
&< \delta\delta + |x_0|\delta + \delta|y_0| \leq \sqrt{\frac{\varepsilon}{3}} \cdot \sqrt{\frac{\varepsilon}{3}} + |x_0|\frac{\varepsilon}{3|x_0|} + \frac{\varepsilon}{3|y_0|}|y_0| = \varepsilon,
\end{aligned}$$

mostrando a continuidade da multiplicação. O inverso ser contínuo é consequência do Corolário 41 e do Teorema 43. Concluímos que $(\mathbb{K}, +, \cdot, \tau)$ é corpo topológico. Finalmente, para mostrar que o valor absoluto é contínuo, considere $a \in \mathbb{K}$, $\varepsilon > 0$ e tome $\delta = \varepsilon$. Para $x \in \mathbb{K}$ tal que $|x - a| < \delta$, temos, do teorema 38, $||x| - |a|| \leq |x - a| < \delta = \varepsilon$, provando a continuidade do valor absoluto.

∎

Exemplo 45. *Tomando $\mathbb{K}$ subcorpo de $\mathbb{C}$ e $|\cdot|$ o valor absoluto usual, temos que a métrica d induzida é a métrica usual de $\mathbb{K}$.*

Exemplo 46. *Tomando $\mathbb{K}$ qualquer e $|\cdot|$ o valor absoluto trivial, a métrica d induzida é a métrica discreta. De fato, se $x \neq y$, então*

$d(x,y) = |x-y| = 1$. *Como é conhecido, essa métrica induz a topologia discreta, na qual todos os subconjuntos são abertos e em particular, os compactos são precisamente os conjuntos finitos. Temos que nesse caso* $\overline{B_2(0)} = \mathbb{K}$ *e portanto, se assumirmos que* $\mathbb{K}$ *é infinito, temos que nem sempre o fecho de uma bola é um compacto. Da mesma forma, a bola fechada* $B_2[0] := \{y \in \mathbb{K}; d(y,0) \leq 2\} = \mathbb{K}$*, e portanto nem toda bola fechada é um compacto. Observe que nem sempre essas duas noções se coincidem:* $\overline{B_1(0)} = \{0\}$ *e* $B_1[0] = \mathbb{K}$.

Como de costume, é interessante definir critérios para sabermos se dois objetos são essencialmente os mesmos. Utilizaremos dois critérios aqui: um deles, equivalência, irá nos dizer quando dois valores absolutos sobre o mesmo corpo induzem a mesma topologia, já isomorfismo nos dirá quando dois corpos com valor absoluto tem a mesma estrutura algébrica. O primeiro será dado pela definição abaixo, enquanto o segundo será dado na próxima seção.

Teorema 47. *Dados valores absolutos* $|\cdot|_1$ *e* $|\cdot|_2$ *não-triviais sobre* $\mathbb{K}$*, são equivalentes:*

1) Existe $s \in \mathbb{R}_+^*$ *tal que para todo* $x \in \mathbb{K}$, $|x|_1 = |x|_2^s$.
2) $|\cdot|_1$ *e* $|\cdot|_2$ *induzem a mesma topologia.*
3) Para todo $x \in \mathbb{K}$*, tem-se* $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$.

Demonstração. ($1 \implies 2$) Seja $x \in \mathbb{K}$ e $r \in \mathbb{R}$, $r > 0$. Mostraremos que a bola $B^1 = B_r^1(x)$ relativa à $|\cdot|_1$ contém alguma bola $B^2 = B_{r'}^2(x)$ relativa à $|\cdot|_2$. De fato, seja $r' = r^{\frac{1}{s}}$. Então, dado $y \in B^2$, temos $|x-y|_1 = |x-y|_2^s < r'^s = (r^{\frac{1}{s}})^s = r$, logo $|x-y|_1 < r$ e $y \in B^1$. Para mostrar que toda bola $B^2 = B_r^2(x)$ relativa à $|\cdot|_2$ contém alguma bola relativa à $|\cdot|_1$, note que $|\cdot|_2 = |\cdot|_1^{\frac{1}{s}}$ com $\frac{1}{s} > 0$ e aplique o que acaba de ser provado. Isso mostra que as métricas induzidas são equivalentes, logo as topologias são as mesmas.

($2 \implies 3$) Suponha que $|x|_1 < 1$ e considere a sequência $\left(|x|_1^i\right)_{i\in\mathbb{N}} = \left(|x^i|_1\right)_{i\in\mathbb{N}}$. Então como $|x|_1 < 1$, essa sequência converge para 0 e do resultado anterior, $\lim\limits_{i\to\infty} x^i = 0$ na métrica de $|\cdot|_1$. Então, como as topologias geradas são iguais, temos que $\lim\limits_{i\to\infty} x^i = 0$ na métrica de $|\cdot|_2$ e $\lim\limits_{i\to\infty} |x|_2^i = \lim\limits_{i\to\infty} |x^i|_2 = 0$, o que nos garante que $|x|_2 < 1$. Supondo que $|x|_2 < 1$, usamos a simetria da hipótese: observe que $|\cdot|_2$ e $|\cdot|_1$ induzem a mesma topologia, por hipótese, e aplicando o que acabamos de provar, $|x|_1 < 1$.

($3 \implies 1$) Como $|\cdot|$ é não trivial, existe $y \in \mathbb{K}$ tal que $|y|_1 > 1$.

Defina $s = \frac{\ln|y|_1}{\ln|y|_2}$. Então, considere $m, n \in \mathbb{Z}$ e $i \in \{1,2\}$ quaisquer. Temos

$$\frac{m}{n} < \frac{\ln|x|_i}{\ln|y|_i} \Leftrightarrow m\ln|y|_i < n\ln|x|_i \Leftrightarrow \ln|y|_i^m < \ln|x|_i^n \Leftrightarrow$$
$$\Leftrightarrow |y|_i^m < |x|_i^n \Leftrightarrow \frac{|y|_i^m}{|x|_i^n} < 1 \Leftrightarrow |\frac{y^m}{x^n}|_i < 1.$$

Isto é,

$$\frac{m}{n} < \frac{\ln|x|_1}{\ln|y|_1} \Leftrightarrow |\frac{y^m}{x^n}|_1 < 1 \Leftrightarrow |\frac{y^m}{x^n}|_2 < 1 \Leftrightarrow \frac{m}{n} < \frac{\ln|x|_2}{\ln|y|_2}$$

Como $\frac{m}{n}$ representa um número racional qualquer, temos que $\frac{\ln|x|_1}{\ln|y|_1} = \frac{\ln|x|_2}{\ln|y|_2}$, logo, $\ln|x|_1 = \frac{\ln|y|_1}{\ln|y|_2}\ln|x|_2 = s\ln|x|_2 = \ln|x|_2^s$ o que resulta em $|x|_1 = |x|_2^s$.

■

Definição 48. *Dois valores absolutos em $\mathbb{K}$ são ditos* equivalentes *se valem as condições do teorema 47.*

4 COMPLETAMENTO

Um teorema importante sobre espaços métricos diz que todo espaço métrico admite completamento, que é único a menos de isometrias. Em particular, os espaços métricos induzidos por valores absolutos também o admitem e é relevante perguntar se tal completamento pode ser munido de operações que o tornem um corpo, e neste caso, se quaisquer corpos com essa propriedade são isomorfos. Esse resultado é verdadeiro, e o objetivo dessa sessão é enunciá-lo e prová-lo, mas não assumiremos o resultado sobre espaços métricos para isso. Em vez disso, iremos definir um completamento e, dado um corpo com valor absoluto, iremos usar a própria estrutura do corpo para completá-lo. A abordagem utilizada será a mesma: iremos considerar o conjunto de todas as sequências de Cauchy, e então tomar o quociente pelo conjunto das sequências que convergem para 0, mas no nosso caso, esse quociente será visto como um quociente de anéis, istó é, provaremos que o conjunto das sequências de Cauchy com as operações de adição e multiplicação pontuais formam um anel (que não é um corpo) e que o conjunto das sequências que convergem para 0 é um ideal maximal. Além disso, definiremos o que é uma imersão e um isomorfismo, e mostraremos que quaisquer completamentos são isomorfos. A seção termina com o Teorema de Ostrowski, que motiva o estudo de valores absolutos não-arquimedianos.

Definição 49. *Sejam $\mathbb{K}$, $\mathbb{L}$ corpos com respectivos valores absolutos $|\cdot|_{\mathbb{K}}$ e $|\cdot|_{\mathbb{L}}$. Um homomorfismo $\lambda : \mathbb{K} \to \mathbb{L}$ é dito uma* imersão *de $(\mathbb{K}, |\cdot|_{\mathbb{K}})$ em $(\mathbb{L}, |\cdot|_{\mathbb{L}})$ se para qualquer $x \in \mathbb{K}$ tem-se $|x|_K = |\lambda(x)|_{\mathbb{L}}$. Se λ é bijetora, então λ é dito um isomorfismo entre os corpos com valor absoluto.*

Observação 50. *Nas notações acima, λ é injetora pois dado $x \in Ker(\lambda)$, temos $0 = |0|_{\mathbb{L}} = |\lambda(x)|_{\mathbb{L}} = |x|_{\mathbb{K}}$, logo $x = 0$. Também podemos justificar isso dizendo que todo homomorfismo não nulo entre corpos é injetor. Aqui, convencionaremos que homomorfismos entre corpos são sempre tais que a unidade é preservada, então todo homomorfismo entre corpos é, de fato, injetor.*

Teorema 51. *Sejam $\mathbb{K}$, $\mathbb{L}$ corpos com respectivos valores absolutos $|\cdot|_{\mathbb{K}}$ e $|\cdot|_{\mathbb{L}}$ e $\lambda : \mathbb{K} \to \mathbb{L}$ uma imersão. Então λ é contínua.*

Demonstração. Considere $a \in \mathbb{K}$. Dado $\varepsilon > 0$, tome $\delta = \varepsilon$. Se $x \in \mathbb{K}$ é tal que $|x-a|_{\mathbb{K}} < \delta$, então $|\lambda(x)-\lambda(a)|_{\mathbb{L}} = |\lambda(x-a)|_{\mathbb{L}} = |x-a|_{\mathbb{K}} < \delta = \varepsilon$. Concluímos que λ é contínua. ∎

Definição 52. *Considere um corpo $\mathbb{K}$ com um valor absoluto $|\cdot|$. Um corpo $\mathbb{K}'$ com um valor absoluto $|\cdot|'$ é dito um* completamento *de $\mathbb{K}$ se $\mathbb{K}'$ é completo e existe uma imersão ι de $\mathbb{K}$ em $\mathbb{K}'$ tal que $\iota(\mathbb{K})$ seja denso em $\mathbb{K}'$.*

A seguir, precisaremos do seguinte teorema de espaços métricos:

Teorema 53. *Sejam X, Y espaços métricos, $f : X \to Y$ uma função uniformemente contínua e $(x_i)_{i\in\mathbb{N}}$ uma sequência de Cauchy de X. Então, $(f(x_i))_{i\in\mathbb{N}}$ é uma sequência de Cauchy de Y.*

Demonstração. Tome $\varepsilon > 0$. Então existe um $\delta > 0$ tal que para quaisquer $x, y \in X$ com $d(x, y) < \delta$ temos $d(f(x), f(y)) < \varepsilon$. Além disso, existe um $i_0 \in \mathbb{N}$ tal que para $i, j \geq i_0$, temos $d(x_i, x_j) < \delta$. Dessas duas afirmações, $i, j \geq i_0 \implies d(x_i, x_j) < \delta \implies d(f(x_i), f(x_j)) < \varepsilon$ e $(f(x_i))_{i\in\mathbb{N}}$ é de Cauchy.

■

Lema 54. *Seja $(\mathbb{K}, |\cdot|)$ um corpo com valor absoluto, C o conjunto das sequências de Cauchy de $\mathbb{K}$ e O o conjunto das sequências de $\mathbb{K}$ que convergem para 0. Então dado $(x_n)_{n\in\mathbb{N}} \in C \setminus O$, existe $n_0 \in \mathbb{N}$ tal que se $n \geq n_0$, então $x_n \neq 0$. Além disso, se $\forall n \in \mathbb{N}, x_n \neq 0$, então $\left(\frac{1}{x_n}\right)_{n\in\mathbb{N}} \in C$.*

Demonstração. Para a primeira afirmação, usaremos a contrapositiva da seguinte forma: seja $(x_n)_{n\in\mathbb{N}} \in C$. Se para todo $n_0 \in \mathbb{N}$ existe $n \geq n_0$ tal que $x_n = 0$, então $(x_n)_{n\in\mathbb{N}} \in O$. De fato, tome $\varepsilon > 0$. Então existe $n_0 \in \mathbb{N}$ tal que para todo $n, m \geq n_0$, $|x_n - x_m| < \varepsilon$. Pela hipótese da contrapositiva, existe $k \geq n_0$ tal que $x_k = 0$ e logo, para todo $n \geq n_0$, temos $n, k \geq n_0$, o que implica $|x_n| = |x_n - 0| = |x_n - x_k| < \varepsilon$ e $(x_n)_{n\in\mathbb{N}} \in O$.

Para a segunda afirmação, note que da hipótese de não convergir para 0 existe $\varepsilon' > 0$ tal que para $n_0 = 0 \in \mathbb{N}$ existe $n \geq 0$ tal que $|x_n| = |x_n - 0| \geq \varepsilon'$. Tome $\varepsilon = \min(|x_0|, ..., |x_{n-1}, \varepsilon')$ e note que $(x_n)_{n\in\mathbb{N}}$ é sequência de $D_\varepsilon = \{x \in \mathbb{K}; |x| \geq \varepsilon\}$. Do que foi provado anteriormente, a função
$f_\varepsilon : D_\varepsilon \to \mathbb{K}^*$ definida por $f_\varepsilon(x) = \frac{1}{x}$ é uniformemente contínua. Disso e do teorema acima, obtemos que $\left(\frac{1}{x_n}\right)_{n\in\mathbb{N}}$ é de Cauchy. ■

Lema 55. *Seja $(\mathbb{K}, |\cdot|)$ um corpo com valor absoluto. Então:*

1) O conjunto C das sequências de Cauchy de $\mathbb{K}$ formam um anel com a soma e produto entrada a entrada.

2) O conjunto O das sequências de $\mathbb{K}$ que convergem para 0 formam um ideal maximal de C.

3) A função $F : C \to \mathbb{R}$ definida por $F(\{x_i\}_{i\in\mathbb{N}}) = \lim\limits_{i\to\infty} |x_i|$ está bem definida e é tal que $F(x) = F(y) \Leftrightarrow x - y \in O$, e portanto induz uma função $f : C/O \to \mathbb{R}$.

Demonstração. A primeira propriedade é verificada mostrando que C é subanel do anel das sequências de $\mathbb{K}$. De fato, C é não-vazio, pois $(0)_{i\in\mathbb{N}} \in C$. Além disso, sejam $(x_i)_{i\in\mathbb{N}}, (y_i)_{i\in\mathbb{N}} \in C$. Temos que dado $\varepsilon > 0$, existem $n_1, n_2 \in \mathbb{N}$ tais que se $n, m > n_1$, então $|x_n - x_m| < \frac{\varepsilon}{2}$ e se $n, m > n_2$, então $|y_n - y_m| < \frac{\varepsilon}{2}$. Além disso, $(|x_i|)_{i\in\mathbb{N}}$ e $(|y_i|)_{i\in\mathbb{N}}$ são de Cauchy, logo são limitadas por, digamos, M_x e M_y. Agora seja $n_0 = \max(n_1, n_2)$. Temos que se $n, m > n_0$, então

$$|x_n - y_n - (x_m - y_m)| \leq |x_n - x_m| + |y_n - y_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

$$\begin{aligned}|x_n y_n - x_m y_m| &= |x_n y_n - x_n y_m + x_n y_m - x_m y_m| \leq \\ &\leq |x_n y_n - x_n y_m| + |x_n y_m - x_m y_m| = |x_n||y_n - y_m| + |x_n - x_m||y_m| < \\ &< |x_n|\frac{\varepsilon}{2} + \frac{\varepsilon}{2}|y_m| \leq \frac{\varepsilon}{2}(M_x + M_y).\end{aligned}$$

Podemos tomar ε' arbitrário, e aplicar o resultado acima para $\varepsilon = \frac{2\varepsilon'}{M_x + M_y}$ para obter $|x_n y_n - x_m y_m| < \varepsilon'$. Disso, concluímos que $(x_i - y_i)_{i\in\mathbb{N}}, (x_i y_i)_{i\in\mathbb{N}} \in C$.

Agora tome $(x_i)_{i\in\mathbb{N}}, (y_i)_{i\in\mathbb{N}} \in O$. Temos que $\lim\limits_{i\to\infty} x_i = \lim\limits_{i\to\infty} y_i = 0$, logo, da continuidade de soma e do oposto, $\lim\limits_{n\to\infty} x_i - y_i = 0 - 0 = 0$. Além disso, seja $(k_i)_{i\in\mathbb{N}} \in C$. Como $(k_i)_{i\in\mathbb{N}}$ é de Cauchy, temos $(|k_i|)_{i\in\mathbb{N}}$ limitada por algum M. Além disso, dado $\varepsilon > 0$, existe n_0 tal que se $n > n_0$, então $|x_n| < \frac{\varepsilon}{M}$. Para $n > n_0$, temos $|k_n x_n| = |k_n||x_n| < M\frac{\varepsilon}{M} = \varepsilon$. Obtemos disso e do resultado anterior que $(x_i - y_i)_{i\in\mathbb{N}}, (k_i x_i)_{i\in\mathbb{N}} \in O$, logo O é um ideal. Para mostrar que ele é maximal, considere uma sequência $(x_i)_{i\in\mathbb{N}} \in C \setminus O$. Defina $x'_i \in \mathbb{K}$ por $x'_i = x_i$, se $x_i \neq 0$, e $x'_i = 1$ caso contrário. Do lema 54, existe $i_0 \in \mathbb{N}$ tal que se $i \geq i_0$, então $x_i \neq 0$, isto é, se $i \geq i_0$, então $x'_i = x_i$. Como conhecido de espaços métricos, isso implica que $(x'_i)_{i\in\mathbb{N}}$ é de Cauchy, uma vez que $(x_i)_{i\in\mathbb{N}}$ o é. Além disso, como nenhum termo de $(x'_i)_{i\in\mathbb{N}}$ é nulo e $(x'_i)_{i\in\mathbb{N}} \notin O$, temos, do lema, $(x'_i)_{i\in\mathbb{N}}$ inversível. Agora considere I ideal de C tal que $O \subsetneq I \subseteq C$. Então existe $(x_i)_{i\in\mathbb{N}} \in I \setminus O \subseteq C \setminus O$. Construindo $(x'_i)_{i\in\mathbb{N}}$ como antes, temos que para algum $i_0 \in \mathbb{N}$, se $i \geq i_0$, então $x'_i = x_i$, isto é, $x'_i - x_i = 0$. Então, como $(x'_i - x_i)_{i\in\mathbb{N}}$ se anula a partir de i_0, temos que $(x'_i - x_i)_{i\in\mathbb{N}} \in O \subseteq I$. Como I é ideal, temos

$(x_i')_{i\in\mathbb{N}} = (x_i' - x_i)_{i\in\mathbb{N}} + (x_i)_{i\in\mathbb{N}} \in I$, mas $(x_i')_{i\in\mathbb{N}}$ é inversível, logo, da teoria de anéis, $I = O$.

F está bem definida pois $(x_i)_{i\in\mathbb{N}} \in C \implies (|x_i|)_{i\in\mathbb{N}}$ de Cauchy (pois $|\cdot|$ é uniformemente contínua, como provamos na seção anterior), logo $|x_i|$ é convergente. Se $x - y \in O$, temos que $x - y$ converge para 0, e logo x e y convergem para o mesmo valor, assim como $|x|$ e $|y|$. Então, $F(x) = F(y)$. A recíproca é provada analogamente. Isso resulta na função f procurada.

■

Teorema 56. *Todo corpo com valor absoluto admite completamento.*

Demonstração. Seja $(\mathbb{K}, |\cdot|)$ um corpo com valor absoluto. Afirmamos que $(C/O, f)$ como definido no lema 55 é um completamento de $\mathbb{K}$. De fato, considere $(x_i)_{i\in\mathbb{N}}, (y_i)_{i\in\mathbb{N}} \in C$. Então:

$$\begin{aligned}
f\left(\overline{(x_i)_{i\in\mathbb{N}}}\right) &= 0 \Leftrightarrow F((x_i)_{i\in\mathbb{N}}) = 0 = F((0)_{i\in\mathbb{N}}) \Leftrightarrow (x_i)_{i\in\mathbb{N}} \in O \Leftrightarrow \\
&\Leftrightarrow \overline{(x_i)_{i\in\mathbb{N}}} = \overline{(0)_{i\in\mathbb{N}}} \\
f\left(\overline{(x_i)_{i\in\mathbb{N}} + (y_i)_{i\in\mathbb{N}}}\right) &= F((x_i)_{i\in\mathbb{N}} + (y_i)_{i\in\mathbb{N}}) = F((x_i + y_i)_{i\in\mathbb{N}}) = \\
&= \lim_{i\to\infty} |x_i + y_i| \leq \lim_{i\to\infty} |x_i| + \lim_{i\to\infty} |y_i| = \\
&= F((x_i)_{i\in\mathbb{N}}) + F((y_i)_{i\in\mathbb{N}}) = f\left(\overline{(x_i)_{i\in\mathbb{N}}}\right) + f\left(\overline{(y_i)_{i\in\mathbb{N}}}\right) \\
f\left(\overline{(x_i y_i)_{i\in\mathbb{N}}}\right) &= F((x_i y_i)_{i\in\mathbb{N}}) = \lim_{i\to\infty} |x_i y_i| = \lim_{i\to\infty} |x_i| \lim_{i\to\infty} |y_i| = \\
&= F((x_i)_{i\in\mathbb{N}}) F((y_i)_{i\in\mathbb{N}}) = f\left(\overline{(x_i)_{i\in\mathbb{N}}}\right) f\left(\overline{(y_i)_{i\in\mathbb{N}}}\right).
\end{aligned}$$

Concluímos que f é, de fato, um valor absoluto sobre C/O. Além disso, podemos definir a função $\iota : \mathbb{K} \to C/O$ por $\iota(x) = \overline{(x)_{i\in\mathbb{N}}}$. Sabemos que ι é homomorfismo, e provaremos agora a propriedade da imersão:

Seja $x \in \mathbb{K}$. Temos que $f(\iota(x)) = f\left(\overline{(x)_{i\in\mathbb{N}}}\right) = \lim\limits_{i\to\infty} |x| = |x|$.

