Universidade Federal de Santa Catarina

Curso de Pós-Graduação em Matemática e

Computação Científica

Valorizações

Ronie Peterson Dario

Orientador: Prof. Dr. Oscar Ricardo Janesch

Florianópolis

Fevereiro de 2004

Universidade Federal de Santa Catarina

Curso de Pós-Graduação em Matemática e

Computação Científica

Valorizações

Dissertação apresentada ao Curso de Pós-Graduação em Matemática e Computação Científica, do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina, para a obtenção do grau de Mestre em Matemática, com Área de Concentração em Álgebra.

Ronie Peterson Dario

Orientador: Prof. Dr. Oscar Ricardo Janesch

Florianópolis

Fevereiro de 2004

Valorizações

por

Ronie Peterson Dario

Esta Dissertação foi julgada para a obtenção do Título de "Mestre", área de Concentração em Álgebra, e aprovada em sua forma final pelo Curso de Pós-Graduação em Matemática e Computação Científica.

Prof. Dr. Igor Mozolevski
Coordenador

Comissão Examinadora

Prof. Dr. Oscar Ricardo Janesch (UFSC - Orientador)

Prof. Dr. Antonio José Engler (UNICAMP)

Prof^{a}. Dra. Albertina Zatelli (UFSC)

Florianópolis, fevereiro de 2004.

À Deus, o maior matemático.

Agradecimentos

Meu maior agradecimento é à Leonara. Obrigado por ter ficado ao meu lado em todos os momentos e em especial, nos que mais precisei. Obrigado por ter me ajudado a superar as dificuldades e ter me feito acreditar que é possível reverter algumas situações aparentemente sem saída.

Meu profundo agradecimento aos meus pais Hedi e Daniel e meus irmãos Vagner e Douglas. À vocês devo absolutamente tudo.

Agradeço aos professores Ruy Coimbra Crarão, Igor Mozolevski, Fermin S. V. Bazán e Celso M. Doria pelos conhecimentos que transmitiram durante as disciplinas do mestrado. Também agradeço a todos os amigos da Pós-Graduação, com os quais convivi nestes últimos anos. Registro que me proporcionaram muita alegria em fazerem parte da minha vida. Em especial, Anderson, André, Claires, Cláudio, Cleuzir, Cleverson, Danilo, Franco, Hilbert, Jocemar, Maicon e Vanderlei.

Gostaria de citar meus professores de graduação Christian Pinedo, Santos Richard W. S. e Fred Maglório e agradecê-los pelo incentivo constante.

À CAPES, pelo auxílio financeiro recebido.

De maneira muito especial agradeço ao Professor Oscar Ricardo Janesch, pela orientação segura e dedicada, pela amizade valoroza e pelos conhecimentos que adquiri durante as disciplinas e durante a produção deste trabalho.

Sumário

Resumo

Este trabalho é um estudo sobre Teoria de Valorização em Corpos e duas formas de generalização dessa teoria para estruturas não necessariamente comutativas. Em corpos são estudadas os anéis de valorização, as funções valorização e os places. Uma demonstração do conhecido Teorema da Extensão é apresentada de forma direta, sem a utilização de places. A primeira forma de generalizar essa teoria é trabalhando em anéis divisão, utilizando os anéis de valorização totais e invariantes. Obtem-se várias propriedades semelhantes ao caso comutativo e são apresentados exemplos de anéis de valorização totais e invariantes e também anéis de valorização totais e não invariantes. É apresentado também um contra-exemplo para o Teorema da Extensão no caso dos anéis de valorização totais e invariantes. A segunda e mais adequada maneira de estudar a Teoria de Valorização em estruturas não comutativas é através dos anéis de valorização de Dubrovin que são definidos nos anéis de matrizes sobre um anel de divisão, isto é, os anéis artinianos simples. A partir do estudo dos anéis artinianos simples são apresentadas propriedades dos anéis de valorização de Dubrovin. Definindo-se places sobre os anéis artinianos simples, demonstra-se que a um anel de valorização de Dubrovin sempre está associado um place e reciprocamente, dado um place, o conjunto dos elementos que assumem imagem finita é um anel de valorização de Dubrovin. Finalmente, são apresentadas as funções valorização sobre anéis artinianos simples e demonstrada sua relação com os anéis de valorização de Dubrovin.

Introdução

A Teoria de Valorização teve início em 1912 quando o matemático húngaro Josef Kürschák formulou os axiomas de valorização que são utilizados até hoje. A principal motivação foi a tentativa de melhorar a fundamentação da teoria de corpos $p-$ádicos definidos por Kurt Hensel. Na terminologia moderna a valorização definida por Kürschák é denominada valor absoluto, enquanto o termo valorização é dedicado a um conceito mais geral proposto posteriormente por Wolfgang Krull.

Nas décadas seguintes houve um rápido desenvolvimento da Teoria de Valorização devido à seus métodos e conceitos mostrarem-se eficientes na solução de problemas em Teoria dos Números.

Independente de aplicações em Teoria dos Números, contribuições importantes para a Teoria de Valorização foram dadas em 1934, na publicação dos trabalhos de Alexander Ostrowski. Ao mesmo tempo, Wolfgang Krull apresentou uma definição mais geral de valorização, que mostrou-se aplicável em várias outras áreas da Matemática, tais como Geometria Algébrica, Álgebra Comutativa e Análise Funcional.

A eficiência da Teoria de Valorização no estudo de corpos levou naturalmente a tentativa de generalizá-la a estruturas mais gerais, por exemplo, aos anéis de divisão. Essa tentativa passa obrigatoriamente pelos trabalhos de Schilling, apresentados por volta da metade do século passado. Shilling aplica o conceito de anel de valorização em corpos para anéis de divisão, produzindo os anéis de valorização totais. Por sua vez, estes anéis são chamados invariantes quando são invariantes por automorfismos internos do anel de divisão. Para estes anéis são demonstrados resultados análogos aos conhecidos no caso de corpos.

Um dos principais resultados da Teoria de Valorização em corpos é o Teorema da Extensão, que assegura que se $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão de corpos e V é um anel de valorização de $\mathbb{K}$, então existe um anel de valorização R de $\mathbb{L}$ tal que $R \cap \mathbb{K} = V$. O Teorema da Extensão não é válido para o caso de anéis de valorização de Shilling. Esse fato e a relativa escassez dos anéis de valorização totais e invariantes em anéis de divisão levou a conclusão de que os anéis de valorização de Shilling não são a melhor generalização dos anéis de valorização estudados em corpos. No entanto, até a metade da década de 80, nenhum conceito mas preciso foi obtido e, conseqüentemente houve um decrescimento da motivação para estudar o assunto.

Em 1982, N.I. Dubrovin publicou um trabalho, originalmente em russo e traduzido para o inglês em 1984, onde apresenta uma generalização para a definição de anel de valorização não apenas para anéis de divisão, mas também para anéis de matrizes sobre anéis de divisão, que são os anéis artinianos simples. Mais do que isso, a definição de Dubrovin é mais geral que a definição de Shilling, e Dubrovin provou o Teorema da Extensão para seus anéis de valorização.

A partir da divulgação dos trabalhos de Dubrovin houve maior concentração de pesquisas sobre valorização, gerando uma quantidade substancial de trabalhos científicos sobre o assunto, como pode ser visto em indicadores de produção científica.

No primeiro capítulo deste trabalho estudaremos as três formas equivalentes de abordar a Teoria de Valorização em Corpos, a saber, os anéis de valorização, as funções valorização, e os places. Os anéis de valorização são ordens específicas de um corpo. As funções valorização surgem como uma generalização natural do conceito de valor absoluto não arquimediano e os places são aplicações entre corpos projetivos, que podem ser vistos como extensões de homomorfismos.

Trataremos dos anéis de valorização totais e invariantes no segundo capítulo. Devido à relativa escassez desses anéis, daremos algum destaque a apresentação e construção de exemplos. Provaremos que o anel $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$, onde $\alpha = \frac{1}{2}(1+i+j+k)$, é um anel de valorização total e invariante do anel de divisão dos quatérnios racionais. Através do Anel das Séries Formais de Laurent contruiremos anéis de valorização totais e invariantes e totais não invariantes. Apresentamos também a construção completa de um contra-exemplo para o Teorema da Extensão em anéis de divisão.

Com um prévio estudo dos anéis artinianos simples, introduzimos o conceito de anel de valorização de Dubrovin sobre um anel artiniano simples. Demonstramos algumas de suas propriedades e explicitamos como esta classe de anéis generaliza corretamente a definição do caso comutativo. A definição de place sobre anéis artinianos simples permite mostrar que a Teoria de Valorização sobre anéis artinianos simples pode ser abordada tanto pelos anéis de valorização de Dubrovin quanto pelos places. As funções valorizações também têm uma generalização aos anéis artinianos simples, como veremos na última seção do trabalho.

Em todo este trabalho um anel sempre é um anel com unidade e subanel sempre tem a mesma unidade do anel. Um corpo é sempre comutativo e um anel de divisão é uma estrutura que satisfaz todos os axiomas de corpo exceto possivelmente a comutatividade.

Se R é um domínio comutativo, denotamos por $c.fr(R)$ o corpo de frações de R.

Dado um anel R com centro $\mathbb{F}$, denotamos:

R^* = $\{x \in R;\ x \text{ é regular}\}$.

$U(R)$ = $\{x \in R;\ x^{-1} \in R\}$.

$J(R)$ = Radical de Jacobson de R.

$M_n(R)$ = anel de matrizes $n \times n$ sobre R.

$[R : \mathbb{F}]$ = dimensão de R sobre $\mathbb{F}$ como espaço vetorial, quando R é anel artiniano simples.

Além disso,

- O único ideal maximal do anel local V é denotado por $\mathfrak{M}_V$.

- A ordem do grupo G é denotada por $|G|$.

- Dados os conjuntos A e B, denotamos por $A \setminus B$ o conjunto $\{x \in A;\ x \notin B\}$.

Capítulo 1

Valorização em Corpos

Neste capítulo apresentaremos os principais conceitos e resultados da Teoria de Valorização sobre corpos. Dividimos o capítulo em três seções, abordando em cada uma delas um dos enfoques da Teoria de Valorização, a saber, anéis de valorização, funções valorização e places.

Iniciamos provando propriedades dos anéis de valorização, com destaque para uma demonstração direta do Teorema da Extensão, sem utilizar places. Em seguida estudamos as funções valorização, definimos uma relação de equivalência no conjunto de tais funções e explicitamos uma correspondência biunívoca entre anéis de valorização e classes de funções valorização sobre um corpo. Finalmente apresentamos os places, definimos uma relação de equivalência no conjunto dos places sobrejetores e explicitamos uma correspondência biunívoca entre anéis de valorização e as classes de places sobrejetores.

1.1 Anéis de Valorização

Veremos nesta seção que entre os principais resultados e propriedades envolvendo anéis de valorização de um corpo, destacam-se o Teorema da Extensão e o Teorema da Correspondência, além do fato de anéis de valorização terem reticulado de ideais totalmente ordenado por inclusão.

Definição 1.1.1 *Seja $\mathbb{K}$ um corpo. O subanel V de $\mathbb{K}$ é um anel de valorização de $\mathbb{K}$, se para cada $x \in \mathbb{K}^*$, temos $x \in V$ ou $x^{-1} \in V$.*

Observação 1.1 Se V é um anel de valorização de $\mathbb{K}$, então V é um subdomínio de $\mathbb{K}$.

Observação 1.2 O próprio corpo $\mathbb{K}$ é um anel de valorização de $\mathbb{K}$, chamado de *anel de valorização trivial.*

Observação 1.3 Se V é um anel de valorização de $\mathbb{K}$ e $\mathbb{L}$ é um subcorpo de $\mathbb{K}$, então $V \cap \mathbb{L}$ é anel de valorização de $\mathbb{L}$.

Observação 1.4 Se V é um anel de valorização de $\mathbb{K}$, então $\mathbb{K}$ é o corpo de frações de V. De fato, seja $x \in \mathbb{K}$. Se $x = 0$, temos que $x = 0.1^{-1}$, com $0, 1 \in V$. Para $x \neq 0$ e $x \in V$, temos $x = x.1^{-1}$, com $x, 1 \in V$. Para $x \neq 0$ e $x^{-1} \in V$, temos $x = 1.(x^{-1})^{-1}$, com $1, x^{-1} \in V$.

Note que não vale a recíproca da Observação 1.4. Por exemplo, $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, mas $\mathbb{Z}$ não é anel de valorização de $\mathbb{Q}$, já que $\frac{5}{9}$ e $\frac{9}{5}$ não estão em $\mathbb{Z}$.

O lema abaixo é útil para apresentar exemplos de anéis de valorização. Em particular, ele assegura que se um corpo tem característica p, com p um número primo, e é algébrico sobre seu corpo primo, então ele só tem anel de valorização trivial.

Lema 1.1.1 *Seja* $\mathbb{K}$ *um corpo.*

(a) *Se* $\mathbb{K}$ *é finito, então* $\mathbb{K}$ *não possui anel de valorização próprio.*

(b) *Se* $\mathbb{K}$ *é uma extensão algébrica de um corpo finito, então* $\mathbb{K}$ *não possui anel de valorização próprio.*

Demonstração

(a) Seja V anel de valorização de $\mathbb{K}$. Então $(V, +)$ é subgrupo de $(\mathbb{K}, +)$. Vamos supor que $\mid \mathbb{K} \mid = 2 + 2k + r$ e $\mathbb{K} = \{0, 1, x_1, x_2, ..., x_r, y_1, y_2, ..., y_{2k-1}, y_{2k}\}$, onde

$$x_j.x_j = y_i.y_{i+1} = 1 \text{ para } j \in \{1, 2, ..., r\} \text{ e } i \in \{1, 3, ..., 2k-1\},$$

isto é, x_j tem ordem 2 em $(\mathbb{K}^*, \cdot)$ e y_{i+1} é o inverso de y_i em $(\mathbb{K}^*, \cdot)$. Como V é anel de valorização de $\mathbb{K}$, temos que $0, 1, x_1, x_2, ..., x_r$ estão em V. Além disso, $y_i \in V$ ou $y_{i+1} \in V$, para $i = 1, 3, ..., 2k - 1$. Segue que V tem pelo menos 2+r+k elementos. Pelo teorema de Lagrange, temos que $\mid V \mid = \mid \mathbb{K} \mid$. Portanto $V = \mathbb{K}$.

(b) Seja $\mathbb{K}$ uma extensão algébrica do corpo finito $\mathbb{K}_0$ e V anel de valorização de $\mathbb{K}$. Como $A = V \cap \mathbb{K}_0$ é um anel de valorização de $\mathbb{K}_0$, pelo item (a) temos que $A = \mathbb{K}_0$. Assim, $\mathbb{K}_0 \subseteq V$. Seja $\alpha \in \mathbb{K}^*$. Então $\alpha \in V$ ou $\alpha^{-1} \in V$. Se $\alpha^{-1} \in V$, temos $\mathbb{K}_0[\alpha^{-1}] \subseteq V$. Como

$\mathbb{K}$ é algébrico sobre $\mathbb{K}_0$ e $\alpha^{-1} \in \mathbb{K}$, temos que $\mathbb{K}_0[\alpha^{-1}]$ é corpo contendo $(\alpha^{-1})^{-1}$. Segue que $\alpha = (\alpha^{-1})^{-1} \in \mathbb{K}_0[\alpha^{-1}] \subseteq V$. Assim, mostramos que se $\alpha \in \mathbb{K}$ e $\alpha^{-1} \in V$, temos que $\alpha \in V$. Logo, $\alpha \in \mathbb{K}$ implica em $\alpha \in V$, isto é, $V = \mathbb{K}$. $\square$

Exemplo 1.1 Se p é primo, então $\mathbb{Z}_p$ só tem anel de valorização $\mathbb{Z}_p$.

Exemplo 1.2 Vimos que $\mathbb{Z}$ não é anel de valorização de $\mathbb{Q}$. No entanto, $\mathbb{Q}$ possui anéis de valorização próprios. Dado $p \in \mathbb{Z}$ um número primo, o conjunto $\mathbb{Z}_{(p)} = \{ab^{-1};\ a, b \in \mathbb{Z},\ p \nmid b\}$ é um anel de valorização próprio de $\mathbb{Q}$, denominado *anel de valorização p-ádico* de $\mathbb{Q}$. Claro que $\mathbb{Z}_{(p)}$ é próprio, pois $\frac{1}{p} \in \mathbb{Q} \setminus \mathbb{Z}_{(p)}$. Considerando $\frac{a}{b}$ uma fração irredutível em $\mathbb{Q}$ e supondo que $\frac{a}{b} \notin \mathbb{Z}_{(p)}$, temos que $p \mid b$ e $p \nmid a$, pois $\frac{a}{b}$ é fração irredutível. Logo, $(\frac{a}{b})^{-1} = \frac{b}{a} \in \mathbb{Z}_{(p)}$.

Exemplo 1.3 O corpo dos números reais possui anéis de valorização próprios. Provaremos isso após a demonstração do Teorema da Extensão.

Provaremos na Proposição 1.1.9 que qualquer anel de valorização próprio de $\mathbb{Q}$ é da forma $\mathbb{Z}_{(p)}$. Veremos também que $\mathbb{Z}_{(p)}$ é a localização de $\mathbb{Z}$ segundo o sistema multiplicativo $S = \mathbb{Z} \backslash p\mathbb{Z}$.

Vamos estudar agora a estrutura dos ideais de um anel de valorização e obter resultados bastante utilizados nas próximas seções.

Proposição 1.1.1 *Seja V um domínio que não é corpo. A interseção dos ideais não nulos de V é trivial.*

Demonstração

Seja $\{I_\lambda\}_{\lambda \in \Lambda}$ a família de todos os ideais não nulos de V. Vamos supor que $0 \neq y \in \bigcap_{\lambda \in \Lambda} I_\lambda$. Como $\bigcap_{\lambda \in \Lambda} I_\lambda$ é ideal que contém y, temos que $yV \subseteq \bigcap_{\lambda \in \Lambda} I_\lambda \subseteq yV$. Logo $y^2V \subseteq yV = \bigcap_{\lambda \in \Lambda} I_\lambda \subseteq y^2V$ implica em $y^2V = yV$. Assim, $y = y^2v$, para algum $v \in V$. Portanto, y é inversível em V. Assim, todo ideal não nulo de V contém o elemento inversível y, isto é, V é o único ideal não nulo de V. Segue que V é corpo, o que é uma contradição. $\square$

Corolário 1.1.1 *Se V é anel de valorização próprio do corpo $\mathbb{K}$, então a interseção dos ideais não nulos de V é trivial.*

Demonstração

Se V é corpo, então $V = c.fr(V) = \mathbb{K}$. Logo V não é corpo e basta aplicar a proposição anterior. $\square$

A seguir provaremos que a relação de inclusão é uma relação de ordem total no conjunto dos ideais de um anel de valorização de um corpo.

Proposição 1.1.2 *Seja V um anel de valorização do corpo $\mathbb{K}$. O conjunto dos ideais de V é totalmente ordenado por inclusão.*

Demonstração

Basta mostrar que se I e J são ideais de V, então $I \subseteq J$ ou $J \subseteq I$. Se $I \nsubseteq J$, então existe $x \in I \setminus J$ e $x \neq 0$. Seja $y \in J$. Caso $y = 0$, é imediato que $y \in I$. Caso $y \neq 0$, temos $x^{-1}y \in \mathbb{K}^*$. Como V é anel de valorização de $\mathbb{K}$, temos $x^{-1}y \in V$ ou $(x^{-1}y)^{-1} = xy^{-1} \in V$. No primeiro caso, $x \in I$ e $x^{-1}y \in V$ implica que $y \in I$. No segundo caso, $y \in J$ e $xy^{-1} \in V$ implica que $x \in J$, o que contradiz nossa hipótese. Portanto, $I \subseteq J$ ou $J \subseteq I$. $\square$

Observe que a Proposição 1.1.2 pode ser usada para provar que $\mathbb{Z}$ não é anel de valorização de $\mathbb{Q}$, pois $2\mathbb{Z}$ e $3\mathbb{Z}$ são ideais de $\mathbb{Z}$ e não são comparáveis.

Se o anel V for um domínio comutativo, é válida uma recíproca da proposição anterior, conforme afirma a proposição seguinte.

Proposição 1.1.3 *Sejam V um domínio comutativo e $\mathbb{K}$ seu corpo de frações. Se os ideais de V estão totalmente ordenados por inclusão, então V é um anel de valorização de $\mathbb{K}$.*

Demonstração

Seja $x \in \mathbb{K}^*$, $x = ab^{-1}$ com $a, b \in V$. Por hipótese, $aV \subseteq bV$ ou $bV \subseteq aV$. No primeiro caso, $a = bc$, para algum $c \in V$. Assim, $x = ab^{-1} = bcb^{-1} = c \in V$. No segundo caso, $b = ad$, para algum $d \in V$. Assim, $x^{-1} = ba^{-1} = ada^{-1} = d \in V$. $\square$

A proposição seguinte afirma que um anel de valorização de um corpo é um anel de Bezout, isto é, todo ideal finitamente gerado é principal.

Proposição 1.1.4 *Se V é um anel de valorização do corpo $\mathbb{K}$, então todo ideal finitamente gerado de V é principal.*

Demonstração

Seja $I = x_1V + x_2V + \cdots + x_nV$ um ideal finitamente gerado de V. Pela Proposição 1.1.2, existe $i_0 \in \{1, \cdots, n\}$ tal que $x_iV \subseteq x_{i_0}V$, para todo $i \in \{1, \cdots, n\}$. Logo, $I = x_{i_0}V$. $\square$

Utilizaremos o lema seguinte para mostrar que um anel de valorização de um corpo é local e para descrever o seu ideal maximal. Denotaremos por $\mathfrak{M}_V$ o único ideal maximal do anel local V.

Lema 1.1.2 *Seja V um anel com unidade. São equivalentes:*

(i) O anel V é local;

(ii) O conjunto $V \backslash U(V)$ é um ideal de V.

Nesse caso, $\mathfrak{M}_V = V \backslash U(V)$.

Demonstração

$(i) \Rightarrow (ii)$ Para provar que $V \backslash U(V)$ é um ideal de V, consideremos $x, y \in V \backslash U(V)$. Se $x = 0$ ou $y = 0$, é claro que $x - y \in V \backslash U(V)$. Se $x \neq 0$ e $y \neq 0$ então xV e yV são ideais não nulos de V. Se $xV = V$ ou $yV = V$, temos que x ou y é inversível, contradizendo nossa escolha de x e de y. Logo, xV e yV são ideais próprios de V e portanto xV deve estar contido em algum ideal maximal de V, e o mesmo vale para yV. Como V é local, temos que xV e yV estão contidos em $\mathfrak{M}_V$. Assim $x, y \in \mathfrak{M}_V \subseteq V \backslash U(V)$. Com isso, $x - y \in V \backslash U(V)$. Agora, dado $a \in V$, é claro que $xa \notin U(V)$, pois caso contrário, $x \in U(V)$, contradizendo a escolha de x. Portanto $V \backslash U(V)$ é um ideal de V.
$(ii) \Rightarrow (i)$ Seja I um ideal de V tal que $V \backslash U(V) \subsetneqq I \subseteq V$. Então existe $x \in I \subseteq V$ tal que $x \notin V \setminus U(V)$. Decorre que $x \in U(V)$ e assim $I = V$. Portanto $V \backslash U(V)$ é um ideal maximal de V. Como $V \backslash U(V)$ contém qualquer outro ideal próprio de V, segue que $V \backslash U(V)$ é o único ideal maximal de V. Assim, V é um anel local e $\mathfrak{M}_V = V \setminus U(V)$. $\square$

Definiremos agora um radical muito utilizado em Teoria dos Anéis, o *Radical de Jacobson*, e vamos relacioná-lo com os anéis de valorização de um corpo. No próximo capítulo estudaremos este radical com mais detalhes.

Definição 1.1.2 *O Radical de Jacobson de um anel A é a interseção de todos os ideais maximais de A, e é denotado por $J(A)$.*

Proposição 1.1.5 *Se V é um anel de valorização do corpo $\mathbb{K}$, então V é um anel local e seu único ideal maximal é $J(V) = V\backslash U(V)$.*

Demonstração

Sejam I e J ideais maximais de V. Sabemos que $I \subseteq J$ ou $J \subseteq I$. Assim, $I \subseteq J \subseteq V$ implica que $J = I$ ou $J = V$, pois I maximal. Como J também é ideal maximal, temos $J = I$. Da mesma maneira, $J \subseteq I \subseteq V$ implica que $I = J$. Logo, V tem único ideal maximal, que por definição é $J(V)$. Assim V é local e pelo lema anterior, $J(V) = \mathfrak{M}_V = V \setminus U(V)$. $\square$

Na proposição anterior note que a igualdade $J(V) = V\backslash U(V)$ é válida para qualquer subanel local do corpo $\mathbb{K}$, não necessariamente anel de valorização. Assim, quando V é um anel local temos $\mathfrak{M}_V = J(V) = V\backslash U(V)$.

A igualdade entre anéis de valorização do mesmo corpo $\mathbb{K}$ é equivalente a igualdade dos elementos não inversíveis desses anéis, como mostra o corolário abaixo.

Corolário 1.1.2 *Sejam V_1 e V_2 anéis de valorização do corpo $\mathbb{K}$. São equivalentes:*

(i) $V_1 = V_2$,

(ii) $\mathfrak{M}_{V_1} = \mathfrak{M}_{V_2}$.

Demonstração

É claro que só precisamos provar $(ii) \Rightarrow (i)$ e que para isso basta verificar a inclusão $V_1 \subseteq V_2$, pois a outra é análoga. Seja $x \in {V_1}^* \subseteq \mathbb{K}^*$. Dentre as quatro possibilidades

$$x, x^{-1} \notin V_2,\ x \notin V_2 \text{ e } x^{-1} \in V_2,\ x \in V_2 \text{ e } x^{-1} \notin V_2,\ x, x^{-1} \in V_2,$$

devemos excluir as duas primeiras. Como V_2 é anel de valorização de $\mathbb{K}$, não ocorre $x, x^{-1} \notin V_2$. No caso $x \notin V_2$ e $x^{-1} \in V_2$, temos que $x^{-1} \in V_2 \setminus U(V_2) = \mathfrak{M}_{V_2} = \mathfrak{M}_{V_1}$. Como $x \in V_1$, isso leva a contradição $1 = xx^{-1} \in \mathfrak{M}_{V_1}$. Portanto, $V_1 \subseteq V_2$. $\square$

A próxima proposição prova que um anel de valorização de um corpo é um domínio integralmente fechado, o que pode ser usado para ver que $\mathbb{R}$ não é um anel de valorização de $\mathbb{C}$, já que $i = \sqrt{-1} \in \mathbb{C} \setminus \mathbb{R}$ e é inteiro sobre $\mathbb{R}$.

Proposição 1.1.6 *Se V é um anel de valorização do corpo $\mathbb{K}$, então V é integralmente fechado, isto é, $\{x \in \mathbb{K};\ x \text{ é inteiro sobre } V\} = V$.*

Demonstração

Seja $\overline{V} = \{x \in \mathbb{K};\ x \text{ inteiro sobre V}\}$. Claro que $V \subseteq \overline{V}$, pois dado $a \in V$, a é raiz de $X - a \in V[X]$. Seja $x \in \overline{V}$. Podemos supor $x \neq 0$ e $x^{-1} \in V$. Temos que $x \in \mathbb{K}$ e $p(x) = 0$, para algum $p(X)$ mônico em $V[X]$. Então,

$$p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0, \text{ com } a_i \in V \text{ e } x \in \mathbb{K}.$$

Multiplicando a igualdade $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$ por $x^{-n+1} = (x^{-1})^{n-1} \in V$, temos

$$x = -(a_{n-1} + a_{n-2}x^{-1} + ... + a_2x^{-n+3} + a_1x^{-n+2} + a_0x^{-n+1}).$$

Como cada parcela está em V, concluímos que $x \in V$. Portanto, $\overline{V} = V$. $\square$

Seja V um anel comutativo e com unidade. Lembramos que V é um anel noetheriano quando satisfaz a condição das cadeias ascendentes (CCA) com relação aos seus ideais, isto é, se $I_1 \subseteq I_2 \subseteq \cdots$ é uma cadeia de ideais de V, então existe $n_0 \in \mathbb{N}$, tal que $n \geq n_0$ implica em $I_n = I_{n_0}$. Se além disso, V for domínio, dizemos que V é domínio noetheriano. Lembramos ainda que todo ideal do anel noetheriano V é finitamente gerado.

Veremos agora que os anéis de valorização de um corpo, que são domínios principais, são exatamente os domínios de Dedekind do corpo.

Definição 1.1.3 *Seja V uma anel comutativo e com unidade. Dizemos que V é um domínio de Dedekind se é integralmente fechado, noetheriano e se todo ideal primo não nulo de V é maximal.*

Proposição 1.1.7 *Seja V um anel de valorização do corpo $\mathbb{K}$. São equivalentes:*

(i) *V é domínio de Dedekind;*

(ii) *V é anel noetheriano;*

(iii) *V é domínio principal.*

Demonstração

$(i) \Rightarrow (ii)$ É imediato da definição de domínio de Dedekind.

$(ii) \Rightarrow (iii)$ Por hipótese, V é noetheriano. Então todo ideal de V é finitamente gerado. Pela Proposição 1.1.4, todo ideal de V é principal.

$(iii) \Rightarrow (i)$ Como V é domínio principal, temos que V é integralmente fechado e é domínio noetheriano. Resta provar que se I é um ideal primo não nulo de V, então I é maximal. Também por hipótese, $I = <p>$, com $p \neq 0$ e p é elemento primo em V. Seja $J = <q>$ um ideal contendo I, isto é, $<p> \subseteq <q>$. Assim, $p = qt$, para algum $t \in V$. Como p é primo, temos que $p|q$ ou $p|t$. No segundo caso temos que $ps = t$, para algum $s \in V$. Assim, $p = qt = qps$ implica em $p(1 - qs) = 0$ e daí $qs = 1 \in <q> = J$. Portanto, $J = V$. No caso $p|q$, temos $q = rp$, para algum $r \in V$. Assim, $q \in <p>$ e então $J = <q> \subseteq <p> = I$. Portanto, $J = I$. □

Na proposição anterior note que para provarmos as implicações $(i) \Rightarrow (ii)$ e $(iii) \Rightarrow (i)$ não é necessário utilizarmos o fato de V ser um anel de valorização do corpo $\mathbb{K}$.

Conforme citamos anteriormente, vamos provar que todo anel de valorização de $\mathbb{Q}$ é da forma $\mathbb{Z}_{(p)}$, para algum número primo p. Para isso, vamos precisar de uma proposição preliminar, que assegura a maximalidade dos anéis $\mathbb{Z}_{(p)}$ no corpo dos racionais.

Proposição 1.1.8 *Se p é um número primo, então $\mathbb{Z}_{(p)}$ é subanel maximal de $\mathbb{Q}$.*

Demonstração

Consideremos F um subanel de $\mathbb{Q}$ que contenha $\mathbb{Z}_{(p)}$ propriamente, isto é, existe $\frac{m}{n} \in F \subseteq \mathbb{Q}$ tal que $\frac{m}{n} \notin \mathbb{Z}_{(p)}$, com $mdc\{m, n\} = 1$. Assim, temos que $p \mid n$ e $p \nmid m$. Vamos denotar por s a maior potência de p que divide n. Podemos escrever $n = p^s\alpha$, com $\alpha \in \mathbb{Z}$ e $p \nmid \alpha$. Note que $\frac{\alpha}{m} \in \mathbb{Z}_{(p)} \subseteq F$, pois $p \nmid m$. Assim, $\frac{m}{n}\frac{\alpha}{m} = \frac{\alpha}{n} = \frac{\alpha}{p^s\alpha} = \frac{1}{p^s} \in F$. Também $p^{s-1} \in \mathbb{Z}_{(p)} \subseteq F$ e assim, $\frac{1}{p} = \frac{p^{s-1}}{1}\frac{1}{p^s} \in F$. Concluímos que $\frac{1}{p^c} \in F$, para todo $c \in \mathbb{N}$. Vamos utilizar este fato para mostrar que $F = \mathbb{Q}$. Seja $\frac{a}{b} \in \mathbb{Q}$, com $mdc\{a, b\} = 1$. Analisemos o caso em que $p \nmid b$. Isso assegura que $\frac{a}{b} \in \mathbb{Z}_{(p)} \subseteq F$. O outro caso é quando $p \mid b$. Temos $\frac{a}{b} = \frac{a}{p^u r}$, com $r \in \mathbb{Z}$ e $p \nmid r$, isto é, $\frac{a}{r} \in \mathbb{Z}_{(p)} \subseteq F$. Assim, $\frac{a}{b} = \frac{1}{p^u}\frac{a}{r} \in F$. Portanto, $\mathbb{Q} = F$. □

Proposição 1.1.9 *Se V é um anel de valorização de $\mathbb{Q}$, então $V = \mathbb{Q}$ ou $V = \mathbb{Z}_{(p)}$, para algum número primo p.*

Demonstração

Como $1 \in V$, temos que $\mathbb{Z} \subseteq V$. Pela Proposição 1.1.5, sabemos que $\mathfrak{M}_V = V \setminus U(V)$ é o único ideal maximal de V. Vamos provar que $\mathfrak{M}_V \cap \mathbb{Z}$ é ideal primo de $\mathbb{Z}$. Claro que

$\mathfrak{M}_V \cap \mathbb{Z}$ é fechado por somas. Sejam $x \in \mathfrak{M}_V \cap \mathbb{Z}$ e $y \in \mathbb{Z}$. Como $y \in V$ e $x \in \mathfrak{M}_V$, temos que $xy \in \mathfrak{M}_V$. Logo $xy \in \mathfrak{M}_V \cap \mathbb{Z}$, provando que $\mathfrak{M}_V \cap \mathbb{Z}$ é ideal de $\mathbb{Z}$. Para ver que $\mathfrak{M}_V \cap \mathbb{Z}$ é ideal primo, consideremos $a, b \in \mathbb{Z}$ tais que $ab \in \mathfrak{M}_V \cap \mathbb{Z}$. Assim, $a, b \in V$ e $ab \in \mathfrak{M}_V$. Como $\mathfrak{M}_V$ é ideal primo de V, temos que $a \in \mathfrak{M}_V$ ou $b \in \mathfrak{M}_V$. Portanto, $a \in \mathfrak{M}_V \cap \mathbb{Z}$ ou $b \in \mathfrak{M}_V \cap \mathbb{Z}$. Assim, como $\mathfrak{M}_V \cap \mathbb{Z}$ é ideal primo de $\mathbb{Z}$, temos duas possibilidades: $\mathfrak{M}_V \cap \mathbb{Z} = p\,\mathbb{Z}$ para algum número primo p, ou $\mathfrak{M}_V \cap \mathbb{Z} = \{0\}$. Vamos supor que seja válido o primeiro caso e vamos considerar $b \in \mathbb{Z} \setminus p\,\mathbb{Z} = \mathbb{Z} \setminus (\mathfrak{M}_V \cap \mathbb{Z})$. Decorre que $b \notin \mathfrak{M}_V = V \setminus U(V)$. Resulta que $b \in U(V)$ e assim, $b^{-1} \in V$. Portanto, como $\mathbb{Z}_{(p)} = \{ab^{-1};\ a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus p\,\mathbb{Z}\}$, temos que $\mathbb{Z}_{(p)} \subseteq V$, pois $a, b^{-1} \in V$. Note que $V \subsetneqq \mathbb{Q}$, pois $\mathfrak{M}_V \cap \mathbb{Z} = p\mathbb{Z}$. Assim, $\mathbb{Z}_{(p)} \subseteq V \subsetneqq \mathbb{Q}$. Como $\mathbb{Z}_{(p)}$ é subanel maximal de $\mathbb{Q}$, temos que $V = \mathbb{Z}_{(p)}$. Conforme citamos, a segunda possibilidade é que $\mathfrak{M}_V \cap \mathbb{Z} = \{0\}$. Nesse caso, vamos provar que $V = \mathbb{Q}$. Seja $x = ab^{-1} \in \mathbb{Q}$. Então $a \in \mathbb{Z} \subseteq V$. Também $b \in \mathbb{Z} \subseteq V$ e $b \notin \{0\} = \mathfrak{M}_V \cap \mathbb{Z}$. Assim, temos que $b \notin \mathfrak{M}_V = V \setminus U(V)$, isto é, $b^{-1} \in V$. Portanto, $x = ab^{-1} \in V$ e $V = \mathbb{Q}$. $\square$

Veremos agora alguns resultados sobre localização comutativa. Este tópico será utilizado para estender a proposição anterior, caracterizando os anéis de valorização do corpo de frações de um domínio principal. Também utilizaremos localização na demonstração do Teorema da Correspondência e do Teorema da Extensão. Vamos considerar V um anel comutativo e com unidade.