Agora, mostraremos que a imagem de ι é densa em C/O. De fato, mostraremos que dada uma sequência $(\iota(x_i))_{i\in\mathbb{N}}$ com elementos na imagem de ι, temos $\lim\limits_{i\to\infty} \iota(x_i) = \overline{(x_i)_{i\in\mathbb{N}}}$. Dado $\varepsilon > 0$, como $(x_i)_{i\in\mathbb{N}}$ é de Cauchy, existe $n_0 \in \mathbb{N}$ tal que se $n, m \geq n_0$, então $|x_n - x_m| < \varepsilon$. Para $n \geq n_0$, temos que se $m \geq n_0$, então $|x_n - x_m| < \varepsilon$ e portanto

$\lim\limits_{i\to\infty} |x_n - x_i| < \varepsilon$. Então,

$$f\left(\iota(x_n) - \overline{(x_i)_{i\in\mathbb{N}}}\right) = f\left(\overline{(x_n - x_i)_{i\in\mathbb{N}}}\right) = \lim_{i\to\infty} |x_n - x_i| < \varepsilon.$$

Agora que sabemos disso, concluímos que dada um elemento $x = \overline{(x_i)_{i\in\mathbb{N}}} \in C/O$, a sequência $(\iota(x_i))_{i\in\mathbb{N}}$ converge para x, logo a imagem de ι é densa em C/O.

Finalmente, iremos provar que C/O é completo. Considere uma sequência de Cauchy $(X_i)_{i\in\mathbb{N}}$ de elementos de C/O. Como $\mathrm{Im}(\iota)$ é densa em C/O, dado $i \in \mathbb{N}$, existe uma sequência de $\mathrm{Im}(\iota)$ que converge para X_i. Em particular, existe um elemento $y_i \in \mathbb{K}$ tal que $f(X_i - \iota(y_i)) < \frac{1}{i+1}$. Então, $\lim\limits_{i\to\infty} f(X_i - \iota(y_i)) = 0$ e portanto $\lim\limits_{i\to\infty} X_i - \iota(y_i) = 0$. Somando $\lim\limits_{i\to\infty} \iota(y_i)$ aos dois lados, que sabemos que existe do que acabamos de ver, obtemos $\lim\limits_{i\to\infty} X_i = \lim\limits_{i\to\infty} \iota(y_i) = \overline{(y_i)_{i\in\mathbb{N}}}$. Isso prova a densidade de C/O, terminando assim a demonstração. ∎

Teorema 57. *(Propriedade universal do completamento) Seja $\mathbb{K}'$ um completamento de $\mathbb{K}$ com $\iota : \mathbb{K} \to \mathbb{K}'$ como na definição. Então dada uma imersão λ de $\mathbb{K}$ em um corpo $\mathbb{L}$ com valor absoluto $|\cdot|_{\mathbb{L}}$ completo, existe uma única imersão $\lambda' : \mathbb{K}' \to \mathbb{L}$ tal que $\lambda = \lambda' \circ \iota$.*

Demonstração. Seja $x \in \mathbb{K}'$ e seja $(\iota(x_i))_{i\in\mathbb{N}}$ sequência de $\iota(\mathbb{K})$ que converge para x. Afirmamos que $(\lambda(x_i))_{i\in\mathbb{N}}$ converge para algum $X \in \mathbb{L}$. De fato, tome $\varepsilon > 0$. Temos que $(\iota(x_i))_{i\in\mathbb{N}}$ converge, logo é de Cauchy, e para algum $i_0 \in \mathbb{N}$, se $i, j > i_0$, temos $|\iota(x_i) - \iota(x_j)| < \varepsilon$. Então, para $i, j > i_0$,

$$|\lambda(x_i) - \lambda(x_j)| = |\lambda(x_i - x_j)| = |x_i - x_j| = |\iota(x_i - x_j)| = |\iota(x_i) - \iota(x_j)| < \varepsilon$$

Logo $(\lambda(x_i))_{i\in\mathbb{N}}$ é de Cauchy. Mas $\mathbb{L}$ é completo, logo $(\lambda(x_i))_{i\in\mathbb{N}}$ converge para algum $X \in \mathbb{L}$. Além disso, seja $(\iota(x_i'))_{i\in\mathbb{N}}$ outra sequência de $\iota(\mathbb{K})$ que converge para x. Como acima, $\big(\lambda((x_i')_{i\in\mathbb{N}})\big)_{i\in\mathbb{N}}$ converge para algum $X' \in \mathbb{L}$. Temos que dado $\varepsilon > 0$, existe algum i_0 tal que para $i > i_0$, $|\iota(x_i) - x| < \frac{\varepsilon}{2}$ e $|\iota(x_i') - x| < \frac{\varepsilon}{2}$. Para $i > i_0$:

$$\begin{aligned} &|\lambda(x_i) - \lambda(x_i')| = |\lambda(x_i - x_i')| = |x_i - x_i'| = |\iota(x_i) - \iota(x_i')| = \\ &= |(\iota(x_i) - x) - (\iota(x_i') - x)| \leq |\iota(x_i) - x| + |\iota(x_i') - x| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \end{aligned}$$

Concluímos $X - X' = \lim_{i\to\infty} x_i - \lim_{i\to\infty} x'_i = \lim_{i\to\infty} x_i - x'_i = 0$, logo, está bem definida a função $\lambda' : \mathbb{K}' \to \mathbb{L}$ definida por $\lambda'(\lim_{i\to\infty} \iota(x_i)) = \lim_{i\to\infty} \lambda(x_i)$. Além disso, podemos fazer verificações simples para mostrar que λ' é imersão (lembrando que as operações de corpo e a função módulo são contínuas):

$$\begin{aligned}
\lambda'(x+y) &= \lim_{i\to\infty} \lambda(x_i + y_i) = \lim_{i\to\infty} \lambda(x_i) + \lim_{i\to\infty} \lambda(y_i) = \lambda'(x) + \lambda'(y),\\
\lambda'(xy) &= \lim_{i\to\infty} \lambda(x_i y_i) = \lim_{i\to\infty} \lambda(x_i) \lim_{i\to\infty} \lambda(y_i) = \lambda'(x)\lambda'(y),\\
|\lambda'(x)| &= |\lim_{i\to\infty} \lambda(x_i)| = \lim_{i\to\infty} |\lambda(x_i)| = \lim_{i\to\infty} |x_i| = |x|.
\end{aligned}$$

Note que para $x \in \mathbb{K}$, $\lim_{i\to\infty} x = x$ e logo

$$\lambda'(\iota(x)) = \lambda'(\lim_{i\to\infty} \iota(x)) = \lim_{i\to\infty} \lambda(x) = \lambda(x).$$

Finalmente, suponha que $\lambda'' : \mathbb{K}' \to \mathbb{L}$ seja outra imersão com tal propriedade. Então, dado $x \in \mathbb{K}'$, temos que para $x \in \mathbb{K}$,

$$\lambda'(\iota(x)) = \lambda(x) = \lambda''(\iota(x))$$

e então, lembrando que imersões são contínuas, se $x = \lim_{i\to\infty} \iota(x_i) \in \mathbb{K}'$, $x_i \in \mathbb{K}$,

$$\lambda'(x) = \lambda'(\lim_{i\to\infty}(\iota(x_i))) = \lim_{i\to\infty}(\lambda'(\iota(x_i))) = \lim_{i\to\infty}(\lambda''(\iota(x_i))) = \lambda''(\lim_{i\to\infty}(\iota(x_i))) = \lambda''(x).$$

■

Corolário 58. *Seja $\mathbb{K}$ um corpo com valor absoluto $|\cdot|_{\mathbb{K}}$. Se $(\mathbb{L}, |\cdot|_{\mathbb{L}}), (\mathbb{L}', |\cdot|'_{\mathbb{L}})$ são completamentos de $\mathbb{K}$, então $\mathbb{L}$ e $\mathbb{L}'$ são isomorfos.*

Demonstração. Sejam $\iota : \mathbb{K} \to \mathbb{L}$ e $\iota' : \mathbb{K} \to \mathbb{L}'$ as imersões da definição de completamento. Da propriedade universal, existem únicos $\lambda : \mathbb{L}' \to \mathbb{L}$ e $\lambda' : \mathbb{L} \to \mathbb{L}'$ tais que $\iota = \lambda \circ \iota'$ e $\iota' = \lambda' \circ \iota$. Mas então, $\mathrm{Id}_{\mathbb{L}} \circ \iota = \iota = \lambda \circ \lambda' \circ \iota$, isto é, $\mathrm{Id}_{\mathbb{L}}$ e $\lambda \circ \lambda'$ são imersões de $\mathbb{L}$ em $\mathbb{L}$ satisfazendo a propriedade universal de ι. Da unicidade, obtemos $\lambda \circ \lambda' = \mathrm{Id}_{\mathbb{L}}$. De mesma forma, podemos obter $\lambda' \circ \lambda = \mathrm{Id}_{\mathbb{L}'}$, o que implica $\lambda^{-1} = \lambda'$ e λ é isomorfismo. ■

Para o teorema a seguir, ver a referência [3]. Ele será usado de motivação na próxima seção.

Teorema 59. *(Ostrowski) Todo corpo com valor absoluto completo é isomorfo à* $\mathbb{R}$ *ou* $\mathbb{C}$*, com seus respectivos valores absolutos.*

5 VALORAÇÕES

Acima, antes que déssemos o exemplo de valor absoluto p-ádico, definimos uma função v_p e observamos que esse exemplo seria importante futuramente. De fato, esta seção é dedicada a definir e estudar o conceito de valoração. Veremos que valorações são equivalentes a valores absolutos não-arquimedianos, mas é vantajoso estudá-las pela forma simples que elas apresentam em alguns exemplos e também pela facilidade que temos em generalizá-las (as valorações de Krull, definidas posteriormente). Intuitivamente, podemos obter uma valoração tomando um valor absoluto não-arquimediano e aplicando uma transformação da forma $-s\ln(|x|)$ nela (formalizaremos o que isso significa mais abaixo). Dessa forma, transforma-se 0 em ∞, 1 em 0, um número real positivo arbitrário em um número real arbitrário e dualiza-se a ordem, isto é, troca-se $<$ por $>$, $\leq$ por $\geq$, min por max, etc... A definição formal é dada abaixo.

Definição 60. *Seja $\mathbb{K}$ um corpo. Uma função $v : \mathbb{K} \to \widetilde{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$ é dita uma* valoração *sobre $\mathbb{K}$ se valem, para todos $x, y \in \mathbb{K}$:*

1) $v(x) = \infty \Leftrightarrow x = 0$
2) $v(x + y) \geq \min(v(x), v(y))$
3) $v(xy) = v(x) + v(y)$

Exemplo 61. *Em um corpo $\mathbb{K}$ qualquer, defina $v : \mathbb{K} \to \widetilde{\mathbb{R}}$ por $v(0) = \infty$ e $v(x) = 0$, se $x \neq 0$. v é uma valoração em $\mathbb{K}$, denominada* valoração trivial *sobre $\mathbb{K}$.*

Exemplo 62. *Considere a função $v_p : \mathbb{Q} \to \widetilde{\mathbb{R}}$ obtida estendendo por $v_p(0) = \infty$ a função de mesmo nome no teorema 32. Em outras palavras, $v_p(0) = \infty$ e para $x \in \mathbb{Q}^*$, escreva $x = u \prod_{q \in \mathcal{P}} q^{\alpha_q}$ e defina $v_p(x) = \alpha_p$. Como já notamos, essa função está bem definida. Além disso, do que provamos após definirmos essa função, v_p é uma valoração em $\mathbb{Q}$. Faltaria mostrar as propriedades para o caso em que $x = 0$ ou $y = 0$, o que é trivial. Essa valoração é denominada* valoralção p-ádica *em $\mathbb{Q}$.*

Como foi dito no paragrafo de introdução à essa sessão, valoração e valores absolutos não-arquimedianos tem uma equivalência entre si. O teorema abaixo mostra a primeira parte do que precisamos.

Teorema 63. *Seja $\mathbb{K}$ um corpo, $|\cdot|$ um valor absoluto não-arquimediano* *e $s \in \mathbb{R}$, $s > 0$. Então $v_s : \mathbb{K} \to \widetilde{\mathbb{R}}$ definida abaixo é uma valoração em $\mathbb{K}$ e dita* associada a $|\cdot|$.

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

Além disso, se v é valoração em $\mathbb{K}$, então dado $q \in \mathbb{R}$ com $q > 1$, $|\cdot|_q : \mathbb{K} \to \mathbb{R}$ definida abaixo é valor absoluto não-arquimediano em $\mathbb{K}$ e dito associado a v.

$$|x|_q = \begin{cases} q^{-v(x)}, & se\ x \neq 0 \\ 0, & se\ x = 0 \end{cases}$$

Demonstração. De fato, é claro que $v_s(x) = \infty \Leftrightarrow x = 0$. Além disso, $|x+y| \leq \max(|x|,|y|) \Rightarrow \ln|x+y| \leq \ln\max(|x|,|y|) \Rightarrow$
$\Rightarrow v_s(x+y) = -s\ln|x+y| \geq -s\ln\max(|x|,|y|) = \min(-s\ln|x|, -s\ln|y|) = \min(v_s(x), v_s(y))$ e também,
$v_s(xy) = -s\ln xy = -s(\ln x + \ln y) = -s\ln x - s\ln y = v_s(x) + v_s(y)$.

De maneira semelhante, temos $|x|_q = 0 \Leftrightarrow x = 0$ e $|xy|_q = q^{-v(xy)} = q^{-v(x)-v(y)} = q^{-v(x)}q^{-v(y)} = |x|_q|y|_q$. Para $|x+y|_q \leq |x|_q + |y|_q$, as contas são análogas ao que foi feito para v_p.

■

A seguir, mostraremos que, em termos topológicos, a escolha do q acima é irrelevante. Também definiremos equivalência entre valorações, que terá uma forma similar ao que foi definido para valores absolutos.

Teorema 64. *Seja $\mathbb{K}$ um corpo e v uma valoração em $\mathbb{K}$. Então todos os valores absolutos associados a v são equivalentes.*

Demonstração. Sejam $p, q \in \mathbb{R}$ com $p > 0$ e $q > 0$ e fixe $x \in \mathbb{K}$. Temos dois casos: $\left(\frac{p}{q}\right)^{v(x)} \leq 1$ ou $\left(\frac{p}{q}\right)^{v(x)} > 1$. No primeiro caso:

$$|x|_q < 1 \Leftrightarrow q^{-v(x)} < 1 \Leftrightarrow p^{-v(x)}\frac{q^{-v(x)}}{p^{-v(x)}} < 1 \Leftrightarrow p^{-v(x)} < \frac{p^{v(x)}}{q^{v(x)}} \leq 1 \Leftrightarrow |x|_p < 1.$$

Disso, concluímos que os valores absolutos são equivalentes. O outro caso é consequência desse, trocando p e q.

■

Teorema 65. *Seja $\mathbb{K}$ um corpo e v_1, v_2 valorações sobre $\mathbb{K}$. Então são equivalentes:*

1) Quaisquer valores absolutos associados a v_1 e v_2 são equivalentes.

2) Existe $s \in \mathbb{R}, s > 0$ tal que para $x \in \mathbb{K}$, $v_1(x) = sv_2(x)$.

3) Dado $x \in \mathbb{K}$, $v_1(x) > 0 \Leftrightarrow v_2(x) > 0$

Demonstração. ($1 \implies 2$) Sejam $|\cdot|_1 = p^{-v_1}$ e $|\cdot|_2 = q^{-v_2}$ valores absolutos associados a v_1 e v_2, respectivamente. Então, de 1, existe $s \in \mathbb{R}$ tal que $|\cdot|_1 = |\cdot|_2^s$. Então, $v_1(x) = -\log_p |x|_1 = -\log_p |x|_2^s = -s \log_p |x|_2 = sv(x)$.

($2 \implies 3$) Seja $x \in \mathbb{K}$. Então $v_(x) > 0 \Leftrightarrow sv_2(x) > 0 \Leftrightarrow v_2(x) > 0$.

($3 \implies 1$) Sabemos que quaisquer valores absolutos associado a v_1 (resp. v_2) são equivalentes entre si. Basta provar que algum valor absoluto associado a v_1 é equivalente a algum valor absoluto associado a v_2. De fato, Sejam $|\cdot|_1 = p^{-v_1}$ e $|\cdot|_2 = p^{-v_2}$ valores absolutos associados a v_1 e v_2, respectivamente. Temos

$$|x|_1 < 1 \Leftrightarrow p^{-v_1(x)} < 1 \Leftrightarrow -v_1(x) < \log_p 1 = 0 \Leftrightarrow v_1(x) > 0 \Leftrightarrow$$
$$\Leftrightarrow v_2(x) > 0 \Leftrightarrow -v_2(x) < 0 = \log_p 1 \Leftrightarrow p^{-v_2(x)} < 1 \Leftrightarrow |x|_2 < 1.$$

Então, os valores absolutos são equivalentes.

■

Definição 66. *Duas valorações em um corpo $\mathbb{K}$ são ditas* equivalentes *se valem as condições acima.*

As seguintes propriedades são análogas ao que foi feito para valores absolutos:

Teorema 67. *Seja v uma valoração em $\mathbb{K}$. Temos que:*

1) $v(1) = 0$

2) Para toda raiz $u \in \mathbb{K}$ da unidade, $v(u) = 0$.

3) Se $x \in \mathbb{K}$, então $v(-x) = v(x)$ e se $x \neq 0$, então $v(x^{-1}) = -v(x)$.

4) Se $x, y \in \mathbb{K}$ são tais que $v(x) \neq v(y)$, então $v(x+y) = \min(v(x), v(y))$.

Demonstração. A demonstração é similar ao que foi feito para valores absolutos.

1) $v(1) = v(1 \cdot 1) = v(1) + v(1) \implies v(1) = 0$

2) Seja $n \in \mathbb{N}^*$ tal que $u^n = 1$. $0 = v(1) = v(u^n) = nv(u)$, logo, de $n > 0$, $v(u) = 0$.

3) Como $(-1)^2 = 1$, temos que -1 é raíz da unidade, o que resulta em $v(-x) = v(-1 \cdot x) = v(-1) + v(x) = 0 + v(x) = v(x)$. Além disso, se $x \neq 0$, então $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) \implies v(x^{-1}) = -v(x)$.

4) Vendo que os casos $x = 0$ e $y = 0$ são triviais, suponha $x \neq 0$ e $y \neq 0$. Seja $|\cdot|$ um valor absoluto associado a v. Do teorema 38, item 4, temos que $|x + y| = \max(|x|, |y|)$ e então

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

■

Assim como feito para valores absolutos, podemos dar uma estrutura de espaço métrico para valorações. Esta será topologicamente equivalente à do seu valor absoluto associado. Formalmente:

Teorema 68. *Seja $\mathbb{K}$ um corpo, v uma valoração sobre $\mathbb{K}$ e $|\cdot|$ um valor absoluto associado à v. Para $r \in \mathbb{R}$, defina $B_r(x) = \{y \in \mathbb{K}; v(x - y) > r\}$. Então o coleção τ de todos os subconjuntos $U \subseteq \mathbb{K}$ tais que para todo $x \in U$, existe $r \in \mathbb{R}$ tal que $B_r(x) \subseteq U$ é uma topologia metrizável em $\mathbb{K}$ e, de fato, é equivalente a topologia induzida por $|\cdot|$.*

Demonstração. $\emptyset$ e $\mathbb{K}$ são trivialmente elementos de τ. Dados $U, V \in \tau$, seja $x \in U \cap V$. Então existem $r, s \in \mathbb{R}$ tais que $B_r(x) \subseteq U$ e $B_s(x) \subseteq V$. Seja $m = \min(r, s)$. Então, $B_m(x) \subseteq B_r(x) \cap B_s(x) \subseteq U \cap V$ e $U \cap V \in \tau$. Se $\{U_i\}_{i \in I} \subseteq \tau$, tome $x \in \bigcup_{i \in I} U_i$. Então existe $i_0 \in I$ tal que $x \in U_{i_0}$. Como $U_{i_0} \in \tau$, existe $r \in \mathbb{R}$ tal que $B_r(x) \subseteq U_{i_0} \subseteq \bigcup_{i \in I} U_i$ e portanto temos que $\bigcup_{i \in I} U_i \in \tau$. Agora, como $|\cdot|$ é associada a v, existe $s > 0$ tal que para todo $x \in \mathbb{K}^*$ $v(x) = -s\ln(|x|)$. Seja τ' a topologia induzida por $|\cdot|$. Dado $U \in \tau$, considere $x \in U$ e $r \in \mathbb{R}$ tal que $B_r(x) \subseteq U$. Temos $v(y - x) > r \implies |y - x| < e^{-\frac{r}{s}}$ e portando a bola (em relação a $|\cdot|$) de centro x e raio $e^{-\frac{r}{s}}$ é subconjunto de U. Isso mostra $U \in \tau'$. Reciprocamente, considere $V \in \tau'$. Então, dado $x \in U$, existe $r > 0$ tal que a bola (em relação a $|\cdot|$) de centro x e raio r é subconjunto de U. Note que $|y - x| < r \implies -s\ln(|y - x|) > -s\ln(r)$ e portanto $B_{-s\ln(r)}(x) \subseteq V$. Isso mostra $\tau' \subseteq \tau$ e portanto τ'. Disso, segue τ

metrizável: Basta tomar a métrica induzida de $|\cdot|$.

$\blacksquare$

6 DIVISIBILIDADE E ANÉIS DE VALORAÇÃO

Definição 69. *Seja A um conjunto. Então uma relação $\leq$ em A é dita uma* quase-ordem *(ou uma* pré-ordem*) se valem as seguintes propriedades:*

1) $\forall x \in A, x \leq x$
2) $\forall x, y, z \in A, x \leq y$ *e* $y \leq z \Rightarrow x \leq z$

Ela é dita trivial *se $x \leq y$ vale para todos $x, y \in A$ e* total *se dados $x, y \in A$ temos $x \leq y$ ou $y \leq x$.*

Uma quase-ordem $|$ não trivial em um ***anel*** *A é dita uma* divisibilidade *se dados $x, y, z \in A$ também valem:*

1) $x|y$ *e* $x|z \Rightarrow x|(y-z)$
2) $x|y \Rightarrow xz|yz$

Lema 70. *Seja A um anel e $|$ uma divisibilidade em um corpo $\mathbb{K}$. Então dado $x \in A$, $x|0$. Além disso, $0|x$ se, e somente se, $x = 0$.*

Demonstração. De $x|x$, temos $x|(x-x) = 0$. Supondo $x = 0$, segue que $0|x = 0$ e supondo que $0|x$ com $x \neq 0$, temos $0 = 0x^{-1}|xx^{-1} = 1$ e logo, para $y \in \mathbb{K}$, $y|0$ e $0|1$, logo $y|1$. Mais ainda, para $z \in \mathbb{K}^*$, $yz^{-1}|1$ e logo $y|z$. Como $y|0$, obtemos que $|$ é trivial, contradizendo a hipótese. ■

Teorema 71. *Seja K um corpo e denote*

$$\mathcal{D} := \{| \subseteq \mathbb{K} \times \mathbb{K}; | \text{ é uma divisibilidade em } \mathbb{K}\},$$

$$\mathcal{A} := \{A \subseteq \mathbb{K}; A \text{ é subanel unitário de } \mathbb{K}\}.$$

Então a função de $\mathcal{A}$ em $\mathcal{D}$ que leva $A \in \mathcal{A}$ em $|_A$ definida por

$$x|_A x' \Leftrightarrow x = x' = 0 \text{ ou } x \neq 0 \text{ e } x'x^{-1} \in A$$

é uma bijeção. Além disso, $Inv(A) = \{x \in A; x|_A 1\}$.

Demonstração. Mostraremos que essa função está bem definida. Seja $A \in \mathcal{A}$. Temos que dado $x \in \mathbb{K}^*$, $1 = xx^{-1} \in A$, pois A é unitário, disso e de $0|0$ resulta $x|_A x$. Para $x, y, z \in \mathbb{K}$, suponha inicialmente que x, y e z são não nulos. Se $x|_A y$ e $y|_A z$, temos $yx^{-1} \in A$ e $zy^{-1} \in A$, do que resulta $zx^{-1} = zy^{-1}yx^{-1} \in A$ e $(y-z)x^{-1} = yx^{-1} - zx^{-1} \in A$, logo $x|_A z$ e $x|_A(y-z)$. Ainda, se $x|_A y$, então para qualquer z temos

$yz(xz)^{-1} = yzz^{-1}x^{-1} = yx^{-1} \in A$, logo $xz|_A yz$. Notando que para qualquer $0|z \Leftrightarrow z = 0$, temos que se $x = 0$, então $0|y \implies y = 0$ e $x = 0|0 = 0z = yz$, $0|z \implies z = 0$ e $x = 0|0 = (y - z)$. Notando ainda que para qualquer $x \in \mathbb{K}$, $x|0$, temos que se $z = 0$, $x|0 = yz$ e se $x|y$, então $x|(y-z)$. Também, supondo $x \neq 0, z \neq 0$ e $y = 0$, então $x|0 = yz$ e se $x|z$, então $zx^{-1} \in A \implies -zx^{-1} \in A \implies x| - z = (y - z)$. Como, da definição, $0 \nmid 1$, $|$ não é trivial e concluímos que $|_A$ é relação de divisibilidade, e portanto a função está bem definida.

,Agora sejam $A, B \in \mathcal{A}$ tais que $|_A = |_B$. Temos que se $x \in A$, então $x \cdot 1^{-1} \in A$ e $1|_A x$. Então, $1|_B x$ e portanto $x = x \cdot 1^{-1} \in B$. Então sai $A \subseteq B$. A outra inclusão é análoga, o que prova que a função é injetora. Considere $|$ uma divisibilidade em $\mathbb{K}$. Defina $A = \{x \in \mathbb{K}; 1|x\}$ e mostraremos que A é subanel unitário de $\mathbb{K}$. Temos que se $x, y \in A$, então $1|x$ e $1|y$, logo $1|(x - y)$ e $x - y \in A$. Além disso, $1|x \implies y|xy \implies 1|y, y|xy \implies 1|xy$, logo $xy \in A$. Também, como $1|1$, temos $1 \in A$, o que prova a afirmação. Finalmente, mostremos que $| = |_A$. De fato, considere $x, y \in \mathbb{K}$. Se $x = 0$, então $x|_A y \Leftrightarrow y = 0 \Leftrightarrow x = 0|y$. Suponha agora que $x \neq 0$. Temos

$$x|_A y \Leftrightarrow yx^{-1} \in A \Leftrightarrow 1|yx^{-1} \Leftrightarrow x|yx^{-1}x = y.$$

Obtemos que a função é bijetora. Para mostrar a segunda parte do teorema, note que $x \in A$ é inversível se, e somente se, $1x^{-1} = x^{-1} \in A$, ou seja, se e somente se $x|_A 1$.

■

A demonstração acima contém também a demonstração do seguinte teorema:

Teorema 72. *Nas notações do teorema anterior, dado $A \in \mathcal{A}$ e $x \in \mathbb{K}$, temos $x \in A \Leftrightarrow 1|_A x$.*

Definição 73. *Seja $\mathbb{K}$ um corpo. Um subanel unitário $A \in \mathbb{K}$ é dito um* anel de valoração *de $\mathbb{K}$ se para qualquer $x \in \mathbb{K}$ temos $x \in A$ ou $x^{-1} \in A$.*

O estudo de anéis de valoração será importante mais a frente, por isso é interessante obter caracterizações deles. Uma delas é dada por divisibilidades da seguinte forma:

Teorema 74. *Seja $\mathbb{K}$ um corpo. Um subanel unitário A de $\mathbb{K}$ é um anel de valoração de $\mathbb{K}$ se, e somente se, a divisibilidade $|_A$ é total.*

Demonstração. Suponha que A seja um anel de valoração e considere $x, y \in \mathbb{K}^*$. Então como $xy^{-1} \in \mathbb{K}$ e A é de valoração, temos $xy^{-1} \in A$

ou $yx^{-1} = (xy^{-1})^{-1} \in A$. No primeiro caso, $y|_A x$, já no segundo, $x|_A y$. Falta o caso em que $x = 0$ ou $y = 0$, mas notando que do lema 70 $x|0$ e $y|0$, concluímos que $|_A$ é total.

Suponha agora que $|_A$ seja total. Dado $x \in \mathbb{K}^*$, temos $x|_A 1$ ou $1|_A x$. No primeiro caso, $x^{-1} \in A$ e no segundo, $x \in A$. Concluímos que A é anel de valoração.

■

Definição 75. *Um anel A é dito* local *se possui um único ideal maximal. Nesse caso, seu ideal maximal é denotado por $\mathfrak{M}_A$.*

Observação 76. *Note que nesse caso $\mathfrak{M}_A = A \setminus Inv(A)$. De fato, como $\mathfrak{M}_A$ é maximal, ele é próprio e nenhum inversível de A está nele, isto é, $\mathfrak{M}_A \subseteq A \setminus Inv(A)$. Agora, seja $x \in A \setminus Inv(A)$. Então $\langle x \rangle$ é um ideal próprio de A, e portanto está contido em um ideal maximal de A. Mas $\mathfrak{M}_A$ é o único ideal maximal de A e logo $x \in \langle x \rangle \subseteq \mathfrak{M}_A$. Como x foi qualquer, $\mathfrak{M}_A \supseteq A \setminus Inv(A)$, concluindo a prova.*

Lema 77. *Seja $A \subseteq \mathbb{K}$ um anel de valoração. Então o conjunto dos ideais de A é totalmente ordenado pela inclusão.*

Demonstração. Considere I, J ideais de A e suponha que $I \subsetneq J$. Queremos mostrar que $J \subseteq I$. Seja $x \in J \setminus \{0\}$ e fixe $y \in I \setminus J$, notando que $y \neq 0$. Então, $yx^{-1}x = y \notin J$ e como J é ideal e $x \in J$, temos $yx^{-1} \notin A$. De A anel de valoração, $xy^{-1} \in A$ e como $y \in I$ e I é ideal, obtemos $x = xy^{-1}y \in I$. De $0 \in I$, concluímos $J \subseteq I$.

■

Teorema 78. *Todo anel de valoração de um corpo $\mathbb{K}$ é um anel local.*

Demonstração. Se $A = \mathbb{K}$, então A é corpo e portanto só tem ideais triviais. Então, $\{0\}$ é o seu único ideal maximal. Caso contrário, temos que existe $x \in \mathbb{K} \setminus A$. Como $0 \in A$, temos $x \neq 0$ e portanto $x^{-1} \in A$. Isso quer dizer que $x^{-1} \notin \mathrm{Inv}(A)$ e logo A não é corpo. Isso quer dizer que A possui ideal não-trivial I. Sabemos que I está contido em algum ideal maximal $\mathbb{M}$ de A, logo a existência de um ideal maximal está provada. A unicidade é garantida do lema pois se $\mathbb{M}'$ também é maximal, o lema nos garante $\mathbb{M} \subseteq \mathbb{M}'$ ou $\mathbb{M}' \subseteq \mathbb{M}$, e em ambos os casos, da maximalidade, obtemos $\mathbb{M} = \mathbb{M}'$.

■

Teorema 79. *Seja $\mathbb{K}$ um corpo, v uma valoração sobre $\mathbb{K}$ e $|\cdot|$ um valor absoluto associado a v. Então:*

1) O conjunto

$$\mathcal{O} := \{x \in \mathbb{K}; v(x) \geq 0\} = \{x \in \mathbb{K}; |x| \leq 1\}$$

é um anel de valoração e um subanel maximal de $\mathbb{K}$*, chamado* anel de valoração associado com v.

2) Inv$(\mathcal{O}) = \{x \in \mathbb{K}; v(x) = 0\} = \{x \in \mathbb{K}; |x| = 1\}$

3) O conjunto

$$\mathfrak{M} := \mathcal{O} \setminus Inv(\mathcal{O}) = \{x \in \mathbb{K}; v(x) > 0\} = \{x \in \mathbb{K}; |x| < 1\}$$

é o único ideal maximal de $\mathcal{O}$*.*

Demonstração. 1) Como $v(1) = 0$, temos $1 \in \mathcal{O}$. Além disso, se $x, y \in \mathcal{O}$, $v(x - y) = v(x + (-y)) \geq \min(v(x), v(-y)) = \min(v(x), v(y)) \geq 0$, logo $x - y \in \mathcal{O}$ e também $v(xy) = v(x) + v(y) \geq 0$, logo $xy \in \mathcal{O}$. Dado $x \in \mathbb{K}$, se $x \notin \mathcal{O}$, então $v(x) < 0$. Então, $v(x^{-1}) = -v(x) > 0$, logo $x^{-1} \in \mathcal{O}$, o que prova que $\mathcal{O}$ é anel de valoração. Também, se B é subanel de $\mathbb{K}$ tal que $A \subseteq B$, então dado $x \in B \setminus \{0\}$, temos $x \in A$ ou $x^{-1} \in A$. Se $x \in A$, então está provado que $B \subseteq A$, logo $A = B$. Se $x \notin A$, então $v(x) < 0$. Agora tome $y \in \mathbb{K}$ qualquer. Temos que para algum $k \in \mathbb{N}$, $v(y) > kv(x)$. Disso, $v(yx^{-k}) = v(y) - kv(x) > 0$ e portanto $z = yx^{-k} \in A \subseteq B$. Como $x \in B$, temos $x^k \in B$ e logo $y = zx^k \in B$, portanto $\mathbb{K} \subseteq B$ e $B = \mathbb{K}$.

2) $x \in \mathrm{Inv}(\mathcal{O}) \Leftrightarrow x \in \mathcal{O}$ e $x^{-1} \in \mathcal{O} \Leftrightarrow v(x) \geq 0$ e $-v(x) = v(x^{-1}) \geq 0 \Leftrightarrow v(x) = 0$.

3) Segue da observação dada logo após a definição de anel local e do teorema 78.

∎

Daremos abaixo a definição de corpo de resíduos. O estudo desse corpo, que não será feito aqui em detalhes, nos revela informações importantes sobre a valoração em questão. Daremos a definição pois a mesma será usada mais tarde.

Definição 80. $\mathcal{K} := \mathcal{O}/\mathfrak{M}$ *é dito* corpo de resíduos de $\mathcal{O}$*.*

7 GRUPOS ABELIANOS ORDENADOS E VALORAÇÕES DE KRULL

O estudo acima nos remete a uma pergunta: Será que todo anel de valoração de um corpo é induzido de alguma valoração nele? A resposta para isso é não. De fato, daremos um exemplo abaixo, com uma construção geral. Uma construção explicita é possível usando series de potências formais, mas não faremos tal construção aqui. Ao longo dessa seção, teremos mais ferramentas para construir anéis de valoração desse tipo.

Exemplo 81. *Seja $\mathbb{K}$ um corpo e A um anel de valoração de $\mathbb{K}$ tal que A possui ideal primo $\mathfrak{P}$ satisfazendo $0 \subsetneq \mathfrak{P} \subsetneq \mathfrak{M}_A$. Suponha, por absurdo, que A é induzido por uma valoração $v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$. Sejam $x, y \in A$ tais que*
$x \in \mathfrak{M}_A \setminus \mathfrak{P}$ e $y \in \mathfrak{P} \setminus \{0\}$, notando que $x \neq 0$, já que $\mathfrak{P}$ é ideal. Temos $\forall n \in \mathbb{N}^*, x^n \notin \mathfrak{P}$. De fato, o caso $n = 1$ segue da construção de x e supondo, para algum n fixo, que $x^n \notin \mathfrak{P}$, temos $x^{n+1} = x^n \cdot x \notin \mathfrak{P}$ pois $\mathfrak{P}$ é primo. Como $\mathbb{R}$ é arquimediano, existe $m \in \mathbb{N}^*$ tal que $m \cdot v(x) \geq v(y)$. Mas então, $v(\frac{x^m}{y}) = v(x^m) - v(y) = m \cdot v(x) - v(y) \geq 0$ e portanto $\frac{x^m}{y} \in A$. Disso, de $y \in \mathfrak{P}$ e de $\mathfrak{P}$ ideal de A, temos $x^m = y \cdot \frac{x^m}{y} \in \mathfrak{P}$, o que é uma contradição.

Note que a contradição acima só foi possível porque $\mathbb{R}$ é arquimediano. Além disso, note que na definição de valoração, usamos apenas a soma e a ordem de $\mathbb{R}$. Isso nos motiva a estender a noção de valoração para outras estruturas $(\Gamma, +, \leq)$ "semelhantes"a $(\mathbb{R}, + \leq)$, mas que não sejam necessariamente arquimedianas. De fato, faremos isso para grupos abelianos ordenados Γ, e veremos posteriormente que todo anel de valoração é induzido de uma valoração estendida a tais grupos (valoração de Krull).

Definição 82. *Sejam $(G, +)$ um grupo abeliano e $\leq$ uma ordem total em G. Dizemos que $(G, +, \leq)$ é um* grupo abeliano ordenado *se $\leq$ é compatível com a operação de G, isto é, se para quaisquer $a, b, c, d \in G$ temos que $a \leq b$ e $c \leq d \Rightarrow a + c \leq b + d$. Dado $a \in G$, definiremos $|a| := a$, se $a \geq 0$, e $|a| := -a$ caso contrário. Diremos que $(G, +, \leq)$ é arquimediano se para quaisquer $a, b \in G$ com $a > 0$ e $b > 0$, existe $n \in \mathbb{N}$ tal que $a \leq nb$.*

Similarmente a antes, omitiremos a operação e a ordem quando as mesmas ficarem claras no contexto.

Definição 83. *Seja G um grupo abeliano ordenado. Então um subgrupo I de G é dito* isolado *se para todo $x \in I$ temos $\{y \in G; 0 \leq y \leq x\} \subseteq I$.*

Observação 84. *Note que se $x < 0$, temos $\{y \in G; 0 \leq y \leq x\} = \emptyset \subseteq I$ e que para $x = 0$, temos $\{y \in G; 0 \leq y \leq x\} = \{0\} \subseteq I$, pois I é subgrupo. Disso, quando queremos mostrar que um subgrupo é isolado, basta mostrar $\{y \in G; 0 \leq y \leq x\} \subseteq I$ quando $x > 0$.*

Teorema 85. *Seja G um grupo abeliano ordenado. Então dado $a \in G$ com $a > 0$, o menor subgrupo isolado de G que contem a é dado por*

$$I_a := \bigcup_{n \in \mathbb{N}} \{b \in G; -na \leq b \leq na\}.$$

Além disso, $\{0\}$ e G são subgrupos isolados de G e G é arquimediano se, e somente se, esses dois subgrupos são os únicos subgrupos isolados de G.

Demonstração. É claro que $a \in I_a$, pois de $a > 0$, $-a \leq a \leq a$. Sejam $x, y \in I_a$. Então existem $n_1, n_2 \in \mathbb{N}$ tais que $x \in \{b \in G; -n_1 a \leq x \leq n_1 a\}$ e
$y \in \{b \in G; -n_2 a \leq y \leq n_2 a\}$. Temos que $-(n_1 - n_2)a \leq x - y \leq (n_1 - n_2)a$.

Isso mostra que I_a é subgrupo. Ele é isolado, pois dado $x, y \in G$ tais que $x \in I_a$ e $0 \leq y \leq x$. Então $x \leq na$, para algum $n \in \mathbb{N}$. Disso, obtemos $-na \leq 0 \leq y \leq x \leq na$, logo, $y \in I_a$. Também, dado I subgrupo isolado de G que contém a, seja $x \in I_a$. Então $0 \leq |x| \leq na$ para algum $n \in \mathbb{N}$. Como $a \in I$ e I é grupo, temos $na \in I$. De I isolado, $|x| \in I$. Mas I é grupo, logo $x \in I$ e $I_a \subseteq I$. Concluímos a primeira parte do teorema.

É claro que $\{0\}$ e G são isolados. Suponha G arquimediano e considere $I \subseteq G$ um subgrupo isolado não-nulo de G. Então existe $a \in I$ com $a > 0$. Dado $b \in G$, a propriedade arquimediana garante a existência de $n \in \mathbb{N}$ tal que $|b| \leq na$, logo obtemos $-na \leq b \leq na$ e portanto

$$b \in \{x \in G; -na \leq x \leq na\} \subseteq I_a \subseteq I.$$

Isso prova $G \subseteq I$, logo $G = I$. Suponha agora que G tenha apenas subgrupos isolados triviais. Então, tome $a, b \in G$. Como I_a é isolado, temos $I_a = G$, logo $b \in I_a$, isto é, existe $n \in \mathbb{N}$ tal que $-na \leq b \leq na$. Disso, G é arquimediano.

■

Definição 86. *Sejam G e H grupos abelianos ordenados. Uma função*

$f : G \to H$ *é um* homomorfismo de ordem *se* f *for homomorfismo de grupo e para quaisquer* $a, b \in G$ *temos* $a \leq b \Rightarrow f(a) \leq f(b)$*. Se* f *for bijetora, dizemos que* f *é um* isomorfismo de ordem *e dizemos que* G *e* H *são* isomorfos.