Definição 1.1.4 *Um subconjunto S de V é um sistema multiplicativo quando:*

(a) $1 \in S$;

(b) $0 \notin S$;

(c) $x, y \in S$ implica em $xy \in S$.

Exemplo 1.4 Seja $S = U(V)$. Claro que $1 \in S$ e $0 \notin S$. Também, para $x, y \in S$, existem $a, b \in S$ tais que $xa = 1$ e $yb = 1$. Assim $(xa)(yb) = 1$ implica que $(xy)(ab) = 1$. Portanto $U(V)$ é um sistema multiplicativo.

Exemplo 1.5 Lembramos que $V^* = \{x \in V;\ x \text{ é regular}\}$. Vamos provar que V^* é um sistema multiplicativo. Claro que $1 \in V^*$ e $0 \notin V^*$. Sejam $x, y \in V^*$. Se $(xy)r = 0$, temos

$yr = 0$ pois x é regular. Agora, como y também é regular, temos que $r = 0$. Assim, xy é regular.

Exemplo 1.6 Seja I ideal próprio de V e $S = 1 + I = \{1 + x;\ x \in I\}$. Claro que $1 \in S$, pois $1 = 1 + 0$, com $0 \in I$. Note que $0 \notin S$, pois $0 = 1 + (-1)$ e se $-1 \in I$, temos que $I = S$, uma contradição. Considerando $x, y \in S$, com $x = 1 + x_1$ e $y = 1 + y_1$, temos $xy = 1 + (x_1y_1 + x_1 + y_1) \in 1 + I$. Portanto $1 + I$ é um sistema multiplicativo.

Exemplo 1.7 Seja P um ideal primo de V. Vamos provar que $S = V \backslash P$ é um sistema multiplicativo. Claro que $1 \in V$ e $1 \notin P$. Também $0 \in P$ e $0 \in V$ implicam que $0 \notin V \backslash P$. Sejam $x, y \in V \backslash P$. Como P é ideal primo, temos que $xy \notin P$. Assim, $xy \in V \backslash P$.

Seja S um sistema multiplicativo em um anel V com unidade. Em $V \times S$, definimos

$$(a, s) \equiv (b, t) \Leftrightarrow\ \exists\ u \in S : u(at - bs) = 0.$$

É fácil provar que $\equiv$ é uma relação de equivalência em $V \times S$. Denotamos

$$\tfrac{a}{s} := \{(b, t) \in V \times S;\ (b, t) \equiv (a, s)\} \quad \text{e} \quad S^{-1}V := \{\tfrac{a}{s};\ a \in V, s \in S\}.$$

Em $S^{-1}V$ vamos definir as operações: $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ e $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$. Também não é difícil mostrar que estas operações estão bem definidas.

Proposição 1.1.10 *Com as operações definidas acima, $S^{-1}V$ é anel comutativo com unidade $\frac{1}{1}$.*

Demonstração

Sejam $\frac{a}{s}, \frac{b}{t} \in S^{-1}V$. Desde que $s, t \in S$ e S é um sistema multiplicativo em V, temos que $st \in S$. Segue que $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ e $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$ estão em $S^{-1}V$. Os axiomas que garantem que $S^{-1}V$ é anel são verificados facilmente. □

Definição 1.1.5 *Dizemos que o anel $S^{-1}V$ descrito acima é o anel de frações de V segundo o sistema multiplicativo S. O anel $S^{-1}V$ também é denominado a localização (ou o localizado) de V segundo S.*

Temos interesse especial nas localizações feitas em sistemas multiplicativos do tipo visto no Exemplo 1.7, isto é, sistemas multiplicativos gerados por ideais primos.

Observe que se P é um ideal primo do anel V e $S = V \setminus P$, então a localização de V segundo o sistema multiplicativo S é descrito por $S^{-1}V = \{as^{-1};\ a, s \in V,\ s \notin P\}$. Nesse caso é comum a notação $S^{-1}V = V_{(P)}$, que utilizaremos neste trabalho.

Observação 1.5 Se S_1 e S_2 são sistemas multiplicativos em V, então $S_1 \subseteq S_2$ implica que ${S_1}^{-1}V \subseteq {S_2}^{-1}V$.

Observação 1.6 Se P_1 e P_2 são ideais primos de V, então $P_1 \subseteq P_2$ implica em $V \backslash P_2 \subseteq V \backslash P_1$ e daí $V_{(P_2)} \subseteq V_{(P_1)}$.

Observação 1.7 Considerando a relação de ordem dada pela inclusão de conjuntos, temos que V^* é o maior sistema multiplicativo de um domínio V. Assim, dado outro sistema multiplicativo S de V, vem que $S^{-1}V \subseteq (V^*)^{-1}V = c.fr(V)$. Com isso, domínios localizados são subanéis do corpo de frações.

Observamos ainda que o anel V pode ser entendido como subanel de $S^{-1}V$. Para isso, consideremos o monomorfismo de anéis

$$\begin{array}{rcl} \phi : V & \longrightarrow & S^{-1}V \\ a & \longmapsto & \frac{a}{1} \end{array}$$

Assim, $V \simeq \phi(V) \subseteq S^{-1}V$. Identificando $a \in V$ com $\frac{a}{1} \in S^{-1}V$, temos que V é um subanel de $S^{-1}V$.

Proposição 1.1.11 *Com a notação acima, se $S^{-1}V = V_{(P)}$, então $V_{(P)}$ é um anel local e seu único ideal maximal é $\{as^{-1};\ a, s \in V,\ a \in P,\ s \notin P\} := PV_{(P)}$.*

Demonstração

Sejam $\frac{a}{s}, \frac{b}{t} \in PV_{(P)}$ e $\frac{u}{v} \in V_{(P)}$. Do fato de P ser ideal primo de V segue que $\frac{a}{s} - \frac{b}{t} \in PV_{(P)}$ e $\frac{a}{s}\frac{u}{v} \in PV_{(P)}$. Assim, $PV_{(P)}$ é ideal de $V_{(P)}$. Vamos provar que ele é um ideal próprio. Supondo que $\frac{1}{1} \in PV_{(P)}$, temos $\frac{1}{1} = \frac{a}{s}$, com $a \in P$ e $s \notin P$. Então existe $t \in V \backslash P$, tal que $t(s - a) = 0$. Na igualdade $ta = ts$, observe que o lado esquerdo está em P, pois $a \in P$; mas o lado direito está em $V \backslash P$, pois tanto s como t estão em S, o que é uma contradição. Afirmamos que $V_{(P)} \backslash PV_{(P)} = U(V_{(P)})$. É fácil ver que $U(V_{(P)}) \subseteq V_{(P)} \backslash PV_{(P)}$, pois $PV_{(P)}$

é ideal próprio. Para a inclusão contrária, note que $V_{(P)}\backslash PV_{(P)} = \{ab^{-1};\ a, b \in V,\ a \notin P,\ b \notin P\}$. Então $\frac{a}{b} \in V_{(P)}\backslash PV_{(P)}$ implica que $a \notin P, b \notin P$, isto é , $a, b \in S$. Assim, $\frac{a}{b}$ é inversível, o que prova nossa afirmação. Agora a igualdade $V_{(P)}\backslash PV_{(P)} = U(V_{(P)})$ garante que $V_{(P)} \setminus U(V_{(P)}) = PV_{(P)}$ que, como vimos, é ideal de $V_{(P)}$. Segue do Lema 1.1.2 que $V_{(P)}$ é anel local cujo único ideal maximal é $PV_{(P)}$. □

Exemplo 1.8 Seja p um número primo. O anel $\mathbb{Z}_{(p)} = \{ab^{-1};\ a, b \in \mathbb{Z},\ p \nmid b\}$ que vimos no Exemplo 1.2, é a localização de $\mathbb{Z}$ segundo o sistema multiplicativo $\mathbb{Z} \setminus p\mathbb{Z}$. Pela proposição anterior, seu ideal maximal é $\mathfrak{M}_{\mathbb{Z}_{(p)}} = \{ab^{-1};\ a, b \in \mathbb{Z},\ a \in P,\ b \notin P\} = \{ab^{-1};\ a, b \in \mathbb{Z},\ p \mid a,\ p \nmid b\}$. Também vamos denotar $\mathfrak{M}_{\mathbb{Z}_{(p)}}$ por $p\mathbb{Z}_{(p)}$.

Encerramos aqui a exposição sobre localização comutativa. A primeira aplicação desse conteúdo é na generalização da Proposição 1.1.9, que afirma que todos os anéis de valorização próprios do corpo dos racionais são do tipo $\mathbb{Z}_{(p)}$, para algum número primo p. A proposição seguinte ao lema abaixo afirma que dado um domínio principal V e $\mathbb{K}$ seu corpo de frações, os únicos anéis de valorização próprios de $\mathbb{K}$ que contém V são as localizações de V segundo o sistema multiplicativo $V \setminus P$, onde P é ideal primo de V. O próximo lema será útil na demonstração da Proposição 1.1.12 e do Teorema da Extensão.

Lema 1.1.3 *Seja V um anel de valorização do corpo $\mathbb{K}$.*

(a) *Se B é um subanel de $\mathbb{K}$ tal que $V \subseteq B$, então B também é um anel de valorização de $\mathbb{K}$ e $J(B) \subseteq J(V)$;*

(b) *Sejam B_1, B_2 subanéis de $\mathbb{K}$ tais que $V \subseteq B_1$ e $V \subseteq B_2$. Se $B_1 \subseteq B_2$, então $J(B_2) \subseteq J(B_1)$.*

Demonstração

É imediato que B é um anel de valorização de $\mathbb{K}$. Para o restante, basta provar o segundo item e tomar $B_1 = V$ e $B_2 = B$. Seja $x \in J(B_2) = B_2\backslash U(B_2)$. Podemos assumir $x \neq 0$. Então, $x \in B_2$ e $x^{-1} \notin B_2$ implicam que $x^{-1} \notin B_1$. Assim, $x \in B_1$ e segue que $x \in B_1\backslash U(B_1) = J(B_1)$. Portanto, $J(B_2) \subseteq J(B_1)$ e isto conclui a prova do lema. □

Proposição 1.1.12 *Seja V um domínio principal e $\mathbb{K}$ seu corpo de frações. Seja $P = \langle p \rangle$ um ideal primo não nulo de V e $S = V \setminus P$. Então*

(a) *O conjunto* $V_{(P)} := V_{<p>} = \{ab^{-1},\ a, b \in V,\ b \in S\}$ *é um anel de valorização próprio de* $\mathbb{K}$ *que contém* V.

(b) *Os únicos anéis de valorização próprios de* $\mathbb{K}$ *que contém* V *são os anéis da forma* $V_{<p>}$ *descritos no item* (a), *onde* p *é um elemento primo de* V.

Demonstração

(a) Vimos na Proposição 1.1.11 que $V_{<p>}$ é anel e já observamos anteriormente que as localizações de um domínio estão contidas no seu corpo de frações. Assim, $V_{<p>}$ é subanel de $\mathbb{K}$ e claramente é próprio pois $V_{<p>} = \{ab^{-1};\ a, b \in V,\ b \notin <p>\}$ e daí $\frac{1}{p} \in \mathbb{K} \setminus V_{<p>}$. Também sabemos que $V \subseteq V_{<p>}$. Para ver que $V_{<p>}$ é anel de valorização de $\mathbb{K}$, tomemos $\frac{a}{b} \in \mathbb{K}^*$ uma fração irredutível, isto é, não existe um elemento de V^* que divide a e b ao mesmo tempo. Se $\frac{a}{b} \notin V_{<p>}$, então $p \mid b$. Logo $p \nmid a$ e $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \in V_{<p>}$.

(b) Seja A um anel de valorização de $\mathbb{K}$ tal que $V \subseteq A \subsetneqq \mathbb{K}$. Afirmamos que $V \cap \mathfrak{M}_A$ é ideal primo não nulo de V. Para ver que $V \cap \mathfrak{M}_A \neq \{0\}$, basta tomar $x^{-1} = \frac{b}{a} \in \mathbb{K}^*,\ a, b \in V^* \subseteq A$, tal que $x^{-1} \notin A$. Como $b \in V \subseteq A$ e $x^{-1} = ba^{-1} \notin A$, temos que $a^{-1} \notin A$ e daí $0 \neq a \in A \setminus U(A) = \mathfrak{M}_A$. Logo $V \cap \mathfrak{M}_A \neq \{0\}$. Provemos que $V \cap \mathfrak{M}_A$ é ideal de V. Claro que $V \cap \mathfrak{M}_A$ é fechado por diferenças. Tomemos então $\alpha \in V$ e $\beta \in V \cap \mathfrak{M}_A$. Desde que $\beta \in \mathfrak{M}_A$ e $\alpha \in V \subseteq A$, temos $\beta\alpha \in V \cap \mathfrak{M}_A$. Falta provar que $V \cap \mathfrak{M}_A$ é ideal primo de V. Para isso, tomemos agora $u, v \in V$ tais que $uv \in V \cap \mathfrak{M}_A$. Como $u, v \in V \subseteq A$ e $\mathfrak{M}_A$ é ideal primo de A, devemos ter $u \in V \cap \mathfrak{M}_A$ ou $v \in V \cap \mathfrak{M}_A$. Isso prova a afirmação de que $V \cap \mathfrak{M}_A$ é ideal primo não nulo do domínio principal V, e então existe um elemento primo $p \in V^*$ tal que $V \cap \mathfrak{M}_A = < p > = P$. Fazendo a localização do anel V no sistema multiplicativo $S = V \setminus P$ obtemos $V_{<p>}$, que é sobreanel de V e $V_{<p>} \subseteq \mathbb{K}$. Note que $V_{<p>} \subseteq A$, pois se $rs^{-1} \in V_{<p>}$, então $r, s \in V \subseteq A$ e $s \notin <p> = V \cap \mathfrak{M}_A$. Mas como $s \notin A \setminus U(A)$ e $s \in A$, temos que $s^{-1} \in A$, isto é, $rs^{-1} \in A$. Pelo Lema 1.1.3, a inclusão $V_{<p>} \subseteq A$ garante que $\mathfrak{M}_A \subseteq \mathfrak{M}_{V_{<p>}}$. Vamos mostrar que $\mathfrak{M}_{V_{<p>}} \subseteq \mathfrak{M}_A$. Seja $rs^{-1} \in \mathfrak{M}_{V_{<p>}} = PV_{<p>} = \{\frac{r}{s};\ r, s \in V,\ r \in <p>,\ \ s \notin <p>\}$. Assim, $r \in <p> \subseteq \mathfrak{M}_A = A \setminus U(A)$. Mas $s \in V \subseteq A$ e daí $s^{-1} \in A$. Logo $\frac{r}{s} = rs^{-1} \in \mathfrak{M}_A$. Isso estabelece a igualdade $\mathfrak{M}_A = \mathfrak{M}_{V_{<p>}}$ e pelo Corolário 1.1.2 da Proposição 1.1.5, concluímos que $A = V_{<p>}$. $\square$

Nosso próximo objetivo é demonstrar o Teorema da Correspondência. Precisaremos de alguns resultados e definições preliminares.

Seja V um anel de valorização do corpo $\mathbb{K}$. Consideremos os conjuntos

$$\mathcal{B} = \{B \subseteq \mathbb{K};\ B \text{ é subanel de } \mathbb{K} \text{ e } V \subseteq B\},$$

$$\mathcal{P} = \{P \subseteq V;\ P \text{ é ideal primo de } V\}.$$

Observamos que $V \subseteq B \subseteq \mathbb{K}$ implica que B é local, pois B também é anel de valorização de $\mathbb{K}$. Logo, $J(B) = B \backslash U(B)$ é seu único ideal maximal. Vamos provar que se $B \in \mathcal{B}$, então $J(B)$ é ideal primo de V. Pelo Lema 1.1.3, temos que $J(B) \subseteq J(V) \subseteq V \subseteq B$ e assim $J(B)$ é ideal primo de V. Desta maneira, a aplicação

$$\begin{aligned} \psi : \mathcal{B} &\longrightarrow \mathcal{P} \\ B &\longmapsto J(B) \end{aligned}$$

está bem definida. Também a aplicação ψ reverte a inclusão, conforme o segundo item do Lema 1.1.3.

Definimos a aplicação

$$\begin{aligned} \delta : \mathcal{P} &\longrightarrow \mathcal{B} \\ P &\longmapsto V_{(P)} \end{aligned}$$

Note que δ está bem definida, pois $V \subseteq V_{(P)} \subseteq c.fr(V) = \mathbb{K}$.

A aplicação δ também reverte a inclusão, pois,

$$P_1 \subseteq P_2 \Rightarrow V \backslash P_2 \subseteq V \backslash P_1 \Rightarrow S_2 \subseteq S_1 \Rightarrow {S_2}^{-1}V \subseteq {S_1}^{-1}V \Rightarrow V_{(P_2)} \subseteq V_{(P_1)}.$$

Vamos provar que $\psi^{-1} = \delta$, isto é, vamos provar o teorema seguinte.

Teorema 1.1.1 (Teorema da Correspondência) *Seja V anel de valorização do corpo $\mathbb{K}$. Existe uma correspondência biunívoca, que reverte a inclusão, entre ideais primos de V e sobreanéis de V em $\mathbb{K}$.*

Demonstração

Com a notação acima, basta provar que

(1) $\delta(\psi(B)) = B, \forall\ B \in \mathcal{B}$,

(2) $\psi(\delta(P)) = P, \forall\ P \in \mathcal{P}$.

(1) $\delta(\psi(B)) = \delta(J(B)) = V_{(J(B))}$. Seja $x \in V_{(J(B))}$. Temos que $x = ab^{-1}$, com $a, b \in V \subseteq B$, $b \notin J(B)$. Assim, $b \notin J(B) = B \backslash U(B)$ implica que $b \in U(B)$, isto é $b^{-1} \in B$. Logo, $x \in B$. Por outro lado, seja $x \in B^*$. Então $x \in V$ ou $x^{-1} \in V$. No primeiro caso, nada temos a demonstrar, pois $V \subseteq V_{(J(B))}$. No segundo caso, temos que $x^{-1} \in B$. Logo, $x^{-1} \notin J(B)$. Então, $x = 1.(x^{-1})^{-1} \in V_{(J(B))}$.
(2) $\psi(\delta(P)) = \psi(V_{(P)}) = J(V_{(P)})$. Observe que

$$(*) \quad V \subseteq V_{(P)} \Rightarrow J(V_{(P)}) \subseteq J(V) \subseteq V.$$

Vimos que o único ideal maximal de $V_{(P)}$ é

$$J(V_{(P)}) = PV_{(P)} = \{as^{-1},\ a \in P,\ s \in V,\ s \notin P\}.$$

Assim, sendo $x \in P$, $x = x.(1)^{-1} \in J(V_{(P)})$. Por outro lado, seja $x = as^{-1} \in J(V_{(P)})$, $a \in P$, $s \notin P$. Por (*), $x = as^{-1} \in V$. Então $a = xs \in P$, com $x, s \in V$. Como P é ideal primo de V e $s \notin P$, temos $x \in P$. $\square$

O último resultado que provaremos nesta seção é o Teorema da Extensão, que assegura que se R é um anel de valorização do corpo $\mathbb{L}$ e $\mathbb{K}$ é uma extensão de corpos de $\mathbb{L}$, então o anel de valorização R de $\mathbb{L}$ pode ser estendido a um anel de valorização V de $\mathbb{K}$ tal que $V \cap \mathbb{L} = R$.

As demonstrações que encontramos do Teorema da Extensão usam resultados sobre places em corpos. No entanto, em [E] Otto Endler afirma que uma demonstração usando apenas anéis de valorização é viável.

Fizemos uma prova do Teorema da Extensão, independente da teoria de places, usando o Lema de Zorn e resultados sobre localização comutativa. A parte essencial de nossa prova está na demonstração da proposição que vem após o lema abaixo.

Lema 1.1.4 *Sejam R um subanel do corpo $\mathbb{K}$ e I um ideal próprio de R. Então para cada $x \in \mathbb{K}^*$, temos que $IR[x]$ é ideal próprio de $R[x]$ ou $IR[x^{-1}]$ é ideal próprio de $R[x^{-1}]$.*

Demonstração

Temos que

$$IR[x] = \left\{ \sum_{i=0}^{n} a_i x^i;\ n \in \mathbb{N},\ a_i \in I \right\} \text{ e } IR[x^{-1}] = \left\{ \sum_{j=0}^{m} b_j x^{-j};\ m \in \mathbb{N},\ b_j \in I \right\}.$$

É fácil ver que $IR[x]$ e $IR[x^{-1}]$ são ideais de $R[x]$ e $R[x^{-1}]$, respectivamente. Vamos supor que ambos não sejam próprios. Então consideremos $m, n \in \mathbb{N}$ e $a_0, a_1, ..., a_n, b_0, b_1, ..., b_m \in I$ tais que $1 = \sum_{i=0}^{n} a_i x^i = \sum_{j=0}^{m} b_j x^{-j}$. Podemos considerar n e m os menores naturais com tal propriedade. Consideremos o caso $m \leq n$. Temos que

$$\begin{aligned} 1 - (b_0 + a_0 - a_0 b_0) &= (1 - b_0)(1 - a_0) \\ &= (1 - b_0) \left(\sum_{i=1}^{n-1} a_i x^i + a_n x^n \right) \\ &= (1 - b_0) \sum_{i=1}^{n-1} a_i x^i + (1 - b_0) a_n x_n \\ &= \sum_{i=1}^{n-1} (1 - b_0) a_i x^i + \sum_{j=1}^{m} a_n x^n b_j x^{-j}. \end{aligned}$$

Assim $1 = b_0 + a_0 - a_0 b_0 + \sum_{i=1}^{n-1} (1 - b_0) a_i x^i + \sum_{j=1}^{m} a_n b_j x^{n-j} = \sum_{i=0}^{n-1} c_i x^i$, onde $c_0 = b_0 + a_0 - a_0 b_0$ quando $m < n$, ou $c_0 = b_0 + a_0 - a_0 b_0 + a_n b_m$ quando $m = n$. Os demais $c_i^{'}s$ são obtidos a partir dos coeficientes correspondentes a x^i nos somatórios do lado esquerdo. Observando que esses coeficientes envolvem apenas $a_0, a_1, ..., a_n, b_0, b_1, ..., b_m \in I$, vem que $c_i \in I$. Obtivemos portanto a igualdade $1 = \sum_{i=0}^{n-1} c_i x^i$, com $c_i \in I$, o que contradiz a minimalidade de n. Analogamente, no caso $n \leq m$ obtêm-se uma contradição com a minimalidade de m. Portanto, a suposição de que $IR[x]$ e $IR[x^{-1}]$ não são ambos ideais próprios não pode ser feita e o lema está provado. $\square$

Proposição 1.1.13 *Seja R um subanel local do corpo $\mathbb{K}$, com ideal maximal $\mathfrak{M}_R$. Existe um anel de valorização V de $\mathbb{K}$, tal que $R \subseteq V$ e $\mathfrak{M}_R \subseteq \mathfrak{M}_V$.*

Demonstração

Seja $\mathcal{F} = \{A \subseteq \mathbb{K};$ A é subanel local, $R \subseteq A$ e $\mathfrak{M}_R \subseteq \mathfrak{M}_A\}$. Note que $R \in \mathcal{F}$, logo $\mathcal{F}$ não é vazio. Vamos definir em $\mathcal{F}$ a relação

$$A \leq B \Leftrightarrow A \subseteq B \text{ e } \mathfrak{M}_A \subseteq \mathfrak{M}_B.$$

É fácil ver que $\leq$ é uma relação de ordem em $\mathcal{F}$. Seja $\{A_\lambda\}_{\lambda\in\Lambda}$ família totalmente ordenada em $\mathcal{F}$. Tome $A = \bigcup_{\lambda\in\Lambda} A_\lambda$ que é subanel de $\mathbb{K}$, pois a família está totalmente ordenada. Afirmamos que A é local. Para provar isso, mostraremos que $J = \bigcup_{\lambda\in\Lambda} \mathfrak{M}_{A_\lambda}$ é ideal de A e $J = A\backslash U(A)$. É claro que J é um subanel de A, pois $\{\mathfrak{M}_{A_\lambda}\}_{\lambda\in\Lambda}$ é cadeia de subanéis de A. Para ver que J é ideal de A, consideremos $a \in A$ e $x \in J$. Então existem $\lambda_i, \lambda_j \in \Lambda$ tais que $a \in A_{\lambda_i}$ e $x \in \mathfrak{M}_{A_{\lambda_j}}$. Podemos ter dois casos:

- $A_{\lambda_i} \subseteq A_{\lambda_j}$ e $\mathfrak{M}_{A_{\lambda_i}} \subseteq \mathfrak{M}_{A_{\lambda_j}}$,

- $A_{\lambda_j} \subseteq A_{\lambda_i}$ e $\mathfrak{M}_{A_{\lambda_j}} \subseteq \mathfrak{M}_{A_{\lambda_i}}$.

Do primeiro caso segue que $a \in A_{\lambda_j}$ e $x \in \mathfrak{M}_{A_{\lambda_j}}$. Assim, $ax \in \mathfrak{M}_{A_{\lambda_j}} \subseteq J$. No segundo caso, temos que $a \in A_{\lambda_i}$ e $x \in \mathfrak{M}_{A_{\lambda_i}}$. Decorre que $ax \in \mathfrak{M}_{A_{\lambda_i}} \subseteq J$. Logo J é um ideal de A. Agora vamos mostrar que $J = A\backslash U(A)$. Sabemos que $J \subseteq A$. Vamos supor que exista $u \in J \cap U(A)$. Assim, $u^{-1} \in A$ e $u \in J$ implicam que $1 \in J = \bigcup_{\lambda\in\Lambda} \mathfrak{M}_{A_\lambda}$. Logo, $1 \in \mathfrak{M}_{A_{\lambda_i}}$, para algum i, e isto contradiz o fato de $\mathfrak{M}_{A_{\lambda_i}}$ ser maximal. Fica provado que $J \subseteq A\backslash U(A)$. Por outro lado, seja $a \in A\backslash U(A)$. Então $a \in A_{\lambda_i}$, para algum $\lambda_i \in \Lambda$. Também $a^{-1} \notin A$, implica que $a^{-1} \notin A_{\lambda_i}$. Assim, $a \notin U(A_{\lambda_i})$. Portanto, $a \in A_{\lambda_i}\backslash U(A_{\lambda_i}) = \mathfrak{M}_{A_{\lambda_i}} \subseteq J$, o que prova a inclusão $A\backslash U(A) \subseteq J$. Assim, $A\backslash U(A)$ é ideal de A. Portanto, A é anel local e o ideal maximal é $\mathfrak{M}_A = A\backslash U(A) = \bigcup_{\lambda\in\Lambda} \mathfrak{M}_{A_\lambda}$. Note que $R \subseteq A_\lambda \subseteq A$, para todo $\lambda \in \Lambda$. Assim, $R \subseteq A$. Note também que

$$\mathfrak{M}_R \subseteq \mathfrak{M}_{A_\lambda} \subseteq \bigcup_{\lambda\in\Lambda} \mathfrak{M}_{A_\lambda} = \mathfrak{M}_A.$$

Logo, $A \in \mathcal{F}$ e A é cota superior para a família $\{A_\lambda\}_{\lambda\in\Lambda}$. Pelo Lema de Zorn, obtemos um elemento maximal $V \in \mathcal{F}$, isto é, V é local, $R \subseteq V$ e $\mathfrak{M}_R \subseteq \mathfrak{M}_V$. Resta mostrar que V é um anel de valorização de $\mathbb{K}$. Seja $x \in \mathbb{K}^*$. Pelo lema anterior, $\mathfrak{M}_V V[\alpha]$ é ideal próprio de $V[\alpha]$, para $\alpha = x$ ou $\alpha = x^{-1}$. Seja P um ideal maximal, portanto primo, de $V[\alpha]$ tal que $\mathfrak{M}_V V[\alpha] \subseteq P$. Considere o sistema multiplicativo $S = V[\alpha]\backslash P$. Então, pela Proposição 1.1.11,

$$S^{-1}V[\alpha] = \{as^{-1};\ a, s \in V[\alpha],\ s \notin P\} \subseteq \mathbb{K}$$

é anel local com ideal maximal $\mathfrak{M}_{S^{-1}V[\alpha]} = \{as^{-1};\ a \in P,\ s \in V[\alpha] \setminus P\}$. Note que

$$R \subseteq V \subseteq V[\alpha] \subseteq S^{-1}V[\alpha] \subseteq \mathbb{K} \quad \text{e} \quad \mathfrak{M}_R \subseteq \mathfrak{M}_V \subseteq \mathfrak{M}_V V \subseteq \mathfrak{M}_V V[\alpha] \subseteq P. \qquad (*)$$

Seja $u \in \mathfrak{M}_V$. Temos que $u = u.1^{-1} \in \mathfrak{M}_{S^{-1}V[\alpha]}$, pois $u \in \mathfrak{M}_V \subseteq P$. Logo, $\mathfrak{M}_R \subseteq \mathfrak{M}_V \subseteq \mathfrak{M}_{S^{-1}V[\alpha]}$. Assim,

$$R \subseteq S^{-1}V[\alpha], \quad \mathfrak{M}_R \subseteq \mathfrak{M}_{S^{-1}V[\alpha]} \quad \text{e} \quad S^{-1}V[\alpha] \text{ é subanel local de } \mathbb{K}.$$

Com isso, $S^{-1}V[\alpha] \in \mathcal{F}$. Também, $\mathfrak{M}_V \subseteq \mathfrak{M}_{S^{-1}V[\alpha]}$ e $V \subseteq S^{-1}V[\alpha]$ implicam que $V \leq S^{-1}V[\alpha]$. Logo, pela maximalidade de V, temos que $V = S^{-1}V[\alpha]$ e assim, por $(*)$, $V = V[\alpha]$. Portanto, $\alpha \in V$. $\square$

Teorema 1.1.2 (Teorema da Extensão) *Seja $\mathbb{L} \subseteq \mathbb{K}$ extensão de corpos e R um anel de valorização de $\mathbb{L}$. Existe um anel de valorização V de $\mathbb{K}$, tal que $V \cap \mathbb{L} = R$.*

$$\begin{tikzcd}
\mathbb{K} \arrow[d, no head] \arrow[r, dotted, no head] & {} \arrow[d, dotted, no head, start anchor=center] \\
\mathbb{L} \arrow[dr, no head] & V \arrow[d, dotted, no head] \\
& R
\end{tikzcd}$$

Demonstração

Como R é um anel de valorização de $\mathbb{L}$, temos que R é subanel local de $\mathbb{K}$ com ideal maximal $\mathfrak{M}_R$. Pela proposição anterior, existe um anel de valorização Vde $\mathbb{K}$ tal que $R \subseteq V$ e $\mathfrak{M}_R \subseteq \mathfrak{M}_V$. Resta demonstrar que $V \cap \mathbb{L} = R$. A inclusão $R \subseteq V \cap \mathbb{L}$ é óbvia. Consideremos $x \in V \cap \mathbb{L}$. Podemos considerar $x \neq 0$. Como $x \in \mathbb{L}$ e R é anel de valorização de $\mathbb{L}$, temos que $x \in R$ ou $x^{-1} \in R$. Vamos supor que $x^{-1} \in R$. Temos que $x^{-1} \notin \mathfrak{M}_V$, pois caso contrário, $1 \in \mathfrak{M}_V$, já que $x \in V$. Assim, $x^{-1} \notin \mathfrak{M}_V$ e $\mathfrak{M}_R \subseteq \mathfrak{M}_V$ implica que $x^{-1} \notin \mathfrak{M}_R = R \backslash U(R)$. Como $x^{-1} \in R$, segue que $x^{-1} \in U(R)$, isto é, $x \in R$. $\square$

Com a notação do teorema anterior, dizemos que V é uma extensão do anel de valorização R, o que justifica a denominação do Teorema da Extensão. Observamos que a extensão V em geral não é única, como pode ser visto em ([BrG$_1$], Corollary 13.5, p. 96).