Teorema 87. *Nas notações da definição acima, se* f *é isomorfismo de ordem, então* f^{-1} *também o é.*

Demonstração. Sejam $a, b \in H$ com $a \leq b$ e suponha por absurdo que $f^{-1}(a) > f^{-1}(b)$. Temos que $f^{-1}(b) \leq f^{-1}(a)$, logo $b = f(f^{-1}(b)) \leq f(f^{-1}(a)) = a$. Mas então $a = b$ e portanto $f^{-1}(a) = f^{-1}(b)$, o que é uma contradição. Isso mostra que f^{-1} preserva a ordem. Como já se sabe da teoria de grupos, f^{-1} é um homomorfismo de grupos, o que prova o teorema.

■

Teorema 88. *Seja* G *um grupo abeliano ordenado e* I *um subgrupo isolado de* G*. Então* G/I *é um grupo abeliano ordenado pela ordem* $[a] \leq [b] \Leftrightarrow$ *existe* $i \in I$ *tal que* $a \leq b + i$*. Além disso,* $\pi : G \to G/I$ *definida por* $\pi(a) := [a]$ *é um homomorfismo de ordem.*

Demonstração. Mostraremos que a relação $\leq$ está bem definida. Suponha $a, b, a', b' \in G$ com $a' - a \in I$ e $b' - b \in I$. Então se existe $i \in I$ tal que $a \leq b + i$, temos $a' = a' - a + a \leq a' - a + b + i = a' - a + b - b' + b' + i$. Considere $i' = i + (a' - a) - (b' - b) \in I$. Então temos $a' \leq b' + i'$, o que mostra que a relação está bem definida. Mostraremos que é uma relação de ordem que respeita a soma do quociente. De fato, dados $a, b, c, d \in G$ temos:

1) $a \leq a + 0$ com $0 \in I$, pois I é subgrupo, logo $[a] \leq [a]$.

2) Se $[a] \leq [b]$ e $[b] \leq [a]$, então existem $i, j \in I$ tais que $a \leq b + i$ e $b \leq a + j$, logo $a - b \leq b + i - b = i \leq \max(i, j)$ e $-(a - b) = b - a \leq a + j - a = j \leq \max(i, j)$, isto é, $0 \leq |a - b| \leq max(i, j) \in I$, logo, de I isolado, $|a - b| \in I$ e $a - b \in I$, o que resulta em $[a] = [b]$.

3) Se $[a] \leq [b]$ e $[b] \leq [c]$, então existem $i, j \in I$ tais que $a \leq b + i$ e $b \leq c + j$. Concluímos que $a \leq b + i \leq c + j + i$ e como $j + i \in I$, temos $[a] \leq [c]$.

4) Se $[a] \leq [b]$ e $[c] \leq [d]$, temos que existem $i, j \in I$ tais que $a \leq b + i$ e $c \leq d + j$. Então, $a + c \leq b + d + i + j$ com $i + j \in I$, portanto $[a + c] \leq [b + d]$.

Para finalizar, sabemos da teoria de grupos que π como definida é um homomorfismo. Provaremos que ele respeita a ordem. De fato, dado $a, b \in G$, $a \leq b$, temos $a \leq b + 0$ com $0 \in I$. Disso, $[a] \leq [b]$.

■

Teorema 89. *(Teorema do homomorfismo) Sejam G e H grupos abelianos ordenados e $f : G \to H$ um homomorfismo de ordem. Então Ker(f) é subgrupo isolado de G e G/Ker(f) é isomorfo à Im(f).*

Demonstração. Como f é homomorfismo de grupo, sabemos, da teoria de grupos, que $\mathrm{Ker}(f)$ é subgrupo de G. Além disso, considere $x \in G$. Temos que se $y \in G$ é tal que $0 \leq y \leq x$, então $0 = f(0) \leq f(y) \leq f(x) = 0$, logo $f(y) = 0$ e $y \in \mathrm{Ker}(f)$. Do teorema do homomorfismo para grupos, segue que está bem definida a função $g : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ definida por $g([x]) = f(x)$ e esta é um homomorfismo de grupos. Falta mostrar que ele respeita a ordem. Suponha que para $[x], [y] \in G/\mathrm{Ker}(f)$ temos $[x] \leq [y]$. Então, existe $i \in \mathrm{Ker}(f)$ tal que $x \leq y + i$. Como f respeita a ordem e $f(i) = 0$, $g([x]) = f(x) \leq f(y + i) = f(y) + f(i) = f(y) = g([y])$, o que conclui a demonstração.

■

Definição 90. *Seja $\mathbb{K}$ um corpo. Uma* valoração de Krull *em $\mathbb{K}$ é uma função sobrejetora $v : \mathbb{K} \to \Gamma \cup \{\infty\}$ onde Γ é um grupo abeliano ordenado e estendemos $x+\infty = \infty+x = \infty$ e $x \leq \infty$ para $x \in \Gamma \cup \{\infty\}$ tal que valem:*

1) $v(x) = \infty$ *se, e somente se,* $x = 0$
2) $v(x + y) \geq \min(v(x), v(y))$
3) $v(xy) = v(x) + v(y)$

Nesse caso, Γ é denominado o grupo de valores *de v e denotado por Γ_v. Além disso, duas valorações v, w de $\mathbb{K}$ são ditas* equivalentes *se existe um isomorfismo de ordem $\iota : \Gamma_v \to \Gamma_w$ tal que $w = \iota \circ v$.*

Observação 91. *Na definição, poderíamos não ter pedido que v fosse sobrejetora. Nesse caso, Im(v) seria um subgrupo de Γ, pois se $a, b \in$ Im(v), considere $x, y \in \mathbb{K}$ tal que $v(x) = a$ e $v(y) = b$. Então $v(xy^{-1}) = v(x) - v(y)$. Definindo o grupo de valores como Im(v), temos, essencialmente, a mesma definição, logo não há perda em considerar v sobrejetora.*

Teorema 92. *Seja $\mathbb{K}$ um corpo e v uma valoração de Krull de $\mathbb{K}$. Temos que:*

1) $v(1) = 0$
2) Para toda raiz $u \in \mathbb{K}$ da unidade, $v(u) = 0$.
3) Se $x \in \mathbb{K}$, então $v(-x) = v(x)$ e se $x \neq 0$, então $v(x^{-1}) = -v(x)$.

Demonstração. Mais uma vez, essa demonstração é similar ao que já fizemos.

1) $v(1) = v(1 \cdot 1) = v(1) + v(1) \implies v(1) = 0$

2) Seja $n \in \mathbb{N}^*$ tal que $u^n = 1$. $0 = v(1) = v(u^n) = nv(u)$, logo, de $n > 0$, $v(u) = 0$.

3) Como $-1^2 = 1$, temos que -1 é raiz da unidade. Então, $v(-x) = v(-1 \cdot x) = v(-1) + v(x) = 0 + v(x) = v(x)$. Se $x \neq 0$, então $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) \implies v(x^{-1}) = -v(x)$.

■

Teorema 93. *Seja $\mathbb{K}$ um corpo e v uma valoração de Krull em $\mathbb{K}$. Então $\mathcal{O}_v := \{x \in \mathbb{K}; v(x) \geq 0\}$ é um anel de valoração de $\mathbb{K}$, denominado* anel de valoração associado a v *e se w é uma valoração de Krull em $\mathbb{K}$, temos $\mathcal{O}_v = \mathcal{O}_w$ se, e somente se, v e w são equivalentes. Além disso, todo anel de valoração de $\mathbb{K}$ é associado a alguma valoração de Krull em $\mathbb{K}$.*

Demonstração. Seja $x \in \mathbb{K}^*$ tal que $x \notin \mathcal{O}_v$. Então $v(x) < 0$ e $v(x^{-1}) = -v(x) > 0$, logo $x^{-1} \in \mathcal{O}_v$, isto é, $\mathcal{O}_v$ é anel de valoração.

Para a segunda parte, suponha primeiro que $\mathcal{O}_v = \mathcal{O}_w$ e seja $a \in \Gamma_v$. Como v é sobrejetora e $a \neq \infty$, existe $x \in \mathbb{K}^*$ tal que $v(x) = a$. Além disso, se $y \in \mathbb{K}^*$ é tal que $v(y) = a$, temos $0 = v(x) - v(y) = v(xy^{-1})$ e $0 = v(y) - v(x) = v(yx^{-1})$, logo $xy^{-1}, yx^{-1} \in \mathcal{O}_v = \mathcal{O}_w$. Então, $0 \leq w(xy^{-1}) = -w(yx^{-1}) \leq 0$, logo $w(x) - w(y) = w(xy^{-1}) = 0$ e $w(x) = w(y)$. Disso, está bem definida a função $\iota : \Gamma_v \to \Gamma_w$ definida por $\iota(v(x)) = w(x)$. Note que dados $a, b \in \Gamma_v$, com $a = v(x), b = v(y)$, temos $\iota(a + b) = \iota(v(x) + v(y)) = \iota(v(xy)) = w(xy) = w(x) + w(y) = \iota(a) + \iota(b)$ e ι é homomorfismo de grupos. Além disso, se $a \leq b$, suponha que $\iota(a) > \iota(b)$. Então, $\iota(a) - \iota(b) > 0$ e $w(xy^{-1}) = \iota(v(xy^{-1})) = \iota(v(x)) - \iota(v(y)) = \iota(a) - \iota(b) > 0$ e $xy^{-1} \in \mathcal{O}_w = \mathcal{O}_v$. Disso, $0 \leq v(xy^{-1}) = v(x) - v(y) = a - b$ e $b \leq a$. De $a \leq b$ obtemos $a = b$ e portanto $\iota(a) = \iota(b)$, contradição. Concluímos que $\iota(a) \leq \iota(b)$ e ι é homomorfismo de ordem. É claro que $w(x) = \iota(v(x))$, da definição, logo só falta mostrar que ι é bijeção. De fato, ι é sobrejetor, pois dado $b \in \Gamma_w$, como w é sobrejetor, existe $x \in \mathbb{K}$ tal que $w(x) = b$. Para $a = v(x)$, $\iota(a) = \iota(v(x)) = w(x) = b$. Para mostrar que ι é injetora, observe que ι é homomorfismo de grupo e considere $a = v(x) \in \mathrm{Ker}(\iota)$. Temos $0 = \iota(a) = \iota(v(x)) = w(x)$, logo $x, x^{-1} \in \mathcal{O}_w = \mathcal{O}_v$. Mas então, $0 \leq v(x^{-1}) = -v(x) \leq 0$ e $a = v(x) = 0$. Isso prova que ι é isomorfismo de ordem.

Reciprocamente, suponha v e w equivalentes e seja $\iota : \Gamma_v \to \Gamma_w$

tal que $w = \iota \circ v$. Se $x \in \mathcal{O}_v$, então $0 \leq v(x)$. Como ι é isomorfismo de ordem, $0 = \iota(0) \leq \iota(v(x)) = w(x)$ e $x \in \mathcal{O}_w$, concluindo $\mathcal{O}_v \subseteq \mathcal{O}_w$. Além disso, note que $\iota^{-1} : \Gamma_w \to \Gamma_v$ é isomorfismo de ordem tal que $v = \iota^{-1} \circ w$. Do que provamos, isso implica $\mathcal{O}_w \subseteq \mathcal{O}_v$ e portanto $\mathcal{O}_v = \mathcal{O}_w$.

Finalmente, seja $\mathcal{O}$ um anel de valoração de $\mathbb{K}$. $(\mathbb{K}^*, \cdot)$ é grupo abeliano e $(\text{Inv}(A), \cdot)$ é subgrupo de $\mathbb{K}^*$. Da teoria de grupos, todo subgrupo de um grupo abeliano é normal, logo podemos fazer o grupo quociente $\Gamma = K^*/\text{Inv}(A)$, que é abeliano. Além disso, considere a divisibilidade $|_A$. Dados $x, x', y, y' \in \mathbb{K}^*$ tais que $[x] = [x']$, $[y] = [y']$ e $x|_A y$, temos $y'y^{-1}, xx'^{-1} \in A$ e portanto, do que vimos na seção anterior, $1|_A xx'^{-1}$ e $1|_A y'y^{-1}$. Aplicando a definição de divisibilidade, obtemos $x' = 1x'|_A xx'^{-1}x' = x|_A y = y1|_A y'y^{-1}y = y'$ e $x'|_A y'$. Resulta que a relação $\leq$ em Γ tal que $[x] \leq [y] \Leftrightarrow x|_A y$ está bem definida. Mais ainda, essa ordem é total, pois dados $[x], [y] \in \Gamma$, temos $xy^{-1} \in A$ ou $yx^{-1} \in A$. No primeiro caso, $[x] \leq [y]$ e no segundo $[y] \leq [x]$. Também, se $[x], [x'], [y], [y'] \in \Gamma$ são tais que $[x] \leq [y]$ e $[x'] \leq [y']$, então $x|_A y$ e $x'|_A y'$ o que resulta $yx'|_A yy'$ e $xx'|_A yx'|_A yy'$, isto é, $[x][x'] = [xx'] \leq [yy'] = [y][y']$ e $\leq$ respeita a operação do grupo. Defina $v : \mathbb{K} \to \Gamma \cup \{\infty\}$ por $v(x) = [x]$, se $x \neq 0$ e $v(0) = \infty$. Queremos mostrar que v é valoração de Krull. Observe inicialmente que v é sobrejetora e considere $x \in \mathbb{K}$. Claramente, $v(x) = \infty \Leftrightarrow x = 0$ e além disso se $y \in \mathbb{K}$, podemos verificar as demais propriedades de valoração. Caso $x = 0$ ou $y = 0$, elas são triviais, então suponha $x \neq 0$ e $y \neq 0$. Então, $v(xy) = [xy] = [x][y]$ (lembrando que a operação nesse grupo é denotada multiplicativamente) e supondo $v(x) \leq v(y)$, temos da definição de $\leq$ que $x|_A y$ e como $x|_A x$, temos $x|_A(x + y)$ e $v(x + y) \geq v(x) = \min(v(x), v(y))$. Isso conclui o teorema.

■

A seguir, veremos a topologia de uma valoração de Krull. Essa não é necessariamente metrizável, mas ela tem uma estrutura boa.

Definição 94. *Seja $\mathbb{K}$ um corpo com uma valoração de Krull v com grupo de valores Γ. Dados $x \in \mathbb{K}$ e $r \in \Gamma$, a* bola com centro x e raio r *é definida como o conjunto $B_r(x) := \{y \in \mathbb{K}; v(y - x) > r\}$.*

Teorema 95. *Seja $\mathbb{K}$ um corpo e v uma valoração de Krull em $\mathbb{K}$ com grupo de valores Γ. Defina uma família τ de subconjuntos de $\mathbb{K}$ da seguinte forma: $U \in \tau$ se, e somente se para todo $x \in U$ existe $r \in \Gamma$ tal que $B_r(x) \subseteq U$. Então τ é uma topologia em $\mathbb{K}$ e $\beta = \{B_r(x); r \in \Gamma, x \in \mathbb{K}\}$ é um base de τ. Além disso, as operações de subtração e multiplicação são contínuas.*

Demonstração. A demonstração que τ é topologia é a padrão: $\emptyset$ e $\mathbb{K}$ são trivialmente elementos de τ. Dados $U, V \in \tau$, seja $x \in U \cap V$. Então existem $r, s \in \Gamma$ tais que $B_r(x) \subseteq U$ e $B_s(x) \subseteq V$. Como Γ é totalmente ordenado, existe $m = \min(r, s)$. Então, $B_m(x) \subseteq B_r(x) \cap B_s(x) \subseteq U \cap V$ e $U \cap V \in \tau$. Se $\{U_i\}_{i \in I} \subseteq \tau$, tome $x \in \bigcup\limits_{i \in I} U_i$. Então existe $i_0 \in I$ tal que $x \in U_{i_0}$. Como $U_{i_0} \in \tau$, existe $r \in \Gamma$ tal que $B_r(x) \subseteq U_{i_0} \subseteq \bigcup\limits_{i \in I} U_i$ e portanto temos que $\bigcup\limits_{i \in I} U_i \in \tau$. Concluímos que τ é uma topologia em $\mathbb{K}$. Para mostrar que β é uma base, observe inicialmente que $B_r(x)$ é aberto para todo $x \in \mathbb{K}, r \in \Gamma$. De fato, dado $y \in B_r(x)$, tome u um elemento positivo de Γ e $s = r + u$, notando que $s - r = r + u - r = u > 0$ e logo $s > r$. Temos que $B_s(y) \subseteq B_r(x)$, pois para $z \in B_s(y)$ temos $v(z - y) > s$ por definição e

$$v(z - x) = v(z - y + y - x) \geq \min(v(z - y), v(y - x)) > \min(s, r) = r.$$

Agora sai direto da definição de τ que todo aberto é união de bolas. De fato, seja $U \in \tau$. Dado $x \in U$, existe $r_x \in \Gamma$ tal que $x \in B_r(x) \subseteq U$. Disso, $U \subseteq \bigcup\limits_{x \in U} B_{r_x}(x) \subseteq U$. Falta mostrar a continuidade das operações do enunciado. Para isso, considere $x, y \in \mathbb{K}$. Dado uma vizinhança W de $x - y$, existe $r \in \Gamma$ tal que $B_r(x - y) \subseteq W$. Considere as vizinhanças $U = B_r(x), V = B_r(y)$ de x e y, respectivamente. Se $(x', y') \in U \times V$, temos

$$v(x' - y') \geq \min(v(x'), v(-y')) = \min(v(x'), v(y')) > r,$$

logo $x' - y' \in B_r(x - y) \subseteq W$. Temos que a operação de subtração é contínua para cada par (x, y), logo ela é contínua. Agora, seja $s = \max(r, 0)$. Usando as vizinhanças $U = B_s(x), V = B_s(y)$ de x e y, respectivamente, para $(x', y') \in U \times V$, temos $v(x'y') = v(x') + v(y') > s + s \geq r + 0 = r$ e obtemos que a operação de multiplicação é contínua.

■

8 CORPOS PROJETIVOS E LUGARES

Já vimos anteriormente duas equivalências aos anéis de valoração de um corpo: Valorações de Krull e divisibilidades. Veremos agora uma terceira caracterização via corpos projetivos. Nessa seção, veremos uma versão algébrica de um conceito recorrente na matemática. Assim como podemos criar a reta real estendida e o plano complexo estendido acrescentando um elemento extra, denotado ∞, e estendendo parcialmente as operações, podemos também fazer o mesmo em um corpo qualquer, definindo a noção do corpo projetivo associado a ele. Topologicamente, essa noção corresponde à compactificação de Alexandrov. Intuitivamente, as operações serão estendidas de maneira a torná-las contínuas, com a convergência para ∞ (usaremos o termo "convergência"nesse caso, pois ∞ é um elemento do corpo projetivo) sendo interpretada como os elementos ficando cada vez maiores (em módulo). Essa noção faz sentido para $\mathbb{R}$ ou $\mathbb{C}$, que tem uma topologia e um valor absoluto padrão, mas para o caso de um corpo $\mathbb{K}$ qualquer não temos essa noção formal. De qualquer maneira, as extensões seguirão a mesma linha desses dois casos particulares. Usaremos o seguinte guia, lembrando que a discussão a seguir é informal e usada apenas para motivar a definição:

1) Assumiremos que as operações de corpo já são contínuas, logo para $x, y \in \mathbb{K}$, $x + y$ e xy será como em $\mathbb{K}$.

2) Se $x \in \mathbb{K}$, tome (x_i) convergindo para x e (y_i) convergindo para ∞. Temos (x_i) limitada e portanto $(x_i + y_i)$ converge para ∞. Disso, $x + \infty = \infty$ e da mesma forma, $\infty + x = \infty$. Além disso,se $x \neq 0$, $(x_i y_i)$ também converge para ∞, e logo $x \cdot \infty = \infty \cdot x = \infty$.

3) Se (x_i) e (y_i) ambas convergem para ∞, o mesmo pode ser dito para $(x_i y_i)$, e portanto $\infty \cdot \infty = \infty$.

4) Observe que em $\mathbb{R}$ temos $(1, 2, 3, ...)$ e $(-1, -2, -3, ...)$ ambas convergindo para ∞, mas por um lado $(2, 4, 6, ...)$ converge para ∞ e por outro $(0, 0, 0, ...)$ não, logo $\infty + \infty$ não fica definido. O mesmo pode ser dito sobre $0 \cdot \infty$ observando as sequências $(1; 0,1; 0,01; ...)$ e $(1, 10, 100, ...)$, assim como as sequências $(0, 0, 0, ...)$ e $(1, 10, 100, ...)$.

Guiando-se nos pontos acima, segue a definição formal de corpo projetivo.

Definição 96. *Seja* $\mathbb{K}$ *um corpo.* O corpo projetivo de $\mathbb{K}$*, denominado* $\widetilde{\mathbb{K}}$*, é definido como o conjunto* $\mathbb{K} \cup \{\infty\}$ *(com* $\infty \notin \mathbb{K}$*). Nesse caso, as operações do corpo* $\mathbb{K}$ *são (parcialmente) estendidas para* $\widetilde{\mathbb{K}}$ *por*

$$x + \infty = \infty + x = \infty, \forall x \in \mathbb{K} \text{ e}$$

$$x \cdot \infty = \infty \cdot x = \infty, \forall x \in \widetilde{\mathbb{K}}^* := \widetilde{\mathbb{K}} \setminus \{0\}$$

e também estendemos $-\infty = \infty = 0^{-1}$ e $\infty^{-1} = 0$. Ainda, dado um corpo $\mathbb{L}$, um lugar *de $\mathbb{K}$ em $\mathbb{L}$ é uma função $f : \widetilde{\mathbb{K}} \to \widetilde{\mathbb{L}}$ tal que para quaisquer $x, y \in \widetilde{\mathbb{K}}$ valem:*

1) Se $x + y$ e $f(x) + f(y)$ estão definidas, então $f(x + y) = f(x) + f(y)$.
2) Se xy e $f(x)f(y)$ estão definidos, então $f(xy) = f(x)f(y)$.
3) $f(1_{\mathbb{K}}) = 1_{\mathbb{L}}$.

Observação 97. *A definição de lugar dada acima segue as linhas da definição de homomorfismo. De fato, um lugar de $\mathbb{K}$ em $\mathbb{L}$ pode ser visto como uma espécie de homomorfismo de $\widetilde{\mathbb{K}}$ em $\widetilde{\mathbb{L}}$.*

Observação 98. *Note que $x + y$ está definida se e só se $x \neq \infty$ ou $y \neq \infty$ e a condição de xy estar definido pode ser vista da seguinte forma: caso $x = 0$, é verdadeira precisamente quando $y = \infty$, caso $x = \infty$, é verdadeira precisamente quando $y \neq 0$ e caso nenhuma das duas, é sempre verdadeira.*

Teorema 99. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos e f um lugar de $\mathbb{K}$ em $\mathbb{L}$. Então para quaisquer $x, y \in \mathbb{K}$ valem:*

(a) $f(0) = 0$ e $f(\infty) = \infty$.
(b) Se $f(x) + f(y)$ está definida, então $x + y$ está definida. Se $f(x)f(y)$ está definido, então xy está definido.
(c) $f(-x) = -f(x)$ e $f(x^{-1}) = f(x)^{-1}$.

Demonstração. Primeiro, note que $0 + 1$ e $f(0) + f(1)$ estão definidas, pois $f(1) = 1 \neq 0$ (ver observação acima e a propriedade 3 da definição de lugar). Então, $1 = f(1) = f(0 + 1) = f(0) + f(1) = f(0) + 1$. Disso obtemos $f(0) \neq \infty$ e logo $f(0) \in \mathbb{L}$. Como $\mathbb{L}$ é corpo, $1 = f(0) + 1 \implies 0 = f(0)$. Agora, note que pelo mesmo motivo de antes, também estão definidas $\infty + 1$ e $f(\infty) + f(1)$. Obtemos $f(\infty) = f(\infty + 1) = f(\infty) + f(1) = f(\infty) + 1$. Se tivéssemos $f(\infty) \in \mathbb{L}$, obteríamos $0 = 1$, o que é uma contradição, logo $f(\infty) = \infty$, provando (a).

Para provar (b), suponha que $f(x) + f(y)$ esteja definida. Então $f(x) \neq \infty$ ou $f(y) \neq \infty$. Mas como por (a), $f(\infty) = \infty$, temos $x \neq \infty$ ou $y \neq \infty$, logo $x + y$ está definida. Agora, olhando para a contrapositiva, suponha que xy não esteja definido. Então temos dois casos: quando $x = 0$, temos $y = \infty$ e logo $f(x) = 0$ e $f(y) = \infty$, o que resulta em $f(x)f(y)$ não estar definido. No caso $x \neq 0$, temos, de xy não definido, $x = \infty$ e $y = 0$. Então, $f(x) = \infty$ e $f(y) = 0$, o que resulta em $f(x)f(y)$ não estar definido.

Finalmente, precisamos provar (c). Para isso, note que quando $f(x) \neq \infty$, temos $x \neq \infty$ e $f(-x) = -f(x)$ pode ser provado da mesma forma que na teoria de corpos e também note que se adicionalmente $f(x) \neq 0$, temos $x \neq 0$ e $f(x^{-1}) = f(x)^{-1}$ pode ser provado analogamente. Agora provaremos o três casos restantes:

$$
\begin{aligned}
f(-\infty) = f(\infty) = \infty = -\infty = -f(\infty) \\
f(\infty^{-1}) = f(0) = 0 = \infty^{-1} = f(\infty)^{-1} \\
f(0^{-1}) = f(\infty) = \infty = 0^{-1} = f(0)^{-1}
\end{aligned}
$$

Isso prova (c), concluindo a demonstração.

■

Observação 100. *Esse teorema nos diz que a condição 1 da definição de lugar é equivalente a "Se $f(x) + f(y)$ está definida, então $x + y$ está definida e*
$f(x + y) = f(x) + f(y)$"e a condição 2 da definição é equivalente a "Se $f(x)f(y)$ está definido, então xy está definido e $f(xy) = f(x)f(y)$". Mas note que essas condições alternativas sempre implicam as da definição, mesmo quando f não é lugar. Por exemplo, assumindo as condições alternativas, se $f(x + y)$ e $f(x) + f(y)$ estão definidas, em particular $f(x) + f(y)$ está e logo $f(x + y) = f(x) + f(y)$. Concluímos que se f satisfaz $f(1) = 1$, as condições da definição são equivalentes a essas. A hipótese de que $f(1) = 1$ (que foi usada na demonstração) é importante. Sem ela, podemos definir $f(\infty) = 0$ e $f(x) = \infty$ se $x \neq \infty$. Essa função satisfaz as condições 1 e 2 da definição, mas $f(\infty) + f(\infty)$ está definida sem que $\infty + \infty$ esteja.

Teorema 101. *Sejam $\mathbb{K}, \mathbb{L}, \mathbb{M}$ corpos, f lugar de $\mathbb{K}$ em $\mathbb{L}$ e g lugar de $\mathbb{L}$ em $\mathbb{M}$. Então $g \circ f$ é um lugar de $\mathbb{K}$ em $\mathbb{M}$.*

Demonstração. Sejam $x, y \in \mathbb{K}$ tais que $x + y$ e $g \circ f(x) + g \circ f(y)$ estejam definidas. Então, como g é lugar, $f(x) + f(y)$ está definida, do teorema 99. Então, $g \circ f(x + y) = g(f(x) + f(y)) = g \circ f(x) + g \circ f(y)$. Por argumentos análogos, se xy e $g \circ f(x) g \circ f(y)$ estão definidos, temos que $g \circ f(xy) = g \circ f(x) g \circ f(y)$. Ainda, $g \circ f(1) = g(1) = 1$, logo, por definição, $g \circ f$ é lugar.

■

Diferente do caso de homomorfismo de corpos, nem todo lugar é injetor, mas similarmente ao caso de homomorfismo de anel, lugares injetores podem ser caracterizados pelos elementos que são levados em 0. Outras caracterizações são possíveis, como é visto abaixo.

Teorema 102. *Sejam $\mathbb{K}, \mathbb{L}$ corpos e f lugar de $\mathbb{K}$ em $\mathbb{L}$. Então são equivalentes:*

1) f é injetora.
2) $Ker(f) = \{x \in \widetilde{\mathbb{K}}; f(x) = 0\} = \{0\}$
3) $f^{-1}(\{\infty\}) = \{x \in \widetilde{\mathbb{K}}; f(x) = \infty\} = \{\infty\}$
4) $f^{-1}(\mathbb{L}) = \{x \in \widetilde{\mathbb{K}}; f(x) \in \mathbb{L}\} = \mathbb{K}$

Demonstração. $(1 \implies 2)$: Como $f(0) = 0$ e f é injetora, segue que $\mathrm{Ker}(f) = \{0\}$.

$(2 \implies 3)$: Sabemos que $f(\infty) = \infty$. Agora, tome $x \in \mathbb{K}$ tal que $f(x) = \infty$. Temos $f(x^{-1}) = f(x)^{-1} = \infty^{-1} = 0$ e logo $x^{-1} = 0$, nos garantindo $x = \infty$. Então, $f^{-1}(\{\infty\}) = \{\infty\}$.

$(3 \implies 4)$: Temos

$$f^{-1}(\mathbb{L}) = \{x \in \mathbb{K}; f(x) \in \mathbb{L}\} = \widetilde{\mathbb{K}} \setminus \{x \in \mathbb{K}; f(x) = \infty\} = \widetilde{\mathbb{K}} \setminus \{\infty\} = \mathbb{K}.$$

$(4 \implies 1)$: Sejam $x, y \in \widetilde{\mathbb{K}}$ tais que $f(x) = f(y)$. Se $f(x) = f(y) = \infty$, temos $x \notin f^{-1}(\mathbb{L}) = \mathbb{K}$ e $y \notin f^{-1}(\mathbb{L}) = \mathbb{K}$, logo $x = y = \infty$. Caso $f(x) = f(y) \neq \infty$, temos $f(x) - f(y)$ definida e logo $f(x) + f(-y)$ também, o que nos dá $x + (-y) = x - y$ definida e $f(x - y) = f(x) - f(y) = 0$. Agora, $f((x - y)^{-1}) = f(x - y)^{-1} = 0^{-1} = \infty$ e portanto $(x - y)^{-1} \notin f^{-1}(\mathbb{L}) = \{x \in \mathbb{K}; f(x) \in \mathbb{L}\} = \mathbb{K}$. Obtemos $(x - y)^{-1} = \infty$ e logo $x - y = 0$, o que resulta em $x = y$.

■

Definiremos uma relação entre lugares mais à frente. Essa relação não será uma ordem, e sim uma quase-ordem. Dessa forma, podemos definir uma relação de equivalência entre lugares. Usaremos as classes de equivalência por essa relação para estabelecer a conexão entre lugares e anéis de valoração.

Teorema 103. *Sejam $\mathbb{K}, \mathbb{L}, \mathbb{M}$ corpos, f lugar sobrejetor de $\mathbb{K}$ em $\mathbb{L}$ e g lugar sobrejetor de $\mathbb{K}$ em $\mathbb{M}$. Então são equivalentes:*

1) $f^{-1}(\mathbb{L}) \subseteq g^{-1}(\mathbb{M})$
2) Existe uma função $\phi : \widetilde{\mathbb{M}} \to \widetilde{\mathbb{L}}$ tal que $f = \phi \circ g$.

Nesse caso, ϕ é um lugar de $\mathbb{M}$ em $\mathbb{L}$ e é a única função de $\widetilde{\mathbb{M}}$ em $\widetilde{\mathbb{L}}$ tal que $f = \phi \circ g$.

Demonstração. $(1 \implies 2)$: Queremos mostrar inicialmente que dados $x, y \in K$ tais que $g(x) = g(y)$, então $f(x) = f(y)$. De fato, se $g(x) = g(y) = \infty$, temos $x \notin g^{-1}(\mathbb{M})$ e $y \notin g^{-1}(\mathbb{M})$. Da hipótese, $x \notin g^{-1}(\mathbb{M})$ e $y \notin g^{-1}(\mathbb{M})$ e logo $f(x) = \infty = f(y)$. Agora, se $g(x) = g(y) \neq \infty$, temos $g(x)-g(y)$ definida e portanto $g(x)-g(y) = 0$. Então, $g(x-y) = g(x)-g(y) = 0$ e do teorema 102, $g((x-y)^{-1}) = g(x-y)^{-1} = 0^{-1} = \infty$. Temos $(x-y)^{-1} \notin g^{-1}(\mathbb{M})$ e portanto $(x-y)^{-1} \notin f^{-1}(\mathbb{L})$ o que resulta em $f(x-y)^{-1} = f((x-y)^{-1}) = \infty$ e portanto $f(x-y) = 0$. Como f é lugar, temos $f(x) - f(y) = 0$ e logo $f(x) = f(y)$. Com esse resultado, podemos definir uma função ϕ da seguinte forma: Dado $x \in \widetilde{\mathbb{M}}$, tome $y \in \mathbb{K}$ tal que $g(y) = x$ (tal y existe pois por hipótese g é sobrejetor). Defina $\phi(x) := f(y)$. Pelo que acabamos de provar, ϕ está definida. Agora, dado $y \in \mathbb{K}$, temos $\phi(g(y)) = f(y)$ por definição.

$(2 \implies 1)$: Seja $x \in f^{-1}(\mathbb{L})$. Então $\phi(g(x)) = f(x) \neq \infty$. Por outro lado, $\phi(g(\infty)) = f(\infty) = \infty$ e logo $g(x) \neq g(\infty) = \infty$. Disso, $x \in g^{-1}(\mathbb{M})$.

Agora, mostraremos que ϕ é lugar. De fato, sejam $x, y \in \mathbb{M}$. Se $x + y$ e $\phi(x) + \phi(y)$ estão definidas, sejam $x', y' \in \mathbb{K}$ tais que $g(x') = x$ e $g(y') = y$. Então, como $x+y = g(x')+g(y')$ está definida e g é lugar, $g(x'+y') = g(x')+g(y') = x+y$. Além disso, $\phi(x)+\phi(y) = f(x')+f(y')$ está definida e portanto obtemos $\phi(x+y) = \phi(g(x'+y')) = f(x'+y') = f(x') + f(y') = \phi(x) + \phi(y)$. O caso da multiplicação segue de maneira análoga: Se xy e $\phi(x) \cdot \phi(y)$ estão definidos, sejam $x', y' \in \mathbb{K}$ tais que $g(x') = x$ e $g(y') = y$. Então, como $xy = g(x') \cdot g(y')$ está definido e g é lugar, $g(x' \cdot y') = g(x') \cdot g(y') = xy$. Além disso, $\phi(x) \cdot \phi(y) = f(x') \cdot f(y')$ está definido e portanto obtemos $\phi(xy) = \phi(g(x' \cdot y')) = f(x' \cdot y') = f(x') \cdot f(y') = \phi(x) \cdot \phi(y)$.

Para concluir o teorema, considere $\psi : \mathbb{M} \to \mathbb{L}$ função tal que $f = \psi \circ g$. Dado $x \in \mathbb{M}$, seja $x' \in \mathbb{K}$ tal que $g(x') = x$. Temos $\psi(x) = \psi(g(x')) = f(x') = \phi(g(x')) = \phi(x)$, o que prova $\psi = \phi$.

∎

Definição 104. *Nas notações do teorema anterior, dizemos que $f \preccurlyeq g$ se as condições equivalentes da mesma são satisfeitas. Se $f \preccurlyeq g$ e $g \preccurlyeq f$, dizemos que f e g são equivalentes.*

Teorema 105. *Nas notações do teorema anterior, são equivalentes:*

1) f e g são equivalentes.
2) $f^{-1}(\mathbb{L}) = g^{-1}(\mathbb{M})$.

3) Existe $\phi : \mathbb{M} \to \mathbb{L}$ bijetora tal que $f = \phi \circ g$.
4) Existe $\phi : \mathbb{M} \to \mathbb{L}$ tal que $f = \phi \circ g$ e $\phi^{-1}(\mathbb{L}) = \mathbb{M}$.

Demonstração. $(1 \implies 2)$: Da hipótese e da definição de equivalência, temos $f \preccurlyeq g$ e $g \preccurlyeq f$. Então, $f^{-1}(\mathbb{L}) \subseteq g^{-1}(\mathbb{M}) \subseteq f^{-1}(\mathbb{L})$, isto é, $f^{-1}(\mathbb{L}) = g^{-1}(\mathbb{M})$.

$(2 \implies 3)$: Tiramos como caso particular da hipótese que $f^{-1}(\mathbb{L}) \subseteq g^{-1}(\mathbb{M})$ e portanto, do teorema 103, existe uma única $\phi : \mathbb{M} \to \mathbb{L}$ tal que $f = \phi \circ g$. Iremos mostrar que ϕ é bijetora. Seja $x \in \mathbb{M}$ tal que $\phi(x) = \infty$ e $x' \in \mathbb{K}$ tal que $g(x') = x$. Temos $f(x') = \phi(g(x')) = \phi(x) = \infty$ e então, $x' \notin f^{-1}(\mathbb{L}) = g^{-1}(\mathbb{M})$ e portanto $x = g(x') = \infty$. Como provado anteriormente, isso é suficiente para garantir ϕ injetora, uma vez que já sabemos que ϕ é lugar. Para mostrar que ϕ é sobrejetora, considere $y \in \mathbb{L}$. Temos que existe $x' \in \mathbb{K}$ tal que $f(x') = y$. Então, para $x = g(x')$, temos $\phi(x) = \phi(g(x')) = f(x') = y$ e ϕ é sobrejetora.

$(3 \implies 4)$: Tome ϕ como na hipótese e note que de ϕ lugar temos $\phi^{-1}(\mathbb{L}) \subseteq \mathbb{M}$. Agora seja $x \in \mathbb{M}$. Como $x \neq \infty$ e $\phi(\infty) = \infty$ temos, de ϕ injetora, $\phi(x) \neq \infty$ e portanto $x \in \phi^{-1}(\mathbb{L})$.

$(4 \implies 1)$: É imediato da definição que $f \preccurlyeq g$. Além disso, do que vimos, a condição $\phi^{-1}(\mathbb{L}) = \mathbb{M}$ é equivalente à ϕ ser injetora, e portanto ϕ admite uma inversa à esquerda ψ. Aplicando ψ na equação da hipótese, obtemos $\psi \circ f = \psi \circ \phi \circ g = g$ e logo $g \preccurlyeq f$, o que prova f equivalente à g.

■

Teorema 106. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos e f um lugar sobrejetor de $\mathbb{K}$ em $\mathbb{L}$. Então $\mathcal{O}_f := f^{-1}(\mathbb{L})$ é um anel de valoração de $\mathbb{K}$, denominado* anel de valoração associado a f*. Nesse caso, $f|_{\mathcal{O}_f}$ é um homomorfismo de $\mathcal{O}_f$ em $\mathbb{L}$ com núcleo $\mathfrak{M}_{\mathcal{O}_f}$. Além disso, dado $\mathbb{M}$ um corpo e g um lugar sobrejetor de $\mathbb{K}$ em $\mathbb{M}$, $\mathcal{O}_f = \mathcal{O}_g$ se, e somente se, f e g são equivalentes. Reciprocamente, todo anel de valoração de $\mathbb{K}$ é associado a algum lugar sobrejetor de $\mathbb{K}$ em algum corpo.*

Demonstração. Se $x, y \in \mathcal{O}_f$, temos $f(x) \in \mathbb{L}$ e $g(x) \in \mathbb{L}$, e portanto $f(x-y) = f(x) - f(y) \in \mathbb{L}$ e $f(xy) = f(x) \cdot f(y) \in \mathbb{L}$. Temos que $\mathcal{O}_f$ é subanel de $\mathbb{K}$. Além disso, dado $x \in \mathbb{K}$, temos $f(x) \in \mathbb{L}$ ou $f(x) = \infty$. No primeiro caso $x \in \mathcal{O}_f$ e no segundo caso $f(x^{-1}) = 0$, logo $x^{-1} \in \mathcal{O}_f$. Seja $g = f|_{\mathcal{O}_f}$ e note que dados $x, y \in \mathcal{O}_f$, $f(x), f(y) \in \mathbb{L}$ e portanto $g(x+y) = f(x+y) = f(x)+f(y) = g(x)+g(y)$ e $g(xy) = f(xy) = f(x) \cdot f(y) = g(x) \cdot g(y)$. Também, se $g(x) = 0$, temos $f(x) = 0$ e portanto $f(x^{-1}) = \infty$. Disso, $x \notin \mathrm{Inv}(\mathcal{O}_f)$ e então, $x \in \mathfrak{M}_{\mathcal{O}_f}$. Reciprocamente, se $x \in \mathfrak{M}_{\mathcal{O}_f}$, temos que $x^{-1} \notin \mathcal{O}_f$. Então, $f(x^{-1}) = \infty$ e portanto

$f(x) = 0$. Obtemos $g(x) = 0$ e $x \in \mathrm{Ker}(g)$. Do teorema 105, temos $\mathcal{O}_f = \mathcal{O}_g \Leftrightarrow f^{-1}(\mathbb{L}) = f^{-1}(\mathbb{M}) \Leftrightarrow f$ e g são equivalentes. Para a recíproca, considere $\mathcal{O}$ um anel de valoração de $\mathbb{K}$. Tomando $\mathbb{L} = \mathcal{K} = \mathcal{O}/\mathfrak{M}_{\mathcal{O}}$ como na definição 80, considere a projeção canônica $\pi : \mathcal{O} \to \mathbb{L}$. Defina uma função $f : \widetilde{\mathbb{K}} \to \widetilde{\mathbb{L}}$ da seguinte forma: $f(x) = \pi(x)$ para $x \in \mathcal{O}$ e $f(x) = \infty$ caso contrário. Sejam $x, y \in \widetilde{\mathbb{K}}$ e suponha que $f(x)+f(y)$ e $x+y$ estejam definidas. Se $x = \infty$, $f(x) = \infty$, o que resulta em $y \neq \infty$ e $f(y) \neq \infty$. Então, $f(x+y) = \infty = \infty+f(y) = f(x)+f(y)$. Se $y = \infty$, temos $f(x + y) = f(y + x) = f(y) + f(x) = f(x) + f(y)$. Caso $x, y \in \mathcal{O}$, temos que $x + y \in \mathcal{O}$ e então, $f(x + y) = \pi(x + y) = \pi(x) + \pi(y) = f(x) + f(y)$. Suponha agora que xy e $f(xy)$ estejam definidos. Caso $x = \infty$, $f(x) = \infty$ e então concluímos que $y \neq 0$ e $f(y) \neq 0$. Então, $xy = \infty$ e $f(xy) = \infty = \infty \cdot f(y) = f(x) \cdot f(y)$. Se $y = \infty$, temos $f(xy) = f(yx) = f(y) \cdot f(x) = f(x) \cdot f(y)$. Caso $x \neq \infty$ e $y \neq \infty$, temos $x, y \in \mathcal{O}$ e logo $f(xy) = \pi(xy) = \pi(x) \cdot \pi(y) = f(x) \cdot f(y)$. Finalmente, $1 \in \mathcal{O}$, logo $f(1) = \pi_1 = 1_{\mathbb{L}}$, mostrando que f é lugar de $\mathbb{K}$ em $\mathbb{L}$.