Corolário 1.1.3 *Seja $\mathbb{L} \subseteq \mathbb{K}$ extensão de corpos. Para cada anel de valorização próprio de $\mathbb{L}$ existe um anel de valorização próprio de $\mathbb{K}$.*

Demonstração

Seja R um anel de valorização próprio de $\mathbb{L}$. Pelo Teorema da Extensão, existe um anel de valorização V de $\mathbb{K}$ tal que $V \cap \mathbb{L} = R$. Supondo $V = \mathbb{K}$, temos $\mathbb{L} = \mathbb{L} \cap \mathbb{K} = \mathbb{L} \cap V = R$, o que contradiz o fato de R ser próprio. $\square$

Corolário 1.1.4 *O corpo $\mathbb{R}$ dos números reais possui uma infinidade de anéis de valorização próprios.*

Demonstração

Sabemos que os anéis $\mathbb{Z}_{(p)}$, com p um número primo, são anéis de valorização próprios de $\mathbb{Q}$. Aplicando o Teorema da Extensão, concluímos que para cada número primo p, existe um anel de valorização V_p de $\mathbb{R}$, tal que $V_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$. Pelo corolário anterior, para cada número primo p, V_p é anel de valorização próprio de $\mathbb{R}$. Note que se p_1 e p_2 são números primos distintos, temos que $\frac{1}{p_1} \in V_{p_2}$ e $\frac{1}{p_1} \notin V_{p_1}$. Logo, $V_{p_1} \neq V_{p_2}$, o que conclui a prova do corolário. $\square$

Observamos que no corolário anterior, se substituirmos $\mathbb{R}$ pelo corpo $\mathbb{C}$ dos números complexos, a mesma demonstração assegura que $\mathbb{C}$ também possui uma infinidade de anéis de valorização próprios. O mesmo vale para qualquer subcorpo de $\mathbb{C}$ contendo $\mathbb{Q}$, por exemplo, os corpos $\mathbb{Q}\left[\sqrt{p}\right]$, com p um número primo.

1.2 Funções Valorização

Nesta seção definiremos as valorizações de Krull de um corpo, verificaremos algumas de suas propriedades e provaremos que existe uma correspondência biunívoca entre anéis de valorização e classes de valorizações de Krull.

Seja $(G, +)$ grupo totalmente ordenado pela relação $\leq$. Denotaremos a união do símbolo ∞ ao grupo G por $G \cup \{\infty\}$ e vamos considerar as convenções:

- $g + \infty = \infty + g = \infty + \infty = \infty$, $\forall\ g \in G$;
- $g < \infty$, $\forall\ g \in G$;
- $g_1 \leq g_2 \Rightarrow g_1 + h \leq g_2 + h$, $\forall\ g_1, g_2, h \in G$.

Definição 1.2.1 *Seja $\mathbb{K}$ um corpo. Uma função $v : \mathbb{K} \longrightarrow G \cup \{\infty\}$ é uma valorização de Krull, se:*

(a) $v(x) = \infty \Leftrightarrow x = 0$;

(b) $v(xy) = v(x) + v(y)$, $\forall\ x, y \in \mathbb{K}$;

(c) $v(x + y) \geq min\{v(x), v(y)\}$, $\forall\ x, y \in \mathbb{K}$.

Chamaremos as valorizações de Krull somente de *valorizações*.

Sempre se pode considerar v sobrejetora. De fato, os itens (a) e (b) dizem que v é um homomorfismo entre os grupos $(\mathbb{K}^*, \cdot)$ e $(G, +)$. Então, se necessário, podemos trocar G pelo grupo $v(\mathbb{K}^*)$. O grupo $v(\mathbb{K}^*)$ é chamado de *grupo de valores* de v.

Assumiremos que v é sobrejetora. Note que neste caso o grupo de valores $G = v(\mathbb{K}^*)$ é abeliano, pois dados $a, b \in G$, temos $a = v(x)$, $b = v(y)$ com $x, y \in \mathbb{K}^*$ e $a + b = v(x) + v(y) = v(xy) = v(yx) = v(y) + v(x) = b + a$. Portanto, trabalharemos sempre com v sobrejetora e G abeliano.

O lema seguinte apresenta propriedades básicas de uma valorização.

Lema 1.2.1 *Seja v uma valorização do corpo $\mathbb{K}$. Então:*

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

(b) $v(-x) = v(x)$, $\forall\ x \in \mathbb{K}$;

(c) $v(x^{-1}) = -v(x)$, $\forall\ x \in \mathbb{K}^*$.

Demonstração

(a) $v(1) = v(1.1) = v(1) + v(1)$. Logo, $v(1) = 0$. Também $0 = v(1) = v((-1)(-1)) = v(-1) + v(-1)$. Como G é totalmente ordenado, podemos ter $v(-1) > 0$, $v(-1) < 0$ ou $v(-1) = 0$. Supondo $v(-1) > 0$, temos $0 < v(-1) < v(-1) + v(-1) = v(1)$. Da mesma forma, se $v(-1) < 0$, temos $0 > v(-1) > v(-1) + v(-1) = v(1)$. Portanto, $v(-1) = 0$.
(b) $v(-x) = v(-1.x) = v(-1) + v(x) = v(x)$.
(c) $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$. Logo $v(x^{-1}) = -v(x)$. □

No próximo teorema veremos que é possível associar a uma valorização um anel de valorização do corpo. Este anel é composto dos elementos cuja imagem pela valorização é maior ou igual à imagem do elemento neutro da multiplicação.

Teorema 1.2.1 *Seja v uma valorização de $\mathbb{K}$. Então:*

(a) $A_v = \{x \in \mathbb{K};\ v(x) \geq 0\}$ *é um anel de valorização de* $\mathbb{K}$*;*

(b) $J_v = \{x \in \mathbb{K};\ v(x) > 0\}$ *é o único ideal maximal de* A_v*;*

(c) $J(A_v) = J_v = \{x \in A_v;\ x = 0$ *ou* $x^{-1} \notin A_v\}$.

Demonstração

(a) Como $v(0) = \infty$ e $v(1) = 0$, temos que $0, 1 \in A_v$. Sejam $x, y \in A_v$. Observe que

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

Logo, A_v é subanel de $\mathbb{K}$. Consideremos $x \in \mathbb{K}^*$. Como $v(x^{-1}) = -v(x)$, temos que $v(x) \geq 0$ ou $v(x^{-1}) \geq 0$ e isto diz que $x \in A_v$ ou $x^{-1} \in A_v$. Portanto, A_v é um anel de valorização de $\mathbb{K}$.

(b) Analogamente ao item anterior, é fácil ver que J_v é fechado por diferenças. Agora, sejam $x \in J_v$ e $y \in A_v$. Então $v(x) > 0$ e $v(y) \geq 0$ implicam que $v(x) + v(y) > 0$. Assim, $xy \in J_v$. Logo J_v é ideal de A_v. Do fato de A_v ser anel de valorização de $\mathbb{K}$ decorre que seu único ideal maximal é $A_v \backslash U(A_v)$. Provemos que $J_v = A_v \backslash U(A_v)$. Lembremos que $v(1) = 0$ implica que $1 \notin J_v$. Isto nos diz que J_v é ideal próprio de A_v. Logo $J_v \subseteq A_v \backslash U(A_v)$, pois J_v deve estar contido num ideal maximal e o único ideal maximal é $A_v \backslash U(A_v)$. Por outro lado, seja $x \in A_v \backslash U(A_v)$. Então $x \in A_v$ e $x^{-1} \notin A_v$. Assim, $v(x) \geq 0$ e $-v(x) = v(x^{-1}) < 0$ implicam que $v(x) > 0$. Logo, $x \in J_v$.

(c) Por definição, $J(A_v)$ é a interseção de todos os ideais maximais de A_v. Então, $J(A_v) = J_v$, pois J_v é o único ideal maximal. Resta provar que $J_v = \{x \in A_v, x = 0$ ou $x^{-1} \notin A_v\}$. Seja $x \in J_v$. Podemos supor $x \neq 0$. Temos que $v(x^{-1}) = -v(x) < 0$. Logo, $x^{-1} \notin A_v$. Por outro lado, seja $x \in A_v$ tal que $x \neq 0$ e $x^{-1} \notin A_v$. Assim, $-v(x) = v(x^{-1}) < 0$ implica que $v(x) > 0$. Logo, $x \in J_v$. $\square$

A cada valorização v do corpo $\mathbb{K}$ associamos o anel de valorização A_v de $\mathbb{K}$. Para termos uma correspondência bem definida, trabalheremos com classes de valorizações. Para isso usamos a definição abaixo.

Definição 1.2.2 *Sejam* u *e* v *valorizações do corpo* $\mathbb{K}$*. Dizemos que* $u \sim v$ *(*u *é equivalente a* v*) quando* $A_u = A_v$*.*

É fácil ver que $\sim$ é uma relação de equivalência. Denotamos por $[v]$ a classe de equivalência da valorização v. Assim, temos uma aplicação bem definida

$$\begin{array}{rcl} \psi : \{[v],\ v \text{ valorização de } \mathbb{K}\} & \longrightarrow & \{A;\ A \text{ anel de valorização de } \mathbb{K}\} \\ [v] & \longmapsto & A_v \end{array}$$

Mostraremos que ψ é bijetora, isto é, existe uma correspondência $1-1$ entre anéis de valorização do corpo $\mathbb{K}$ e classes de valorizações de $\mathbb{K}$. Para isso construiremos a inversa de ψ.

Seja A anel de valorização do corpo $\mathbb{K}$. Considere o conjunto

$$G = \{xA;\ x \in \mathbb{K}^*\}$$

onde a igualdade é definida por $xA = yA \Leftrightarrow xy^{-1} \in U(A)$. Nestas condições, a aplicação

$$\begin{array}{rcl} + : G \times G & \longrightarrow & G \\ (xA, yA) & \longmapsto & (xy)A \end{array}$$

é uma operação bem definida em G. De fato, se $x_1A = x_2A$ e $y_1A = y_2A$, então $x_1A + y_1A = x_1y_1A = x_1y_2A = x_1Ay_2 = x_2Ay_2 = x_2y_2A = x_2A + y_2A$. É fácil ver que $(G, +)$ é grupo abeliano com elemento neutro $A = 1A$ e cujo simétrico de $xA \in G$ é $x^{-1}A$. Também G é isomorfo ao grupo multiplicativo $\frac{\mathbb{K}^*}{U(A)}$. Para ver isso, basta notar que $\varphi : \frac{\mathbb{K}^*}{U(A)} \longrightarrow G$, dada por $\varphi(xU(A)) = xA$ é um isomorfismo de grupos.

Dados $xA, yA \in G$, definimos

$$xA \leq yA \Leftrightarrow yA \subseteq xA$$

Vamos mostrar que a relação acima é uma relação de ordem total em G. Para $x, y \in \mathbb{K}^*$, temos que $y^{-1}x \in \mathbb{K}^*$. Daí $y^{-1}x \in A$ ou $x^{-1}y \in A$. Se $y^{-1}x \in A$, então $y^{-1}xA \subseteq A$ implica em $xA \subseteq yA$. Analogamente, $x^{-1}y \in A$ implica em $yA \subseteq xA$. Portanto, G é um grupo abeliano totalmente ordenado.

Definimos agora a aplicação

$$\begin{aligned} v: \mathbb{K} &\longrightarrow G \cup \{\infty\} \\ 0 &\longmapsto \infty \\ x &\longmapsto xA,\ x \neq 0 \end{aligned}$$

Note que $v|_{\mathbb{K}^*} : \mathbb{K}^* \longrightarrow G$ é um homomorfismo sobrejetor de grupos e $Ker(v) = \{x \in \mathbb{K}^*;\ xA = 1A\} = U(A)$ e assim temos novamente $\frac{\mathbb{K}^*}{U(A)} \simeq G$.

Proposição 1.2.1 *Seja A um anel de valorização do corpo $\mathbb{K}$. Com a notação estabelecida acima, temos que:*

(a) *v é uma valorização de $\mathbb{K}$;*

(b) $A_v = A$;

Demonstração

(a) Claro que $v(x) = \infty \Leftrightarrow x = 0$. Sejam $x, y \in \mathbb{K}$. Vamos mostrar que $v(xy) = v(x)+v(y)$. Note que se $x = 0$ ou $y = 0$, o resultado é imediato. Supondo $x \neq 0$ e $y \neq 0$, temos que $v(xy) = xyA = xA + yA = v(x) + v(y)$. Resta provar que $v(x + y) \geq min\{v(x), v(y)\}$. Se $x + y = 0$ é claro que a afirmação é verdadeira. Supondo $x + y \neq 0$, temos $v(x + y) = (x + y)A \subseteq xA + yA$. Como G é totalmente ordenado, $xA \subseteq yA$ ou $yA \subseteq xA$. Assim, $xA + yA \subseteq xA$ ou $xA + yA \subseteq yA$. Então, podemos afirmar que $xA + yA \subseteq zA$, onde zA é o maior na relação $\subseteq$ entre xA e yA. Conseqüentemente, $zA = min\{xA, yA\}$, segundo $\leq$. Portanto, $v(x + y) \geq zA = min\{xA, yA\} = min\{v(x), v(y)\}$.
(b) Como o elemento neutro de G é A, temos

$$A_v = \{x \in \mathbb{K} : v(x) \geq A\} = \{0\} \cup \{x \in \mathbb{K}^* : xA \subseteq A\}.$$

é fácil provar que $\{0\} \cup \{x \in \mathbb{K}^* : xA \subseteq A\} = A$. Para isso, seja $x \in \mathbb{K}^*$ tal que $xA \subseteq A$. Então $xy \in A$, para todo $y \in A$. Fazendo $y = 1$, vem que $x \in A$. Por outro lado, $x \in A^*$ implica que $xy \in A$, para todo $y \in A$. $\square$

O item (a) da proposição anterior assegura que a cada anel de valorização A do corpo

$\mathbb{K}$ podemos associar a valorização

$$\begin{aligned} v : \mathbb{K} &\longrightarrow G \cup \{\infty\} \\ 0 &\longmapsto \infty \\ x &\longmapsto xA,\ x \neq 0 \end{aligned}$$

Definimos agora

$$\begin{aligned} \phi : \{A;\ A \text{ anel de valorização de } \mathbb{K}\} &\longrightarrow \{[v];\ v \text{ valorização de } \mathbb{K}\} \\ A &\longmapsto [v] \end{aligned}$$

onde v é a valorização associada à A.

Mostraremos a seguir que ϕ é a inversa de

$$\begin{aligned} \psi : \{[v];\ v \text{ valorização de } \mathbb{K}\} &\longrightarrow \{A;\ A \text{ anel de valorização de } \mathbb{K}\} \\ [v] &\longmapsto A_v \end{aligned}$$

Teorema 1.2.2 *Existe uma correspondência biunívoca entre anéis de valorização do corpo* $\mathbb{K}$ *e classes de valorizações de* $\mathbb{K}$.

Demonstração

Pelo visto acima, basta provar que $\psi(\phi(A)) = A$ e $\phi(\psi[v]) = [v]$.

Claro que $\psi(\phi(A)) = \psi([v])$, com $A_v = A$ pelo item (b) da Proposição 1.2.1. Mas $\psi([v]) = A_v$. Portanto $\psi(\phi(A)) = A$. Por outro lado, $\phi(\psi[v]) = \phi(A_v)$. Mas $\phi(A_v) = [w]$, com $A_w = A_v$ pelo item (b) da Proposição 1.2.1. Por definição, $A_v = A_w$ implica que $v \sim w$, isto é, $[v] = [w]$. Portanto, $\phi(\psi[v]) = \phi(A_v) = [w] = [v]$. $\square$

Exemplo 1.9 Seja $\mathbb{K}$ um corpo e $G = \{0\}$ o grupo formado apenas pelo elemento neutro. A aplicação

$$\begin{aligned} v : \mathbb{K} &\longrightarrow G \cup \{\infty\} \\ 0 &\longmapsto \infty \\ x &\longmapsto 0,\ x \neq 0 \end{aligned}$$

é uma valorização de $\mathbb{K}$, chamada de valorização trivial. Note que $A_v = \mathbb{K}$, isto é, a valorização trivial corresponde ao anel de valorização trivial.

Exemplo 1.10 Pelo exemplo anterior, para qualquer corpo $\mathbb{K}$ podemos definir a valorização trivial. Mas se $\mathbb{K}$ é um corpo finito ou é uma extensão algébrica de um corpo finito, então o Lema 1.1.1 garante que o único anel de valorização de $\mathbb{K}$ é o próprio $\mathbb{K}$, que corresponde à valorização trivial. Neste caso, pelo Teorema 1.2.2, a única valorização de $\mathbb{K}$ é a trivial.

Exemplo 1.11 Seja $\mathbb{M}$ um subcorpo de $\mathbb{K}$. É fácil ver que a restrição à $\mathbb{M}$ de uma valorização de $\mathbb{K}$ é uma valorização de $\mathbb{M}$.

Exemplo 1.12 Seja $\mathbb{K}$ um corpo. Denotamos por $\partial p(x)$ o grau do polinômio $p(x) \in \mathbb{K}[x]$ e denotamos por $\mathbb{K}(x)$ o corpo de frações de $\mathbb{K}[x]$. A aplicação

$$\begin{aligned} v : \mathbb{K}(x) &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ 0 &\longmapsto \infty \\ \tfrac{p(x)}{q(x)} &\longmapsto \partial q(x) - \partial p(x) \end{aligned}$$

é uma valorização de $\mathbb{K}(x)$ em $\mathbb{Z} \cup \{\infty\}$. De fato, $v\left(\frac{p(x)}{q(x)}\right) = \infty \Leftrightarrow \frac{p(x)}{q(x)} = 0$. Também, se $\alpha = \frac{p(x)}{q(x)}$ e $\beta = \frac{r(x)}{s(x)}$ são elementos de $\mathbb{K}(x)$, é imeditato verificar que $v(\alpha\beta) = v(\alpha) + v(\beta)$. Para mostrar que $v(\alpha\beta) \geq min\{v(\alpha), v(\beta)\}$, note que $v(\alpha + \beta) =$

$$= \partial(q(x)s(x)) - \partial(p(x)s(x) + r(x)q(x)) \geq \partial q(x) + \partial s(x) - max\{\partial(p(x)s(x)),\ \partial(r(x)q(x))\}.$$

Supondo $\partial(p(x)s(x)) = max\{\partial(p(x)s(x)),\ \partial(r(x)q(x))\}$, decorre que

$$\partial q(x) + \partial s(x) - max\{\partial(p(x)s(x)),\ \partial(r(x)q(x))\} = \partial q(x) + \partial s(x) - \partial(p(x)s(x)).$$

Assim, $v(\alpha+\beta) \geq \partial q(x) + \partial s(x) - \partial(p(x)s(x)) = \partial q(x) - \partial p(x) = v(\alpha) \geq min\{v(\alpha),\ v(\beta)\}$. Analogamente, se $\partial(r(x)q(x)) = max\{\partial(p(x)s(x)),\ \partial(r(x)q(x))\}$, temos que $v(\alpha + \beta) \geq v(\beta) \geq min\{v(\alpha),\ v(\beta)\}$. Portanto, v é uma valorização de $\mathbb{K}(x)$.

Exemplo 1.13 Para p primo, vamos definir a *valorização p-ádica* de $\mathbb{Q}$. Se $\frac{a}{b} \in \mathbb{Q}$, então existem $n \in \mathbb{Z}$ e inteiros r, s primos relativos com p, tais que $\frac{a}{b} = p^n.\frac{r}{s}$. Definimos

$$\begin{aligned} v_p : \mathbb{Q} &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ 0 &\longmapsto \infty \\ 0 \neq p^n.\tfrac{r}{s} &\longmapsto n \end{aligned}$$

Não é difícil provar que v_p é uma valorização de $\mathbb{Q}$. Além disso, dada uma fração irredutível $\frac{a}{b} \in \mathbb{Q}$,

$$\tfrac{a}{b} \in A_v \Leftrightarrow v_p(\tfrac{a}{b}) \geq 0 \Leftrightarrow p \nmid b \Leftrightarrow \tfrac{a}{b} \in \mathbb{Z}_{(p)}.$$

Portanto $A_v = \mathbb{Z}_{(p)}$, isto é, a valorização p-ádica está associada ao anel de valorização p-ádico de $\mathbb{Q}$.

As valorizações p-ádicas citadas acima caracterizam completamente as valorizações não triviais de $\mathbb{Q}$. De fato, pela Proposição 1.1.9, os únicos anéis de valorização não triviais de $\mathbb{Q}$ são os anéis de valorizaçao p-ádicos $\mathbb{Z}_{(p)}$, onde p é um número primo. Vimos no Exemplo 1.13 que para as valorizações p-ádicas de $\mathbb{Q}$ correspondem os anéis de valorização p-ádicos de $\mathbb{Q}$. Pelo Teorema 1.2.2, essa correspondência é biunívoca e assim, dada uma valorização não trivial de $\mathbb{Q}$, ela é equivalente à uma valorização do tipo v_p.

1.3 Places

Vimos anteriormente que existe uma correspondência biunívoca entre anéis de valorização de um corpo $\mathbb{K}$ e classes de valorizações de Krull definidas sobre $\mathbb{K}$. Similarmente, vamos mostrar que existe uma correspondência biunívoca entre anéis de valorização de $\mathbb{K}$ e classes de places sobrejetores definidos sobre o corpo projetivo $\mathbb{K} \cup \{\infty\}$. Para fazer isso, iniciaremos provando propriedades dos places e estudaremos suas relações com os homomorfismos de anéis.

Definiremos a equivalência de places com base numa relação que chamaremos de *quase ordem* no conjunto dos places sobrejetores.

As principais proposições desta seção seguem o exposto em ([E], § 8).

Definição 1.3.1 *O corpo projetivo de* $\mathbb{K}$ *é* $\tilde{\mathbb{K}} = \mathbb{K} \cup \{\infty\}$ *onde definimos:*

(*a*) $x + \infty = \infty + x = \infty$, $\forall\ x \in \mathbb{K}$;

(*b*) $x.\infty = \infty.x = \infty$, $\forall\ x \in \tilde{\mathbb{K}}$, $x \neq 0$;

(*c*) $0^{-1} = \infty, \quad \infty^{-1} = 0, \quad -\infty = \infty.$

Note que não estão definidos $\infty + \infty$, $0.\infty$ e $\infty.0$.

Definição 1.3.2 *Um place do corpo $\mathbb{K}$ no corpo $\mathbb{L}$ é uma aplicação $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$ tal que, para todos $x, y \in \tilde{\mathbb{K}}$, tem-se*

(*a*) *Se $x + y$ e $\pi(x) + \pi(y)$ estão definidos, então $\pi(x + y) = \pi(x) + \pi(y)$;*

(*b*) *Se xy e $\pi(x)\pi(y)$ estão definidos, então $\pi(xy) = \pi(x)\pi(y)$;*

(*c*) *Existe $z \in \tilde{\mathbb{K}}$ tal que $\pi(z) = 1$.*

Na proposição seguinte provamos algumas propriedades operacionais dos places. No que segue, vamos utilizá-las bastante sem maiores referências.

Proposição 1.3.1 *Dado um place $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$, são válidas as seguintes afirmações, para todos $x, y \in \tilde{\mathbb{K}}$.*

(*a*) $\pi(1) = 1, \quad \pi(0) = 0, \quad e \quad \pi(\infty) = \infty$*;*

(*b*) *Se $\pi(x)+\pi(y)$ (respectivamente $\pi(x)\pi(y)$) está definido, então também está definido $x + y$ (respectivamente xy);*

(*c*) $\pi(-x) = -\pi(x)$*;*

(*d*) $\pi(x^{-1}) = \pi(x)^{-1}$*;*

Demonstração

(*a*) Seja $z \in \tilde{\mathbb{K}}$ tal que $\pi(z) = 1$. Então $z.1$ e $\pi(z)\pi(1)$ estão definidos. Segue que $1 = \pi(z) = \pi(z.1) = \pi(z)\pi(1) = 1.\pi(1) = \pi(1)$.

Como $1+0$ e $\pi(1)+\pi(0)$ estão definidos, temos $1 = \pi(1) = \pi(1+0) = \pi(1)+\pi(0) = 1+\pi(0)$. Logo, $\pi(0) = 0$.

Como $1 + \infty$ e $\pi(1) + \pi(\infty)$ estão definidos, temos $\pi(\infty) = \pi(1 + \infty) = \pi(1) + \pi(\infty) = 1 + \pi(\infty)$. Assim, $\pi(\infty) = \infty$.

(b) Como $\pi(x)+\pi(y)$ está definido, temos que $(\pi(x),\pi(y)) \neq (\infty,\infty)$. Assim, $(x,y) \neq (\infty,\infty)$, isto é, $x \neq \infty$ ou $y \neq \infty$. Dessa forma, $x+y$ está definido. Se $\pi(x)\pi(y)$ está definido, temos que $(\pi(x),\pi(y)) \notin \{(0,\infty),(\infty,0)\}$ e pelo item anterior $(x,y) \notin \{(0,\infty),(\infty,0)\}$. Logo, xy está definido.
(c) Se $\pi(-x)+\pi(x)$ não está definido, então $\pi(x) = \pi(-x) = \infty$. Isso implica que $-\pi(x) = -\infty = \infty = \pi(x)$. Se $\pi(-x)+\pi(x)$ está definido, pelo item anterior, $-x+x$ está definido. Assim, $0 = \pi(0) = \pi(-x+x) = \pi(-x)+\pi(x)$. Portanto, $\pi(-x) = -\pi(x)$.
(d) Se $\pi(x^{-1})\pi(x)$ não está definido, então $(\pi(x^{-1}),\pi(x)) \in \{(0,\infty),(\infty,0)\}$. Logo, $\pi(x^{-1}) = (\pi(x))^{-1}$. Se $\pi(x^{-1})\pi(x)$ está definido, então $x^{-1}x$ também está definido, e assim, $1 = \pi(1) = \pi(x^{-1}x) = \pi(x^{-1})\pi(x)$. Logo, $\pi(x^{-1}) = (\pi(x))^{-1}$. $\square$

Note que os itens (a), (c) e (d) são propriedades idênticas às propriedades de homomorfismos de anéis, porém agora, elas são válidas para todo o corpo projetivo.

Utilizando o que foi definido e demonstrado anteriormente, já podemos associar à um place um anel de valorização.

Proposição 1.3.2 *Seja $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$ um place. Então,*

(a) *$\pi^{-1}(\mathbb{L})$ é um anel de valorização A_π de $\mathbb{K}$, e $\pi|_{A_\pi} : A_\pi \longrightarrow \mathbb{L}$ é um homomorfismo de anéis com núcleo $J(A_\pi) = \mathfrak{M}_{A_\pi}$;*

(b) *$\pi^{-1}(\mathbb{L}^*) = U(A_\pi)$ e $\pi|_{U(A_\pi)} : U(A_\pi) \longrightarrow \mathbb{L}^*$ é um homomorfismo de grupos com núcleo $1+\mathfrak{M}_{A_\pi}$.*

Demonstração
(a) Como $\pi(\infty) = \infty$, é claro que $\pi^{-1}(\mathbb{L}) \subseteq \mathbb{K}$. Vamos provar, primeiramente, que $\pi^{-1}(\mathbb{L})$ é um subanel de $\mathbb{K}$. Como $1 \in \pi^{-1}(\mathbb{L})$, temos que $\pi^{-1}(\mathbb{L})$ não é vazio. Sejam $x, y \in \pi^{-1}(\mathbb{L})$. Então $\pi(x) \neq \infty$ e $\pi(y) \neq \infty$. Desta forma, $\pi(x)+\pi(y)$ e $\pi(x)\pi(y)$ estão definidos e conseqüentemente, $x+y$ e xy também estão definidos. Assim, como

$$\pi(x+y) = \pi(x)+\pi(y) \in \mathbb{L} \text{ e } \pi(xy) = \pi(x)\pi(y) \in \mathbb{L},$$

temos que $x+y$, $xy \in \pi^{-1}(\mathbb{L})$. Também, $\pi(x) \in \mathbb{L}$ implica em $-\pi(x) = \pi(-x) \in \mathbb{L}$. Segue que $-x \in \pi^{-1}(\mathbb{L})$. Logo, $\pi^{-1}(\mathbb{L})$ é um subanel de $\mathbb{K}$.
Considerando $x \in \mathbb{K}\backslash A_\pi$, tem-se que $x \notin \{y \in \mathbb{K}; \pi(y) \in \mathbb{L}\}$ e assim, $\pi(x) = \infty$. Com isso, $(\pi(x))^{-1} = \pi(x^{-1}) = 0 \in \mathbb{L}$, implica que $x^{-1} \in A_\pi$. Portanto, A_π é anel de valorização de

$\mathbb{K}$.

Seja $\pi^* = \pi|_{A_\pi}$. Para $a, b \in A_\pi$, temos $\pi^*(a) = \pi(a) \neq \infty$ e $\pi^*(b) = \pi(b) \neq \infty$. Logo, $\pi(a)+\pi(b)$ e $\pi(a)\pi(b)$ estão definidos, o que implica que $a+b$ e ab estão definidos. Assim, $\pi^*(a+b) = \pi(a+b) = \pi(a)+\pi(b) = \pi^*(a)+\pi^*(b)$. Analogamente, $\pi^*(ab) = \pi^*(a)\pi^*(b)$. Logo, π^* é um homomorfismo de A_π em $\mathbb{L}$. Também, $\pi^*(A_\pi)$ é subanel de $\mathbb{L}$, já que é a imagem do homomorfismo π^*. Observamos que $\mathfrak{M}_{A_\pi} = J(A_\pi)$, pois A_π é anel de valorização de $\mathbb{K}$. Resta provar que $Ker(\pi^*) = \mathfrak{M}_{A_\pi}$. Observando que $\pi(1) = 1$ e $1 \in A_\pi$, tem-se que $1 \notin Ker(\pi^*)$. Assim, $Ker(\pi^*)$ é um ideal próprio de A_π, logo deve estar contido em algum ideal maximal de A_π. Como $\mathfrak{M}_{A_\pi}$ é o único ideal maximal, temos que $Ker(\pi^*) \subseteq \mathfrak{M}_{A_\pi}$. Por outro lado, $x \in \mathfrak{M}_{A_\pi}$ implica que $x^{-1} \notin A_\pi = \pi^{-1}(\mathbb{L})$. De fato, se $x^{-1} \in A_\pi$, então $xx^{-1} = 1 \in \mathfrak{M}_{A_\pi}$, contradizendo a maximalidade de $\mathfrak{M}_{A_\pi}$. Como $(\pi(x))^{-1} = \pi(x^{-1}) \notin \mathbb{L}$, segue que $(\pi(x))^{-1} = \pi(x^{-1}) = \infty$. Logo $\pi(x) = 0$. Portanto, $x \in Ker(\pi^*)$.

(b) Vimos que $Ker(\pi^*) = \mathfrak{M}_{A_\pi}$. Então $\pi^{-1}(\mathbb{L}^*) = \{x \in A_\pi;\ \pi(x) \neq 0\} = A_\pi \backslash \mathfrak{M}_{A_\pi} = U(A_\pi)$. Também $\pi|_{U(A_\pi)} : U(A_\pi) \longrightarrow \mathbb{L}^*$ é um homomorfismo entre grupos multiplicativos. É fácil ver que seu núcleo é $1 + \mathfrak{M}_{A_\pi}$. De fato,

$$\pi(x) = 1 \Leftrightarrow \pi(x-1) = 0 \Leftrightarrow x - 1 \in \mathfrak{M}_{A_\pi} \Leftrightarrow x \in 1 + \mathfrak{M}_{A_\pi},$$

concluindo assim a demonstração. □

Pelo item (a) da proposição anterior, qualquer place de $\mathbb{K}$ em $\mathbb{L}$ induz um homomorfismo $\lambda : A \longrightarrow \mathbb{L}$ de um anel de valorização A de $\mathbb{K}$ em $\mathbb{L}$, com núcleo $\mathfrak{M}_A$. A recíproca também é verdadeira, conforme afirma a próxima proposição.

Proposição 1.3.3 *Seja A um anel de valorização de $\mathbb{K}$ e $\lambda : A \longrightarrow \mathbb{L}$ um homomorfismo sobre um corpo $\mathbb{L}$, com núcleo $\mathfrak{M}_A$. Então, a aplicação*

$$\begin{array}{rcl} \pi : \tilde{\mathbb{K}} & \longrightarrow & \tilde{\mathbb{L}} \\ x & \longmapsto & \lambda(x),\ \text{se } x \in A \\ x & \longmapsto & \infty,\ \text{se } x \in \tilde{\mathbb{K}} \backslash A \end{array}$$

é um place de $\mathbb{K}$ em $\mathbb{L}$ com $A_\pi = A$.

Demonstração

Inicialmente vamos provar que π é um place, verificando as condições (a), (b) e (c) da

Definição 1.3.2.

(c) Como $1 \in A \subseteq \tilde{\mathbb{K}}$ temos que $\pi(1) = \lambda(1) = 1$.

(a) Sejam $x, y \in \tilde{\mathbb{K}}$ tais que $x + y$ e $\pi(x) + \pi(y)$ estão definidos. Desde que $\pi(x) + \pi(y)$ está definido, devemos ter $(\pi(x), \pi(y)) \neq (\infty, \infty)$. Basta analisar dois casos:

$$\pi(x) \neq \infty \text{ e } \pi(y) = \infty \quad \text{ e } \quad \pi(x) \neq \infty \text{ e } \pi(y) \neq \infty.$$

No primeiro caso, $\pi(x) + \pi(y) = \pi(x) + \infty = \infty$. Por outro lado, nesse caso temos que $x \in A$ e $y \in \tilde{\mathbb{K}} \backslash A$ pela definição de π. Isso leva a $x + y \in \tilde{\mathbb{K}} \backslash A$. Portanto $\pi(x + y) = \infty = \pi(x) + \pi(y)$.

Do segundo caso segue que $x, y \in A$. Daí $x + y \in A$ e $\pi(x + y) = \lambda(x + y) = \lambda(x) + \lambda(y) = \pi(x) + \pi(y)$.

(b) Iniciamos observando que $(\pi(x), \pi(y)) \in \{(0, \infty), (\infty, 0)\}$ implica que $\pi(x)\pi(y)$ não está definido. Assim, como no caso anterior, basta analisarmos dois casos:

$$\pi(x) = \infty \text{ e } \pi(y) \neq 0 \quad \text{ e } \quad \pi(x) \neq \infty \text{ e } \pi(y) \neq \infty.$$

No segundo caso, como $\pi(x) \neq \infty$ e $\pi(y) \neq \infty$, temos que $x, y \in A$. Logo

$$\pi(xy) = \lambda(xy) = \lambda(x)\lambda(y) = \pi(x)\pi(y).$$

No primeiro caso, consideremos $x, y \in \tilde{\mathbb{K}}$ tais que $\pi(x) = \infty$ e $\pi(y) \neq 0$. Assim, analisando as possibilidades para x e y, temos:

$$x = \infty \text{ ou } y = \infty \Rightarrow \pi(xy) = \infty = \pi(x)\pi(y);$$

$$x \neq \infty \text{ e } y \neq \infty \Rightarrow x \in \mathbb{K} \backslash A \text{ e } y \in U(A).$$

Para ver que de fato $y \in U(A)$, devemos provar que $y \neq 0$ e $y, y^{-1} \in A$. Claro que $y \neq 0$, pois, caso contrário, $0 = y \in A$ implica que $\pi(y) = \lambda(y) = 0$. Sabemos que $y \in A$ ou $y^{-1} \in A$. Se $y \in A$, temos que $\infty \neq \pi(y) = \lambda(y) \in \mathbb{L}$. Como $\lambda(y) \neq 0$, segue que $(\lambda(y))^{-1} = \lambda(y^{-1}) \in \mathbb{L}$. Com isso, $\lambda(y^{-1}) \neq \infty$. Assim, $y^{-1} \in A$. Da mesma forma, prova-se que se $y^{-1} \in A$, então $y \in A$. Concluímos que $y \in U(A)$. Lembrando que $x \in \mathbb{K} \backslash A$, temos que $xy \in \mathbb{K} \backslash A$. Assim, $\pi(xy) = \infty = \pi(x)\pi(y)$.

Resta mostrar que $A_\pi = A$. Provamos que π é um place, logo, $A_\pi = \pi^{-1}(\mathbb{L})$. Dessa forma,

$$x \in A_\pi \Leftrightarrow x \in \mathbb{K} \text{ e } \pi(x) \in \mathbb{L} \Leftrightarrow \pi(x) \neq \infty \Leftrightarrow x \in A,$$

o que conclui a demonstração. $\square$

Observação 1.8 Para qualquer place $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$, temos que $\pi(A_\pi)$ é um subcorpo de $\mathbb{L}$. De fato, consideremos $0 \neq y \in \pi(A_\pi) \subseteq \mathbb{L}$. Então $y = \pi(x)$, para algum $x \in A_\pi^*$. Mas $\pi(x^{-1}) = (\pi(x))^{-1} = y^{-1} \in \mathbb{L}^*$ implica em $x^{-1} \in A_\pi$ e $y^{-1} \in \pi(A_\pi)$.

Observação 1.9 O corpo $\pi(A_\pi)$ definido no item anterior é chamado de *corpo residual* de π.

Observação 1.10 Um place π definido sobre o corpo projetivo $\tilde{\mathbb{K}}$ também pode ser considerado como um place de $\mathbb{K}$ em $\pi(A_\pi)$. Assim, $\mathbb{L} = \pi(A_\pi)$ se, e somente se, $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$ for sobrejetor, nesse caso, chamaremos π de *place sobrejetor*.

Observação 1.11 Se A é anel de valorização do corpo $\mathbb{K}$, então pela proposição anterior, o homomorfismo canônico $\pi_A^* : A \longrightarrow \frac{A}{\mathfrak{M}_A}$ pode ser estendido para um place $\pi_A : \tilde{\mathbb{K}} \longrightarrow \frac{A}{\mathfrak{M}_A} \cup \{\infty\}$, que é sobrejetor pois π_A^* é sobrejetor. Este place é chamado de *place canônico* correspondente ao anel A.

Exemplo 1.14 Vimos anteriormente que dado um número primo p, o anel $\{ab^{-1};\ a, b \in \mathbb{Z},\ p \nmid b\}$ é um anel de valorização próprio de $\mathbb{Q}$ com ideal maximal $p\mathbb{Z}_{(p)} = \{ab^{-1};\ a, b \in \mathbb{Z},\ p \mid a\ ,\ p \nmid b\}$. Vamos descrever um place definido sobre $\tilde{\mathbb{Q}}$ cujo anel de valorização é $\mathbb{Z}_{(p)}$. Seja $\mathbb{L} = \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}}$. Consideremos o homomorfismo canônico:

$$\lambda : \mathbb{Z}_{(p)} \longrightarrow \mathbb{L}$$

$$\frac{a}{b} \longmapsto \left[\frac{a}{b}\right]$$

onde $\left[\frac{a}{b}\right]$ representa a classe do elemento $\frac{a}{b}$. Claramente, $Ker(\lambda) = p\mathbb{Z}_{(p)}$. Aplicando a Proposição 1.3.3, temos que a aplicação π_p, dada por

$$\pi_p : \tilde{\mathbb{Q}} \longrightarrow \tilde{\mathbb{L}}, \text{ tal que } \pi_p\left(\frac{a}{b}\right) = \begin{cases} \lambda\left(\frac{a}{b}\right) = \left[\frac{a}{b}\right], & \text{se } \frac{a}{b} \in \mathbb{Z}_{(p)},\ (\ p \nmid b) \\ \infty, & \text{se } \frac{a}{b} \notin \mathbb{Z}_{(p)},\ (p \mid b) \end{cases}$$

é um place de $\mathbb{Q}$ em $\mathbb{L}$, cujo anel de valorização é $\mathbb{Z}_{(p)}$.

Definição 1.3.3 *Seja p um número primo. O place π_p descrito acima é denominado o place p-ádico de $\mathbb{Q}$.*

Além de garantir que dado um anel de valorização de um corpo é possível associar a ele um place sobrejetor, a Proposição 1.3.3 ainda permite o cálculo efetivo de tal place, conforme fizemos no Exemplo 1.14.

Definiremos agora uma classe especial de places, os *places triviais*, que serão úteis nos próximos resultados.

Definição 1.3.4 *Um place $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$ é chamado de place trivial se $A_\pi = \mathbb{K}$, ou, equivalentemente, $\mathfrak{M}_{A_\pi} = \{0\}$.*

Os places triviais de $\mathbb{K}$ em $\mathbb{L}$ são exatamente os monomorfismos $\mu : \mathbb{K} \longrightarrow \mathbb{L}$, estendidos por $\mu(\infty) = \infty$.

A Proposição 1.3.3 ainda pode ser aplicada para garantir que se A é o anel de valorização trivial do corpo $\mathbb{K}$ (isto é, $A = \mathbb{K}$), então podemos associar à A um place trivial. Para isso observe que $A = \mathbb{K}$ implica que $\mathfrak{M}_A = \{0\}$ e assim $\frac{A}{\mathfrak{M}_A} = A$. Então, a aplicação

$$\begin{aligned} \lambda : A &\longrightarrow \tfrac{A}{\mathfrak{M}_A} = A \\ a &\longmapsto a \end{aligned}$$

é um homomorfismo de corpos. Consideremos a aplicação identidade estendida à $\tilde{\mathbb{K}}$:

$$\begin{aligned} \pi : \tilde{\mathbb{K}} &\longrightarrow \tilde{\mathbb{K}} \\ x &\longmapsto x \\ \infty &\longmapsto \infty \end{aligned}$$

Pela Proposição 1.3.3, temos que π é um place com $A_\pi = A = \mathbb{K}$, isto é, ao anel de valorização trivial corresponde um place trivial.

Veremos agora como um place π de $\mathbb{K}$ em $\mathbb{L}$ se relaciona com subcorpos de $\mathbb{K}$.

Inicialmente consideremos $\mathbb{M}$ um subcorpo do corpo $\mathbb{K}$. Note que $\pi|_{\tilde{\mathbb{M}}} : \tilde{\mathbb{M}} \longrightarrow \tilde{\mathbb{L}}$ é um place de $\mathbb{M}$ em $\mathbb{L}$.

Em particular, se $\mathbb{M}$ é o corpo primo de $\mathbb{K}$, é possível saber quando a restrição de π à $\mathbb{M}$ é um place não-trivial. Veremos isso no Lema 1.3.2, que provaremos usando o lema seguinte.

Lema 1.3.1 *Se p é um número primo, então $\mathbb{Z}_p \simeq \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}}$.*

Demonstração

Vamos definir a aplicação

$$\begin{array}{rcl}\varphi : \mathbb{Z} & \longrightarrow & \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \\ a & \longmapsto & \left[\frac{a}{1}\right]\end{array}$$

Note que $\varphi(a) = \frac{a}{1} + p\mathbb{Z}_{(p)}$. Provemos que φ é um homomorfismo. De fato,

- $\varphi(a+b) = \frac{a+b}{1} + p\mathbb{Z}_{(p)} = \left(\frac{a}{1} + p\mathbb{Z}_{(p)}\right) + \left(\frac{b}{1} + p\mathbb{Z}_{(p)}\right) = \varphi(a) + \varphi(b)$,

- $\varphi(ab) = \frac{ab}{1} + p\mathbb{Z}_{(p)} = \left(\frac{a}{1} + p\mathbb{Z}_{(p)}\right)\left(\frac{b}{1} + p\mathbb{Z}_{(p)}\right) = \varphi(a)\varphi(b)$.

Afirmamos também que $Ker(\varphi) = p\mathbb{Z}$. Para provar isto, note que

$$a \in Ker(\varphi) \Leftrightarrow \frac{a}{1} + p\mathbb{Z}_{(p)} = 0 + p\mathbb{Z}_{(p)} \Leftrightarrow \frac{a}{1} \in p\mathbb{Z}_{(p)} \Leftrightarrow p \mid a \Leftrightarrow a \in p\mathbb{Z}.$$

Demonstraremos agora que φ é sobrejetora. Dado $\frac{a}{b} + p\mathbb{Z}_{(p)} \in \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}}$, temos que $\frac{a}{b} \in \mathbb{Z}_{(p)}$, e daí $p \nmid b$. Segue que $\text{mdc}\{b, p\} = 1$. Logo, existem $r, s \in \mathbb{Z}$ tais que $rb + sp = 1$. Decorre de $arb + asp = a$ que $a - arb = asp \in p\mathbb{Z}$. Assim, $\frac{a-arb}{b} \in p\mathbb{Z}_{(p)}$. Logo $\frac{a}{b} - \frac{ar}{1} \in p\mathbb{Z}_{(p)}$. Desta forma, $\frac{a}{b} + p\mathbb{Z}_{(p)} = \frac{ar}{1} + p\mathbb{Z}_{(p)}$. Tomando então $ar \in \mathbb{Z}$, temos que $\varphi(ar) = \frac{ar}{1} + p\mathbb{Z}_{(p)} = \frac{a}{b} + p\mathbb{Z}_{(p)}$. Logo, φ é sobrejetora e $\frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{Z}_p$. $\square$

Lema 1.3.2 *Seja π um place de $\mathbb{K}$ em $\mathbb{L}$. São equivalentes:*

(i) A restrição de π ao corpo primo de $\mathbb{K}$ é um place não-trivial;

(ii) $Char(\mathbb{L}) \neq Char(\mathbb{K})$.

Nesse caso, $Char(\mathbb{K}) = 0$.

Demonstração

$(i) \Rightarrow (ii)$ Seja $\mathbb{P}$ o corpo primo de $\mathbb{K}$. Então $\mathbb{P} \simeq \mathbb{Q}$ ou $\mathbb{P} \simeq \mathbb{Z}_p$ para algum primo p. Desde que $\pi|_{\tilde{\mathbb{P}}} : \tilde{\mathbb{P}} \longrightarrow \tilde{\mathbb{L}}$ é não trivial por hipótese, temos $(\pi|_{\tilde{\mathbb{P}}})^{-1}(\mathbb{L}) \neq \mathbb{P}$. Mas $(\pi|_{\tilde{\mathbb{P}}})^{-1}(\mathbb{L})$ é anel de valorização de $\mathbb{P}$, isto é, $\mathbb{P}$ tem anel de valorização próprio. Segue do Lema 1.1.1 que $\mathbb{P}$ não é corpo finito e então devemos ter $\mathbb{P} \simeq \mathbb{Q}$. Assim, $Char(\mathbb{P}) = Char(\mathbb{K}) = 0$. Como $(\pi|_{\tilde{\mathbb{P}}})^{-1}(\mathbb{L})$ é anel de valorização de $\mathbb{P}$ e $\mathbb{P} \simeq \mathbb{Q}$, temos duas possibilidades: $(\pi|_{\tilde{\mathbb{P}}})^{-1}(\mathbb{L}) = \mathbb{Q}$ ou $(\pi|_{\tilde{\mathbb{P}}})^{-1}(\mathbb{L}) = \mathbb{Z}_{(p)}$. A primeira possibilidade diz que $(\pi|_{\tilde{\mathbb{P}}})$ é trivial, e portanto, contradiz a hipótese (i). Resta então $(\pi|_{\tilde{\mathbb{P}}})^{-1}(\mathbb{L}) = \mathbb{Z}_{(p)}$. No entanto, vimos na Proposição 1.3.2, que o homomorfismo $(\pi|_{\tilde{\mathbb{P}}})|_{\mathbb{Z}_{(p)}} : \mathbb{Z}_{(p)} \longrightarrow \mathbb{L}$ tem núcleo $\mathfrak{M}_{\mathbb{Z}_{(p)}}$, e sabemos que $\mathfrak{M}_{\mathbb{Z}_{(p)}} = p\mathbb{Z}_{(p)}$.

Pelo lema anterior, temos que $\mathbb{Z}_p \simeq \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}}$. Logo $\mathbb{Z}_p \simeq \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} = \frac{\mathbb{Z}_{(p)}}{\mathfrak{M}_{\mathbb{Z}_{(p)}}} \simeq Im(\mathbb{Z}_p) \subseteq \mathbb{L}$. Com isso, concluímos que $\mathbb{L}$ tem característica p. Lembramos que $Char(\mathbb{K}) = 0$. Logo, $Char(\mathbb{L}) \neq Char(\mathbb{K})$.

$(ii) \Rightarrow (i)$ Veremos inicialmente que $Char(\mathbb{K}) \neq 0$ implica em $Char(\mathbb{L}) = Char(\mathbb{K})$. Sejam p um número primo e $Char(\mathbb{K}) = p$. Então temos em $\mathbb{K}$ a identidade $1+1+\ldots 1 = 0$, para p parcelas. Aplicando π, temos $0 = \pi(0) = \pi(1+1+\ldots 1) = \pi(1)+\ldots \pi(1) = 1+\ldots+1$ que é a soma de p vezes a unidade do corpo $\mathbb{L}$. Logo $Char(\mathbb{L}) = p = Char(\mathbb{K})$. Portanto, a hipótese $Char(\mathbb{L}) \neq Char(\mathbb{K})$ implica em $Char(\mathbb{K}) = 0$ e $Char(\mathbb{L}) = p$, p um número primo. Chamando de $\mathbb{P}$ o corpo primo de $\mathbb{K}$ e π_1 a restrição de π à $\mathbb{P}$, vem que $\mathbb{P} \simeq \mathbb{Q}$, e $A_{\pi_1} = (\pi|_{\tilde{\mathbb{P}}})^{-1}(\mathbb{L})$ é anel de valorização de $\mathbb{Q}$ e $(\pi|_{\tilde{\mathbb{P}}})|_{A_{\pi_1}} : A_{\pi_1} \longrightarrow \mathbb{L}$ é homomorfismo de anéis com núcleo $\mathfrak{M}_{A_{\pi_1}}$. Supondo, por absurdo, que $\pi|_{\tilde{\mathbb{P}}}$ é trivial, temos $A_{\pi_1} = \mathbb{Q}$ e $\mathfrak{M}_{A_{\pi_1}} = \{0\}$. Daí, $(\pi|_{\tilde{\mathbb{P}}}) : \mathbb{Q} \longrightarrow \mathbb{L}$ é monomorfismo, o que implica em $Char(\mathbb{L}) = 0$. Essa condição mostra que $\pi|_{\tilde{\mathbb{P}}}$ não é trivial. $\square$

Vimos na demonstração de $(ii) \Rightarrow (i)$ do lema anterior que se $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$ é um place e $Char(\mathbb{K}) \neq 0$, então $Char(\mathbb{K}) = Char(\mathbb{L})$.

Em particular, se $\pi : \tilde{\mathbb{Z}}_p \longrightarrow \tilde{\mathbb{L}}$ é um place, então $Char(\mathbb{L}) = p$ e usando o Lema 1.3.2 concluímos que π é place trivial, pois $\mathbb{Z}_p$ é seu próprio corpo primo. Logo, $\mathbb{Z}_p$ só tem place trivial.

O lema também garante que o único place $\pi : \tilde{\mathbb{Q}} \longrightarrow \tilde{\mathbb{Q}}$ é o place trivial.

Analogamente aos homomorfismos, a composição de places continua sendo um place, conforme a próxima proposição.

Proposição 1.3.4 *Sejam dois places $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$, $\sigma : \tilde{\mathbb{L}} \longrightarrow \tilde{\mathbb{M}}$ e $A_\pi \subseteq \mathbb{K}$, $A_\sigma \subseteq \mathbb{L}$ seus respectivos anéis de valorização. Então, $\sigma \circ \pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{M}}$ é um place e $A_{\sigma\circ\pi} = \pi^{-1}(A_\sigma) \subseteq A_\pi$. Se π é um place sobrejetor de $\mathbb{K}$ em $\mathbb{L}$, então $\pi(A_{\sigma\circ\pi}) = A_\sigma$.*

Demonstração

Inicialmente vamos provar que $\sigma \circ \pi$ é um place, novamente verificando os itens (a), (b) e (c) da Definição 1.3.2.

(a) Se $\sigma(\pi(x)) + \sigma(\pi(y))$ está definido então $\pi(x) + \pi(y)$ também está definido pois σ é place e daí $\sigma(\pi(x)+\pi(y)) = \sigma(\pi(x))+\sigma(\pi(y))$. Da mesma forma, $\pi(x)+\pi(y)$ está definido implica que $x + y$ está definido e como π é place temos $\pi(x + y) = \pi(x) + \pi(y)$. Assim,

$$(\sigma\circ\pi)(x)+(\sigma\circ\pi)(y)=\sigma(\pi(x)+\pi(y))=\sigma(\pi(x+y))=(\sigma\circ\pi)(x+y).$$

(b) A prova de que $(\sigma\circ\pi)(xy)=(\sigma\circ\pi)(x)(\sigma\circ\pi)(y)$ é análoga ao item anterior.

(c) $(\sigma\circ\pi)(1)=\sigma(\pi(1))=\sigma(1)=1$. Portanto, $\sigma\circ\pi$ é um place.

Para provar que $A_{\sigma\circ\pi}=\pi^{-1}(A_\sigma)\subseteq A_\pi$, consideremos $x\in\tilde{\mathbb{K}}$. Então,

$$x\in A_{\sigma\circ\pi}\Leftrightarrow\sigma(\pi(x))\neq\infty\Leftrightarrow\pi(x)\in A_\sigma\Leftrightarrow x\in\pi^{-1}(A_\sigma).$$

Assim, $A_{\sigma\circ\pi}=\pi^{-1}(A_\sigma)\subseteq\pi^{-1}(\mathbb{L})=A_\pi$, como queríamos demonstrar. Decorre que $\pi(A_{\sigma\circ\pi})\subseteq A_\sigma$. Agora, se $\pi:\tilde{\mathbb{K}}\longrightarrow\tilde{\mathbb{L}}$ é sobrejetor e $y\in A_\sigma$, então existe $x\in\mathbb{K}$, tal que $\pi(x)=y$. Assim, $x\in\pi^{-1}(A_\sigma)=A_{\sigma\circ\pi}$. Concluímos que $y\in\pi(A_{\sigma\circ\pi})$. $\square$

Utilizaremos a próxima proposição para definir uma relação de equivalência no conjunto dos places sobrejetores.

Proposição 1.3.5 *Sejam* $\pi_0:\tilde{\mathbb{K}}\longrightarrow\tilde{\mathbb{L}}_0$ *e* $\pi_1:\tilde{\mathbb{K}}\longrightarrow\tilde{\mathbb{L}}_1$ *places sobrejetores,* $A_0={\pi_0}^{-1}(\mathbb{L}_0)$ *e* $A_1={\pi_1}^{-1}(\mathbb{L}_1)$ *seus respectivos anéis de valorização. São equivalentes:*

(i) $A_1\subseteq A_0$*;*

(ii) *Existe uma aplicação* $\sigma:\tilde{\mathbb{L}}_0\longrightarrow\tilde{\mathbb{L}}_1$*, tal que* $\pi_1=\sigma\circ\pi_0$*.*

Nesse caso, σ *é um place sobrejetor (unicamente determinado) de* $\mathbb{L}_0$ *em* $\mathbb{L}_1$*.*

$$\begin{tikzcd} & \tilde{\mathbb{K}} \arrow[dl, "\pi_0"'] \arrow[dr, "\pi_1"] & \\ \tilde{\mathbb{L}}_0 \arrow[rr, dotted, "\sigma"] & & \tilde{\mathbb{L}}_1 \end{tikzcd}$$

Demonstração

$(i)\Rightarrow(ii)$ Por hipótese, π_0 é sobrejetor. Então dado $y\in\tilde{\mathbb{L}}_0$, existe $x\in\tilde{\mathbb{K}}$, tal que $\pi_0(x)=y$. Podemos definir

$$\sigma:\tilde{\mathbb{L}}_0\longrightarrow\tilde{\mathbb{L}}_1$$

$$y\longmapsto\sigma(y)=\sigma(\pi_0(x))=\pi_1(x).$$

Para provar que σ está bem definida, consideremos $\pi_0(u)=\pi_0(v)\in\tilde{\mathbb{L}}_0$. Basta verificar que $\pi_1(u)=\pi_1(v)$, ou seja, $\sigma(\pi_0(u))=\sigma(\pi_0(v))$. Temos que $u,v\in\tilde{\mathbb{K}}$. Primeiro, vamos supor que $u\notin A_0$. Então, como $\pi_0(u)=\pi_0(v)=\infty$, temos que $v\notin A_0$. Conseqüentemente, $u,v\notin A_1$. Logo, $\pi_1(u)=\pi_1(v)=\infty$. Supondo que $u\in A_0$, temos $\pi_0(u)\neq\infty$ implica que

$\pi_0(u) + \pi_0(-v)$ está definido e $\pi_0(u - v) = \pi_0(u) + \pi_0(-v) = \pi_0(u) - \pi_0(v) = 0$. Assim, $u - v \in Ker(\pi_0) = \mathfrak{M}_{A_0} \subseteq \mathfrak{M}_{A_1} \subseteq A_1$. Então, faz-se necessário analisar os casos em que $u \notin A_1$ e $u \in A_1$. No primeiro caso, temos que $v \notin A_1$. De fato, se $v \in A_1$, então $u = (u-v)+v \in A_1$. Logo, $\pi_1(u) = \pi_1(v) = \infty$. No segundo caso, temos $\pi_1(v) \neq \infty$, o que implica que $\pi_1(u)+\pi_1(-v)$ está definido e $\pi_1(u)+\pi_1(-v) = \pi_1(u)-\pi_1(v) = \pi_1(u-v) = 0$. Logo, $\pi_1(u) = \pi_1(v)$.

$(ii) \Rightarrow (i)$ Vamos provar que σ é um place. Sejam $x, y \in \tilde{\mathbb{L}}_0$ tais que $x + y$ e $\sigma(x) + \sigma(y)$ estão definidos e $x^*, y^* \in \tilde{\mathbb{K}}$ tais que $x = \pi_0(x^*)$ e $y = \pi_0(y^*)$. Assim, temos que $\sigma(x) = \pi_1(x^*)$ e $\sigma(y) = \pi_1(y^*)$. Então, $x + y = \pi_0(x^*) + \pi_0(y^*)$ está definido implica que $\pi_0(x^* + y^*) = \pi_0(x^*) + \pi_0(y^*)$. Também $\sigma(x) + \sigma(y) = \pi_1(x^*) + \pi_1(y^*)$ está definido implica que $\pi_1(x^* + y^*) = \pi_1(x^*) + \pi_1(y^*)$. Assim,

$$\sigma(x + y) = \sigma(\pi_0(x^* + y^*)) = \pi_1(x^* + y^*) = \pi_1(x^*) + \pi_1(y^*) = \sigma(x) + \sigma(y).$$

A prova de que $\sigma(xy) = \sigma(x)\sigma(y)$ é inteiramente análoga. Escolhendo $z = \pi_0(1) \in \tilde{\mathbb{L}}_0$, temos que $\sigma(z) = \sigma(\pi_0(1)) = \pi_1(1) = 1$. Isso conclui a prova de que π é um place. Agora, como π_0 e π_1 são sobrejetores, temos que σ é um place sobrejetor e unicamente determinado de $\mathbb{L}_0$ em $\mathbb{L}_1$. De fato, supondo que $\pi_1 = \sigma \circ \pi_0$ e $\pi_1 = \sigma^* \circ \pi_0$, temos que $\pi_1 = \sigma \circ \pi_0 = \sigma^* \circ \pi_0$ e tomando $x \in \tilde{\mathbb{L}}_0$, sabemos que existe $x^* \in \tilde{\mathbb{K}}$, tal que $\pi_0(x^*) = x$. Assim, $\sigma(x) = \sigma(\pi_0(x^*)) = \sigma^*(\pi_0(x^*)) = \sigma^*(x)$. Também supondo $y \in \tilde{\mathbb{L}}_1$, existe $y^* \in \tilde{\mathbb{K}}$, tal que $\pi_1(y^*) = y$. Logo, $\sigma(\pi_0(y^*)) = \pi_1(y^*) = y$, o que implica que σ é sobrejetor. Pela proposição anterior, $A_1 = A_{\sigma\circ\pi_0} \subseteq A_0$. $\square$

Finalmente podemos definir a relação $<$, com base na qual definiremos a relação de equivalência no conjunto dos places sobrejetores.

Definição 1.3.5 *Sejam $\pi_0 : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}_0$ e $\pi_1 : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}_1$ places sobrejetores. Dizemos que $\pi_1 < \pi_0$ se as condições equivalentes da proposição anterior são válidas, ou seja,*

(a) $A_1 \subseteq A_0$

(b) *Existe uma aplicação $\sigma : \tilde{\mathbb{L}}_0 \longrightarrow \tilde{\mathbb{L}}_1$,* tal que $\pi_1 = \sigma \circ \pi_0$.

Note que $<$ não é uma relação de ordem (chamaremos *quase ordem*), pois não é válida a propriedade anti-simétrica. De fato, $\pi_1 < \pi_0$ implica que $A_1 \subseteq A_0$ e $\pi_0 < \pi_1$ implica que

$A_0 \subseteq A_1$. Assim $A_0 = A_1$. Mas isso não implica que $\pi_0 = \pi_1$, pois seus contradomínios podem ser diferentes.

No entanto, são válidas a reflexividade e a transitividade. Para provar a reflexividade basta tomar σ como a função identidade. Para a propriedade transitiva, sejam π_0, π_1 e π_2 places sobrejetores de $\mathbb{K}$ tal que $\pi_0 < \pi_1$ e $\pi_1 < \pi_2$. Assim, $A_0 \subseteq A_1 \subseteq A_2$. Também $\pi_0 = \sigma_1 \circ \pi_1$ e $\pi_1 = \sigma_2 \circ \pi_2$, implica que $\pi_0 = (\sigma_1 \circ \sigma_2) \circ \pi_2$.

Exemplo 1.15 Seja $i_{\mathbb{K}}$ o place trivial determinado pela função identidade. Claro que $A_{i_{\mathbb{K}}} = \mathbb{K}$. Para qualquer place sobrejetor π de $\mathbb{K}$, temos que $\pi < i_{\mathbb{K}}$, pois $A_\pi \subseteq \mathbb{K}$. Também, $i_{\mathbb{K}} < \pi$ se, e somente se, $\mathbb{K} \subseteq A_\pi$. Assim, $A_\pi = \mathbb{K}$. Portanto, $i_{\mathbb{K}} < \pi$ se, e somente se, π for o place trivial.

Definição 1.3.6 *Dois places sobrejetores π_0 e π_1 de $\mathbb{K}$ são chamados de equivalentes se $\pi_0 < \pi_1$ e $\pi_1 < \pi_0$. Nesse caso, denotaremos $\pi_0 \sim \pi_1$.*

É fácil provar que a relação $\sim$ é de equivalência no conjunto dos places sobrejetores de $\mathbb{K}$. Vamos representar por $[\pi]$ a classe dos places sobrejetores equivalentes à π.

Utilizaremos o próximo lema na demonstração do Teorema 1.3.1, que estabalece uma correspondência biunívoca entre classes de places sobrejetores e anéis de valorização de um corpo.

Lema 1.3.3 *Sejam $\pi_0 : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}_0$ e $\pi_1 : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}_1$ places sobrejetores, $A_0 = {\pi_0}^{-1}(\mathbb{L}_0)$ e $A_1 = {\pi_1}^{-1}(\mathbb{L}_1)$ seus respectivos anéis de valorização. São equivalentes:*

(i) $A_1 = A_0$;

(ii) $\pi_1 = \sigma \circ \pi_0$, *para alguma bijeção* $\sigma : \tilde{\mathbb{L}}_0 \longrightarrow \tilde{\mathbb{L}}_1$;

(iii) $\pi_1 = \sigma \circ \pi_0$, *para algum place trivial* σ *de* $\mathbb{L}_0$;

(iv) π_1 *é equivalente a* π_0.

Demonstração

(i) $\Rightarrow$ *(ii)* Como $A_1 \subseteq A_0$, pela Proposição 1.3.5, existe um place sobrejetor $\sigma : \tilde{\mathbb{L}}_0 \longrightarrow \tilde{\mathbb{L}}_1$ tal que $\pi_1 = \sigma \circ \pi_0$. Sejam $x, y \in \tilde{\mathbb{L}}_0$, tais que $\sigma(x) = \sigma(y)$. Consideremos também $x^*, y^* \in \tilde{\mathbb{K}}$ tais que $x = \pi_0(x^*)$ e $y = \pi_0(y^*)$. Como $\sigma(\pi_0(x^*)) = \sigma(\pi_0(y^*))$, temos $\pi_1(x^*) = \pi_1(y^*)$. De $\pi_1(x^* - y^*) = 0$, segue que $x^* - y^* \in Ker(\pi_1)$. Mas $Ker(\pi_1) = \mathfrak{M}_{A_1} = \mathfrak{M}_{A_0} = Ker(\pi_0)$.

Assim, $\pi_0(x^* - y^*) = 0$ implica que $\pi_0(x^*) = \pi_0(y^*)$. Portanto, $x = y$.

$(ii) \Rightarrow (iii)$ A hipótese (ii) junto com a Proposição 1.3.4, garante que σ é um place sobrejetor. Então, não existe $x \in \mathbb{L}_0$ tal que $\sigma(x) = \infty$. Logo, $\sigma^{-1}(\mathbb{L}_1) = \mathbb{L}_0$ e portanto σ é place trivial.

$(iii) \Rightarrow (iv)$ A hipótese implica que $A_1 \subseteq A_0$, com isso $\pi_1 < \pi_0$. Agora, σ é place trivial, implica que σ é injetora (tem inverso à esquerda), e de $\pi_1 = \sigma \circ \pi_0$ segue que $\sigma^{-1} \circ \pi_1 = \pi_0$. Assim, $A_0 \subseteq A_1$, isto é, $\pi_0 < \pi_1$.

$(iv) \Rightarrow (i)$ $\pi_1 \sim \pi_0 \Rightarrow \pi_1 < \pi_0$ e $\pi_0 < \pi_1$. Assim, $A_1 \subseteq A_0$ e $A_0 \subseteq A_1$. Portanto $A_0 = A_1$.