$\blacksquare$

9 TEOREMA DE EXTENSÃO

Até o presente momento, desenvolvemos a teoria de valorações sem nos focar muito em possíveis aplicações da mesma. Apesar disso, tais aplicações existem em outras teorias da matemática, e as próximas seções às trarão. Além de vermos como as valorações, estudadas até agora, nos ajudam a encontrar resultados em outras teorias, também veremos que estas naturalmente "retribuem", nos dando mais resultados sobre valorações. Nessa sessão, nos ateremos a provar o chamado Teorema de Extensão e estudar suas consequências para nos ajudar nesse objetivo.

Por hora, fixaremos algumas notações. Dado um anel comutativo com unidade A, denotaremos seu anel de polinômios (em uma variável X) por $A[X]$. Nesse caso, como já é conhecido, para qualquer anel comutativo com unidade B, qualquer homomorfismo $f : A \to B$ e qualquer $x \in B$, existe um único homomorfismo $\phi : A[X] \to B$ tal que $f = \phi_A$ e $\phi(X) = x$. Denotaremos $\mathrm{Im}(\phi)$ por $A_f[x]$. Normalmente, f ficará explícita no contexto e denotaremos $\mathrm{Im}(\phi)$ simplesmente por $A[x]$, em particular esse será o caso quando $A \subseteq B$, no qual consideraremos f como sendo a inclusão canônica de A em B a não ser que se diga o contrário.

Teorema 107. *Seja A um anel comutativo com unidade e I um ideal de A. Se B é um anel comutativo que contém A como subanel unitário (isto é, $1_A = 1_B$) e $x \in B$, então $I[x] := \left\{ \sum_{i=0}^{n} a_n x^n ; n \in \mathbb{N}, a_n \in I \right\}$ é ideal de $A[x]$. Em particular, $I[X]$ é ideal de $A[X]$.*

Demonstração. Tome $p, q \in I[x]$. Então, para $a_0, ..., a_n, b_0, ..., b_m \in I$ convenientes, $p = \sum_{i=0}^{n} a_i x^i$ e $q = \sum_{j=0}^{m} b_j x^j$. Então, com $a_i = 0$ para $i > n$ e $b_i = 0$ para $i > m$, $p + q = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i \in I[x]$. Além disso, se $r = \sum_{k=0}^{o} c_k x^k \in A[x]$ temos $pr = \sum_{i=0}^{n} \sum_{k=0}^{o} a_i c_k x^{i+k}$. Como cada $a_i c_k \in I$, temos que cada $a_i c_k x^{i+k} \in I[x]$ e portanto $pr \in I[x]$, pois $I[x]$ é anel. Concluímos que $I[x]$ é ideal de $A[x]$. Para mostrar que $I[X]$ é ideal de $A[X]$, tome $B = A[X]$ e $x = X$, e aplique o resultado que obtemos. ∎

Teorema 108. *Sejam $\mathbb{K}$ um corpo, A um subanel unitário de $\mathbb{K}$ e*

I ideal próprio de A. Então dado $x \in \mathbb{K}^*$, temos $I[x] \neq A[x]$ ou $I[x^{-1}] \neq A[x^{-1}]$.

Demonstração. Suponha, por absurdo, que $I[x] = A[x]$ e $I[x^{-1}] = A[x^{-1}]$. Então $1 \in I[x]$, para $a_i, b_j \in I$ convenientes temos $1 = \sum_{i=0}^{n} a_i x^i = \sum_{j=0}^{m} b_j x^{-j}$. Podemos tomar m e n os menores possíveis e vamos supor inicialmente que $m \leq n$. Note que $1 - a_0 = \sum_{i=1}^{n} a_i x^i$ e $1 - b_0 = \sum_{j=1}^{m} b_j x^{-j}$ e considere o elemento $p = \sum_{i=1}^{n-1}(1 - b_0)a_i x^i + \sum_{j=n-m}^{n-1} a_n b_{n-j} x^j = (1-b_0)\sum_{i=1}^{n-1} a_i x^i + a_n \sum_{j=n-m}^{n-1} b_{n-j} x^j$. O passo que faremos abaixo pode ser visto como uma "mudança de variável" $j \to n-j$. É possível ver que, de fato, as duas expressões são equivalentes.

$$p = (1-b_0)\sum_{i=1}^{n-1} a_i x^i + a_n \sum_{j=1}^{m} b_j x^{n-j} = (1-b_0)\sum_{i=1}^{n-1} a_i x^i + a_n x^n \sum_{j=1}^{m} b_j x^{-j} =$$
$$= (1-b_0)(1-a_0-a_n x^n) + a_n x^n (1-b_0) = (1-b_0)(1-a_0-a_n x^n + a_n x^n) =$$
$$= (1-b_0)(1-a_0) = 1 - a_0 - b_0 + a_0 b_0.$$

Note então que $p + a_0 + b_0 - a_0 b_0 = 1$. Lembrando que p foi definido como duas somas, podemos juntar as duas somas e a expressão $a_0 + b_0 - a_0 b_0$ em um único somatório, obtendo algo da forma $\sum_{k=0}^{n-1} c_k x^k$ e como cada a_i e cada b_i está em I, concluímos que cada c_i também está em I, mas isso contradiz a minimalidade de n. Concluímos que $n < m$, mas o mesmo argumento, substituindo x por x^{-1} e vice-versa nos resulta em uma contradição semelhante com a minimalidade de m. Por absurdo, o resultado é verdadeiro.

■

Definição 109. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos com $\mathbb{L}$ algebricamente fechado, isto é, $\mathbb{L}$ contém uma raiz de cada polinômio em $\mathbb{L}[X]$. Defina o conjunto $\mathcal{R}(\mathbb{K}, \mathbb{L})$ de todos o pares da forma (A, f) tais que A é subanel de $\mathbb{K}$ e $f : A \to \mathbb{L}$ é homomorfismo. Ainda, defina a relação $\leq$ em $\mathcal{R}(\mathbb{K}, \mathbb{L})$ por $(A, f) \leq (B, g)$ se, e somente se, $A \subseteq B$ e $g|_A = g$.*

Teorema 110. *Nas notações acima, $\leq$ é uma relação de ordem. Além disso, $Ker(f)$ é um ideal primo de A.*

Demonstração. De fato, $A \subseteq A$ e $f|_A = f$, logo $(A, f) \leq (A, f)$. Além disso, se $(A, f) \leq (B, g)$, então $A \subseteq B \subseteq A$ e $f = g|_A = g|_B = g$, logo $(A, f) = (B, g)$. Finalmente, se $(A, f) \leq (B, g)$ e $(B, g) \leq (C, h)$, então $A \subseteq B \subseteq C$ e para $x \in A \subseteq B$, $h|_A(x) = h(x) = h|_b(x) = g(x) = g_A(x) = f(x)$ de onde resulta $(A, f) \subseteq (C, h)$.

Que $I = \mathrm{Ker}(f)$ é ideal de A sai da teoria de anéis. Para mostrar que I é primo, o que sairá como consequência de $\mathbb{L}$ ser domínio de integridade, considere $x, y \notin I$. Como x e y não estão no núcleo de f, $f(x) \neq 0$ e $f(y) \neq 0$. Mas então, $f(xy) = f(x)f(y) \neq 0$ e $xy \neq I$.

■

A demonstração do teorema a seguir pode ser encontrada na referência principal [1].

Teorema 111. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos com $\mathbb{L}$ algebricamente fechado. Dados $(A, f) \in \mathcal{R}(\mathbb{K}, \mathbb{L})$ e $x \in \mathbb{K}$, existe $(B, g) \in \mathcal{R}(\mathbb{K}, \mathbb{L})$ tal que $(A, f) \leq (B, g)$ e $\{x, x^{-1}\} \cap B \neq \emptyset$.*

Teorema 112. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos com $\mathbb{L}$ algebricamente fechado. Então existe uma bijeção entre o conjunto de todos os lugares de $\mathbb{K}$ em $\mathbb{L}$ e o conjunto dos elementos maximais de $\mathcal{R}(\mathbb{K}, \mathbb{L})$.*

Demonstração. Seja S o conjunto dos lugares de $\mathbb{K}$ em $\mathbb{L}$ e T o conjunto dos elementos maximais de $\mathcal{R}(\mathbb{K}, \mathbb{L})$. Lembrando que para cada $f \in S$ definimos anteriormente $\mathcal{O}_f := f^{-1}(\mathbb{L})$, defina a função $\phi : S \to T$ por $\phi(f) = (\mathcal{O}_f, f|_{\mathcal{O}_f})$. Essa função está bem definida pois se existir $(B, g) \in \mathcal{R}(\mathbb{K}, \mathbb{L})$ tal que $(\mathcal{O}_f, f|_{\mathcal{O}_f}) \leq (B, g)$ e $\mathcal{O}_f \neq B$ temos que para $x \in B \setminus \mathcal{O}_f$, $f(x) = \infty$. Mas então, $f(x^{-1}) = 0$ e $x^{-1} \in \mathcal{O}_f \subseteq B$ e então $g(x^{-1}) = 0$. Como g é homomorfismo, temos $0 = 0 \cdot g(x) = g(x^{-1}) \cdot g(x) = g(x^{-1}x) = g(1) = 1$, o que é uma contradição. Notando que basta saber o valor de f em $\mathcal{O}_f$ para determinar toda a f (nos demais pontos x, $f(x) = \infty$) concluímos que ϕ é injetora. Para mostrar que ϕ é sobrejetora, considere $(A, f) \in T$. Dado $x \in \mathbb{K}^*$, temos que ter $x \in A$ ou $x^{-1} \in A$, pois caso o contrário, o teorema 111 nos garante que é possível estender (A, f), contradizendo a maximalidade de (A, f). Disso, concluímos que A é um anel de valoração. Defina $\hat{f} : \widetilde{\mathbb{K}} \to \widetilde{\mathbb{L}}$ como o lugar de $\mathbb{K}$ em $\mathbb{L}$ que estende f e tal que $\hat{f}(x) = \infty$ para $x \in \mathbb{K} \setminus A$. É imediato que $\mathcal{O}_{\hat{f}} = A$ e $\hat{f}|_A = f$, provando o teorema.

■

Disso, obtemos uma maneira de encontrar os lugares de $\mathbb{K}$ em $\mathbb{L}$: São os lugares associados a um elemento maximal de $\mathcal{R}(\mathbb{K}, \mathbb{L})$. Normalmente, encontrar elementos maximais exige o uso do Lema de Zorn, e de fato, faremos justamente isso abaixo.

Teorema 113. *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos com* $\mathbb{L}$ *algebricamente fechado. Então para todo* $(A, f) \in \mathcal{R}(\mathbb{K}, \mathbb{L})$, *existe* $(A', f') \in \mathcal{R}(\mathbb{K}, \mathbb{L})$ *tal que* (A', f') *é maximal e* $(A, f) \leq (A', f')$.

Demonstração. Seja $S = \{(B, g) \in \mathcal{R}(\mathbb{K}, \mathbb{L}); (A, f) \leq (B, g)\}$. Se T é um subconjunto totalmente ordenado de S, considere $B' = \bigcup_{(B,g)\in T} B$. Claramente, $B' \subseteq \mathbb{K}$ e $B \subseteq A'$. Agora, dados $x, y \in B'$, temos que para $(B_1, g_1), (B_2, g_2) \in T$ convenientes, $x \in B_1$ e $y \in B_2$. Mas T é totalmente ordenado, logo $B_1 \subseteq B_2$ ou $B_2 \subseteq B_1$. Em ambos os casos, $B = B_1 \cup B_2 \in \{B_1, B_2\}$ e então, $x, y \in B$. Concluímos $x - y, xy \in B \subseteq B'$ e logo B' é anel. Defina $g' : B' \to \mathbb{L}$ da seguinte forma: dado $x \in B'$, escolha $(B, g) \in T$ com $x \in B$, e defina $g'(x) = g(x)$. Note que essa definição não depende da escolha de B, pois T é totalmente ordenado e em qualquer outra escolha (C, h) teríamos que g estende h ou que h estende g. Note também que dados $x, y \in B'$, escolhendo $(B, g) \in T$ tal que $x, y \in B$, temos $g'(x + y) = g(x + y) = g(x) + g(y) = g'(x) + g'(y)$, $g'(xy) = g(xy) = g(x)g(y) = g'(x)g'(y)$ e $g'(1) = g(1) = 1$ e portanto g' é um homomorfismo. Finalmente, para $(B, g) \in T$ e $x \in B$, temos $g'(x) = g(x)$, logo $g'|_B = g$ e $(B, g) \leq (B', g')$, isto é, (B', g') é cota superior de T em S. Do Lema de Zorn, S admite elemento maximal (A', f'), como queríamos demonstrar.

■

Teorema 114. *(Teorema de Extensão) Sejam* $\mathbb{K}, \mathbb{L}$ *corpos com* $\mathbb{L}$ *algebricamente fechado e* $(A, f) \in \mathcal{R}(\mathbb{K}, \mathbb{L})$. *Então existe um lugar de* $\mathbb{K}$ *em* $\mathbb{L}$ *que estende* f. *Além disso, dado um ideal primo* $\mathfrak{P}$ *de* A, *existe um anel de valoração* B *de* $\mathbb{K}$ *tal que* $A \subseteq B$ *e* $\mathfrak{P} = \mathfrak{M}_B \cap A$.

Demonstração. Seja $(A', f') \in \mathcal{R}(\mathbb{K}, \mathbb{L})$ maximal tal que $(A, f) \leq (A', f')$. Como (A', f') é maximal, do teorema anterior, podemos estender f' a um lugar $\hat{f}$ de $\mathbb{K}$ em $\mathbb{L}$ definindo $\hat{f}(x) = \infty$ se $x \notin A'$. Fica claro que esse lugar estende f. Agora considere $\mathfrak{P}$ um ideal primo de A e $\pi : A \to A/\mathfrak{P}$ a projeção canônica. Considerando o fecho algébrico $\mathbb{L}$ de $A/\mathfrak{P}$, podemos estender π a um lugar $\hat{\pi}$ de $\mathbb{K}$ em $\mathbb{L}$ e tomar $B = \hat{\pi}^{-1}(\mathbb{L})$. Temos que B é anel de valoração e além disso, para $x \in A$, $\hat{\pi}(x) = \pi(x) \in A/\mathfrak{P} \subseteq \mathbb{L}$. Concluímos que $A \subseteq B$. Finalmente, note que $x \in \mathfrak{M}_B$ se, e somente se, $\hat{\pi}(x) \neq 0$. Então, $x \in \mathfrak{P} \Leftrightarrow x \in \mathfrak{M}_B \cap A$.

■

10NOÇÕES DE MÓDULO

No próximo capítulo, precisaremos utilizar módulos. Para isso, faremos aqui uma breve introdução à teoria, como temos feito até o momento. A ideia de um módulo é similar a de um espaço vetorial, mas em vez de termos escalares em um corpo (ou especificamente subcorpos de $\mathbb{C}$, em algumas abordagens), nossos escalares estarão em um anel, que não necessariamente precisará ter unidade.

Definição 115. *Seja A um anel. Um A-*módulo (à esquerda) *é um grupo abeliano M munido de uma função $\cdot : A \times M \to M$, denominada* multiplicação por escalar*, que tem as seguintes propriedades, para todos $\lambda, \mu \in A$ e $x, y \in M$:*

1) $(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$,
2) $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot y$,
3) $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$,
4) Se A possui unidade 1_A, então $1_A \cdot x = x$.

Observação 116. *Normalmente, denotaremos $\lambda \cdot x$ por λx.*

É fácil ver que todo espaço vetorial sobre $\mathbb{K}$ é um $\mathbb{K}$-módulo. Além disso, veremos abaixo alguns exemplos vindos da teoria de anéis. Em todos os exemplos abaixo, A é um anel.

Exemplo 117. *A é um A-módulo, se considerarmos A como um grupo abeliano com a sua operação de adição.*

Exemplo 118. *Se B é subanel de A, então A é um B-módulo com o produto por escalar definido como a multiplicação em A.*

Exemplo 119. *Suponha que A seja um anel e S um conjunto e considere o anel B das funções de S em A com as operações pontuais. Podemos considerar A' como o subanel de B das funções constantes. Sabe-se que A é isomorfo a A' e o A'-módulo seguindo o exemplo acima pode ser transformado em um A-módulo definindo $(\lambda f)(x) = (\iota(\lambda)f)(x) = \lambda f(x)$, onde ι leva $\lambda \in A$ na função constante que leva cada $x \in S$ em λ.*

Exemplo 120. *Seja I um ideal de A. Podemos ver A como um I-módulo, mas também podemos ver I como um A-módulo, uma vez que a multiplicação em A leva um elemento de A e um elemento de I em um elemento de I.*

Também precisaremos da definição de um sub-módulo.

Definição 121. *Seja A um anel e M um A-módulo. Um subconjunto N é dito um A-*submódulo de *M quando N for um subgrupo de M e para quaisquer $\lambda \in A, x \in N$ vale $\lambda x \in N$.*

Como é comum na álgebra, podemos caracterizar um submódulo da seguinte forma, cuja demonstração é trivial:

Teorema 122. *Seja A um anel e M um A-módulo. Então $N \subseteq M$ é um A-submódulo se, e somente se, N for um A-módulo com as operações do módulo M restritas à N.*

A noção de base, muito estudada em espaços vetoriais, não nos interessará aqui, mas a noção de conjunto gerador será útil.

Definição 123. *Seja A um anel, M um A-módulo e $S \subset M$ não vazio. Defina*

$$span(S) := \left\{ \sum_{i \in S'} \lambda_i \cdot i; S' \subset S \text{ finito e } \lambda_i \in A \right\}$$

Para cada $x \in span(S)$, dizemos que S gera *x. Dizemos que S* gera *M quando $M = span(S)$. Além disso, se M é gerado por algum conjunto finito, diremos que M* é finitamente gerado.

Exemplo 124. *Note que não definimos dimensão. Essa definição é delicada, pois, por exemplo, diferente de um espaço vetorial, nem todo módulo tem um conjunto gerador minimal, por exemplo. Evitaremos a discussão geral sobre dimensão de um módulo arbitrário.*

A seguinte afirmação será útil na próxima seção:

Teorema 125. *Considere A, B anéis tais que $B \subseteq A$ e M um A-módulo. Então M é um B-módulo com as operações restritas de A e se M é finitamente gerado como A-módulo e A é finitamente gerado como B-módulo, então M é finitamente gerado como B-módulo.*

Demonstração. Fica claro que M é um B-módulo. Para mostrar que M é finitamente gerado como B-módulo, considere geradores finitos $G = \{x_1, ..., x_n\}$ de M como A-módulo e $H = \{\lambda_1, ..., \lambda_m\}$ de A como B-módulo. Afirmamos que $I = \{\lambda x; \lambda \in H, x \in G\}$ é um gerador de M. De fato, dado $m \in M$, temos que $m = \sum_{i=1}^{n} \lambda_i x_i$ para $\lambda_i \in A$ convenientes e cada λ_i se escreve como $\lambda_i = \sum_{j=1}^{m} \mu_{i,j} \lambda_i$ com $\mu_{i,j} \in B$

convenientes. Então, escrevemos $m = \sum_{i=1}^{n} \sum_{m=1}^{m} \mu_{i,j} \lambda_j x_i$, mostrando que I é gerador de M. ■

11ELEMENTOS INTEGRAIS

Quando estudamos polinômios com coeficientes em um corpo, é importante estudar os elementos algébricos desse corpo. Se x é algébrico, então ele é raiz de um polinômio $\sum_{i=0}^{n} a_i X^i$ com $a_n \neq 0$. Podemos dividir cada coeficiente desse polinômio por a_n e concluir que x é raiz de um polinômio mônico. Quando estudamos polinômios com coeficientes em um domínio de integridade, não podemos necessariamente fazer isso o que quer dizer que nem todo elemento algébrico é raiz de um polinômio mônico. Estudaremos nessa seção os elementos que são dessa forma.

Definição 126. *Sejam A e B domínios de integridade tais que $A \subset B$ e $x \in B$. x é dito* integral sobre A *se x é raiz de um polinômio mônico de $A[X]$. Além disso, o conjunto $I_B(A)$ de todos os elementos de B integrais sobre A é denominado* fecho integral de A em B. *Se todo elemento de B for integral sobre A, diremos que B é* integral sobre A.