$\square$

Teorema 1.3.1 *Seja $\mathbb{K}$ um corpo. Existe uma correspondência biunívoca entre anéis de valorização de $\mathbb{K}$ e classes de places sobrejetores de $\mathbb{K}$.*

Demonstração

Vamos definir

$$\begin{aligned} \psi : \{[\pi];\ \text{classes de places sobrejetores de } \mathbb{K}\} &\longrightarrow \{A;\ A \text{ anel de valorização de } \mathbb{K}\} \\ [\pi] &\longmapsto A_\pi \end{aligned}$$

Na Proposição 1.3.4, vimos que $\psi([\pi])$ pertence ao conjunto $\{A;\ A$ anel de valorização de $\mathbb{K}\}$. É fácil ver que ψ está bem definida e é injetora, pois

$$\psi([\pi_1]) = \psi([\pi_2]) \Leftrightarrow A_{\pi_1} = A_{\pi_2} \Leftrightarrow \pi_1 \sim \pi_2 \Leftrightarrow [\pi_1] = [\pi_2].$$

Também ψ é sobrejetora, pois dado A um anel de valorização de $\mathbb{K}$, define-se $\mathbb{L} = \frac{A}{\mathfrak{M}_A}$ e

$$\begin{aligned} \lambda : A &\longrightarrow \mathbb{L} \\ a &\longmapsto \bar{a} \end{aligned}$$

Assim, aplicando a Proposição 1.3.3, existe um place $\pi : \tilde{\mathbb{K}} \longrightarrow \tilde{\mathbb{L}}$, tal que $A_\pi = A$. Também π é sobrejetor, pois λ é epimorfismo. $\square$

Conforme vimos anteriormente, ao anel de valorização $\mathbb{Z}_{(p)}$ de $\mathbb{Q}$ está associado o place p-ádico π_p. Temos que π_p é definido em $\tilde{\mathbb{Q}}$ e é um place sobrejetor. Segue imediatamente do teorema anterior que existe uma correspondência biunívoca entre os places p-ádicos definidos em $\tilde{\mathbb{Q}}$ e os anéis de valorização p-ádicos de $\mathbb{Q}$. Assim, qualquer outro place sobrejetor não trivial definido em $\tilde{\mathbb{Q}}$ é equivalente à algum place p-ádico de $\mathbb{Q}$. Conforme provamos na Proposição 1.1.9, os anéis de valorização $\mathbb{Z}_{(p)}$ de $\mathbb{Q}$ são os únicos anéis de valorização próprios de $\mathbb{Q}$. Portanto, os places sobrejetores não triviais definidos em $\tilde{\mathbb{Q}}$ são exatamente os places p-ádicos.

Capítulo 2

Valorização em Anéis de Divisão

Neste capítulo vamos estender aos anéis de divisão os principais resultados da Teoria de Valorização em corpos. Também apresentaremos resultados essenciais para o estudo dos anéis de valorização de Dubrovin, a serem vistos no capítulo seguinte.

Abordaremos inicialmente os anéis de valorização de um anel de divisão utilizando a definição apresentada por Schilling em 1945, que adiciona a invariância à definição vista anteriormente.

Veremos que é possível preservar em anéis de divisão muitas propriedades dos anéis de valorização que são válidas em corpos, por exemplo, a ordenação total no conjunto dos ideais. Outro exemplo a ser destacado é o Teorema da Correspondência, que agora estabelece uma correspondência biunívoca, que reverte a inclusão, entre ideais completamente primos e sobreanéis do anel de valorização.

Na seqüência, demonstraremos propriedades do Radical de Jacobson de um anel não necessariamente comutativo e apresentaremos resultados básicos envolvendo anel quociente clássico. Estes dois tópicos serão usados na generalização para anéis de divisão de outras propriedades dos anéis de valorização válidas para corpos.

Na segunda seção deste capítulo veremos um exemplo de anel de valorização total e invariante em um anel de divisão que não é corpo.

Na Seção 3 apresentaremos um procedimento para obtenção de anéis de valorização totais e invariantes através do anel de divisão das séries formais de Laurent. Num caso particular, obteremos exemplos de anéis de valorização totais e não invariantes, que é o objetivo principal da referida seção.

As funções valorização também serão destacadas e veremos que existe uma correspondência biunívoca entre classes de valorizações e anéis de valorização totais e invariantes de um anel de divisão. Isso será feito na quinta seção.

A tarefa de estender todos os resultados do capítulo anterior para anéis de divisão é impossível de ser completada. O fato que ratifica essa afirmação é a inexistência de uma versão, em anéis de divisão, do Teorema da Extensão visto em corpos. A construção completa de um contra-exemplo será feita na quarta seção.

2.1 Anéis de Valorização Totais e Invariantes

Nesta seção daremos ênfase ao estudo das propriedades dos anéis de valorização em anéis de divisão.

Conforme mencionamos anteriormente, vamos utilizar propriedades específicas do Radical de Jacobson e resultados envolvendo anel quociente clássico.

A definição abaixo, apresentada por Schilling em 1945, estende aos anéis de divisão o conceito de anel de valorização.

Definição 2.1.1 *Seja B um subanel do anel de divisão D. Dizemos que B é um anel de valorização total e invariante de D quando:*

(*a*) *Para cada $d \in D^*$, $d \in B$ ou $d^{-1} \in B$;*

(*b*) *Para cada $d \in D^*$, $dBd^{-1} = B$.*

Observação 2.1 Os itens (a) e (b) são chamados, respectivamente, de *totalidade* e *invariância*.

Observação 2.2 Se é válido apenas o primeiro item da definição, dizemos que B é um *anel de valorização total* do anel de divisão D.

Observação 2.3 O adjetivo *invariante* da definição se justifica pelo fato da condição (b) garantir que B é invariante por automorfismos internos do anel de divisão D.

Observação 2.4 A segunda condição da definição assegura que todo ideal de B é bilateral. De fato, considere I um ideal à direita de B e sejam $x \in I$ e $b \in B$. Se $x = 0$, então

$bx = 0 \in I$. Caso $x \neq 0$, temos $xbx^{-1} \in B$. Observe que também temos que $x^{-1}bx \in B$. Logo, $x^{-1}bx = b' \in B$ implica em $bx = xb'$, com $x \in I$ e $b' \in B$. Como I é ideal à direita de B, temos que $bx \in I$. Assim, I também é ideal à esquerda de B e portanto é um ideal bilateral de B.

Observação 2.5 Vamos considerar B um anel de valorização total do anel de divisão D e vamos supor que $dBd^{-1} \subseteq B$, para todo $d \in D^*$. Dado $b \in B$, podemos escrever $b = d^{-1}(dbd^{-1})d$. Como $dbd^{-1} \in B$, temos que $b \in d^{-1}Bd$. Como isso vale para todo $d \in D^*$, temos que $b \in dBd^{-1}$. Assim $B \subseteq dBd^{-1}$, para todo $d \in D^*$. Portanto, para que um anel de valorização total seja invariante, basta que $dBd^{-1} \subseteq B$.

Observação 2.6 É claro que somente a invariância de um subanel de um anel de divisão não implica na totalidade do subanel. Por exemplo, é fácil ver que o subanel $\mathbb{Q}$ de $\mathbb{R}$ é invariante mas não é total em $\mathbb{R}$.

Num corpo um automorfismo interno é a aplicação identidade. Assim, todo anel de valorização de um corpo é total e invariante. Portanto, todos os exemplos de anéis de valorização de um corpo servem para exemplificar anéis de valorização totais e invariantes num anel de divisão.

Conforme mencionamos anteriormente, nas Seções 2 e 3 trataremos, respectivamente, de exemplo de anel de valorização total e invariante em anel de divisão que não é corpo e exemplo de anel de valorização total mas não invariante num anel de divisão.

Veremos agora propriedades dos anéis de valorização totais e invariantes em anéis de divisão que se assemelham às vistas para corpos.

Notamos que as demonstrações das Proposições 2.1.1, 2.1.2 e 2.1.3 são análogas, respectivamente, às demonstrações das Proposições 1.1.2, 1.1.4 e 1.1.6.

O primeiro resultado afirma que é válida a ordenação total no conjunto dos ideais de um anel de valorização total de um anel de divisão. Como não dispomos mais da comutatividade, veremos que esta ordenação vale para o conjunto dos ideais à direita, dos ideais à esquerda e para o conjunto dos ideais bilaterais.

Proposição 2.1.1 *Seja B um anel de valorização total do anel de divisão D. Os ideais à direita (à esquerda, bilaterais) de B estão totalmente ordenados por inclusão.*

Demonstração

Sejam I e J ideais à direita de D. Provaremos que $I \subseteq J$ ou $J \subseteq I$. Vamos supor que $J \nsubseteq I$. Assim, existe $b \in J \setminus I$ e $b \neq 0$. Seja $a \in I$. Se $a = 0$, então $a \in J$. Se $a \neq 0$, temos $b^{-1}a \in D^*$. Como B é anel de valorização total de D, segue que $b^{-1}a \in B$ ou $(b^{-1}a)^{-1} = a^{-1}b \in B$. No primeiro caso, $b \in J$ e $b^{-1}a \in B$ implicam em $a \in J$. No segundo caso, $a \in I$ e $a^{-1}b \in B$ implicam em $b \in I$, contradizendo nossa hipótese. Portanto, $I \subseteq J$ ou $J \subseteq I$. Analogamente, prova-se que os ideais à esquerda estão totalmente ordenados por inclusão. Conseqüentemente, os ideais bilaterais de B também estão totalmente ordenados por inclusão. $\square$

Proposição 2.1.2 *Seja B um anel de valorização total do anel de divisão D. Todo ideal à direita (à esquerda ou bilateral), finitamente gerado de B, é principal.*

Demonstração

Seja $I = x_1B + x_2B + \cdots + x_nB$ um ideal à direita finitamente gerado de B. Pela Proposição 2.1.1, os ideais à direita $x_1B, x_2B, \cdots, x_nB$ estão ordenados por inclusão. Então, existe $k \in \{1, 2, \cdots, n\}$ tal que $x_iB \subseteq x_kB$, para todo $i \in \{1, 2, \cdots, n\}$. Logo, $I = x_kB$. Analogamente, prova-se esta proposição para ideais à esquerda de B e como conseqüência, ela vale também para ideais bilaterais de B. $\square$

Proposição 2.1.3 *Seja B um anel de valorização total do anel de divisão D. Então $B = \{b \in D;\ b$ é inteiro sobre $B\}$.*

Demonstração

Seja $\overline{B} = \{b \in D;\ b$ inteiro sobre B$\}$. Desde que $b \in B$ é raiz de $X - b \in B[X]$, temos que $B \subseteq \overline{B}$. Seja $b \in \overline{B}$. Podemos supor $b \neq 0$ e $b^{-1} \in B$. Assim, $b \in D$ e $p(b) = 0$, para algum $p(X)$ mônico em $B[X]$. Então,

$$p(b) = b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 = 0, \text{ com } a_i \in B.$$

Multiplicando a igualdade $b^n = -(a_{n-1}b^{n-1} + \cdots + a_1b + a_0)$ por $b^{-n+1} = (b^{-1})^{n-1} \in B$, temos

$$b = -(a_{n-1} + a_{n-2}b^{-1} + \cdots + a_2b^{-n+3} + a_1b^{-n+2} + a_0b^{-n+1}).$$

Como cada parcela está em B, concluímos que $b \in B$. Portanto, $\overline{B} = B$. $\square$

Estudaremos agora resultados sobre o Radical de Jacobson de anéis não necessariamente comutativos. Utilizaremos este radical para estudar a estrutura dos ideais de um anel de valorização total de um anel de divisão. No próximo capítulo usaremos o Radical de Jacobson para tratar de anéis de valorização de Dubrovin.

Definição 2.1.2 *Seja B um anel com unidade. O Radical de Jacobson $J(B)$ é a interseção dos ideais à esquerda maximais de B.*

A definição do Radical de Jacobson poderia ser a interseção dos ideais à direita maximais, pois veremos em seguida que a interseção dos ideais à esquerda maximais coincide com a interseção dos ideais à direita maximais. Portanto, não é necessário destacar isso na definição, chamando, por exemplo, este radical de Radical de Jacobson à esquerda.

Proposição 2.1.4 *Seja B um anel com unidade. O Radical de Jacobson $J(B)$ é um ideal bilateral de B e as seguintes afirmações são equivalentes:*

(i) $r \in J(B)$;

(ii) *O elemento r pertence à interseção de todos os ideais à direita maximais de B;*

(iii) $\varphi(r) = 0$, *para todo B-homomorfismo φ de B em um B-módulo à esquerda simples M.*

(iv) $\phi(r) = 0$, *para todo B-homomorfismo ϕ de B em um B-módulo à direita simples M.*

(v) $rM = 0$ *para todo B-módulo à esquerda simples M.*

(vi) $Nr = 0$ *para todo B-módulo à direita simples N.*

(vii) *O elemento $1 - xr$ é inversível, para todo $x \in B$;*

(viii) *O elemento $1 - rx$ é inversível, para todo $x \in B$;*

Demonstração

Inicialmente demonstraremos $(i) \Leftrightarrow (iii) \Leftrightarrow (v)$. Com isso, mostraremos que $J(B)$ é um ideal bilateral de B. A seguir, provaremos $(i) \Leftrightarrow (vii) \Leftrightarrow (viii) \Leftrightarrow (ii) \Leftrightarrow (iv) \Leftrightarrow (vi)$.

$(i) \Rightarrow (iii)$ Consideremos φ um $B-$homomorfismo de B num $B-$módulo à esquerda simples M. Podemos supor que φ não é o $B-$homomorfismo nulo. Como $\varphi(B)$ é um submódulo de M e M é simples, temos que $\varphi(B) = M$ ou $\varphi(B) = \{0\}$. Como excluímos o caso $\varphi(B) = \{0\}$, temos que $\varphi(B) = M$. Assim, $\frac{B}{Ker(\varphi)} \simeq M$ implica que $\frac{B}{Ker(\varphi)}$ é simples. Pelo Segundo Teorema dos Homomorfismos, $Ker(\varphi)$ é um ideal à esquerda maximal de B. Por hipótese, $r \in J(B) \subseteq Ker(\varphi)$, isto é, $\varphi(r) = 0$.

$(iii) \Rightarrow (i)$ Temos que $r \in B$ e r satisfaz a hipótese (iii). Seja L um ideal à esquerda maximal de B. Basta provar que $r \in L$. Inicialmente afirmamos que o $B-$módulo à esquerda $\frac{B}{L}$ é simples. Para provar isso, consideremos N um submódulo de $\frac{B}{L}$. Pelo Segundo Teorema dos Homomorfismos, é garantida a existência de único $B^{'}$ submódulo de B, tal que L é um submódulo de $B^{'}$ e $\frac{B^{'}}{L} = N$. Mas L é um ideal à esquerda maximal de B e portanto, $B^{'} = L$ ou $B^{'} = B$. Se $B^{'} = L$, temos que $N = \{\bar{0}\}$. Caso $B^{'} = B$, segue que $N = \frac{B}{L}$. Portanto, $\frac{B}{L}$ é simples. Logo, a aplicação canônica $\pi : B \longrightarrow \frac{B}{L}$, $a \longmapsto \bar{a}$, é um B-homomorfismo de B sobre o B-módulo à esquerda simples $\frac{B}{L}$. Aplicando a hipótese (iii), $\pi(r) = 0$. Assim, $r \in Ker(\pi) = L$ e portanto, $r \in J(B)$.

$(iii) \Rightarrow (v)$ Novamente temos $r \in B$ e r satifaz (iii). Seja M um B-módulo à esquerda simples e $m \in M$. É fácil ver que a aplicação $\varphi_m : B \longrightarrow M$, dada por $\varphi_m(x) = xm$, é um B-homomorfismo. Então $\varphi_m(r) = rm = 0$. Assim, para cada $m \in M$ temos um B-homomorfismo φ_m tal que $\varphi_m(r) = 0$, isto é, para cada $m \in M$, $rm = 0$. Portanto, $rM = 0$.

$(v) \Rightarrow (iii)$ Seja φ um $B-$homomorfismo de B no B-módulo à esquerda simples M. Segue que $\varphi(r) = r\varphi(1) = 0 \in rM = 0$. Logo, $\varphi(r) = 0$.

Decorre da definição e das equivalências que provamos acima que $J(B)$ é um ideal bilateral de B. De fato, por definição $J(B)$ é ideal à esquerda de B. Resta provar que $J(B)$ também é ideal à direita. Para isso, consideremos $u \in B$, $v \in J(B)$ e M um $B-$módulo à esquerda simples. Tal M sempre existe, como pode ser visto em ([Go], p. 4). Como (i) implica em (v), temos $vM = 0$. Mas $uM \subseteq M$, logo $vuM \subseteq vM = 0$. Agora, como (v) implica em (i), temos que $vu \in J(B)$.

$(i) \Rightarrow (vii)$ Por hipótese, $r \in J(B)$. Vamos supor que exista $x \in B$ tal que $1 - xr$ não seja inversível à esquerda. Então $B(1 - xr)$ é um ideal à esquerda próprio de B. Logo, existe um ideal à esquerda maximal N de B tal que $B(1 - xr) \subseteq N$. Segue que $1 - xr \in N$. Por outro lado, $r \in J(B)$ implica em $r \in N$ e por conseguinte $xr \in N$, já que N é ideal à esquerda de B. Desta forma, como $1 - xr \in N$ e $xr \in N$, temos que $1 \in N$, contradizendo a maximalidade de N. Portanto, $1 - xr$ é inversível à esquerda, para todo $x \in B$. Seja $s \in B$ tal que $s(1 - xr) = 1$. Então $1 - s = -sxr \in J(B)$, já que $J(B)$ é ideal à esquerda de B. Assim $s = 1 - (1 - s)$ é inversível à esquerda, digamos $ts = 1$. Então $t = t1 = ts(1 - xr) = 1 - xr$ e $s(1 - xr) = 1 = ts = (1 - xr)s$. Segue que $1 - xr$ é inversível, para todo $x \in B$.

$(vii) \Rightarrow (i)$ Seja L um ideal à esquerda maximal de B e seja $r \in B$ tal que $1 - xr$ é inversível, para todo $x \in B$. Assim $1 - xr \notin L$ implica que $1 \notin Br + L$. Decorre que $L \subseteq Br + L \subsetneqq B$. Como L é um ideal à esquerda maximal de B, temos que $L = Br + L$ e portanto $r \in L$.

$(vii) \Rightarrow (viii)$ Seja $r \in B$ tal que $1 - xr$ é inversível para todo $x \in B$. Como (vii) é equivalente a (i), temos que $r \in J(B)$. Segue que $rx \in J(B)$, para todo $x \in B$, pois $J(B)$ é ideal à direita de B. Assim, para todo $x \in B$, rx também satisfaz (vii), isto é, $1 - y(rx)$ é inversível, para todo $y \in B$. Decorre que $1 - rx$ é inversível, para todo $x \in B$.

$(ii) \Leftrightarrow (iv) \Leftrightarrow (vi)$ Análogo a $(i) \Leftrightarrow (iii) \Leftrightarrow (v)$.

$(viii) \Rightarrow (vii)$ Análogo a $(vii) \Rightarrow (viii)$.

$(viii) \Leftrightarrow (ii)$ Análogo a $(vii) \Leftrightarrow (i)$. $\square$

Lema 2.1.1 *Se B é um anel com unidade e M é um ideal bilateral maximal de B, então $J(B) \subseteq M$.*

Demonstração

Supondo que exista $x \in J(B) \setminus M$, temos que $M \subsetneqq BxB + M \subseteq B$, o que implica em $B = BxB + M$. Logo, existem $a, b \in B$ e $m \in M$ tais que $1 = axb + m$. Como $J(B)$ é ideal bilateral de B, temos $1 - m = axb \in J(B)$. Do item $(viii)$ da Proposição 2.1.4, temos que $1 - (1 - m)y$ é inversível em B, para todo $y \in B$. Fazendo $y = 1$, concluímos que m é inversível em B. Segue que $1 \in MB \subseteq M$, o que é uma contradição. $\square$

Lema 2.1.2 *Se B é um anel com unidade e M é um ideal bilateral maximal de B, então as seguintes afirmações são equivalentes:*

(i) $1 + M \subseteq U(B)$

(ii) $M = J(B)$.

Demonstração

$(i) \Rightarrow (ii)$ Pelo lema anterior, $J(B) \subseteq M$. Seja $m \in M$. Para cada $x \in B$, temos que $-mx \in M$ e pela hipótese (i), vem que $1 - mx \in U(B)$, para todo $x \in B$. Portanto, $m \in J(B)$.

$(ii) \Rightarrow (i)$ Seja $m \in M$. Por hipótese, $m \in J(B)$ e daí $-m \in J(B)$. Segue que $1-(-m)1 = 1 + m \in U(B)$. □

Vejamos agora como o Radical de Jacobson se relaciona com os anéis de valorização totais de um anel de divisão.

Proposição 2.1.5 *Se B é um anel de valorização total do anel de divisão D, então $J(B)$ é o único ideal à esquerda (à direita) maximal de B e $J(B) = B \backslash U(B)$.*

Demonstração

Pela Proposição 2.1.1, todos os ideais à esquerda (à direita) maximais de B estão totalmente ordenados por inclusão. Assim, é fácil ver que existe único ideal I à esquerda maximal de B e único ideal J à direita maximal de B. Por definição, sabemos que $J(B)$ é a interseção dos ideais à esquerda maximais de B, isto é, $J(B) = I$. Conforme provamos na proposição anterior, a interseção dos ideais à esquerda maximais de B coincide com a interseção dos ideais à direita maximais de B. Logo, $J(B) = J$ e assim, $J(B)$ é o único ideal à esquerda (à direita) maximal de B. Claro que $J(B) \subseteq B \backslash U(B)$, pois se existisse um inversível em $J(B)$ ele não seria maximal. Consideremos $x \in B \backslash U(B)$. Decorre que $x^{-1} \notin B$. Assim, x não tem inverso à esquerda em B. Segue que Bx é um ideal à esquerda próprio de B e assim Bx deve estar contido num ideal à esquerda maximal de B. Como $J(B)$ é o único ideal à esquerda maximal de B, temos que $Bx \subseteq J(B)$. Portanto, $x \in J(B)$. □

Corolário 2.1.1 *Se B é um anel de valorização total do anel de divisão D, então $J(B)$ é o único ideal bilateral maximal de B.*

Demonstração

Conforme provamos na Proposição 2.1.4, $J(B)$ é um ideal bilateral de B. Sabemos que os ideais bilaterais de B estão totalmente ordenados por inclusão. Assim, B tem único ideal bilateral maximal $\mathfrak{M}_B$. Em particular, $\mathfrak{M}_B$ é ideal à esquerda de B. Logo, pela proposição anterior, $\mathfrak{M}_B \subseteq J(B)$. Como $J(B) \subsetneqq B$ e $\mathfrak{M}_B$ é ideal maximal, temos que $\mathfrak{M}_B = J(B)$. $\square$

Obteremos agora um análogo, para anéis de divisão, do Teorema da Correspondência estudado em corpos.

Definição 2.1.3 *Seja B um anel com unidade e $P \subseteq B$. Dizemos que P é um ideal completamente primo de B, se P é um ideal bilateral próprio de B e satisfaz a condição:*

(1) *Para todos $a, b \in B$, tais que $ab \in P$, temos $a \in P$ ou $b \in P$.*

Em particular, quando B for um anel de valorização total do anel de divisão D e P for um ideal completamente primo de B, podemos estender a condição (1) para todo o anel de divisão, isto é,

(1^*) *Para todos $a, b \in D$, tais que $ab \in P$, temos $a \in P$ ou $b \in P$.*

De fato, sejam $a, b \in D^*$. Se $a, b \in B$, nada temos a fazer. Se $a \notin B$ ou $b \notin B$, então $a^{-1} \in B$ ou $b^{-1} \in B$. Como P é um ideal bilateral de B, temos $b = a^{-1}(ab) \in P$ ou $a = (ab)b^{-1} \in P$.

Seja B um anel de valorização total do anel de divisão D. Consideremos os conjuntos

$$\mathcal{B} = \{A \subseteq D;\ A \text{ é subanel de } D \text{ e } B \subseteq A\},$$

$$\mathcal{P} = \{P \subseteq B;\ P \text{ é ideal completamente primo de } B\}.$$

Observe que se $A \in \mathcal{B}$, então A é um anel de valorização total de D contendo B.

Proposição 2.1.6 *Se $P \in \mathcal{P}$, então $A_P := \{d \in D:\ d = 0 \text{ ou } d^{-1} \notin P\} \in \mathcal{B}$.*

Demonstração

Primeiramente provemos que $B \subseteq A_P$. Podemos supor $a \in B^*$. Segue que $a^{-1} \notin P$, pois caso contrário, $1 = aa^{-1} \in P$. Veremos agora que A_P é um subanel de D. Sejam $x, y \in A_P$. Se $x = 0$ ou $y = 0$, temos que $xy \in A_P$. Se $x, y \in D^*$, então $x^{-1} \notin P$ e $y^{-1} \notin P$. Como P é um ideal completamente primo de B, temos que $y^{-1}x^{-1} = (xy)^{-1} \notin P$. Decorre que $xy \in A_P$. Resta provar que $x - y \in A_P$. Podemos admitir $x, y, x - y \in D^*$. Vamos supor por absurdo que $(x-y)^{-1} \in P$. Então existe $w \in P$ tal que $(x-y)w = w(x-y) = 1$. Segue que $w = x^{-1}(1+yw)$. Decorre de (1^*) e do fato que $x^{-1} \notin P$, que $1+yw = xw \in P$.

Também $w = y^{-1}(xw - 1)$ implica em $1 - xw \in P$. Decorre que $1 \in P$, contradizendo o fato de P ser ideal próprio de B. Portanto, $x - y \in A_P$. $\square$

Vamos considerar $P_1 \subseteq P_2$, onde $P_1, P_2 \in \mathcal{P}$. Seja $x \in A_{P_2}$. Temos que $x = 0$ ou $x^{-1} \notin P_2$. Segue que $x = 0$ ou $x^{-1} \notin P_1$, isto é, $x \in A_{P_1}$. Assim, $A_{P_2} \subseteq A_{P_1}$. Dessa afirmação e da proposição anterior, segue que a aplicação

$$\begin{aligned} \sigma : \mathcal{P} &\longrightarrow \mathcal{B} \\ P &\longmapsto A_P \end{aligned}$$

está bem definida e reverte a inclusão.

Seja $A \in \mathcal{B}$. Afirmamos que $J(A)$ é ideal completamente primo de A. De fato, já vimos que $J(A)$ é ideal bilateral e próprio de A. Resta provar a condição (1) para $J(A)$. Sejam $x, y \in A$ tais que $xy \in J(A)$. Vamos supor que $x \notin J(A)$ e considerar o ideal à esquerda $J(A) + Ax$ do anel A. Desde que $J(A)$ é ideal à esquerda maximal de A e $J(A) \subsetneqq J(A) + Ax \subseteq A$, devemos ter $A = J(A) + Ax$. Assim, existem $\alpha \in J(A)$ e $a \in A$ tais que $1 = \alpha + ax$. Segue que $y = \alpha y + axy \in J(A)$, pois $xy, \alpha \in J(A)$. Concluímos assim a prova de que $J(A)$ é ideal completamente primo de A.

Tomemos agora $A_1, A_2 \in \mathcal{B}$ tais que $A_1 \subseteq A_2$. De maneira análoga à que fizemos para corpos, concluímos que $J(A_2) \subseteq J(A_1)$. Em particular, dado $A \in \mathcal{B}$, temos que $B \subseteq A$ e então $J(A) \subseteq J(B) \subseteq B \subseteq A$. Portanto, $J(A)$ é ideal completamente primo de B. Isso garante que a aplicação

$$\begin{aligned} \tau : \mathcal{B} &\longrightarrow \mathcal{P} \\ A &\longmapsto J(A) \end{aligned}$$

está bem definida e reverte a inclusão.

Utilizando as aplicações τ e σ definidas acima, vamos demonstrar o Teorema da Correspondência para anéis de divisão.

Teorema 2.1.1 (Teorema da Correspondência) *Seja B anel de valorização total do anel de divisão D. Existe uma correspondência biunívoca, que reverte a inclusão, entre ideais completamente primos de B e sobreanéis de B em D.*

Demonstração

Considerando as aplicações $\sigma : \mathcal{P} \longrightarrow \mathcal{B}$ e $\tau : \mathcal{B} \longrightarrow \mathcal{P}$ definidas anteriormente, vamos mostrar que $\tau^{-1} = \sigma$. Provaremos dois itens:

(1) $\tau(\sigma(P)) = P$, $\forall\ P \in \mathcal{P}$;

(2) $\sigma(\tau(A)) = A$, $\forall\ A \in \mathcal{B}$.

(1) $\tau(\sigma(P)) = \tau(A_P) = J(A_P) = A_P \backslash U(A_P)$. Lembrando que $A_P = \{d \in D :\ d = 0 \text{ ou } d^{-1} \notin P\}$, é fácil ver que $U(A_P) = \{d \in D :\ d \notin P \text{ e } d^{-1} \notin P\}$. Segue que $A_P \backslash U(A_P) \subseteq P$ e é claro que $P \subseteq A_P \backslash U(A_P)$. Logo, $A_P \backslash U(A_P) = P$.
(2) $\sigma(\tau(A)) = \sigma(J(A)) = A_{J(A)} = \{d \in D :\ d = 0 \text{ ou } d^{-1} \notin J(A)\}$. Seja $x \in A_{J(A)} \setminus \{0\}$. Temos que $x \in D$ e $x^{-1} \notin A \backslash U(A) = J(A)$. Logo, $x^{-1} \in D \backslash A$ ou $x^{-1} \in U(A)$. No segundo caso, é claro que $x \in A$. No primeiro caso também temos $x \in A$, pois A é um anel de valorização total de D. Logo, $A_{J(A)} \subseteq A$. Por outro lado, seja $x \in A^*$. Pode ocorrer $x^{-1} \in U(A)$ ou $x^{-1} \notin U(A)$. No primeiro caso, segue imediatamente que $x^{-1} \notin A \setminus U(A) = J(A)$ e assim $x \in A_{J(A)}$. No segundo caso, $x^{-1} \notin U(A)$ implica que $x^{-1} \notin A$ ou $(x^{-1})^{-1} = x \notin A$. Desde que $x \in A$, só resta $x^{-1} \notin A$. Decorre que $x^{-1} \notin A \setminus U(A) = J(A)$ e portanto $x \in A_{J(A)}$. Logo, $A_{J(A)} = A$. $\square$

Quando estudamos anéis de valorização em corpos, provamos na Observação 1.4 que se V é um anel de valorização do corpo $\mathbb{K}$, então $\mathbb{K}$ é o corpo de frações de V. Na Proposição 1.1.3 provamos que se o subanel V de $\mathbb{K}$ é um domínio e seus ideais estão totalmente ordenados por inclusão, então V é um anel de valorização de $\mathbb{K}$. Para obter um análogo em anéis de divisão para esses fatos, precisamos estender a noção de corpo de frações para domínios não necessariamente comutativos. Isso nos leva ao conceito de *anel quociente clássico*, que também utilizaremos para estudar os anéis de valorização de Dubrovin.

Para introduzir a definição de anel quociente clássico recordamos o procedimento usual para obter o corpo de frações de um domínio comutativo.

Seja D um domínio comutativo. Em $D \times D^*$ temos a relação de equivalência

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Lembramos que a comutividade é indispensável para provar que $\sim$ é de fato uma relação de equivalência.

Denotando a classe $\overline{(a,b)}$ por $\frac{a}{b}$, escrevemos o conjunto quociente

$$\mathbb{K} = \frac{D \times D^*}{\sim} = \left\{\frac{a}{b};\ a \in D,\ b \in D^*\right\}.$$

O conjunto $\mathbb{K}$ com as operações usuais é um corpo. Além disso, $\hat{D} = \{\frac{a}{1};\ a \in D\}$ é um subdomínio de $\mathbb{K}$ isomorfo à D através da aplicação $\varphi : D \longrightarrow \hat{D}$, dada por $\varphi(a) = \frac{a}{1}$. Identificando D com $\hat{D}$ temos:

(a) D é subanel de $\mathbb{K}$;

(b) Todo elemento não nulo de D tem inverso em $\mathbb{K}$;

(c) $\mathbb{K} = \{ab^{-1};\ a \in D,\ b \in D^*\}$.

Dizemos então que $\mathbb{K}$ é o *corpo de frações* de D.

Usaremos as condições (a), (b) e (c) acima para motivar a definição de anel quociente clássico.

Antes, recordamos que se R é um anel com unidade e $x \in R$, então x é *regular à direita* quando $r \in R$ e $rx = 0$ implicam em $r = 0$. Analogamente, define-se elemento *regular à esquerda*. Dizemos que $x \in R$ é *regular* quando for regular à direita e à esquerda. Conforme mencionamos na introdução deste trabalho, vamos denotar $R^* = \{x \in R;\ x$ é regular$\}$.

Observação 2.7 Se R é um domínio, comutativo ou não, então todo elemento não nulo é regular, isto é, $R^* = R\backslash\{0\}$.

Observação 2.8 A regularidade é condição necessária para um elemento do anel R ser inversível. De fato, consideremos $x \in R$ com inverso à direita $y \in R$. Supomos também $rx = 0$, com $r \in R$. Então $rxy = 0$. Mas $rxy = r1 = r$. Logo $r = 0$, isto é, x é regular à direita. Analogamente, se $x \in R$ é inversível à esquerda, prova-se que x é regular à esquerda. Portanto, se $x \in R$ é inversível, temos que x é regular.

Observação 2.9 A regularidade não é suficiente para um elemento do anel R ser inversível, como pode ser visto no anel dos inteiros $\mathbb{Z}$.

Definição 2.1.4 *Seja R um anel com unidade. Um anel Q é um anel quociente clássico à direita para R quando:*

(a) *R é subanel de Q;*

(b) *Todo elemento regular de R tem inverso em Q;*

(c) $Q = \{ab^{-1};\ a \in R,\ b \in R^*\}$.

Um *anel quociente clássico à esquerda* para R é definido analogamente, substituindo a condição (c) por $Q = \{a^{-1}b;\ b \in R,\ a \in R^*\}$.

Se Q é anel quociente clássico à direita e à esquerda para R, dizemos que Q é *anel quociente clássico para R.*

Não é verdade, em geral, que um anel com unidade possui anel quociente clássico à direita ou à esquerda, conforme ([Go], p. 96).