Observação 127. *Note que B é integral sobre A se, e somente se, $I_B(A) = B$.*

Iremos caracterizar elementos integrais de duas formas. Para isso, precisamos da seguinte definição, relacionada com a Teoria de Módulos:

Definição 128. *Sejam A e B domínios de integridade tal que $B \subseteq A$. Então B é dita uma* extensão finita de A *se B (visto como A-módulo) for finitamente gerado.*

Teorema 129. *Sejam A e B domínios de integridade tais que $B \subseteq A$. Dado $x \in B$, as seguintes condições são equivalentes:*

1) x é integral sobre A.

2) $A[x]$ é extensão finita de A.

3) Existe um A-módulo não nulo M que é extensão finita de B tal que

$$x \cdot M := \{xm; m \in M\} \subseteq M$$

Demonstração. ($1 \implies 2$) Seja $p = \sum_{i=0}^{n} a_i X^i$ um polinômio de $A[X]$ tal que x seja raiz desse polinômio e $a_n = 1$. Afirmamos que $G = \{1, x, x^2, ..., x^{n-1}\}$ gera $A[x]$. Provaremos essa afirmação em três partes. Primeiro, note que x^n é gerado por G. De fato, $x^n = a_n x^n = \sum_{i=0}^{n-1} -a_i x^i$.

Agora, se $k \in \mathbb{N}$ é tal que G gera x^{n+k}, então considere $b_0, ..., b_{n-1} \in A$ tais que $x^{n+k} = \sum_{i=0}^{n-1} b_i x^i$. Temos

$$x^{n+k+1} = xx^{n+k} = x\sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{n-1} b_i x^{i+1} = \sum_{i=0}^{n-2} b_i x^{i+1} + b_{n-1}x^n =$$
$$= \sum_{i=0}^{n-2} b_i x^{i+1} + b_{n-1}\sum_{i=0}^{n-1} -a_i x^i$$

Juntando as duas expressões em um único somatório, mostramos que G gera x^{n+k+1}. Por indução, G gera todos monômios mônicos de grau pelo menos n. Como $x^i \in G$ para $i < n$, G gera todos os monômios mônicos. Como todo elemento de $A[x]$ é uma combinação linear de monômios mônicos, temos que G gera $A[x]$ e de G finito, concluímos que $A[x]$ é extensão finita de A.

($2 \implies 3$) Tome $M = A[x]$, que é extensão finita por hipótese. Como nesse caso M é anel e $x \in M$, temos $x \cdot M \subseteq M$.

($3 \implies 1$) Suponha que M seja finitamente gerado e considere um conjunto gerador $G = \{x_1, ..., x_n\}$. Da hipótese, para $i \in \{1, ..., n\}$, $xx_i \in M$, logo xx_i pode ser escrito como $xx_i = \sum_{j=1}^{n} \lambda_{i,j} x_j$. Considerando $v = (x_1, ..., x_n)$ e $M = [\lambda_{i,j}]$, temos $xv = Mv$, onde as operações de multiplicação por escalar e multiplicação matriz-vetor são definidas da maneira usual. Como estabelecido na referência, essa equação de auto-valores implica que x é raiz de um polinômio mônico com coeficientes em A, obtido através do determinante de $M - xI$, onde I é a matriz identidade de mesma ordem que M e o determinante é definido de forma análoga a da álgebra linear.

■

Corolário 130. *Sejam A e B domínios de integridade tais que $B \subseteq A$. Se $x_1, ..., x_n \in I_B(A)$, então $A[x_1, ..., x_n]$ é uma extensão finita de A.*

Demonstração. Para $i \in \{1, ..., n\}$, defina $A_i = A[x_1, ..., x_i]$. Do teorema 129, A_1 é extensão finita de A. Agora suponha que para algum i, A_i seja extensão finita de A. Temos que x_{i+1} é raiz de um polinômio mônico de $A \subseteq A_i$, logo x_{i+1} é integral em A_i e portanto A_{i+1} é extensão finita de A_i. Como A_i é extensão finita de A, temos A_{i+1} extensão finita de A_i.

■

Teorema 131. *Sejam A e B domínios de integridade tais que $B \subseteq A$. Então $A \subseteq I_B(A) \subseteq B$ e $I_B(A)$ é um anel. Além disso, se A' é anel tal que $A \subseteq A' \subseteq B$, então $I_B(A) = I_B(I_{A'}(A)) \subseteq I_B(A')$ e se B é integral sobre A' e A' é integral sobre A, então B é integral sobre A.*

Demonstração. Por definição, $I_B(A) \subseteq B$ e dado $x \in A$, x é raiz do polinômio mônico $X \in A[X]$, logo $x \in I_B(A)$ e $A \subseteq I_B(A)$. Para mostrar que $I_B(A)$ é anel, basta mostrar que é subanel de B. Considere $x, y \in I_B(A)$. Temos que $A[x, y]$ é finitamente gerado. Considere G um gerador finito de $A[x, y]$. Do teorema binomial, $(x - y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i (-y)^{n-i} \in A[x, y]$, logo cada $(x - y)^n$ é gerado por G. Então, como um elemento de $A[x - y]$ é uma combinação linear dos $(x - y)^n$ com coeficientes em A, temos que G gera $A[x - y]$ e $x - y$ é integral sobre A. Semelhantemente, $(xy)^n = x^n y^n \in A[x, y]$ e concluímos que G gera $A[xy]$, logo xy é integral sobre A e $I_B(A)$ é anel.

Seja $x \in I_B(A)$. Então x é raiz de um polinômio mônico de $A[X]$ e logo é raiz de um polinômio mônico em $I_{A'}(A)[X]$, isto é, $I_B(A) \subseteq I_B(I_{A'}(A))$. Também, como $I_{A'}(A) \subseteq A'$, temos, pelo mesmo motivo, $I_B(I_{A'}(A)) \subseteq I_B(A')$. Para provar $I_B(A) = I_B(I_{A'}(A))$, só nos resta mostrar uma das inclusões. Seja $x \in I_B(I_{A'}(A))$. Então existe um $I_B(I_{A'}(A))$-módulo M tal que $x \cdot M = M \subseteq B$. Sabemos que M é módulo, logo a adição é fechada em M. Além disso, se $y \in M$ e $\lambda \in A \subseteq I_B(I_{A'}(A))$, $\lambda y \in M$ e M é A-módulo, provando que x é integral sobre A e a igualdade segue.

Finalmente, suponha que B seja integral sobre A' e A' seja integral sobre A. Temos $I_B(A') = B$ e $I_{A'}(A) = A'$, e do que acabamos de provar, $I_B(A) = I_B(I_{A'}(A)) = I_B(A') = B$ e B é integral sobre A.

■

Agora, iremos mostrar um resultado relacionando anéis de valoração e elementos integrais. Este será dada via anéis integralmente fechados, como definido abaixo. Estaremos interessados no caso em que B for corpo.

Definição 132. *Sejam A e B domínios de integridade tais que $A \subset B$. A é dito* integralmente fechado *em B se $I_B(A) = A$. Nesse caso, quando B for o corpo de frações de A, diremos simplesmente que A é* integralmente fechado.

Lema 133. *Todo anel de valoração é integralmente fechado.*

Demonstração. Seja $\mathcal{O}$ um anel de valoração de um corpo $\mathbb{K}'$ e $\mathbb{K}$ o corpo de frações de $\mathcal{O}$. Como $\mathcal{O} \subseteq \mathbb{K}'$, podemos supor, por um isomorfismo conveniente, que $\mathbb{K} \subseteq \mathbb{K}'$. Agora, note que dado $x \in \mathbb{K}$, temos $x \in \mathbb{K}'$ e portanto $x \in \mathcal{O}$ ou $x^{-1} \in \mathcal{O}$. Então, $\mathcal{O}$ é um anel de valoração de $\mathbb{K}$. Considere $x \in \mathbb{K}^*$ integral sobre $\mathcal{O}$. Temos que para alguma escolha de $n \in \mathbb{N}$ e $a_1, ..., a_{n-1} \in \mathcal{O}$ com $a_n = 1$, $\sum_{i=0}^{n} a_i x^i = 0$. Então, $x^n = \sum_{i=1}^{n-1} a_i x^i$, isto é, $x = \sum_{i=1}^{n-1} a_i x^{i-n}$. Suponha por absurdo que $x \notin \mathcal{O}$. Então $x^{-1} \in \mathcal{O}$ e como para $i \in \{0, ..., n-1\}$ temos $i - n < 0$, e portanto $x^{i-n} \in \mathcal{O}$. Concluímos $x \in \mathcal{O}$, o que contradiz a hipótese e nos leva a concluir que, de fato, $x \in \mathcal{O}$. Como $0 \in \mathcal{O}$, temos que $\mathcal{O}$ é integralmente fechado.

■

Teorema 134. *Seja A um domínio de integridade e seja $\mathbb{K}$ um corpo que contém A. Se V é o conjunto dos aneis de valoração de L que contém A e V' é o conjunto dos $\mathcal{O} \in V$ tais que $\mathfrak{M}_{\mathcal{O}} \cap A$ é um ideal maximal de A, então $I_{\mathbb{K}}(A) = \bigcap_{\mathcal{O} \in V} \mathcal{O} = \bigcap_{\mathcal{O} \in V'} \mathcal{O}$.*

Demonstração. Seja $x \in I_{\mathbb{K}}(A)$ e $B \in V$, e note que B é integralmente fechado, pelo lema. Então, $x \in I_{\mathbb{K}}(A) \subseteq I_{\mathbb{K}}(\mathcal{O}) = \mathcal{O}$ e logo $I_{\mathbb{K}}(A) \subseteq \mathcal{O}$. Então, $I_{\mathbb{K}}(A) \subseteq \bigcap_{\mathcal{O} \in V} \mathcal{O}$. Como $V' \subseteq V$, segue diretamente que $\bigcap_{\mathcal{O} \in V} \mathcal{O} \subseteq \bigcap_{\mathcal{O} \in V'} \mathcal{O}$. Finalmente, considere $x \in \mathbb{K} \setminus I_{\mathbb{K}}(A)$ e vamos provar que $x \notin \bigcap_{\mathcal{O} \in V'} \mathcal{O}$. Note primeiramente que dado um elemento $p = \sum_{i=0}^{n} a_i x^{-i} \in A[x^{-1}]$, temos $x^n \cdot (x - p) = x^{n+1} - \sum_{i=0}^{n} a_i x^{n-i} \neq 0$, pois x não é integral sobre A, e portanto $x - p \neq 0$. Disso, x^{-1} não é inversível em $A[x^{-1}]$ e portanto está contido em um ideal maximal $\mathfrak{M}$ de $A[x^{-1}]$. Do Teorema de Extensão, existe algum anel de valoração $\mathcal{O}$ de $\mathbb{K}$ que contém $\mathfrak{M}$ e tal que $\mathfrak{M} = \mathfrak{M}_{\mathcal{O}} \cap A[x^{-1}]$. Notando que $A = A[x^{-1}] \cap A$, temos $\mathfrak{M} \cap A = \mathfrak{M}_{\mathcal{O}} \cap A$. Considere a função $\pi_A : A \to A[x^{-1}]/\mathfrak{M}$ levando cada elemento de A em sua classe de equivalência. Como $x^{-1} \in \mathfrak{M}$, temos que $\overline{\sum_{i=0}^{n} a_i x^{-1}} = \overline{a_0}$, e portanto π_A é sobrejetora. Como $\mathfrak{M}$ é ideal maximal em $A[x^{-1}]$, a imagem de π_A é um corpo, e portando, $\mathrm{Ker}(\pi_A) = \mathfrak{M} \cap A = \mathfrak{M}_{\mathcal{O}} \cap A$ é ideal maximal de A. Obtemos que $\mathcal{O} \in V'$ e $x \notin \mathcal{O}$. Concluímos $\bigcap_{\mathcal{O} \in V'} \mathcal{O} \subseteq A$, finalizando a demonstração.

■

Corolário 135. *Um subanel de um corpo $\mathbb{K}$ é integralmente fechado* *em $\mathbb{K}$ se, e somente se, for a interseção de algum conjunto de anéis de valoração de $\mathbb{K}$.*

Demonstração. Seja A subanel integralmente fechado em $\mathbb{K}$. Considerando V como no teorema 134, $A = I_{\mathbb{K}}(A) = \bigcap_{\mathcal{O}\in V} \mathcal{O}$. Reciprocamente, seja V o conjunto dos aneis de valoração de $\mathbb{K}$ que contém A e suponha que A seja a interseção de um conjunto $V_0 \subseteq V$. Então, $I_{\mathbb{K}}(A) = \bigcap_{\mathcal{O}\in V} \mathcal{O} \subseteq \bigcap_{\mathcal{O}\in V_0} \mathcal{O} = A \subseteq I_{\mathbb{K}}(A)$, provando o resultado.

■

12LOCALIZAÇÕES

Nessa breve sessão, nos desviaremos do que estávamos fazendo até agora para desenvolver o conceito de uma localização, que será usado na seção seguinte. Como esse é análogo ao que é feito para corpo de frações, iremos proceder mais rápido que o usual. Começaremos com a definição de um subconjunto multiplicativamente fechado.

Definição 136. *Seja A um anel e $S \subseteq A$. Então S é dito multiplicativamente fechado se $1 \in S$ e se dados $x, y \in S$, temos $xy \in S$.*

Faremos aqui a localização de um anel por um subconjunto multiplicativamente fechado dele que não contenha divisores do zero (incluindo o próprio zero). É possível estender essa definição para conjuntos que possivelmente contém divisores do zero, mas não precisaremos dessa versão mais geral. Intuitivamente, a localização será similar ao corpo de frações, mas apenas elementos de S serão permitidos no denominador. Formalmente, considere um anel comutativo com unidade A e S um subconjunto multiplicativo de A que não contém divisores do zero (e nem zero). Defina em $A \times S$ as seguintes operações:

$$(x, s) + (y, t) = (xt + ys, st)$$
$$(x, s) \cdot (y, t) = (xy, st)$$

Observe que essas operações estão bem definidas, pois S é multiplicativamente fechado, mas elas não necessariamente tornam $A \times S$ um anel. Para ver isso, tome $A = \mathbb{Z}$ e $S = \mathbb{Z}^*$ e observe que $(x, s) + (0, 1) = (0, 1) + (x, s) = (x, s)$, logo $(0, 1)$ seria o zero do suposto anel, mas $(0, 2) + (y, t) = (2y, 2t) \neq (0, 1)$, pois nenhum $t \in \mathbb{Z}^*$ satisfaz $2t = 1$, isto é, $(0, 2)$ não tem elemento oposto. Lembrando que o par (x, s) representa, intuitivamente, a fração $\frac{x}{s}$, é seguro pensar que queremos identificar os pares (x, s) e (y, t) precisamente quando $xt = ys$. De fato, isso pode ser feito usando relações de equivalência e partições, como de costume. Defina a relação $\sim$ em $A \times S$ da seguinte forma: $(x, s) \sim (y, t) \Leftrightarrow xt = ys$. Note que $xs = xs$, logo $(x, s) \sim (x, s)$ sempre vale e que $(x, s) \sim (y, t) \implies xt = ys \implies ys = xt \implies (y, t) \sim (x, s)$. Finalmente, note que $(x, s) \sim (y, t)$ e $(y, t) \sim (z, u) \implies xt = ys$ e $yu = zt \implies xtu = ysu = yus = zts$ e como o anel e comutativo e S não contém divisores do zero, podemos cancelar t e obter $xu = zs$, isto é, $(x, s) \sim (z, u)$, mostrando que $\sim$ é uma relação de equivalência.

Além disso, note que se $(x,s) \sim (x',s')$ e $(y,t) \sim (y',t')$, então

$$\begin{aligned} xs' = x's,\ yt' = y't \implies (xt+ys)(s't') = xts't' + yss't' = xs'tt' + yt'ss' = \\ = x'stt' + y'tss' = (x't'+y's')(ts) \implies (x,s)+(y,t) \sim (x',s')+(y',t') \end{aligned}$$

$$\begin{aligned} xs' = x's,\ yt' = y't \implies (xy)(s't') = xs'yt' = \\ = x'sy't = (x'y')(st) \implies (x,s)\cdot(y,t) \sim (x',s')\cdot(y',t') \end{aligned}$$

Disso, concluímos que as extensões das operações nas classes de equivalência estão bem definidas. Denotaremos a classe de equivalência de (x,s) por $\frac{x}{s}$ e então, por definição, temos $\frac{x}{s}+\frac{y}{t} = \frac{xt+ys}{st}$ e $\frac{x}{s}\cdot\frac{y}{t} = \frac{xy}{st}$. Denotando por $S^{-1}A$ o conjunto quociente, temos duas operações definidas em $S^{-1}A$. Esse conjunto é de fato um anel, como podemos ver sintetizado abaixo

$$\left(\frac{x}{s}+\frac{y}{t}\right)+\frac{z}{u} = \frac{xt+ys}{st}+\frac{z}{u} = \frac{xtu+ysu+zst}{stu} = \frac{x}{s}+\frac{yu+zt}{tu} = \frac{x}{s}+\left(\frac{y}{t}+\frac{z}{u}\right)$$

$$\frac{x}{s}+\frac{y}{t} = \frac{xt+ys}{st} = \frac{ys+tx}{ts} = \frac{y}{t}+\frac{x}{s}$$

$$\frac{x}{s}+\frac{0}{1} = \frac{x+0}{s} = \frac{x}{s}$$

Para a existência do oposto, precisaremos de uma propriedade extra: $\frac{0}{s} = \frac{0}{t}$. De fato, $0 \cdot t = 0 = 0 \cdot s$.

$$\frac{x}{s}+\frac{-x}{s} = \frac{xs+(-x)s}{ss} = \frac{xs-xs}{ss} = \frac{0}{ss} = \frac{0}{1}$$

$$\left(\frac{x}{s}\cdot\frac{y}{t}\right)\cdot\frac{z}{u} = \frac{xy}{st}\cdot\frac{z}{u} = \frac{xyz}{stu} = \frac{x}{s}\cdot\frac{yz}{tu} = \frac{x}{s}\cdot\left(\frac{y}{t}\cdot\frac{z}{u}\right)$$

$$\frac{x}{s}\cdot\frac{y}{t} = \frac{xy}{st} = \frac{yx}{ts} = \frac{y}{t}\cdot\frac{x}{s}$$

$$\frac{x}{s}\cdot\frac{1}{1} = \frac{x}{s}$$

A distributividade pode ser provada usando a seguinte afirmação: $\frac{x}{s} =$

$\frac{xt}{st}$. De fato, $x(st) = (xt)s$.

$$\frac{x}{s} \cdot \left(\frac{y}{t} + \frac{z}{u}\right) = \frac{x}{s} \cdot \frac{yu + zt}{tu} = \frac{x(yu + zt)}{stu} = \frac{xyu + xzt}{stu} =$$
$$= \frac{(xyu + xzt)s}{(stu)s} = \frac{xysu + xzst}{stsu} = \frac{xy}{st} + \frac{xz}{su} = \frac{x}{s} \cdot \frac{y}{t} + \frac{x}{s} \cdot \frac{z}{u}$$

Além disso, note que se $s, t \in S$, então $\frac{s}{t}$ é inversível: $\frac{s}{t} \cdot \frac{t}{s} = \frac{st}{ts} = \frac{1 \cdot (st)}{1 \cdot (st)} = \frac{1}{1}$. Ainda, se $x \in A$ é inversível e $s \in S$, então $\frac{x}{s}$ também o é, pois $\frac{x}{s} \cdot \frac{x^{-1}s}{1} = \frac{xx^{-1}s}{s} = \frac{1s}{1s} = \frac{1}{1}$, mas nesse caso, não podemos escrever $\left(\frac{x}{s}\right) = \frac{s}{x}$, pois não sabemos se $x \in S$. Similarmente ao caso do corpo de frações, podemos definir um homomorfismo injetor entre A e $S^{-1}A$ (lembrando que sempre estamos tomando S sem divisores do zero e sem o zero) da seguinte forma: Defina $\iota : A \to S^{-1}A$ por $\iota(x) = \frac{x}{1}$. Essa função é um homomorfismo pois:

$$\iota(x + y) = \frac{x + y}{1} = \frac{x}{1} + \frac{y}{1} = \iota(x) + \iota(y)$$
$$\iota(xy) = \frac{xy}{1} = \frac{x}{1} \cdot \frac{y}{1} = \iota(x)\iota(y)$$

E se $\iota(x) = \frac{0}{1}$, temos $\frac{x}{1} = \frac{0}{1}$ e lembrando que essas frações são classes de equivalência, obtemos $(x, 1) \sim (0, 1)$ e logo $x = 0$. Então, $\text{Ker}(\iota) = \{0\}$ e ι é injetora. Como de costume, podemos "confundir"um elemento de A com sua imagem por ι em $S^{-1}A$ e escrever $A \subseteq s^{-1}A$ e $x = \frac{x}{1}$, mas devemos ter em mente que se $x \in A \setminus S$ é inversível, não podemos identificar $x^{-1} = \frac{x^{-1}}{1}$ com $\frac{1}{x}$, já que a última não está definida. Similarmente, é necessário ter cuidado ao cancelar elementos. Por exemplo, considere o anel de valoração associado à valoração 2-ádica de $\mathbb{Q}$. Seja $S = \{4^n; n \in \mathbb{N}\}$ e note que S é multiplicativo. É **errado** afirmar $\frac{2}{4} = \frac{2 \cdot 1}{2 \cdot 2} = \frac{1}{2}$. O motivo para isso é que a última expressão nem ao menos faz sentido: $2 \notin S$. Repetindo o que já foi comentado anteriormente, antes de provarmos a distributividade, podemos cancelar elementos de S: Se $x \in A$ e $s, t \in S$ vale $\frac{xs}{ts} = \frac{x}{t}$, pois $(xs)t = x(ts)$.