As Proposições 2.1.7 e 2.1.8 abaixo serão úteis no restante desta seção. Estes resultados estão enunciados como exercício em ([Go], p. 101,102) e demonstrados em ([B], p. 4,5,6). Demonstraremos a Proposição 2.1.9 no estudo dos anéis artinianos que será feito no Capítulo 3.

Vamos considerar R um anel com unidade.

Proposição 2.1.7 *Se Q_1 e Q_2 são anéis quocientes clássicos à direita (à esquerda) para R, então Q_1 é isomorfo a Q_2.*

Proposição 2.1.8 *Se R tem anel quociente clássico à direita e anel quociente clássico à esquerda, então eles são isomorfos.*

Proposição 2.1.9 *Se R é anel artiniano à direita (à esquerda), então R é seu próprio anel quociente clássico à direita e à esquerda.*

Segue da Proposição 2.1.7 que podemos falar apenas o anel quociente clássico à direita (à esquerda) para R, pois quando existir, será único a menos de isomorfismo.

Exemplo 2.1 O corpo de frações de um domínio comutativo D é o anel quociente clássico para D. Lembre que neste caso $D^* = D\backslash\{0\}$.

Exemplo 2.2 Seja R um anel que tem apenas uma quantidade finita de ideais à direita (à esquerda). Então R é seu próprio anel quociente clássico à direita e à esquerda. De fato, neste caso R é artiniano à direita (à esquerda) e o resultado segue da Proposição 2.1.9.

Exemplo 2.3 Como caso particular do exemplo anterior temos que todo anel de divisão (corpo, inclusive) é seu próprio anel quociente clássico. Também para $1 \leq n \in \mathbb{N}$, temos que $\mathbb{Z}_n$ é seu próprio anel quociente clássico. Isso decorre do fato de todo anel finito ter número finito de ideais.

Naturalmente surge a questão de saber quando um anel com unidade possui um anel quociente clássico à direita (à esquerda) e se possuir, como obtê-lo.

Inicialmente observamos que a construção usada para obter o corpo de frações de um domínio comutativo não pode ser usada como modelo para obter o anel quociente clássico (caso exista) para um anel com unidade. De fato, os exemplos seguintes mostram que a relação usada em $D \times D^*$, para D um domínio comutativo, depende essencialmente de cada uma das hipóteses: domínio e comutativo.

Exemplo 2.4 Para o domínio não comutativo $D = Quat(\mathbb{R})$, a relação em $D \times D^*$ dada por

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

não é transitiva. Basta notar que $(i, -j) \sim (i, j)$ e $(i, j) \sim (k, 1)$, porém, $(i, -j)$ não está relacionado com $(k, 1)$.

Exemplo 2.5 No anel comutativo $D = \mathbb{Z}_8$, a relação em $D \times D^*$ dada por

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

também não é transitiva. Note que $(\bar{1}, \bar{2}) \sim (\bar{6}, \bar{4})$ e $(\bar{6}, \bar{4}) \sim (\bar{3}, \bar{2})$, porém, $(\bar{1}, \bar{2})$ não está relacionado com $(\bar{3}, \bar{2})$.

Em 1931, O. Ore apresentou uma condição necessária e suficiente para a existência de um anel quociente clássico à direita (à esquerda) para um anel R com unidade.

Condição de Ore à Direita *"Um anel com unidade R satisfaz a condição de Ore à direita se dados $a \in R$ e $x \in R^*$, existem $b \in R$ e $y \in R^*$, tais que $ay = xb$."*

O teorema abaixo está enunciado como exercício em ([Go], Exercise 3.D.8, p. 101) e provado em ([B], Proposição 1.1.2, p. 6).

Teorema 2.1.2 *Seja R um anel com unidade. Então R possui anel quociente clássico à direita se, e somente se, R satisfaz a condição de Ore à direita.*

Analogamente temos a condição de Ore à esquerda:

Condição de Ore à Esquerda *"Um anel com unidade R satisfaz a condição de Ore à esquerda se dados $a \in R$ e $x \in R^*$, existem $b \in R$ e $y \in R^*$, tais que $ya = bx$."*

É válido também um teorema análogo ao anterior, isto é, um anel com unidade R possui anel quociente clássico à esquerda se, e somente se, R satisfaz a condição de Ore à esquerda.

Como exemplo, sabemos que os domínios comutativos possuem anel quociente clássico à direita e à esquerda, que é seu corpo de frações. Assim, um domínio comutativo D deve satisfazer ambas as condições de Ore. E isso é imediato, pois dados $a \in D$ e $x \in D^*$, escolhe-se $b = a \in D$ e $y = x \in D^*$. Então $ay = ax = xa = xb$ implica que D satisfaz a condição de Ore à direita. Analogamente, mostra-se que D satisfaz a condição de Ore à esquerda.

Existe exemplo de domínio que não possui anel quociente clássico à direita e nem à esquerda, conforme pode ser visto em ([Go], Exercise 3.D.5, p. 101). Assim, tal domínio não satisfaz nenhuma das condições de Ore.

Proposição 2.1.10 *Seja R um domínio tal que $aR \cap bR \neq 0$ $(Ra \cap Rb \neq 0)$, para quaisquer $a, b \in R^*$. Então R satisfaz a condição de Ore à direita (à esquerda).*

Demonstração

Sejam $a \in R$ e $x \in R^*$. Se $a = 0$, podemos escolher $b = 0$ e $y = 1$, e assim, $0 = ay = xb$, com $y \in R^*$. Se $a \neq 0$, então $a, x \in R^*$ e por hipótese $aR \cap xR \neq 0$. Assim, existem $y, b \in R$ tais que $ay = xb \neq 0$. Claro que $y \in R^*$, pois $ay \neq 0$. Portanto, R satisfaz a condição de Ore à direita. Analogamente, demonstra-se que R satisfaz a condição de Ore à esquerda. □

Definição 2.1.5 *Um domínio de Ore à direita (à esquerda) é um domínio R tal que $aR \cap bR \neq 0$, $(Ra \cap Rb \neq 0)$, para quaisquer $a, b \in R^*$.*

Segue da proposição anterior que todo domínio de Ore à direita (à esquerda) possui anel quociente clássico à direita (à esquerda). Também vale a recíproca.

Teorema 2.1.3 *Seja R um domínio. São equivalentes:*

(i) R é domínio de Ore à direita (à esquerda);

(ii) R tem anel quociente clássico à direita (à esquerda).

Demonstração

$(i) \Rightarrow (ii)$ Segue da Proposição 2.1.10 e do Teorema 2.1.2.

$(ii) \Rightarrow (i)$ Sejam $u, v \in R^*$ e $D = \{ab^{-1};\ a \in R,\ b \in R^*\}$ o anel quociente clássico à direita de R. Desde que $u^{-1}v \in D$, existem $a, b \in R$, $b \neq 0$, tais que $u^{-1}v = ab^{-1}$. Com isso, $0 \neq vb = ua \in uR \cap vR$. □

Observação 2.10 Note que o anel quociente clássico de um domínio de Ore é um anel de divisão.

Observação 2.11 Se D é um domínio comutativo, então D é um domínio de Ore à direita e à esquerda. De fato, dados $a, b \in D^*$, note que $0 \neq ab \in aD$ e $0 \neq ba \in bD$.

Observação 2.12 No caso de D ser um anel de divisão, D também é um domínio de Ore à direita e à esquerda, pois todo ideal não nulo (à direita, à esquerda ou bilateral) coincide com D.

O lema seguinte é útil para provar as próximas proposições.

Lema 2.1.3 *Se B é um anel de valorização total do anel de divisão D, então B é um domínio de Ore à direita e à esquerda.*

Demonstração

Note que $B \subseteq D$ e D é domínio implica imediatamente que B é domínio. Sejam $a, b \in B^*$. Temos que $aB \subseteq bB \neq 0$ ou $bB \subseteq aB \neq 0$. Logo $aB \cap bR \neq 0$. Portanto, B é um domínio de Ore à direita. Analogamente, prova-se que B é um domínio de Ore à esquerda.
□

Dessa forma, todo anel de valorização total de um anel de divisão possui anel quociente clássico à direita e à esquerda, que devem coincidir, pela Proposição 2.1.8.

Conforme citamos anteriormente, obteremos agora um análogo, em anéis de divisão, à Proposição 1.1.3 e ao fato de um corpo $\mathbb{K}$ ser o corpo de frações de um anel de valorização V de $\mathbb{K}$.

Proposição 2.1.11 *Se B é um anel de valorização total do anel de divisão D, então D é o anel quociente clássico para B.*

Demonstração

Claro que B é subanel de D e que todo elemento regular de B tem inverso em D. Também é fácil ver que $\{ab^{-1};\ a \in B,\ b \in B^*\} \subseteq D$ e $\{a^{-1}b;\ a \in B^*,\ b \in B\} \subseteq D$. Consideremos $x \in D$. Se $x = 0$, temos que $x = 0.1^{-1}$, com $0 \in B$ e $1 \in B^*$. Para $x \neq 0$ e $x \in B$, temos $x = x.1^{-1}$, com $x \in B$ e $1 \in B^*$. Para $x \neq 0$ e $x^{-1} \in B$, temos $x = 1.(x^{-1})^{-1}$, com $1 \in B$ e $x^{-1} \in B^*$. Logo $D \subseteq \{ab^{-1};\ a \in B,\ b \in B^*\}$ e assim $D = \{ab^{-1};\ a \in B,\ b \in B^*\}$. Analogamente, mostra-se que $D \subseteq \{a^{-1}b;\ a \in B^*,\ b \in B\}$ e assim $\{a^{-1}b;\ a \in B^*,\ b \in B\} = D$. Portanto, D é o anel quociente clássico para B. $\square$

Proposição 2.1.12 *Seja D anel de divisão e anel quociente clássico à direita para B. São equivalentes:*

(i) *Os ideais à esquerda de B estão totalmente ordenados por inclusão;*

(ii) *B é anel de valorização total de D.*

Demonstração

$(ii) \Rightarrow (i)$ Esta implicação é parte da Proposição 2.1.1 e nem é necessária a hipótese de D ser o anel quociente clássico à direita para B.

$(i) \Rightarrow (ii)$ Seja $x \in D^*$. Como D é o anel quociente clássico à direita para B, podemos escrever $x = ab^{-1}$ com $a \in B$ e $b \in B^*$. Por hipótese, $Ba \subseteq Bb$ ou $Bb \subseteq Ba$. No primeiro caso, $a = vb$, para algum $v \in B$. Assim, $x = ab^{-1} = v \in B$. No segundo caso, $b = ua$, para algum $u \in B$. Assim, $x = a(ua)^{-1} = u^{-1}$. Logo, $x^{-1} = u \in B$. Portanto, B é um anel de valorização total de D. $\square$

Note que trocando *direita* por *esquerda* e *esquerda* por *direita* no enunciado da Proposição 2.1.12 ela continuará sendo válida e a demonstração é análoga. Também é válido o corolário seguinte.

Corolário 2.1.2 *Seja D anel de divisão e anel quociente clássico para B. São equivalentes:*

(i) *Os ideais à direita ou os ideais à esquerda de B estão totalmente ordenados por inclusão;*

(ii) B é anel de valorização total de D.

Demonstração

$(ii) \Rightarrow (i)$ Segue da Proposição 2.1.1.

$(i) \Rightarrow (ii)$ Se os ideais à esquerda estão totalmente ordenados por inclusão, basta aplicar a Proposição 2.1.12. Por outro lado, se os ideais à direita é que estão totalmente ordenados por inclusão, basta usar um análogo da Proposição 2.1.12 que se obtem trocando direita por esquerda e esquerda por direita no seu enunciado. □

2.2 Exemplo de Anel de Valorização Total e Invariante

Conforme citamos na seção anterior, vamos apresentar um exemplo de um anel de valorização total e invariante em um anel de divisão que não é corpo, a saber, a álgebra de divisão dos quatérnios racionais $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$. No final desta seção, utilizaremos este exemplo para algumas discussões a respeito de extensões de anéis de valorização em anéis de divisão.

Nosso exemplo é o conjunto $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$, $\alpha = \frac{1}{2}(1 + i + j + k)$, onde $\mathbb{Z}_{(2)}$ é a localização segundo o sistema multiplicativo $S = \mathbb{Z} \backslash 2\mathbb{Z}$. Temos que

$$\mathbb{Z}_{(2)} = \left\{ab^{-1};\ a, b \in \mathbb{Z},\ 2 \nmid b\right\}.$$

Na Seção 4 vamos mostrar que o anel $V_{(2)} = \mathbb{Z}_{(2)} + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$ não é total em $\mathbb{H}$ (isto é, existe $x \in \mathbb{H}^*$, tal que $x, x^{-1} \notin V_{(2)}$). Veremos a seguir que $\tilde{V}_{(2)}$ contém $V_{(2)}$ propriamente. O conjunto $\tilde{V}_{(2)}$ é o anel $V_{(2)}$ adicionado de elementos suficientes para torná-lo total e invariante em $\mathbb{H}$.

Se em $\tilde{V}_{(2)}$ substituirmos $\mathbb{Z}_{(2)}$ por $\mathbb{Q}$, teremos o anel integral dos quatérnios ou Anel de Hurwitz, que é utilizado por alguns autores (por exemplo [Ha] e [Sa]) na demonstração do conhecido Teorema de Lagrange sobre a representação de um inteiro não negativo como soma de quatro quadrados de números inteiros, que utilizaremos na próxima seção.

A próxima proposição caracteriza mais especificamente os elementos de $\tilde{V}_{(2)}$.

Proposição 2.2.1 *O conjunto $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$, $\alpha = \frac{1}{2}(1 + i + j + k)$, é composto dos elementos $a + bi + cj + dk \in \mathbb{H}$, tais que $a, b, c, d \in \mathbb{Z}_{(2)}$ ou $a, b, c, d \in \frac{1}{2} + \mathbb{Z}_{(2)}$.*

Demonstração

Seja $B = \{a + bi + cj + dk \in \mathbb{H};\ a, b, c, d \in \mathbb{Z}_{(2)}$ ou $a, b, c, d \in \frac{1}{2} + \mathbb{Z}_{(2)}\}$ e seja $x = a + bi + cj + dk \in B$, com $a, b, c, d \in \mathbb{Q}$. Se $a, b, c, d \in \mathbb{Z}_{(2)}$, então $a = \frac{a_0}{a_1}$, $b = \frac{b_0}{b_1}$, $c = \frac{c_0}{c_1}$, $d = \frac{d_0}{d_1}$ e $2 \nmid a_1b_1c_1d_1$. Assim,

$$x = \frac{2a_0}{a_1}\frac{1}{2}(1 + i + j + k) + \left(\frac{b_0}{b_1} - \frac{a_0}{a_1}\right) i + \left(\frac{c_0}{c_1} - \frac{a_0}{a_1}\right) j + \left(\frac{d_0}{d_1} - \frac{a_0}{a_1}\right) k \in \tilde{V}_{(2)}.$$

Se $a, b, c, d \in \frac{1}{2} + \mathbb{Z}_{(2)}$, então $a = \frac{1}{2} + \frac{a_0}{a_1}$, $b = \frac{1}{2} + \frac{b_0}{b_1}$, $c = \frac{1}{2} + \frac{c_0}{c_1}$ e $d = \frac{1}{2} + \frac{d_0}{d_1}$, onde $2 \nmid a_1b_1c_1d_1$. Assim,

$$x = \left(\frac{1}{2} + \frac{a_0}{a_1}\right) + \left(\frac{1}{2} + \frac{b_0}{b_1}\right) i + \left(\frac{1}{2} + \frac{c_0}{c_1}\right) j + \left(\frac{1}{2} + \frac{d_0}{d_1}\right) k = \frac{1}{2}(1+i+j+k) + \frac{a_0}{a_1} + \frac{b_0}{b_1}i + \frac{c_0}{c_1}j + \frac{d_0}{d_1}k.$$

Claramente $\frac{1}{2}(1+i+j+k) \in \tilde{V}_{(2)}$ e pelo caso anterior, temos que $\frac{a_0}{a_1} + \frac{b_0}{b_1}i + \frac{c_0}{c_1}j + \frac{d_0}{d_1}k$ também está em $\tilde{V}_{(2)}$. Como $\tilde{V}_{(2)}$ é fechado por somas, vem que $x \in \tilde{V}_{(2)}$. Provamos portanto que $B \subseteq \tilde{V}_{(2)}$. Por outro lado, consideremos $x = \frac{a_0}{a_1}\frac{1}{2}(1 + i + j + k) + \frac{b_0}{b_1}i + \frac{c_0}{c_1}j + \frac{d_0}{d_1}k \in \tilde{V}_{(2)}$. Então $2 \nmid a_1b_1c_1d_1$. Temos que $x = \frac{a_0}{2a_1} + \left(\frac{a_0}{2a_1} + \frac{b_0}{b_1}\right) i + \left(\frac{a_0}{2a_1} + \frac{c_0}{c_1}\right) j + \left(\frac{a_0}{2a_1} + \frac{d_0}{d_1}\right) k$. Se a_0 é par, então $\frac{a_0}{2a_1} \in \mathbb{Z}_{(2)}$, pois $2 \nmid a_1$. Segue que $\frac{a_0}{2a_1} + \frac{b_0}{b_1}$, $\frac{a_0}{2a_1} + \frac{c_0}{c_1}$, $\frac{a_0}{2a_1} + \frac{d_0}{d_1} \in \mathbb{Z}_{(2)}$, pois $\frac{b_0}{b_1}$, $\frac{c_0}{c_1}$, $\frac{d_0}{d_1} \in \mathbb{Z}_{(2)}$ e $\mathbb{Z}_{(2)}$ é fechado por somas. Daí, $x \in B$. Agora vamos supor a_0 ímpar. Como $2 \nmid a_1$, temos que a_1 também é ímpar. Assim $a_0 - a_1$ é par e segue que $r = \frac{a_0 - a_1}{2} \in \mathbb{Z}$. Desta forma, $\frac{a_0}{2a_1} = \frac{1}{2} + \frac{a_0 - a_1}{2a_1} = \frac{1}{2} + \frac{r}{a_1} \in \frac{1}{2} + \mathbb{Z}_{(2)}$. Segue que

$$\frac{a_0}{2a_1} + \frac{b_0}{b_1} = \frac{1}{2} + \left(\frac{a_0 - a_1}{2a_1} + \frac{b_0}{b_1}\right) \in \frac{1}{2} + \mathbb{Z}_{(2)},$$

$$\frac{a_0}{2a_1} + \frac{c_0}{c_1} = \frac{1}{2} + \left(\frac{a_0 - a_1}{2a_1} + \frac{c_0}{c_1}\right) \in \frac{1}{2} + \mathbb{Z}_{(2)},$$

$$\frac{a_0}{2a_1} + \frac{d_0}{d_1} = \frac{1}{2} + \left(\frac{a_0 - a_1}{2a_1} + \frac{d_0}{d_1}\right) \in \frac{1}{2} + \mathbb{Z}_{(2)}.$$

Portanto, $x \in B$. $\square$

Observação 2.13 Na proposição anterior, cabe observar que dada uma fração irredutível $\frac{a}{b}$, temos que $\frac{a}{b} \in \frac{1}{2} + \mathbb{Z}_{(2)}$ se, e somente se, b é um número par tal que $4 \nmid b$. De fato, $\frac{a}{b} \in \frac{1}{2} + \mathbb{Z}_{(2)}$ implica que $\frac{a}{b} = \frac{1}{2} + \frac{a_0}{a_1}$, com $2 \nmid a_1$. Assim, $\frac{a}{b} = \frac{a_1 + 2a_0}{2a_1}$ e note que $a_1 + 2a_0$ é ímpar e $4 \nmid 2a_1$. Por outro lado, seja $\frac{a}{b} \in \mathbb{Q}$ e b par tal que $4 \nmid b$. Então $\frac{a}{b} = \frac{a}{2k}$, com k ímpar. Com isso, temos que $\frac{a}{b} = \frac{a}{2k} = \frac{1}{2} + \frac{r}{k}$, onde $r = \frac{a-k}{2} \in \mathbb{Z}$. Portanto, $\frac{a}{b} \in \frac{1}{2} + \mathbb{Z}_{(2)}$.

Observação 2.14 A observação anterior e a Proposição 2.2.1 nos permitem concluir que se $x = a + bi + cj + dk \in \mathbb{H}^*$, com $a = \frac{a_0}{a_1}$, $b = \frac{b_0}{b_1}$, $c = \frac{c_0}{c_1}$ e $d = \frac{d_0}{d_1}$, então $x \in \tilde{V}_{(2)}$ se, e somente se, a_1, b_1, c_1, d_1 são todos ímpares ou a_1, b_1, c_1, d_1 são pares e $4 \nmid a_1$, $4 \nmid b_1$, $4 \nmid c_1$ e $4 \nmid d_1$.

Para a demonstração de que $\tilde{V}_{(2)}$ é total e invariante em $\mathbb{H}$ vamos precisar de mais alguns resultados preliminares.

Proposição 2.2.2 *Sejam $a, b, c, d \in \mathbb{Z}$ números ímpares. Então:*

(a) $a^2 + b^2 = 2k_1$, para algum k_1 inteiro ímpar;

(b) $a^2 + b^2 + c^2 + d^2 = 4k_2$, para algum k_2 inteiro ímpar.

Demonstração

Sejam $a = 2a_1 + 1$, $b = 2b_1 + 1$, $c = 2c_1 + 1$ e $d = 2d_1 + 1$.

(i) $a^2 + b^2 = (2a_1 + 1)^2 + (2b_1 + 1)^2 = 4(a_1^2 + a_1 + b_1^2 + b_1) + 2 = 2[2(a_1^2 + a_1 + b_1^2 + b_1) + 1]$. Assim, basta escolher $k_1 = 2(a_1^2 + a_1 + b_1^2 + b_1) + 1$.

(ii) $a^2 + b^2 + c^2 + d^2 = (2a_1 + 1)^2 + (2b_1 + 1)^2 + (2c_1 + 1)^2 + (2d_1 + 1)^2 = 4[(a_1^2 + a_1 + b_1^2 + b_1 + c_1^2 + c_1 + d_1^2 + d_1) + 1]$. Como $a_1^2 + a_1$, $b_1^2 + b_1$, $c_1^2 + c_1$ e $d_1^2 + d_1$ são números pares, basta tomar $k_2 = (a_1^2 + a_1 + b_1^2 + b_1 + c_1^2 + c_1 + d_1^2 + d_1) + 1$. $\square$

Definição 2.2.1 *Seja $x = a + bi + cj + dk \in \mathbb{H}$. Definimos $\bar{x} = a - bi - cj - dk \in \mathbb{H}$ e $N(x) = x\bar{x}$. Dizemos que $\bar{x}$ é o conjugado de x e $N(x)$ é a norma de x.*

É fácil ver que se $x \in \mathbb{H}^*$, então $x^{-1} = \frac{1}{N(x)}\bar{x}$. Também $N(x) = a^2 + b^2 + c^2 + d^2$.

Vamos estudar mais especificamente o inverso de $x = \frac{a_0}{b_0} + \frac{a_1}{b_1}i + \frac{a_2}{b_2}j + \frac{a_3}{b_3}k \in \mathbb{H}^*$. Temos

$$N(x) = \frac{a_0^2}{b_0^2} + \frac{a_1^2}{b_1^2} + \frac{a_2^2}{b_2^2} + \frac{a_3^2}{b_3^2} = \frac{a_0^2b_1^2b_2^2b_3^2 + a_1^2b_0^2b_2^2b_3^2 + a_2^2b_0^2b_1^2b_3^2 + a_3^2b_0^2b_1^2b_2^2}{b_0^2b_1^2b_2^2b_3^2},$$

$$x^{-1} = \frac{b_0b_1^2b_2^2b_3^2a_0}{\beta} - \frac{b_0^2b_1b_2^2b_3^2a_1}{\beta}i - \frac{b_0^2b_1^2b_2b_3^2a_2}{\beta}j - \frac{b_0^2b_1^2b_2^2b_3a_3}{\beta}k \qquad (*)$$

onde $\beta = a_0^2b_1^2b_2^2b_3^2 + a_1^2b_0^2b_2^2b_3^2 + a_2^2b_0^2b_1^2b_3^2 + a_3^2b_0^2b_1^2b_2^2$. Note que se $2 \nmid \beta$, ou se β é um número par tal que $4 \nmid \beta$, então $x^{-1} \in \tilde{V}_{(2)}$.

Teorema 2.2.1 *O conjunto $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$, com $\alpha = \frac{1}{2}(1 + i + j + k)$, é um anel de valorização total e invariante no anel dos quatérnios racionais $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ e $V_{(2)} = \mathbb{Z}_{(2)} + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k \subsetneq \tilde{V}_{(2)}$.*

Demonstração

Usando a Proposição 2.2.1, não é difícil mostar que $\tilde{V}_{(2)}$ é fechado por diferenças e produtos.

Assim, $\tilde{V}_{(2)}$ é subanel de $\mathbb{H}$. Também a Proposição 2.2.1 assegura que $V_{(2)} \subsetneqq \tilde{V}_{(2)}$.Vamos demonstrar que $\tilde{V}_{(2)}$ é total em $\mathbb{H}$. Seja $x = a + bi + cj + dk \in \mathbb{H}^*$, com $a = \frac{a_0}{b_0}$, $b = \frac{a_1}{b_1}$, $c = \frac{a_2}{b_2}$ e $d = \frac{a_3}{b_3}$, onde $\frac{a_i}{b_i}$ são frações irredutíveis. Pela Proposição 2.2.1, se $a, b, c, d \in \mathbb{Z}_{(2)}$ ou $a, b, c, d \in \frac{1}{2} + \mathbb{Z}_{(2)}$, temos que $x \in \tilde{V}_{(2)}$. Se $x \notin \tilde{V}_{(2)}$, segue da Observação 2.14 que existe um elemento par no conjunto $\{b_0, b_1, b_2, b_3\}$, e se todos forem pares, 4 divide um dos elementos de $\{b_0, b_1, b_2, b_3\}$. Vamos separar isso em quatro casos. Os demais são análogos.

(1) $2 \,|\, b_0$ e $2 \nmid b_1b_2b_3$;

(2) $2 \,|\, b_0$, $2 \,|\, b_1$ e $2 \nmid b_2b_3$;

(3) $2 \,|\, b_1$, $2 \,|\, b_2$, $2 \,|\, b_3$ e $2 \nmid b_0$;

(4) $2 \,|\, b_1$, $2 \,|\, b_1$, $2 \,|\, b_2$, $2 \,|\, b_3$, e 4 divide um dos elementos do conjunto $\{b_0, b_1, b_2, b_3\}$.

Para esses casos vamos demonstrar que $x^{-1} \in \tilde{V}_{(2)}$. Denotamos $b_i = 2^{t_i}s_i$, $i \in \{0, 1, 2, 3\}$, com s_i ímpar.

(1) Temos b_0 par e b_1, b_2, b_3 ímpares. Segue imediatamente que a_0 é impar. Por $(*)$, temos que

$$x^{-1} = \frac{b_0b_1^2b_2^2b_3^2a_0}{\beta} - \frac{b_0^2b_1b_2^2b_3^2a_1}{\beta}i - \frac{b_0^2b_1^2b_2b_3^2a_2}{\beta}j - \frac{b_0^2b_1^2b_2^2b_3a_3}{\beta}k,$$

onde $\beta = a_0^2b_1^2b_2^2b_3^2 + a_1^2b_0^2b_2^2b_3^2 + a_2^2b_0^2b_1^2b_3^2 + a_3^2b_0^2b_1^2b_2^2$. Não é difícil ver que β é ímpar. Logo $x^{-1} \in \tilde{V}_{(2)}$.

(2) Temos b_0, b_1 pares e b_2, b_3 ímpares. Vamos supor, sem perda de generalidade, que $t_0 \le t_1$. Temos que

$$\frac{1}{N(x)} = \frac{4^{t_0+t_1}s_0^2s_1^2b_2^2b_3^2}{4^{t_1}a_0^2s_1^2b_2^2b_3^2 + 4^{t_0}a_1^2s_0^2b_2^2b_3^2 + 4^{t_0+t_1}a_2^2s_0^2s_1^2b_3^2 + 4^{t_0+t_1}a_3^2s_0^2s_1^2b_2^2}$$

$$= \frac{4^{t_1}s_0^2s_1^2b_2^2b_3^2}{4^{t_1-t_0}a_0^2s_1^2b_2^2b_3^2 + a_1^2s_0^2b_2^2b_3^2 + 4^{t_1}a_2^2s_0^2s_1^2b_3^2 + 4^{t_1}a_3^2s_0^2s_1^2b_2^2}.$$

Seja ξ o denominador da expressão anterior. Observe que se $t_0 < t_1$, ξ é ímpar. Assim,

$$x^{-1} = \frac{1}{N(x)}\bar{x} = \frac{4^{t_1}s_0^2s_1^2b_2^2b_3^2}{\xi}\Big(\frac{a_0}{2^{t_0}s_0} - \frac{a_1}{2^{t_1}s_1}i - \frac{a_2}{b_2}j - \frac{a_3}{b_3}k\Big)$$

$$= \frac{2^{2t_1-t_0}s_0s_1^2b_2^2b_3^2a_0}{\xi} - \frac{2^{t_1}s_0^2s_1b_2^2b_3^2a_1}{\xi}i - \frac{2^{2t_1}s_0^2s_1^2b_2b_3^2a_2}{\xi}j - \frac{2^{2t_1}s_0^2s_1^2b_2^2b_3a_3}{\xi}k \in \tilde{V}_{(2)}.$$

Caso $t_0 = t_1$, temos

$$\frac{1}{N(x)} = \frac{4^{t_1} s_0^2 s_1^2 b_2^2 b_3^2}{a_0^2 s_1^2 b_2^2 b_3^2 + a_1^2 s_0^2 b_2^2 b_3^2 + 4^{t_1} a_2^2 s_0^2 s_1^2 b_3^2 + 4^{t_1} a_3^2 s_0^2 s_1^2 b_2^2}.$$

Segue do item (a) da Proposição 2.2.2, que o número de fatores 2 de $a_0^2 s_1^2 b_2^2 b_3^2 + a_1^2 s_0^2 b_2^2 b_3^2$ é apenas um, já que temos uma soma de dois quadrados de números ímpares. Assim, podemos denotar $a_0^2 s_1^2 b_2^2 b_3^2 + b_1^2 s_0^2 b_2^2 b_3^2$ por 2γ, com γ ímpar. Dessa forma,

$$\frac{1}{N(x)} = \frac{4^{t_1} s_0^2 s_1^2 b_2^2 b_3^2}{2\gamma + 4^{t_1} a_2^2 s_0^2 s_1^2 b_3^2 + 4^{t_1} a_3^2 s_0^2 s_1^2 b_2^2} = \frac{2^{2t_1-1} s_0^2 s_1^2 b_2^2 b_3^2}{\gamma + 2^{2t_1-1} a_2^2 s_0^2 s_1^2 b_3^2 + 2^{2t_1-1} a_3^2 s_0^2 s_1^2 b_2^2}.$$

Seja $\delta = \gamma + 2^{2t_1-1} a_2^2 s_0^2 s_1^2 b_3^2 + 2^{2t_1-1} a_3^2 s_0^2 s_1^2 b_2^2$. Note que δ é ímpar. Assim,

$$x^{-1} = \frac{1}{N(x)}\bar{x} = \frac{2^{2t_1-1} s_0^2 s_1^2 b_2^2 b_3^2}{\delta}\Big(\frac{a_0}{2^{t_0} s_0} - \frac{a_1}{2^{t_1} s_1} i - \frac{a_2}{b_2} j - \frac{a_3}{b_3} k\Big)$$

$$= \tfrac{2^{t_1-1} s_0 s_1^2 b_2^2 b_3^2 a_0}{\delta} - \tfrac{2^{t_1-1} s_0^2 s_1 b_2^2 b_3^2 a_1}{\delta} i - \tfrac{2^{2t_1-1} s_0^2 s_1^2 b_2 b_3^2 a_2}{\delta} j - \tfrac{2^{2t_1-1} s_0^2 s_1^2 b_2^2 b_3 a_3}{\delta} k \in \tilde{V}_{(2)}.$$

(3) b_0 ímpar e b_1, b_2, b_3 pares. Seja $t = min\{t_2 + t_3,\ t_1 + t_3,\ t_1 + t_2\}$. Podemos supor, sem perda de generalidade, que $t = t_1 + t_2$. Observe que nesse caso $t_3 = max\{t_1, t_2, t_3\}$. Temos que

$$\frac{1}{N(x)} = \frac{4^{t_1+t_2+t_3} b_0^2 s_1^2 s_2^2 s_3^2}{4^{t_1+t_2+t_3} a_0^2 s_1^2 s_2^2 s_3^2 + 4^{t_2+t_3} a_1^2 b_0^2 s_2^2 s_3^2 + 4^{t_1+t_3} a_2^2 b_0^2 s_1^2 s_3^2 + 4^{t_1+t_2} a_3^2 b_0^2 s_1^2 s_2^2}$$

$$= \frac{4^{t_3} b_0^2 s_1^2 s_2^2 s_3^2}{4^{t_3} a_0^2 s_1^2 s_2^2 s_3^2 + 4^{t_3-t_1} a_1^2 b_0^2 s_2^2 s_3^2 + 4^{t_3-t_2} a_2^2 b_0^2 s_1^2 s_3^2 + a_3^2 b_0^2 s_1^2 s_2^2}.$$

Seja ρ o denominador da última expressão. Observe que ρ é ímpar nos casos $t_1 = t_2 = t_3$ e $t_1 \leq t_2 < t_3$. Desta maneira, basta proceder como anteriormente e veremos que $x^{-1} \in \tilde{V}_{(2)}$. Quando $t_1 < t_2 = t_3$, ρ terá as parcelas $a_2^2 b_0^2 s_1^2 s_3^2$ e $a_3^2 b_0^2 s_1^2 s_2^2$ sem coeficiente par. Novamente pela Proposição 2.2.2, $a_2^2 b_0^2 s_1^2 s_3^2 + a_3^2 b_0^2 s_1^2 s_2^2$ tem apenas um fator 2 e procedendo da mesma maneira como no item **(2)**, teremos que $x^{-1} \in \tilde{V}_{(2)}$.

(4) b_0, b_1, b_2, b_3 pares, com pelo menos um deles do tipo $4k$. Temos que

$$\frac{1}{N(x)} = \frac{4^{t_0+t_1+t_2+t_3} s_0^2 s_1^2 s_2^2 s_3^2}{4^{t_1+t_2+t_3} a_0^2 s_1^2 s_2^2 s_3^2 + 4^{t_0+t_2+t_3} a_1^2 s_0^2 s_2^2 s_3^2 + 4^{t_0+t_1+t_3} a_2^2 s_0^2 s_1^2 s_3^2 + 4^{t_0+t_1+t_2} a_3^2 s_0^2 s_1^2 s_2^2}.$$

Vamos considerar o caso em que todos os $t_i{}'$s são iguais. Nesse caso

$$\frac{1}{N(x)}=\frac{4^{t_3}s_0^2s_1^2s_2^2s_3^2}{a_0^2s_1^2s_2^2s_3^2+a_1^2s_0^2s_2^2s_3^2+a_2^2s_0^2s_1^2s_3^2+a_3^2s_0^2s_1^2s_2^2}.$$

Observe que o denominador da expressão anterior é composto de quatro parcelas ímpares que estão elevadas ao quadrado. Aplicando a Proposição 2.2.2, temos que esta expressão possui exatamente dois fatores 2. Então podemos denotá-la por $2^2\lambda$ com λ ímpar. Assim,

$$\frac{1}{N(x)}=\frac{4^{t_3}s_0^2s_1^2s_2^2s_3^2}{2^2\lambda}=\frac{2^{2t_3-1}s_0^2s_1^2s_2^2s_3^2}{2\lambda},$$

$$x^{-1}=\frac{2^{2t_3-1}s_0^2s_1^2s_2^2s_3^2}{2\lambda}\Big(\frac{a_0}{2^{t_0}s_0}-\frac{a_1}{2^{t_1}s_1}i-\frac{a_2}{2^{t_2}s_2}j-\frac{a_3}{2^{t_3}s_3}k\Big)$$
$$=\frac{2^{t_3-1}s_0s_1^2s_2^2s_3^2a_0}{2\lambda}-\frac{2^{t_3-1}s_0^2s_1s_2^2s_3^2a_1}{2\lambda}i-\frac{2^{t_3-1}s_0^2s_1^2s_2s_3^2a_2}{2\lambda}j-\frac{2^{t_3-1}s_0^2s_1^2s_2^2s_3a_3}{2\lambda}k\in\tilde{V}_{(2)}.$$

Claro que os $t_i{}'$s podem não ser todos iguais. Mas, com essa hipótese, não é difícil verificar que recairemos em demonstrações análogas aos casos anteriores. Portanto, $x^{-1}\in\tilde{V}_{(2)}$. E isso conclui, finalmente, a prova de que $\tilde{V}_{(2)}$ é um anel de valorização total de $\mathbb{H}$.

Para demonstrar a invariância do anel $\tilde{V}_{(2)}$, basta mostrar que dado $b\in\tilde{V}_{(2)}$, temos $xbx^{-1}\in\tilde{V}_{(2)}$, para todo $x\in\mathbb{H}^*$. Note que $xbx^{-1}=\frac{1}{N(x)}xb\bar{x}$. Seja $x=a+bi+cj+dk=\frac{a_0}{b_0}+\frac{a_1}{b_1}i+\frac{a_2}{b_2}j+\frac{a_3}{b_3}\in\mathbb{H}^*$. Sabemos que

$$N(x)=\frac{\beta}{b_0^2b_1^2b_2^2b_3^2},\text{ onde }\beta=a_0^2b_1^2b_2^2b_3^2+a_1^2b_0^2b_2^2b_3^2+a_2^2b_0^2b_1^2b_3^2+a_3^2b_0^2b_1^2b_2^2.$$

Assim,

$$xbx^{-1}=\frac{b_0^2b_1^2b_2^2b_3^2}{\beta}\Big(\frac{a_0}{b_0}+\frac{a_1}{b_1}i+\frac{a_2}{b_2}j+\frac{a_3}{b_3}k\Big)b\Big(\frac{a_0}{b_0}-\frac{a_1}{b_1}i-\frac{a_2}{b_2}j-\frac{a_3}{b_3}k\Big)$$

$$=\Big(\frac{1}{\beta}\Big)yb\bar{y},\text{ onde }y=b_1b_2b_3a_0+b_0b_2b_3a_1i+b_0b_1b_3a_2j+b_0b_1b_2a_3k.$$

Se β é ímpar, todos os fatores do produto $\frac{1}{\beta}yb\bar{y}$ estão em $\tilde{V}_{(2)}$ e assim $xbx^{-1}\in\tilde{V}_{(2)}$. Agora, sabemos que $x\in\tilde{V}_{(2)}$ ou $x^{-1}\in\tilde{V}_{(2)}$. Inicialmente vamos supor que $x\in\tilde{V}_{(2)}$. Assim, $a,b,c,d\in\mathbb{Z}_{(2)}$ ou $a,b,c,d\in\frac{1}{2}+\mathbb{Z}_{(2)}$. Se $a,b,c,d\in\frac{1}{2}+\mathbb{Z}_{(2)}$, temos $\frac{a_i}{b_i}\in\frac{1}{2}+\mathbb{Z}_{(2)}$ e então $2\,|\,b_0$, $2\,|\,b_1$, $2\,|\,b_2$ e $2\,|\,b_3$. Segue do quarto caso da demonstração da totalidade que

$x^{-1} \in \tilde{V}_{(2)}$ e assim, $xbx^{-1} \in \tilde{V}_{(2)}$. Admitindo que $a, b, c, d \in \mathbb{Z}_{(2)}$, temos $2 \nmid b_0$, $2 \nmid b_1$, $2 \nmid b_2$, e $2 \nmid b_3$. Basta analisar os seguintes subcasos:

- $2 \,|\, a_0$ e $2 \nmid a_1a_2a_3$;
- $2 \,|\, a_0$, $2 \,|\, a_1$ e $2 \nmid a_2a_3$;
- $2 \,|\, a_0$, $2 \,|\, a_1$, $2 \,|\, a_2$ e $2 \nmid a_3$;
- $2 \nmid a_0a_1a_2a_3$.

O primeiro e o terceiro subcasos implicam que $2 \nmid \beta$ e assim, $xbx^{-1} \in \tilde{V}_{(2)}$. Do segundo subcaso e da Proposição 2.2.2, decorre que a expressão $a_2^2b_0^2b_1^2b_3^2 + a_3^2b_0^2b_1^2b_2^2$ possui apenas um fator 2. Assim, fazendo $a_0 = 2^{t_0}s_0$ e $a_1 = 2^{t_1}s_1$ com s_0, s_1 ímpares, temos que $\beta = a_0^2b_1^2b_2^2b_3^2 + a_1^2b_0^2b_2^2b_3^2 + 2k = 2(2^{2t_0-1}s_0^2b_1^2b_2^2b_3^2 + 2^{2t_1-1}s_1^2b_0^2b_2^2b_3^2 + k)$, com k ímpar. Desta forma, $\beta = 2\sigma$, onde σ é o número ímpar $2^{2t_0-1}s_0^2b_1^2b_2^2b_3^2+2^{2t_1-1}s_1^2b_0^2b_2^2b_3^2+k$. Logo, podemos representar

$$xbx^{-1} = \frac{b_0^2b_1^2b_2^2b_3^2}{\sigma}\Big(\frac{a_0}{2b_0} + \frac{a_1}{2b_1}i + \frac{a_2}{2b_2}j + \frac{a_3}{2b_3}k\Big)b\Big(\frac{2^{t_0}s_0}{b_0} - \frac{2^{t_1}s_1}{b_1}i - \frac{a_2}{b_2}j - \frac{a_3}{b_3}k\Big)$$

Note que cada um dos fatores da expressão anterior está em $\tilde{V}_{(2)}$. Portanto $xbx^{-1} \in \tilde{V}_{(2)}$. No quarto subcaso, temos que β será da forma 4τ, com τ ímpar. Então

$$xbx^{-1} = \frac{b_0^2b_1^2b_2^2b_3^2}{4\tau}\Big(\frac{a_0}{b_0} + \frac{a_1}{b_1}i + \frac{a_2}{b_2}j + \frac{a_3}{b_3}k\Big)b\Big(\frac{a_0}{b_0} - \frac{a_1}{b_1}i - \frac{a_2}{b_2}j - \frac{a_3}{b_3}k\Big)$$

$$= (\tfrac{b_1b_2b_3a_0}{2\tau} + \tfrac{b_0b_2b_3a_1}{2\tau}i + \tfrac{b_0b_1b_3a_2}{2\tau}j + \tfrac{b_0b_1b_2a_3}{2\tau}k)b(\tfrac{b_1b_2b_3a_0}{2} - \tfrac{b_0b_2b_3a_1}{2}i - \tfrac{b_0b_1b_3a_2}{2}j - \tfrac{b_0b_1b_2a_3}{2}k).$$

Como cada um dos fatores pertence a $\tilde{V}_{(2)}$, temos que $xbx^{-1} \in \tilde{V}_{(2)}$. Concluímos desta forma que dado $b \in \tilde{V}_{(2)}$ e $x \in \mathbb{H}^*$, se $x \in \tilde{V}_{(2)}$, então xbx^{-1}. Se $x \notin \tilde{V}_{(2)}$, vimos que $x^{-1} \in \tilde{V}_{(2)}$. Observe que na prova dos Casos $\mathbf{(1)}, \mathbf{(2)}, \mathbf{(3)}$ e $\mathbf{(4)}$ da demonstração da totalidade, quando se fazem as simplificações da fração $\frac{1}{N(x)}$, sempre sobram fatores 2 suficientes para simplificar todos, exceto possivelmente um, dos fatores 2 de a_1, b_1, c_1 e d_1 na expressão:

$$xbx^{-1} = \Big(\frac{a_0}{a_1} + \frac{b_0}{b_1}i + \frac{c_0}{c_1}j + \frac{d_0}{d_1}k\Big)bx^{-1}.$$

Simplificados esses fatores, os três fatores dessa expressão pertencem à $\tilde{V}_{(2)}$. Logo, $xbx^{-1} \in \tilde{V}_{(2)}$, o que conclui a demonstração da invariância de $\tilde{V}_{(2)}$. $\square$

Conforme enunciamos no início desta seção, vamos utilizar o anel de valorização total e invariante $\tilde{V}_{(2)}$ para algumas discussões sobre extensões de um anel de valorização em um anel de divisão.

Proposição 2.2.3 *O anel* $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k, \alpha = \frac{1}{2}(1+i+j+k)$ *é extensão de* $\mathbb{Z}_{(2)}$ *em* $\mathbb{H}$.

Demonstração

Basta mostrar que $\tilde{V}_{(2)} \cap \mathbb{Q} = \mathbb{Z}_{(2)}$. Como $\mathbb{Z}_{(2)} \subseteq V_{(2)} \subsetneqq \tilde{V}_{(2)}$, temos $\mathbb{Z}_{(2)} \subseteq \mathbb{Q} \cap \tilde{V}_{(2)}$. Por outro lado, consideremos $x \in \tilde{V}_{(2)} \cap \mathbb{Q}$. Como $x \in \tilde{V}_{(2)}$, temos que $x = \frac{1}{2}(1+i+j+k)a+bi+cj+dk$, com $a, b, c, d \in \mathbb{Z}_{(2)}$. Segue que $x = \frac{a}{2}+(b+\frac{a}{2})i+(c+\frac{a}{2})j+(d+\frac{a}{2})k$. Como $x \in \mathbb{Q}$, temos que $b+\frac{a}{2} = c+\frac{a}{2} = d+\frac{a}{2} = 0$. Assim, $b = -\frac{a}{2}$ implica que $x = \frac{a}{2} = -b \in \mathbb{Z}_{(2)}$. □

Como pode ser visto em ([W$_1$], §1, Example (c)), $\tilde{V}_{(2)}$ é o único anel de valorização total que estende $\mathbb{Z}_{(2)}$.

Ainda utilizaremos o fato de $\tilde{V}_{(2)}$ ser o anel de valorização total que estende $\mathbb{Z}_{(2)}$ para outra aplicação, conforme segue.

Seja D um anel de divisão com centro $\mathbb{F}$ e $\mathbb{K}$ um corpo intermediário, isto é, $\mathbb{F} \subseteq \mathbb{K} \subseteq D$. Conforme [W$_1$], em geral não se sabe quando um anel de valorização de $\mathbb{K}$ se estende a D. No caso particular do exemplo abaixo esse problema é resolvido.

Exemplo 2.6 Consideremos o anel dos quatérnios racionais $\mathbb{H}$ e o anel $\tilde{V}_{(2)}$ que definimos anteriormente. Note que $\mathbb{Q}[\,i\,]$ é um corpo intermidiário entre $\mathbb{H}$ e seu centro $\mathbb{Q}$, isto é, $\mathbb{Q} \subseteq \mathbb{Q}[\,i\,] \subseteq \mathbb{H}$. Provaremos que o anel $\tilde{V}_{(2)}$ estende o anel de valorização total $\mathbb{Z}_{(2)}+\mathbb{Z}_{(2)}i$ de $\mathbb{Q}[\,i\,]$. Note que basta provar a igualdade $\mathbb{Z}_{(2)}+\mathbb{Z}_{(2)}i = \tilde{V}_{(2)} \cap \mathbb{Q}[\,i\,]$ para concluir que de fato $\mathbb{Z}_{(2)}+\mathbb{Z}_{(2)}i$ é um anel de valorização total de $\mathbb{Q}[\,i\,]$ e que $\tilde{V}_{(2)}$ estende $\mathbb{Z}_{(2)}+\mathbb{Z}_{(2)}i$. Para tal, consideremos $x = \frac{a}{b}+\frac{c}{d}i \in \mathbb{Z}_{(2)}+\mathbb{Z}_{(2)}i$. Temos que $x = 0\alpha+\frac{a}{b}+\frac{c}{d}i+0j+0k \in \tilde{V}_{(2)} \cap \mathbb{Q}[\,i\,]$. Por outro lado, consideremos $x \in \tilde{V}_{(2)} \cap \mathbb{Q}[\,i\,]$. Como $x \in \tilde{V}_{(2)}$, temos que $x = \frac{1}{2}(1+i+j+k)a+bi+cj+dk$, com $a, b, c, d \in \mathbb{Z}_{(2)}$. Segue que $x = \frac{a}{2}+(b+\frac{a}{2})i+(c+\frac{a}{2})j+(d+\frac{a}{2})k$. Como $x \in \mathbb{Q}[\,i\,]$, temos que $c+\frac{a}{2} = d+\frac{a}{2} = 0$. Decorre que $c = -\frac{a}{2} \in \mathbb{Z}_{(2)}$ e também

$\frac{a}{2} \in \mathbb{Z}_{(2)}$. Dessa forma $x = \frac{a}{2} + (b + \frac{a}{2})i \in \mathbb{Z}_{(2)} + \mathbb{Z}_{(2)}i$, já que $\frac{a}{2}$, $b + \frac{a}{2} \in \mathbb{Z}_{(2)}$.

$$\begin{tikzcd}
\mathbb{H} \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}[\,i\,] \arrow[d, dash] \arrow[dr, dash] & \tilde{V}_{(2)} \arrow[d, dash] \\
\mathbb{Q} \arrow[dr, dash] & \mathbb{Z}_{(2)} + \mathbb{Z}_{(2)}i \arrow[d, dash] \\
 & \mathbb{Z}_{(2)}
\end{tikzcd}$$

2.3 Construção de Anéis de Valorização Totais e Invariantes e Totais Não Invariantes

Nesta seção descreveremos um procedimento para obter anéis de valorização totais em anéis de divisão. Um caso particular desse procedimento produz uma maneira de obter anéis de valorização totais e não invariantes. Apresentaremos estas duas construções gerais e mostraremos com um exemplo específico que existem anéis que preenchem os requisitos do caso particular. Em consonância com o restante deste capítulo, continuaremos trabalhando com anéis de divisão de dimensão finita sobre seu centro.

Seja D um anel de divisão e σ um automorfismo de D. Consideremos os conjuntos

$$D[x,\sigma] = \left\{ \sum_{i=0}^{\infty} a_i x^i;\ a_i \in D \right\} \quad \text{e} \quad D[[x,\sigma]] = \left\{ \sum_{i=r}^{\infty} a_i x^i;\ a_i \in D;\ r \in \mathbb{Z} \right\}.$$

Note que $D[x,\sigma] \subseteq D[[x,\sigma]]$. No conjunto $D[[x,\sigma]]$ introduzimos a operação de adição usual e a multiplicação definida pela regra $xa = \sigma(a)x$ e $x^{-1}a = \sigma(a)x^{-1}$. Podemos explicitar a operação de multiplicação conforme segue. Sejam $p(x) = \sum_{i=r}^{\infty} a_i x^i$ e $q(x) = \sum_{j=s}^{\infty} b_j x^j$ dois elementos de $D[[x,\sigma]]$, onde r, s são os menores inteiros tais que $a_r \neq 0$ e $b_s \neq 0$. Denotamos $r = -n$ e $s = -m$, com $m, n \in \mathbb{N}$. Temos

$$p(x) = a_{-n}x^{-n} + \cdots + a_{-1}x^{-1} + a_0 + a_1 x + \cdots,$$

$$q(x) = b_{-m}x^{-m} + \cdots + b_{-1}x^{-1} + b_0 + b_1 x + \cdots, \text{ e}$$

$$p(x)q(x) = c_{-n-m}x^{-n-m} + \cdots + c_{-1}x^{-1} + c_0 + c_1 x + \cdots,$$

onde $c_k = \sum_{i+j=k} a_i \sigma^{|i|}(b_j)$, com $(-n-m) \leq k$, $-n \leq i$ e $-m \leq j$.

Não é difícil (porém trabalhoso) verificar que $D[[x,\sigma]]$ é um domínio, não necessariamente comutativo e com unidade. Além disso, veremos na próxima proposição que $D[[x,\sigma]]$ é um anel de divisão, que denominamos *anel de divisão das séries formais de Laurent.*

Também não é difícil provar que $D[x,\sigma]$ é subanel de $D[[x,\sigma]]$. Os elementos inversíveis de $D[x,\sigma]$ são caracterizados no lema seguinte, que também será utilizado para provar que $D[[x,\sigma]]$ é anel de divisão.

Lema 2.3.1 *Seja D um anel de divisão. Se $a = \sum_{i=0}^{\infty} a_i x^i \in D[x,\sigma]$, então $a \in U(D[x,\sigma])$ se, e somente se, $a_0 \neq 0$.*

Demonstração

($\Rightarrow$) Por hipótese, existe $b = b_0 + b_1 x + b_2 x^2 + \cdots \in D[x,\sigma]$ tal que $ab = 1$. Então $a_0 b_0 = 1$, com $a_0, b_0 \in D$. Portanto, $a_0 \in D^*$.

($\Leftarrow$) Supondo $a_0 \neq 0$, podemos calcular sucessivamente os coeficientes $b_0, b_1, \cdots, b_n, \cdots$, tais que $a_0 b_0 = 1$,

$$a_0 b_1 + a_1 \sigma(b_0) = 0,$$

$$a_0 b_2 + a_1 \sigma(b_1) + a_2 \sigma^2(b_0) = 0,$$

$$\vdots$$

$$a_0 b_n + a_1 \sigma(b_{n-1}) + \vdots + a_{n-1} \sigma^{n-1}(b_1) + a_n \sigma^n(b_0) = 0,$$

$$\vdots$$

Note que $b_0 = a_0^{-1}$,

$$a_0 b_1 + a_1 \sigma(b_0) = 0 \Rightarrow b_1 = -a_0^{-1} a_1 \sigma(b_0) = -a_0^{-1} a_1 \sigma(a_0)^{-1},$$

$$a_0 b_2 + a_1 \sigma(b_1) + a_2 \sigma^2(b_0) = 0 \Rightarrow b_2 = -{a_0}^{-1}(a_1 \sigma(b_1) + a_2 \sigma^2(b_0)), \text{ e assim,}$$

temos $b_0 = {a_0}^{-1}$ e para $k \geq 1$, $b_k = -a_0^{-1}\Big(\sum_{\substack{i+j=k \\ i \geq 1}} a_i \sigma^i(b_j) \Big)$. Portanto, $b = \sum_{i=0}^{\infty} b_i x^i \in D[x,\sigma]$ e $ab = 1$. $\square$

Proposição 2.3.1 *Se D é anel de divisão, então $D[[x,\sigma]] = \left\{ \sum_{i=r}^{\infty} a_i x^i;\ a_i \in D;\ r \in \mathbb{Z} \right\}$ também é um anel de divisão.*

Demonstração

Consideremos $a = \sum_{i=r}^{\infty} a_i x^i$ um elemento não nulo em $D[[x,\sigma]]$, com r o menor inteiro tal que $a_r \neq 0$. Vamos supor $r < 0$ e denotar $r = -n$, com $n \in \mathbb{N}$. Assim, podemos denotar $a = a_{-n}x^{-n} + a_{-n+1}x^{-n+1} + \cdots + a_{-1}x^{-1} + a_0 + a_1 x + \cdots$. Desta forma, $a = a_{-n}x^{-n}g$, onde $g = 1 + \frac{a_{-n+1}}{a_{-n}}x + \cdots + \frac{a_{-1}}{a_{-n}}x^{n-1} + \frac{a_0}{a_{-n}}x^n + \frac{a_1}{a_{-n}}x^{n+1} + \cdots$. Note que $g \in U(D[x,\sigma])$. Assim, $g^{-1} \in D[x,\sigma] \subseteq D[[x,\sigma]]$ e $a^{-1} = g^{-1}x^n a_{-n}^{-1} \in D[[x,\sigma]]$. No caso de $r > 0$, a demonstração é análoga. Observe que se $r = 0$, então $a \in U(D[x,\sigma])$ e assim $a^{-1} \in D[[x,\sigma]]$. Portanto, $D[[x,\sigma]]$ é um anel de divisão. $\square$

O teorema abaixo mostra que a cada anel de valorização total do anel de divisão D, podemos associar um anel de valorização total de $D[[x,\sigma]]$, que pode ser invariante ou não.

Teorema 2.3.1 *Seja W um anel de valorização total do anel de divisão D e $\sigma \in Aut(D)$.*

(a) *O conjunto* $\hat{B} = \left\{ \sum_{i=0}^{\infty} a_i x^i;\ a_0 \in W,\ a_1, a_2, \cdots \in D \right\}$ *é um anel de valorização total de $D[[x,\sigma]]$ e o seu ideal maximal é* $J(\hat{B}) = \left\{ \sum_{i=0}^{\infty} a_i x^i;\ a_0 \in J(W),\ a_1, a_2, \cdots \in D \right\}$.

(b) *Se $\sigma(W) \neq W$, então* $\hat{B} = \left\{ \sum_{i=0}^{\infty} a_i x^i;\ a_0 \in W,\ a_1, a_2, \cdots \in D \right\}$ *é anel de valorização total e não invariante de $D[[x,\sigma]]$.*

Demonstração

(a) Observe que $\hat{B} \subseteq D[x,\sigma]$ e que $\hat{B}$ é subanel de $D[[x,\sigma]]$. Seja $0 \neq a \in D[[x,\sigma]] \setminus \hat{B}$, $a = \sum_{i=r}^{\infty} a_i x^i$, $r \in Z$. Temos duas possibilidades. A primeira é que exista um ou mais índices $i < 0$ tais que $a_i \neq 0$ e a segunda possibilidade é que $a_i = 0$, para todo $i < 0$ e $a_0 \notin W$. Supondo que exista um ou mais índices $i < 0$ tais que $a_i \neq 0$, vamos considerar $r = -n$ o menor destes índices. Procedendo analagomente à demonstração da proposição anterior, segue que $a = a_{-n}x^{-n}g$, com $g \in U(D[x,\sigma])$. Desde que $g^{-1} \in D[x,\sigma]$, não temos expoentes negativos para x em g^{-1} e então, todos os expoentes de x em $a^{-1} = g^{-1}x^n a_{-n}^{-1}$ são estritamente positivos. Logo a^{-1} possui termo independente nulo e portanto pertence à W, o que implica que $a^{-1} \in \hat{B}$. Vamos supor agora que seja válida a segunda possibilidade, isto é, $a_i = 0$, para todo $i < 0$ e $a_0 \notin W$. Nessas condições, aplicando o Lema 2.3.1, temos que $a \in U(D[x,\sigma])$. Assim, existe $a^{-1} = b_0 + b_1 x + \cdots \in D[x,\sigma]$, tal que $aa^{-1} = 1$.

Neste caso $a_0b_0 = 1$. Como $a_0 \notin W$ e W é um anel de valorização total de D, temos que $a_0^{-1} \in W$. Como $a_0^{-1} = b_0$, concluímos que $a^{-1} \in \hat{B}$ e isso conclui a prova de que $\hat{B}$ é um anel de valorização total de $D[[x,\sigma]]$. Segue que $\mathfrak{M}_{\hat{B}} = J(\hat{B}) = \hat{B} \setminus U(\hat{B})$. Vamos provar que $J(\hat{B}) = \{a_0 + a_1x + \cdots;\ a_0 \in J(W),\ a_1, a_2, ... \in D\}$. Seja $c = \sum_{i=0}^{\infty} c_i x^i \in \hat{B}$. Então, $c \in U(\hat{B})$ se, e somente se, existe $c^{-1} \in \hat{B} \subseteq D[x,\sigma]$. Mas isso é equivalente à afirmar que $c_0 \neq 0$ e $c_0^{-1} \in W$. Assim, $c_0 \in U(W)$. Decorre que

$$J(\hat{B}) = \hat{B}\backslash U(\hat{B}) = \left\{\sum_{i=0}^{\infty} a_i x^i;\ a_0 \in W,\ a_1, \cdots \in D\right\} \backslash \left\{\sum_{i=0}^{\infty} a_i x^i;\ a_0 \in U(W),\ a_1, \cdots \in D\right\}$$

$$= \left\{\sum_{i=0}^{\infty} a_i x^i;\ a_0 \in W \setminus U(W),\ a_1, a_2, \cdots \in D\right\} = \left\{\sum_{i=0}^{\infty} a_i x^i;\ a_0 \in J(W),\ a_1, a_2, \cdots \in D\right\}.$$

(b) Vamos provar que $x\hat{B}x^{-1} = \hat{B}$ se, e somente se, $\sigma(W) = W$. Observe que isso é suficiente para demonstrar este item. Consideremos $u \in x\hat{B}x^{-1}$. Assim, $u = x(a_0 + a_1x + a_2x^2 + \cdots)x^{-1}$, com $a_0 \in W$ e $a_i \in D$, para $i \geq 1$. Segue que

$$u = xa_0x^{-1} + xa_1 + xa_2x + \cdots = \sigma(a_0) + \sigma(a_1)x + \sigma(a_2)x^2 + \cdots$$

Assim $u \in \{\sigma(a_0) + \sigma(a_1)x + \sigma(a_2)x^2 + \cdots;\ a_0 \in W,\ a_1, a_2, \cdots \in D\}$. Portanto,

$$x\hat{B}x^{-1} = \{\sigma(a_0) + \sigma(a_1)x + \cdots;\ a_0 \in W,\ a_1, a_2, \cdots \in D\}$$

$$= \{a_0 + a_1x + \cdots;\ a_0 \in \sigma(W),\ a_1, a_2, \cdots \in D\}.$$

A última igualdade decorre da sobrejetividade do automorfismo σ e da igualdade $\{\sigma(a_0);\ a_0 \in W\} = \sigma(W) = \{a_0;\ a_0 \in \sigma(W)\}$. Agora é fácil ver que

$$x\hat{B}x^{-1} = \{a_0 + a_1x + \cdots;\ a_0 \in \sigma(W),\ a_1, a_2, \cdots \in D\} = \hat{B} \Leftrightarrow \sigma(W) = W.$$

□

Vejamos um caso particular do teorema anterior.

Corolário 2.3.1 *Seja D um anel de divisão e $\sigma \in Aut(D)$. O conjunto $B := D[x,\sigma] = \left\{\sum_{i=0}^{\infty} a_i x^i;\ a_i \in D\right\}$ é um anel de valorização total e invariante de $D[[x,\sigma]]$ e o seu ideal* *maximal é* $J(B) = \left\{ \sum_{i=1}^{\infty} a_i x^i;\ a_i \in D \right\}$.

Demonstração

Fazendo $W = D$ no teorema anterior, vem que B é anel de valorização de $D[[x,\sigma]]$ e $J(B) = \{a_1 x + \cdots a_n x^n + \cdots;\ a_i \in D\}$, pois $J(D) = \{0\}$. Resta demonstrar a invariância de B. Seja $a = \sum_{i=0}^{\infty} a_i x^i \in B$ e $b = \sum_{i=-n}^{\infty} b_i x^i \in D[[x,\sigma]]$, $b \neq 0$. Conforme a demonstração da Proposição 2.3.1, sabemos que existe $g \in U(D[x,\sigma]) = U(B)$ tal que $b = b_{-n} x^{-n} g$ e $b^{-1} = g^{-1} x^n b_{-n}^{-1}$. Assim,

$$\begin{aligned} b^{-1}ab &= g^{-1} x^n b_{-n}^{-1} (a_0 + a_1 x + a_2 x^2 + \cdots) b_{-n} x^{-n} g \\ &= g^{-1}(x^n b_{-n}^{-1} a_0 b_{-n} x^{-n} + x^n b_{-n}^{-1} a_1 x b_{-n} x^{-n} + x^n b_{-n}^{-1} a_2 x^2 b_{-n} x^{-n} + \ldots) g \\ &= g^{-1}(\sigma^n(b_{-n}^{-1} a_0 b_{-n}) + \sigma^n(b_{-n}^{-1} a_1) x^{n+1} b_{-n} x^{-n} + \sigma^n(b_{-n}^{-1} a_2) x^{n+2} b_{-n} x^{-n} + \cdots) g \\ &= g^{-1}(\sigma^n(b_{-n}^{-1} a_0 b_{-n}) + \sigma^n(b_{-n}^{-1} a_1) \sigma^{n+1}(b_{-n}) x + \sigma^n(b_{-n}^{-1} a_2) \sigma^{n+2}(b_{-n}) x^2 + \cdots) g. \end{aligned}$$

Da última expressão concluímos que $b^{-1}ab \in B$, já que B é fechado para a multiplicação. Portanto B é um anel de valorização total e invariante de $D[[x,\sigma]]$. □

Conforme o corolário acima, a partir de um anel de divisão D qualquer (corpo inclusive), temos uma maneira de obter outro anel de divisão ($D[[x,\sigma]]$), que possui anel de valorização total e invariante. Se W é anel de valorização total de D, pelo Teorema 2.3.1, podemos associar o anel de valorização total $\hat{B}$ que não será invariante quando $\sigma(W) \neq W$.

Agora vamos trocar o anel de divisão D por um corpo $\mathbb{L}$ e vamos supor que W é um anel de valorização de $\mathbb{L}$. Obtemos assim o anel de divisão $\mathbb{L}[[x,\sigma]]$. Vamos supor ainda que o corpo $\mathbb{L}$ é uma extensão galoisiana e cíclica de grau m de um corpo $\mathbb{K}$. Nestas condições, veremos que $\mathbb{L}[[x,\sigma]]$ tem dimensão finita sobre o seu centro $Z(\mathbb{L}[[x,\sigma]]) = \mathbb{K}[[x^m]]$, para σ que gera $Aut_{\mathbb{K}}(\mathbb{L})$. Pelo Teorema 2.3.1, teremos que $\hat{B} = \left\{ \sum_{i=0}^{\infty} a_i x^i;\ a_0 \in W,\ a_1, a_2, \cdots \in \mathbb{L} \right\}$ é anel de valorização total de $\mathbb{L}[[x,\sigma]]$ e se $\sigma(W) \neq W$, $\hat{B}$ não será invariante. Desta maneira, observa-se que mesmo um anel de divisão de dimensão finita sobre seu centro, pode possuir um anel de valorização total e não invariante. Para $\mathbb{L} = \mathbb{Q}[\,i\,]$, construiremos um anel de valorização W de $\mathbb{L}$ tal que o anel de valorização total $\hat{B}$ de $\mathbb{Q}[\,i\,][[x,\sigma]]$ não é invariante.

Iniciamos esta construção particular recordando alguns resultados e definições de Teoria de Galois Elementar, que podem ser encontrados em [G] e [S].

Definição 2.3.1 *Seja* $\mathbb{K}$ *um corpo e* $f(x) \in \mathbb{K}[x]$. *O corpo de decomposição de* $f(x)$ *é definido como o menor corpo que contém* $\mathbb{K}$ *e todas as raízes de* $f(x)$ *e é denotado por* $Gal(f, \mathbb{K})$.

Todo corpo $\mathbb{K}$ pode ser mergulhado num corpo algebricamente fechado Ω, conforme ([S], Proposition 3, p. 32). Assim, o corpo de decomposição de $f(x) \in \mathbb{K}[x]$ sempre existe. Basta tomar $Gal(f, \mathbb{K})$ como sendo a interseção dos subcorpos de Ω que contém $\mathbb{K}$ e todas as raízes de $f(x)$.

Usaremos no que segue, o seguinte exemplo:

Exemplo 2.7 $Gal(x^2 + 1, \mathbb{Q}) = \mathbb{Q}[\,i\,] = \{a + bi;\ a, b \in \mathbb{Q}\}$.