Para finalizar a sessão, daremos alguns exemplos de localizações. O último deles será de importância à frente e por isso terá uma notação particular e um teorema à respeito.

Exemplo 137. *Seja A um anel comutativo com unidade e $S = \{1\}$. Então $S^{-1}A$ é isomorfo a A. De fato, é fácil ver que ι é sobrejetora, nesse caso, logo ι é o isomorfismo desejado.*

Exemplo 138. *Seja D um domínio de integridade e $S = D^*$. Então $S^{-1}D$ é o corpo de frações de D, como construído usualmente.*

Exemplo 139. *Generalizando o exemplo anterior, seja A um anel comutativo com unidade e S o conjunto dos elementos que não são divisores do zero. Note que se $xy \notin S$, então existe $z \neq 0$ tal que $(xy)z = 0$. Então, $x(yz) = 0$ e logo $yz = 0$ ou $x \notin S$. No caso $yz = 0$, como $z \neq 0$, temos $y \notin S$. Da contrapositiva, se $x, y \in S$, temos $xy \in S$ e como $1 \in S$, S é multiplicativamente fechado. A localização $S^{-1}A$ é chamada de* anel total de frações *de A. Observe que se A for domínio de integridade, caímos no caso anterior.*

Exemplo 140. *Seja A um anel comutativo com unidade e $\mathfrak{P}$ um ideal primo de A. Note que de $\mathfrak{P}$ primo, $\mathfrak{P} \neq A$, logo $1 \notin \mathfrak{P}$. Por mais que $\mathfrak{P}$ não seja multiplicativo, se $x, y \notin \mathfrak{P}$, então $xy \notin \mathfrak{P}$, da definição de ideal primo, logo $S = A \setminus \mathfrak{P}$ é multiplicativo e podemos fazer a localização $S^{-1}A$ dele. Essa localização será denotada por $A_{\mathfrak{P}}$. Note que o conjunto de todos os divisores do zero, junto com o próprio zero, formam um ideal primo de A. O anel total de frações é, portanto, um caso particular desse exemplo.*

Teorema 141. *Seja A um anel comutativo com unidade e $\mathfrak{P}$ um ideal primo de A. Então $A_{\mathfrak{P}}$ é um anel local, e $\mathfrak{M}_{A_{\mathfrak{P}}}$ é o $\mathfrak{P}$-submódulo do corpo de frações de A gerado por $A_{\mathfrak{P}}$*

Demonstração. Seja $\mathfrak{M} = \text{span}_{\mathfrak{P}}(A_{\mathfrak{P}})$ e note que os elementos de $\mathfrak{M}$ são precisamente as frações $\frac{p}{s}$ com $p \in \mathfrak{P}$ e $s \notin \mathfrak{P}$. Como $\mathfrak{M}$ é módulo, sabemos que é fechado na operação de adição. Agora, dado $x \in \mathfrak{M}$ e $\frac{a}{t} \in A$, escreva $x = \frac{p}{s}$, onde $p \in \mathfrak{P}$ e $s \notin \mathfrak{P}$. Temos $ap \in \mathfrak{P}$, pois $\mathfrak{P}$ é ideal de A, e $st \notin \mathfrak{P}$, pois $\mathfrak{P}$ é primo. Concluímos $\frac{a}{t}x = \frac{ap}{ts} \in \mathfrak{M}$, o que resulta em $\mathfrak{M}$ ser ideal. Ainda, considere $\frac{a}{s} \in A_{\mathfrak{P}} \setminus \mathfrak{M}$. Então, $a \notin \mathfrak{P}$ e portanto $\frac{s}{a}$ está definido em $A_{\mathfrak{P}}$ e concluímos $\frac{a}{s}$ inversível. Concluímos que todo não-inversível está em $A_{\mathfrak{P}}$ e como $\frac{1}{1} \notin A_{\mathfrak{P}}$ (pois de $\mathfrak{P}$ primo, $1 \notin \mathfrak{P}$), concluímos que $A_{\mathfrak{P}}$ é anel local com único ideal maximal $\mathfrak{M}$.

■

13ANÉIS DE PRÜFER

Para finalizar, estudaremos os anéis de Prüfer. Esses podem ser usados, por exemplo, para caracterizar valorações em alguns tipos específicos de corpos. Terminaremos a seção mostrando que os anéis de valoração são, precisamente, os subanéis unitários que são Prüfer e locais, nos dando outra caracterização dos anéis de valoração.

Definição 142. *Considere $\mathbb{K}$ um corpo, A um subanel unitário de $\mathbb{K}$ e $\mathcal{O}$ um anel de valoração de $\mathbb{K}$. $\mathcal{O}$ é dito* essencial para *A se existe $M \subseteq A$ multiplicativamente fechado tal que $\mathcal{O} = M^{-1}A$.*

Teorema 143. *Considere $\mathbb{K}$ um corpo e A um subanel unitário de $\mathbb{K}$. Então $\mathbb{K}$ admite anel de valoração essencial para A se, e somente se, $\mathbb{K}$ é o corpo de frações de A. Nesse caso, $\mathbb{K}$ é essencial para A.*

Demonstração. Seja $M^{-1}A$ essencial para A e $\mathbb{L} \subseteq \mathbb{K}$ o corpo de frações de A. Agora considere $y \in \mathbb{K}$. Como $M^{-1}A$ é anel de valoração de $\mathbb{K}$, temos $y \in M^{-1}A$ ou $y^{-1} \in M^{-1}A$. Disso, existem $x \in A$ e $m \in M \subseteq A$ tais que $y = \frac{x}{m} \in \mathbb{L}$ ou $y = \frac{m}{x} \in \mathbb{L}$. Concluímos que $\mathbb{K} \subseteq \mathbb{L}$, e portanto os dois são iguais.

Reciprocamente, suponha que $\mathbb{K}$ seja o corpo de frações de A. Então $\mathbb{K}$ é anel de valoração de $\mathbb{K}$ e $\mathbb{K} = A_{\{0\}}$, provando que $\mathbb{K}$ é essencial para A.

$\blacksquare$

Teorema 144. *Sejam A, B anéis tais que $A \subseteq B$ e I um ideal de B. Então $J = I \cap A$ é um ideal de A. Além disso, se I é primo, então J é primo.*

Demonstração. $J \subseteq A$ é subanel de B, pois é interseção de subanéis, logo é subanel de A e se $x \in A$ e $y \in J$, temos $xy \in A$. Como I é ideal, $xy \in J$, logo $xy \in I$. Supondo que I é primo, se $x, y \in A \setminus J$, temos $x, y \notin I$ e portanto, $xy \notin I$. Concluímos que $xy \notin J$, e logo $\mathfrak{P}$ é primo. $\blacksquare$

Teorema 145. *Considere $\mathbb{K}$ um corpo, A um subanel unitário de $\mathbb{K}$ e $\mathcal{O}$ um anel de valoração de $\mathbb{K}$ que contém A. Para $\mathfrak{P} = \mathfrak{M}_{\mathcal{O}} \cap A$, $\mathcal{O}$ domina $A_{\mathfrak{P}}$ e as seguintes condições são equivalentes:*

1) $\mathcal{O} = A_{\mathfrak{P}}$
2) $A_{\mathfrak{P}}$ é anel de valoração de $\mathbb{K}$.

3) $\mathcal{O}$ é essencial para A.
Nesse caso, todo anel de valoração de $\mathbb{K}$ que contém $\mathcal{O}$ é essencial para A.

Demonstração. Se $x = \frac{a}{m} \in A_{\mathfrak{P}}$, então $m \notin \mathfrak{P}$. Como $m \in A$, temos $m \notin \mathfrak{M}_{\mathcal{O}}$. Mas $A \subseteq \mathcal{O}$ e portanto $m \in \mathcal{O}$. Disso, m é inversível em $\mathcal{O}$ e $m^{-1} \in \mathcal{O}$. Temos $\frac{a}{m} = am^{-1} \in \mathcal{O}$ e concluímos $\mathfrak{P} \subseteq \mathfrak{M}_{\mathcal{O}}$. Falta provar que $\mathfrak{M}_{A_{\mathfrak{P}}} = \mathfrak{M}_{\mathcal{O}} \cap A_{\mathfrak{P}}$. Seja $x \in \mathfrak{M}_{A_{\mathfrak{P}}}$. Como vimos antes, x é da forma $\frac{p}{m}$ onde $p \in \mathfrak{P}$ e $m \notin \mathfrak{P}$. Então, como vimos, $m \in \mathcal{O}$ é inversível e também $p \in \mathfrak{M}_{\mathcal{O}}$. Temos que $m^{-1} \in \mathcal{O}$ e logo $\frac{p}{m} = pm^{-1} \in \mathfrak{M}_{\mathcal{O}}$ nos dando $\mathfrak{M}_{A_{\mathfrak{P}}} \subseteq \mathfrak{M}_{\mathcal{O}} \cap A_{\mathfrak{P}}$. Além disso, se $x = \frac{a}{m} \in \mathfrak{M}_{\mathcal{O}} \cap A_{\mathfrak{P}}$, temos $m \notin \mathfrak{P}$, e portanto, m é inversível em $\mathcal{O}$. Mas x é não-inversível, logo a não pode ser inversível e $a \in \mathfrak{M}_{\mathcal{O}}$. Concluímos $a \in \mathfrak{P}$ e portanto $\frac{a}{m} \in A_{\mathfrak{P}}$, provando a afirmação. Prosseguimos para as equivalências, mas as faremos de uma maneira diferente da usual: faremos as implicações $1 \implies 2$, $1 \implies 3$, $2 \implies 1$ e $3 \implies 1$.

($1 \implies 2$): É trivial, visto que $\mathcal{O}$ é anel de valoração de $\mathbb{K}$.

($1 \implies 3$): É trivial, visto que $A_{\mathfrak{P}} = \mathcal{O}$.

($2 \implies 1$): Sabemos que $A_{\mathfrak{P}} \subseteq \mathcal{O}$. Seja $x \in \mathcal{O}$. Se $x = 0$, então $x \in A_{\mathfrak{P}}$ e se $x \neq 0$, então como $A_{\mathfrak{P}}$ é anel de valoração, $x \in A_{\mathfrak{P}}$ ou $x^{-1} \in A_{\mathfrak{P}}$. Se $x \in A_{\mathfrak{P}}$, segue a afirmação. Se $x^{-1} \in A_{\mathfrak{P}}$, $x^{-1} \in \mathcal{O}$ e portanto $x \notin \mathfrak{M}_{A_{\mathfrak{P}}}\mathcal{O}$. Da definição de $\mathfrak{P}$, obtemos que $x^{-1} \notin \mathfrak{P}$, logo $x = (x^{-1})^{-1} = \frac{1}{x^{-1}} \in A_{\mathfrak{P}}$ e também segue a afirmação.

($3 \implies 1$): Seja $\mathcal{O} = N^{-1}A$, onde N é um subconjunto multiplicativo de A. Sabemos que $A_{\mathfrak{P}} \subseteq \mathcal{O}$. Se $x = \frac{a}{n} \in \mathcal{O}$, $n \in N$, temos que $n^{-1} = \frac{1}{n} \in \mathcal{O}$, e portanto, n é inversível. Obtemos que $n \notin \mathfrak{M}_{\mathcal{O}}$ e logo $n \notin \mathfrak{P}$. Concluímos que $\frac{a}{n} \in A_{\mathfrak{P}}$.

Finalmente, considere um anel de valoração $\mathcal{O}'$ que contém $\mathcal{O}$ e seja $\mathfrak{P}' = \mathfrak{M}_{\mathcal{O}'} \cap A$. Se $\frac{a}{m} \in A_{\mathfrak{P}}$, então $a \in A$ e $m \in A \setminus \mathfrak{P} \subseteq A \setminus \mathfrak{P}'$. Então, se $x \in \mathbb{K}$, $x \in A_{\mathfrak{P}}$ ou $x^{-1} \in A_{\mathfrak{P}}$. Concluímos que $x \in A_{\mathfrak{P}'}$ ou $x^{-1} \in A_{\mathfrak{P}'}$.

■

Teorema 146. *Considere $\mathbb{K}$ um corpo, A um subanel unitário de $\mathbb{K}$ e M um subconjunto multiplicativamente fechado de A. Então um anel de valoração $\mathcal{O}$ de $\mathbb{K}$ que contém $M^{-1}A$ é essencial para $M^{-1}A$ se, e somente se, ele é essencial para A.*

Demonstração. Se $\mathcal{O}$ é essencial para $M^{-1}A$, então $\mathcal{O}$ é uma localização de $M^{-1}A$. Mas então, como $M^{-1}A$ é localização de A, sai que $\mathcal{O}$ é localização de A. Reciprocamente, suponha que $\mathcal{O}$ seja uma localização de A, digamos, $\mathcal{O} = N^{-1}A \subseteq N^{-1}(M^{-1}A)$. Então dado $a \in M^{-1}A$ e $n \in N$, temos $\frac{1}{n} \in N^{-1}A$ e logo $\frac{1}{n} \in \mathcal{O}$ e além disso, $a \in \mathcal{O}$, do que resulta $\frac{a}{n} \in \mathcal{O}$. Isso mostra a igualdade.

■

Teorema 147. *Considere $\mathbb{K}$ um corpo, A um subanel unitário de $\mathbb{K}$ e $\mathcal{O}$ um anel de valoração de $\mathbb{K}$ que contém A. Chamando de π a projeção canônica de $\mathcal{O}$ em $\mathcal{O}/\mathfrak{M}_{\mathcal{O}}$, temos que se $\pi|_A$ é sobrejetora, então $\mathfrak{M}_{\mathcal{O}} \cap A$ é ideal maximal de A. Além disso, a recíproca vale no caso em que $\mathcal{O}$ é essencial para A.*

Demonstração. Calculemos o núcleo de $\pi|_A$. $x \in \text{Ker}(\pi|_A)$ se, e somente se, $x \in A$ e $\pi(x) = 0$ se, e somente se, $x \in A$ e $x \in \mathfrak{M}_{\mathcal{O}}$. Então, $\text{Ker}(\pi|_A) = \mathfrak{M}_{\mathcal{O}} \cap A$. Do Teorema do Homomorfismo, $A/\text{Ker}(\pi|_A)$ é isomorfo à $\text{Im}(\pi_A) = \mathcal{O}/\mathfrak{M}_{\mathcal{O}}$, que é um corpo pois $\mathfrak{M}_{\mathcal{O}}$ é maximal.

■

Teorema 148. *Considere $\mathbb{K}$ um corpo e A um subanel unitário de $\mathbb{K}$. Então, as seguintes condições são equivalentes:*

1) Todo anel de valoração de $\mathbb{K}$ que contém A é essencial para A.

2) Se $\mathfrak{M}$ é ideal maximal de A, então $A_{\mathfrak{M}}$ é anel de valoração de $\mathbb{K}$.

3) Se $\mathfrak{P}$ é ideal primo de A, então $A_{\mathfrak{P}}$ é anel de valoração de $\mathbb{K}$.

Demonstração. ($1 \implies 2$): Do Teorema de Extensão, existe um anel de valoração $\mathcal{O}$ de $\mathbb{K}$ que contém $\mathfrak{M}$ e tal que $\mathfrak{M} = \mathfrak{M}_{\mathcal{O}} \cap A$. Mas da hipótese, $\mathcal{O}$ é essencial para A, logo, do teorema 145, $A_{\mathfrak{M}}$ é um anel de valoração.

($2 \implies 3$): Como $\mathfrak{P}$ é primo, $\mathfrak{P}$ está contido em um ideal maximal $\mathfrak{M}$. Então, se $a \in A$ e $m \in A \setminus \mathfrak{M}$, então $m \in A \setminus \mathfrak{P}$ e portanto $\frac{a}{m} \in A_{\mathfrak{P}}$. Temos $A_{\mathfrak{M}} \subseteq A_{\mathfrak{P}}$. Mas $A_{\mathfrak{M}}$ é anel de valoração de $\mathbb{K}$, logo, se $x \in \mathbb{K}^*$, $x \in A_{\mathfrak{M}}$ ou $x^{-1} \in A_{\mathfrak{M}}$, e então, $x \in A_{\mathfrak{P}}$ ou $x^{-1} \in A_{\mathfrak{P}}$.

($3 \implies 1$): Seja $\mathcal{O}$ um anel de valoração de $\mathbb{K}$ que contém A. Defina $\mathfrak{P} = \mathfrak{M}_{\mathcal{O}} \cap A$ e note que $\mathfrak{P}$ é primo. Além disso, da hipótese, $A_{\mathfrak{P}}$ é anel de valoração de $\mathbb{K}$ e portanto, do teorema 145, temos que $\mathcal{O}$ é essencial para A.

■

Definição 149. *Nas notações do teorema, A é dito um* anel de Prüfer *de $\mathbb{K}$ quando valem as condições equivalentes.*

Teorema 150. *Seja $\mathbb{K}$ um corpo. Um subanel unitário de $\mathbb{K}$ é anel de valoração se, e somente se, ele é Prüfer e local.*

Demonstração. Seja A um subanel unitário de $\mathbb{K}$. Se A é de valoração, já sabemos que ele é local. Ainda, A é essencial para A, pois $A = \{1\}^{-1}A$, e de 145, qualquer anel de valoração que contém A é essencial para A. Isso mostra que A é Prüfer. Caso A seja Prüfer e local, considere o ideal maximal $\mathfrak{M}_A$ e note que $\mathfrak{M}_A = \mathfrak{M}_A \cap A$. Da definição 149, sabemos que $A_{\mathfrak{M}_A}$ é anel de valoração de $\mathbb{K}$, e do teorema 145, isso quer dizer que $A = A_{\mathfrak{M}_A}$, o que resulta em A ser anel de valoração.

■

14CONSIDERAÇÕES FINAIS

Após termos estudado um pouco dessa teoria, algumas perguntas podem surgir. Dentre elas, podemos nos perguntar onde mais valorações são aplicáveis. Pera responder a isso, lembre que mencionamos como exemplo o corpo dos números p-ádicos. Esse corpo é objeto de estudo na teoria de números, e de fato, alguns resultados que podem ser provados para eles seguem em qualquer corpo de frações de um domínio de ideais principais.

A começar, é possível provar que os valores absolutos p-ádicos, o valor absoluto trivial e o valor absoluto usual são os únicos que podem ser definidos em $\mathbb{Q}$. Esse resultado se estende para valorações: As únicas valorações não triviais em $\mathbb{Q}$ são as valorações p-ádicas. Algo análogo pode ser provado em um domínio de ideais principais, como mostra a referência.

Isso pode ser generalizado ainda mais: Dado um corpo e uma coleção α de anéis de valoração dele, dizemos que essa coleção tem caráter discreto se as valorações de Krull induzidas são discretas e que tem caráter finito se dado um elemento do corpo, esse elemento não é inversível em uma quantidade finita de elementos de α. Um anel de Krull é um uma interseção de uma coleção de anéis de valoração do corpo que tem caráter finito e discreto. É possível provar que todo domínio de ideais principais é Prüfer e Krull. Nessa caso, dizemos que ele é um anel de Dedekind, e nesses, podemos também caracterizar as valorações.

Algumas aplicações da teoria aqui introduzida também existem fora da área. Um exemplo de aplicação em uma área relacionada pode ser encontrado no artigo de Elena Olivos [4], onde é construída, como o título deixa claro, uma família de grupos totalmente ordenados. Para essa construção, foram utilizadas, entre outras, valorações de Krull. Além disso, valorações em anéis, caso mais geral do que vimos, foram utilizados por Peter Scholze em seu artigo no qual são introduzidos os espaços perfectóide [5].

Falando um pouco sobre a estrutura topológica das valorações de Krull, não foi mostrado aqui, mas a função inverso também é contínua, o que torna um corpo com a topologia induzida da valoração um corpo topológico. Mais ainda: as bolas são abertas e fechadas e o espaço é totalmente desconexo, o que nos permite encontrar valorações de Krull não triviais nas quais o fecho das bolas abertas e as bolas fechadas não são necessariamente compactos. Também podemos fazer completamento, mas isso requer outras ferramentas, para ser preciso, filtros de Cauchy.

REFERÊNCIAS

ENDLER, O. *Valuation theory*. [S.l.]: Springer-Verlag, 1972. (Universitext (1979)). ISBN 9780387060705.

SUTHERLAND, W.; SUTHERLAND, W. *Introduction to Metric and Topological Spaces*. [S.l.]: Clarendon Press, 1975. (Open university set book). ISBN 9780198531616.

CLARK, P. L. *Algebraic Number Theory II: Valuations, Local Fields and Adeles*. Http://math.uga.edu/~pete/8410FULL.pdf.

OLIVOS, E. A family of totally ordered groups with some special properties. *Annales mathématiques Blaise Pascal*, Annales mathématiques Blaise Pascal, v. 12, n. 1, p. 79–90, 2005.

SCHOLZE, P. Perfectoid spaces. *Publications mathématiques de l'IHÉS*, v. 116, n. 1, p. 245–313, Nov 2012. ISSN 1618-1913.