Definição 2.3.2 *A extensão de corpos* $\mathbb{K} \subseteq \mathbb{L}$ *é galoisiana quando:*

(a) $[\mathbb{L} : \mathbb{K}] < \infty$ ($\mathbb{L}$ *é espaço vetorial de dimensão finita sobre* $\mathbb{K}$),

(b) *Existe* $f(x) \in \mathbb{K}[x]$ *tal que* $\mathbb{L} = Gal(f, \mathbb{K})$.

Desde que $[\mathbb{Q}[\,i\,] : \mathbb{Q}] = 2$, com base $\{1, i\}$, temos que $\mathbb{Q} \subseteq \mathbb{Q}[\,i\,]$ é extensão galoisiana.

Se $\mathbb{K} \subseteq \mathbb{L}$ é extensão de corpos, então

$$Aut_{\mathbb{K}}(\mathbb{L}) = \{\sigma : \mathbb{L} \longrightarrow \mathbb{L};\ \sigma \text{ é automorfismo } e\ \sigma(a) = a,\ \forall\ a \in \mathbb{K}\}$$

é grupo com a operação de composição de funções.

Definição 2.3.3 *Seja* $f(x) \in \mathbb{K}[x]$. *O grupo de Galois de* $f(x)$ *é* $Aut_{\mathbb{K}}(Gal(f, \mathbb{K}))$.

O lema abaixo assegura que para uma extensão galoisiana $\mathbb{K} \subseteq \mathbb{L}$, os elementos fixos por todo $\sigma \in Aut_{\mathbb{K}}(\mathbb{L})$ são exatamente os elementos de $\mathbb{K}$. A demonstração desse fato pode ser encontrada em ([G], Teorema 3, p. 172) e ([S], Theorem 1, p. 86) .

Lema 2.3.2 *Se* $\mathbb{K} \subseteq \mathbb{L}$ *é extensão galoisiana e* $\alpha \in \mathbb{L} \setminus \mathbb{K}$, *então existe* $\sigma \in Aut_{\mathbb{K}}(\mathbb{L})$ *tal que* $\sigma(\alpha) \neq \alpha$.

Definição 2.3.4 *Dizemos que a extensão galoisiana* $\mathbb{K} \subseteq \mathbb{L} = Gal(f, \mathbb{K})$ *é cíclica quando* $f(x)$ *tem grupo de Galois cíclico, isto é, existe* $\sigma \in Aut_{\mathbb{K}}(\mathbb{L})$ *tal que* $<\sigma>= Aut_{\mathbb{K}}(\mathbb{L})$.

Como pode ser visto em ([G], Teorema 3, p. 172), para a extensão galoisiana $\mathbb{K} \subseteq \mathbb{L}$ vale que $|Aut_{\mathbb{K}}(\mathbb{L})| = [\mathbb{L} : \mathbb{K}]$. Segue que

$$|Aut_{\mathbb{Q}}(Gal(x^2+1,\mathbb{Q}))| = |Aut_{\mathbb{Q}}(\mathbb{Q}[\,i\,])| = [\mathbb{Q}[\,i\,] : \mathbb{Q}] = 2.$$

É claro que a conjugação

$$\sigma : \mathbb{Q}[\,i\,] \longrightarrow \mathbb{Q}[\,i\,]$$

$$a + bi \longmapsto a - bi$$

é um elemento de $Aut_{\mathbb{Q}}(\mathbb{Q}[\,i\,])$. Logo, $[\mathbb{Q}[\,i\,] : \mathbb{Q}]$ é uma extensão galoisiana cíclica com grupo de Galois $\{Id, \sigma\} = <\sigma>$.

Voltemos à construção geral. Estamos considerando $\mathbb{K} \subseteq \mathbb{L}$ uma extensão galoisiana cíclica. Consideremos seu grupo de Galois $Aut_{\mathbb{K}}(\mathbb{L}) = <\sigma>$ e W um anel de valorização de $\mathbb{L}$. Já sabemos que

$$\mathbb{L}[[x,\sigma]] = \left\{ \sum_{i=r}^{\infty} a_i x^i;\ a_i \in \mathbb{L};\ r \in \mathbb{Z} \right\}$$

é anel de divisão e pelo Teorema 2.3.1, temos que

$$\hat{B} = \left\{ \sum_{i=0}^{\infty} a_i x^i;\ a_0 \in W,\ a_1, a_2, \cdots \in \mathbb{L} \right\}$$

é anel de valorização total de $\mathbb{L}[[x,\sigma]]$. O Teorema 2.3.1 afirma ainda que se $\sigma(W) \neq W$, então $\hat{B}$ é anel de valorização total mas não invariante de $\mathbb{L}[[x,\sigma]]$.

Agora resta a tarefa de obter um exemplo específico para a situação geral apresentada acima. Devemos obter uma extensão galoisiana $\mathbb{K} \subseteq \mathbb{L}$, com grupo de Galois $Aut_{\mathbb{K}}(\mathbb{L})$ cíclico gerado por σ, e um anel de valorização W de $\mathbb{L}$ tal que $\sigma(W) \neq W$.

Aplicando o Teorema da Extensão ao anel de valorização $5-$ádico $\mathbb{Z}_{(5)}$ de $\mathbb{Q}$, obtemos um anel de valorização W de $\mathbb{Q}[\,i\,]$ tal que $W \cap \mathbb{Q} = \mathbb{Z}_{(5)}$.

$$\begin{tikzcd}[column sep=small]
\mathbb{Q}[\,i\,] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q} \arrow[dr, dash] & W \arrow[d, dash] \\
& \mathbb{Z}_{(5)}
\end{tikzcd}$$

Como W é anel de valorização de $\mathbb{Q}[\,i\,]$, temos que $i \in W$ e como $\mathbb{Z}_{(5)} \subseteq W$, segue que $\mathbb{Z}_{(5)} + \mathbb{Z}_{(5)}i \subseteq W$. Desde que $x = \frac{3}{5} + \frac{4}{5}i$ e $x^{-1} = \frac{3}{5} - \frac{4}{5}i$ são ambos elementos de $\mathbb{Q}[\,i\,] \setminus (\mathbb{Z}_{(5)} + \mathbb{Z}_{(5)}i)$, decorre que $\mathbb{Z}_{(5)} + \mathbb{Z}_{(5)}i$ não é anel de valorização de $\mathbb{Q}[\,i\,]$. Portanto $\mathbb{Z}_{(5)} + \mathbb{Z}_{(5)}i \subsetneqq W$.

Note também que $W \subsetneqq \mathbb{Q}[\,i\,]$. De fato, se $W = \mathbb{Q}[\,i\,]$ então $\mathbb{Z}_{(5)} = W \cap \mathbb{Q} = \mathbb{Q}[\,i\,] \cap \mathbb{Q} = \mathbb{Q}$, o que é uma contradição. Desta forma $\mathbb{Z}_{(5)} + \mathbb{Z}_{(5)}i \subsetneqq W \subsetneqq \mathbb{Q}[\,i\,]$.

Para terminar, verificaremos que para a extensão galoisiana $\mathbb{Q} \subseteq \mathbb{Q}[\,i\,]$, com grupo de Galois $\{Id, \sigma\}$, $\sigma(a+bi) = a-bi$, e para o anel de valorização W de $\mathbb{Q}[\,i\,]$ vale $\sigma(W) \neq W$. Claro que basta obter $y \in W$ tal que $\sigma(y) \notin W$. Tome $x = \frac{3}{5} + \frac{4}{5}i$. Então $y = x \in W$ ou $y = \bar{x} = x^{-1} \in W$. Em qualquer um dos dois casos, supondo que $\sigma(y) \in W$, teremos $x \in W$ e $\bar{x} \in W$. Daí, $x + \bar{x} = \frac{6}{5} \in W \cap \mathbb{Q} = \mathbb{Z}_{(5)}$, que é uma contradição.

Portanto, no caso geral, tome $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}[\,i\,]$ e W a extensão do anel de valorização 5−ádico de $\mathbb{Q}$. Assim, $\mathbb{Q}[\,i\,][[x,\sigma]]$, $\sigma(a+bi) = a-bi$, é anel de divisão e

$$\hat{B} = \left\{ \sum_{i=0}^{\infty} a_i x^i;\ a_0 \in W,\ a_1, a_2, \cdots \in \mathbb{Q}[\,i\,] \right\}$$

é um anel de valorização total mas não invariante de $\mathbb{Q}[\,i\,][[x,\sigma]]$.

Conforme citamos anteriormente, se $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão galoisiana e cíclica de grau m, então $\mathbb{L}[[x,\sigma]]$ tem dimensão finita sobre seu centro, que é exatamente o conjunto $\mathbb{K}[[x^m]]$, para σ tal que $<\sigma>= Aut_{\mathbb{K}}(\mathbb{L})$. Para encerrar a seção, provaremos estes dois fatos nas afirmações seguintes.

Vamos supor $[\mathbb{L} : \mathbb{K}] = m$, isto é, $|<\sigma>| = m$.
Temos $\mathbb{L}[[x,\sigma]] = \left\{ \sum_{i=r}^{\infty} a_i x^i;\ a_i \in \mathbb{L},\ r \in \mathbb{Z} \right\}$.

Afirmação 1 $Z(\mathbb{L}[[x,\sigma]]) = \mathbb{K}[[x^m]] := \left\{\sum_{i=r}^{\infty} b_i(x^m)^i;\ b_i \in \mathbb{K},\ r \in \mathbb{Z}\right\}.$

Demonstração

Para provar que $\mathbb{K}[[x^m]] \subseteq Z(\mathbb{L}[[x,\sigma]])$, basta provar a comutatividade entre monômios de $Z(\mathbb{L}[[x,\sigma]])$ e $\mathbb{K}[[x^m]]$. Inicialmente lembramos que σ^m é a função identidade e $\sigma(u) = u$, para todo $u \in \mathbb{K}$. Sejam $ax^n \in \mathbb{L}[[x,\sigma]]$ e $b(x^m)^r \in \mathbb{K}[[x^m]]$, com $a \in \mathbb{L}$ e $b \in \mathbb{K}$. Assim, $b(x^m)^r ax^n = b\sigma^{mr}(a)(x^m)^r x^n = ba(x^m)^r x^n = ab(x^m)^r x^n = abx^n(x^m)^r = a\sigma^n(b)x^n(x^m)^r = ax^n b(x^m)^r$. Portanto, $\mathbb{K}[[x^m]] \subseteq Z(\mathbb{L}[[x,\sigma]])$. Por outro lado, seja $a = a_{-n}x^{-n} + a_{-n+1}x^{-n+1} + \cdots + a_0 + a_1x + a_2x^2 + \cdots \in Z(\mathbb{L}[[x,\sigma]])$. Então, para todo $\lambda \in \mathbb{L}$, temos que $a\lambda = \lambda a$ implica em $a_\alpha x^\alpha \lambda = \lambda a_\alpha x^\alpha$, para todo $\alpha \in \{-n, -n+1, \cdots\}$. Assim, $a_\alpha \sigma^\alpha(\lambda)x^\alpha = a_\alpha \lambda x^\alpha$. Como $a_\alpha \neq 0$, temos que $\sigma^\alpha(\lambda) = \lambda$, para todo $\lambda \in \mathbb{L}$. Logo, $\sigma^\alpha = Id$. Como $| < \sigma > | = m$, segue que $\alpha = mk$. Logo os expoentes de $a \in Z(\mathbb{L}[[x,\sigma]])$ são da forma $(x^m)^k$, com $k \in \mathbb{Z}$. Também devemos ter $ax = xa$, mas isso leva à $a_\alpha(x^m)^k x = xa_\alpha(x^m)^k = \sigma(a_\alpha)x(x^m)^k$, para todo $\alpha \in \{-n, -n+1, \cdots\}$. Assim, $\sigma(a_\alpha) = a_\alpha$. Desde que $Aut_{\mathbb{K}}(\mathbb{L}) =< \sigma >$, vemos que $\delta(a_\alpha) = a_\alpha$, para todo $\delta \in Aut_{\mathbb{K}}(\mathbb{L})$. Segue do Lema 2.3.2 que $a_\alpha \in \mathbb{K}$, para todo $\alpha \in \{-n, -n+1, \cdots\}$. Portanto, $a = a_{-n}x^{-n} + a_{-n+1}x^{-n+1} + \cdots a_0 + a_1x + a_2x^2 + \cdots \in \mathbb{K}[[x^m]]$. $\square$

Afirmação 2 $[\ \mathbb{L}[[x,\sigma]] : \mathbb{K}[[x^m]]\ ] \leq m^2$.

Demonstração

Desde que $m = |{<}\sigma{>}| = |Aut_{\mathbb{K}}(\mathbb{L})| = [\mathbb{L} : \mathbb{K}]$, existe uma $\mathbb{K}-$base de $\mathbb{L}$ (base de $\mathbb{L}$ com coeficientes em $\mathbb{K}$) com m elementos. Denotemos essa base por $\{1 = e_1, e_2, \cdots, e_m\} \subseteq \mathbb{L}$. Assim, dado $a = a_{-n}x^{-n} + \cdots a_0 + a_1x + a_2x^2 + \cdots \in \mathbb{L}[[x,\sigma]]$ temos que $a_i = \sum_{j=1}^m \lambda_{ij}e_j$ com $\lambda_{ij} \in \mathbb{K} \subseteq \mathbb{K}[[x^m]]$. Note que as potências de x que aparecem nos monômios de a podem ser escritas como combinação linear de $\{1, x, \cdots, x^{m-1}\} \subseteq \mathbb{L}[[x,\sigma]]$, tomando coeficientes em $\mathbb{K}[[x^m]]$. De fato,

$$
\begin{array}{ll}
x^0 = 1.1 & \\
x = 1.x & x^{-1} = (x^m)^{-1}x^{m-1} \\
x^2 = 1.x^2 & x^{-2} = (x^m)^{-1}x^{m-2} \\
\vdots & \vdots
\end{array}
$$

$$
\begin{array}{ll}
x^{m-1} = 1.x^{m-1} & x^{-m+1} = (x^m)^{-1}.x \\
x^m = x^m.1 & x^{-m} = (x^m)^{-1}.1 \\
x^{m+1} = x^m.x & x^{-(m+1)} = (x^m)^{-2}x^{m-1} \\
\vdots & \vdots
\end{array}
$$

Isso assegura que $a = a_{-n}x^{-n} + \cdots a_0 + a_1x + a_2x^2 + \cdots \in \mathbb{L}[[x,\sigma]]$ pode ser escrito como combinação linear de $\{1, x, \cdots, x^{m-1}, e_2, e_2x, \cdots, e_2x^{m-1}, \cdots, e_m, e_mx, \cdots, e_{m-1}x^{m-1}\}$ que tem exatamente m^2 elementos. $\square$

2.4 Inexistência do Teorema da Extensão

Conforme citamos no início deste capítulo, um dos resultados mais relevantes que vale para corpos não pode ser estendido aos anéis de divisão. Esse resultado é o Teorema da Extensão, que afirma que se $\mathbb{L} \subseteq \mathbb{K}$ é extensão de corpos e R é um anel de valorização de $\mathbb{L}$, então existe um anel de valorização V de $\mathbb{K}$, tal que $V \cap \mathbb{L} = R$. Nesta seção apresentaremos um contra-exemplo para este fato, no caso de $\mathbb{K}$ ser um anel de divisão. Mostraremos que para um número primo $p \neq 2$, o anel de valorização p-ádico $\mathbb{Z}_{(p)}$ de $\mathbb{Q}$ não possui extensão no anel dos quatérnios racionais $\mathbb{H}$, isto é, não existe anel de valorização total B de $\mathbb{H}$ tal que $B \cap \mathbb{Q} = \mathbb{Z}_{(p)}$. Note que esse contra-exemplo é o melhor possível, pois verifica que mesmo no caso de um anel de valorização total e invariante do corpo, que é o centro de uma álgebra de divisão de dimensão finita sobre seu centro, não é possível obter sequer um anel de valorização total da álgebra, que estenda o anel de valorização do centro.

Existem várias citações a esse contra-exemplo em artigos, por exemplo [Br], [W_1] e [C].

No entanto, nenhum dos artigos e livros consultados traz uma prova completa desse fato. Portanto, faremos aqui uma demonstração completa baseada em argumentos elementares.

Vamos iniciar com alguns resultados preliminares.

Lema 2.4.1 *Seja $p \neq 2$ um número primo. Se $a \in \mathbb{Q}$ e $a \notin \mathbb{Z}_{(p)}$, então $2^n a \notin \mathbb{Z}_{(p)}$, para todo $n \in \mathbb{N}$.*

Demonstração

Seja $a = \frac{u}{v}$ uma fração irredutível tal que $\frac{u}{v} \notin \mathbb{Z}_{(p)}$. Assim, $p \mid v$ e $p \nmid u$. Agrupando as potências de 2 e de p em v, escrevemos $v = 2^r p^s x$ onde $2 \nmid x$ e $p \nmid x$, com $s \in \mathbb{N}^*$ e $r \in \mathbb{N}$. Assim, $2^n a = \frac{2^n u}{v} = \frac{2^n u}{2^r p^s x}$. Desde que a fração $\frac{u}{v} = \frac{u}{2^r p^s x}$ é irredutível, o único possível fator primo comum ao numerador e ao denominador de $\frac{2^n u}{2^r p^s x}$ é 2. Desta forma, após a devida simplificação para tornar $2^n a = \frac{2^n u}{2^r p^s x}$ um fração irredutível, ainda teremos o fator primo $p \neq 2$ no denominador de $2^n a$. Portanto, $2^n a \notin \mathbb{Z}_{(p)}$. $\square$

Proposição 2.4.1 *Seja $p \neq 2$ um número primo. Então $V_{(p)} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)} i + \mathbb{Z}_{(p)} j + \mathbb{Z}_{(p)} k$ é um subanel maximal de $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$.*

Demonstração

Seja A um subanel de $\mathbb{H}$ tal que $V_{(p)} \subsetneqq A \subseteq \mathbb{H}$. Assim, existe $u = a + bi + cj + dk \in A \backslash V_{(p)}$. Segue que um dos elementos do conjunto $\{a, b, c, d\}$ não pertence à $\mathbb{Z}_{(p)}$. Vamos provar que $4a, 4b, 4c, 4d \in A$. Como $u \in A$ e $i, j, k \in V_{(p)} \subseteq A$, temos

$$\begin{aligned}
v_1 = \quad & ui + iu = & ai - b - ck + dj + ai - b + ck - dj = \quad & 2ai - 2b \in A; \\
v_2 = \quad & uj + ju = & aj + bk - c - di + aj - bk - c + di = \quad & 2aj - 2c \in A; \\
v_3 = \quad & uk + ku = & ak - bj + ci - d + ak + bj - ci - d = \quad & 2ak - 2d \in A.
\end{aligned}$$

E então

$$\begin{aligned}
-jv_1 + v_1 j = & \quad -j(2ai - 2b) + (2ai - 2b)j = & 2ak + 2bj + 2ak - 2bj = & \quad 4ak \in A; \\
jv_1 + v_1 j = & \quad j(2ai - 2b) + (2ai - 2b)j = & -2ak - 2bj + 2ak - 2bj = & \quad -4bj \in A; \\
kv_2 + v_2 k = & \quad k(2aj - 2c) + (2aj - 2c)k = & -2ai - 2ck + 2ai - 2ck = & \quad -4ck \in A; \\
iv_3 + v_3 i = & \quad i(2ak - 2d) + (2ak - 2d)i = & -2aj - 2di + 2aj - 2di = & \quad -4aj \in A.
\end{aligned}$$

Logo, $4a, 4b, 4c, 4d \in A$. Sabemos que um dos elementos do conjunto $\{a, b, c, d\}$ não pertence à $\mathbb{Z}_{(p)}$. Pelo Lema 2.4.1, um dos elementos do conjunto $\{4a, 4b, 4c, 4d\}$ não pertence à $\mathbb{Z}_{(p)}$. Mas, $4a, 4b, 4c, 4d \in A$. Logo, $\mathbb{Z}_{(p)} \subsetneqq A \cap \mathbb{Q} \subseteq \mathbb{Q}$ e como $\mathbb{Z}_{(p)}$ é subanel maximal de $\mathbb{Q}$ (Proposição 1.1.8) temos que $A \cap \mathbb{Q} = \mathbb{Q}$. Decorre que que $\mathbb{Q} \subseteq A$. Agora, como

$i, j, k \in A$, temos que $\mathbb{H} \subseteq A$, isto é, $A = \mathbb{H}$. $\square$

Ainda como preparação para obtermos o contra-exemplo que citamos no início desta seção, teremos que demonstrar que para cada número primo $p \neq 2$, o anel

$$V_{(p)} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)}i + \mathbb{Z}_{(p)}j + \mathbb{Z}_{(p)}k$$

não é total em $\mathbb{H}$. Mostraremos isso para qualquer primo inclusive 2.

Precisamos lembrar alguns resultados básicos de Teoria dos Números. O primeiro desses resultados é o Teorema de Lagrange, cuja demonstração pode ser encontrada em ([Ha], p. 375).

Teorema 2.4.1 (Teorema de Lagrange) *Qualquer número inteiro não negativo pode ser escrito como soma de quadrados de quatro números inteiros.*

Convém observar que o Teorema de Lagrange não garante unicidade da representação, por exemplo, $9 = 3^2 + 0^2 + 0^2 + 0^2$ e $9 = 2^2 + 2^2 + 1^2 + 0^2$.

O Teorema de Lagrange produz algumas conseqüências naturais descritas nos corolários seguintes.

Corolário 2.4.1 *Seja p um número primo e $p = a^2 + b^2 + c^2 + d^2$, com $a, b, c, d \in \mathbb{Z}$. Então pelo menos duas das parcelas de $a^2 + b^2 + c^2 + d^2$ não são nulas.*

Demonstração

Se as quatro parcelas forem nulas teremos $p = 0$, o que é impossível, pois p é primo. Se três parcelas forem nulas, digamos $a = b = c = 0$, temos que $p = d^2$. Caso $d = 1$, segue que $p = 1$ não é primo. Se $d \neq 1$, então p é redutível, contradizendo o fato de p ser primo. $\square$

Corolário 2.4.2 *Seja p um número primo e $p = {a_1}^2 + {b_1}^2 + {c_1}^2 + {d_1}^2$, com $a_1, b_1, c_1, d_1 \in \mathbb{Z}$. Então existem $a, b, c, d \in \mathbb{Z}$ tais que $p^2 = a^2 + b^2 + c^2 + d^2$ e p não divide um dos elementos do conjunto $\{a, b, c, d\}$.*

Demonstração

Se $p = 2$, temos $4 = 1^2 + 1^2 + 1^2 + 1^2$. Assim, podemos supor que p é um número primo ímpar. Temos que

$$p^2 = ({a_1}^2 + {b_1}^2 + {c_1}^2 + {d_1}^2)^2 = ({a_1}^2 - {b_1}^2 - {c_1}^2 - {d_1}^2)^2 + (2a_1b_1)^2 + (2a_1c_1)^2 + (2a_1d_1)^2.$$

Pelo corolário anterior, podemos supor $a_1 \neq 0$ e $b_1 \neq 0$. Consideremos $a = ({a_1}^2 - {b_1}^2 - {c_1}^2 - {d_1}^2)$, $b = (2a_1b_1)$, $c = (2a_1c_1)$ e $d = (2a_1d_1)$. Afirmamos que pelo menos duas dessas parcelas não são nulas. De fato, note que $b \neq 0$ e podemos ter

$$(1) \qquad c_1 \neq 0 \text{ ou } d_1 \neq 0 \qquad \text{ou} \qquad (2) \qquad c_1 = d_1 = 0.$$

No primeiro caso, $c \neq 0$ ou $d \neq 0$, respectivamente. No segundo caso, temos $p^2 = ({a_1}^2 - {b_1}^2)^2 + (2a_1b_1)^2$. Observe que caso $({a_1}^2 - {b_1}^2)^2 = 0$, temos que $p = 2a_1b_1$, o que contradiz o fato de p ser ímpar. Assim, $({a_1}^2 - {b_1}^2)^2 \neq 0$ e $(2a_1b_1)^2 \neq 0$, o que prova a nossa afirmação. Suponha agora que $p \mid a$, $p \mid b$, $p \mid c$ e $p \mid d$, com $p\alpha_1 = a$, $p\alpha_2 = b$, $p\alpha_3 = c$ e $p\alpha_4 = d$. Então $p^2 = p^2({\alpha_1}^2 + {\alpha_2}^2 + {\alpha_3}^2 + {\alpha_4}^2)$ que leva a $1 = {\alpha_1}^2 + {\alpha_2}^2 + {\alpha_3}^2 + {\alpha_4}^2$. Mas isso não é possível pois pelo menos dois elementos no conjunto $\{\alpha_1, \ \alpha_2, \ \alpha_3, \ \alpha_4\}$ são não nulos, já que pelo menos dois elementos no conjunto $\{a, \ b, \ c, \ d\}$ são não nulos. $\square$

Teorema 2.4.2 *Seja p um número primo. O anel $V_{(p)} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)}i + \mathbb{Z}_{(p)}j + \mathbb{Z}_{(p)}k$ não é total em $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$.*

Demonstração

Pelo corolário anterior podemos escrever $p^2 = a^2 + b^2 + c^2 + d^2$, onde p não divide um dos elementos do conjunto $\{a, \ b, \ c, \ d\}$. Escolha $x = p^{-1}(a + bi + cj + dk) \in \mathbb{H}^*$. Note que $x \notin V_{(p)}$, pois p não divide um dos elementos de $\{a, b, c, d\}$ implica que um dos elementos do conjunto $\left\{\frac{a}{p}, \frac{b}{p}, \frac{c}{p}, \frac{d}{p}\right\}$ não pertende à $\mathbb{Z}_{(p)}$. Agora vamos mostrar que $x^{-1} \notin V_{(p)}$. É claro que

$$N(x) = x\overline{x} = p^{-2}(a + bi + cj + dk)(a - bi - cj - dk) = p^{-2}(a^2 + b^2 + c^2 + d^2) = 1$$

e $x^{-1} = \frac{\overline{x}}{N(x)} = p^{-1}(a - bi - cj - dk)$. Assim, $x^{-1} \notin V_{(p)}$ pelo mesmo argumento que $x \notin V_{(p)}$. $\square$

Finalmente, vamos demonstrar a inexistência de um Teorema da Extensão para anéis de divisão, conforme citamos anteriormente.

Teorema 2.4.3 *Seja $\mathbb{H}$ o anel de divisão dos quatérnios racionais com centro $\mathbb{Q}$ e $\mathbb{Z}_{(p)}$ o anel de valorização p-ádico de $\mathbb{Q}$, para um número primo $p \neq 2$. Não existe um anel de valorização total B de $\mathbb{H}$, tal que $B \cap \mathbb{Q} = \mathbb{Z}_{(p)}$.*

Demonstração

Vamos supor que exista um anel de valorização total B de $\mathbb{H}$. De $B \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ vemos que $\mathbb{Z}_{(p)} \subseteq B$. Além disso, por ser total, B deve conter i, j, k, já que $i^{-1} = -i$, $j^{-1} = -j$ e $k^{-1} = -k$. Segue que $V_{(p)} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)}i + \mathbb{Z}_{(p)}j + \mathbb{Z}_{(p)}k \subseteq B$. Pela Proposição 2.4.1, sabemos que $V_{(p)}$ é subanel maximal de $\mathbb{H}$. Logo, devemos ter $B = \mathbb{H}$ ou $B = V_{(p)}$. No primeiro caso, temos que $\mathbb{Z}_{(p)} = B \cap \mathbb{Q} = \mathbb{H} \cap \mathbb{Q} = \mathbb{Q}$, o que é impossível. Só resta $B = V_{(p)}$, o que implica que $V_{(p)}$ é total, contradizendo o Teorema 2.4.2. $\square$

O fato de não ser válido um Teorema da Extensão para anéis de divisão faz pensar que a definição de anel de valorização proposta por Schilling não é a melhor generalização da definição de anel de valorização em corpos. Fica claro que uma nova definição deverá abranger um conjunto mais amplo do que os anéis de valorização totais e invariantes.

Apesar da inexistência de um Teorema da Extensão para anéis de divisão, resultados interessantes sobre o assunto foram obtidos por Brungs e Gräter em 1989.

Como informação, listamos abaixo alguns desses resultados.

Seja D um anel de divisão com centro $\mathbb{F}$ tal que a dimensão de D sobre $\mathbb{F}$ é finita ($[D : \mathbb{F}] < \infty$). Então para um anel de valorização V de $\mathbb{F}$ vale:

- O número de extensões totais (aquelas cuja extensão é um anel de valorização total de D) de V em D é menor ou igual à $\sqrt{[D : \mathbb{F}]}$ ([BrG$_1$], Section 2, Theorem 1).

- Se existe uma extensão total e invariante de V em D, então ela é a única extensão total ([BrG$_1$], Section 1, Corollary).

- Se $V \neq \mathbb{F}$ então todas as extensões totais de V em D são conjugadas, isto é, se V_1 e V_2 estendem V em D, existe $q \in D^*$ tal que $V_1 = qV_2q^{-1}$ ([BrG$_1$], Section 2, Theorem 2).

- Existe uma extensão total de V em D se, e somente se, o conjunto $\{x \in D;\ x$ é integral sobre $V\}$ é subanel de D ([BrG$_1$], Section 3, Theorem 4).

2.5 Funções Valorização em Anéis de Divisão

Veremos nesta seção que é possível definir função valorização em anéis de divisão de maneira idêntica à que definimos em corpos, e que continua válido o teorema que associa biunivocamente valorizações equivalentes a um anel de valorização, com a diferença que agora esse anel de valorização, além de ser total, será também invariante.

Como será facilmente observado, as demonstrações serão análogas àquelas vistas na Seção 2 do Capítulo 1. Faremos aquelas em que a falta de comutatividade causa problemas. Também faremos as construções ou demonstrações que envolvem a invariância do anel de valorização total e invariante associado a uma classe de valorizações.

Seja $(\Gamma, +)$ grupo abeliano totalmente ordenado pela relação $\leq$. Denotemos a união do símbolo ∞ ao grupo Γ por $\Gamma \cup \{\infty\}$ e consideremos as convenções:

- $g + \infty = \infty + g = \infty + \infty = \infty,\ \forall\ g \in \Gamma$;
- $g < \infty,\ \forall\ g \in \Gamma$;
- $g_1 \leq g_2 \Rightarrow g_1 + h \leq g_2 + h,\ \forall\ g_1, g_2, h \in \Gamma$.

Definição 2.5.1 *Seja D um anel de divisão. Uma função $v : D \longrightarrow \Gamma \cup \{\infty\}$ é uma valorização, se:*

(a) $v(x) = \infty \Leftrightarrow x = 0$;

(b) $v(xy) = v(x) + v(y),\ \forall\ x, y \in D$;

(c) $v(x + y) \geq min\{v(x), v(y)\},\ \forall\ x, y \in D$.

Sempre se pode considerar v sobrejetora. De fato, os itens (a) e (b) dizem que v é um homomorfismo entre os grupos $(D^*, .)$ e $(\Gamma, +)$. Então, se necessário, podemos trocar Γ pelo grupo $v(D^*)$. O grupo $v(D^*)$ é chamado o *grupo de valores* de v.

A valorização trivial e as valorizações $p-$ádicas que definimos na segunda seção do primeiro capítulo servem também como exemplos de valorização em anéis de divisão. No final desta seção citaremos exemplos de valorizações em anéis de divisão que não são corpos.

A demonstração do lema seguinte é idêntica à demonstração do Lema 1.2.1.

Lema 2.5.1 *Seja v uma valorização de D. Então:*

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

(b) $v(-x) = v(x)$, $\forall\ x \in D$;

(c) $v(x^{-1}) = -v(x)$, $\forall\ x \in D^*$.

O próximo teorema associa a uma função valorização um anel de valorização total e invariante.

Teorema 2.5.1 *Seja v uma valorização de D. Então:*

(a) $B_v = \{x \in D;\ v(x) \geq 0\}$ *é um anel de valorização total e invariante de D;*

(b) $J_v = \{x \in D;\ v(x) > 0\}$ *é o único ideal bilateral maximal de B_v;*

(c) $J(B_v) = J_v = \{x \in B_v;\ x = 0$ *ou* $x^{-1} \notin B_v\}$.

Demonstração

(a) A prova da totalidade é análoga à vista para corpos no Teorema 1.2.1. Seja $x \in D^*$ e $b \in B_v$. Temos:

$$v(xbx^{-1}) = v(x) + v(b) + v(x^{-1}) = v(b) \geq 0,$$

o que implica que B_v é invariante.

(b) Obviamente, J_v é fechado por diferenças. Sejam $x \in J_v$ e $y \in B_v$. Então $v(x) > 0$ e $v(y) \geq 0$. Assim, $v(xy) = v(x) + v(y) > 0$ implica em $xy \in J_v$. Logo J_v é ideal à direita de B_v. Da mesma maneira, prova-se que J_v também é um ideal à esquerda de J_v. Do fato de B_v ser anel de valorização total de D decorre que seu único ideal bilateral maximal é $B_v \backslash U(B_v)$. Provemos que $J_v = B_v \backslash U(B_v)$. Lembremos que $v(1) = 0$ implica que $1 \notin J_v$. Isso nos diz que J_v é ideal próprio de B_v. Logo $J_v \subseteq B_v \backslash U(B_v)$, pois J_v deve estar contido num ideal maximal e o único maximal é $B_v \backslash U(B_v)$. Por outro lado, seja $x \in B_v \backslash U(B_v)$. Então $x \in B_v$ e $x^{-1} \notin B_v$. Assim, $v(x) \geq 0$ e $v(x^{-1}) < 0$ implicam em $v(x) > 0$. Logo, $x \in J_v$. Portanto, $J_v = B_v \backslash U(B_v)$.

(c) Sabemos que $J(B_v)$ é o único ideal bilateral maximal de B_v. Então, segue que $J(B_v) = J_v$ (pois J_v também é o único ideal bilateral maximal). Resta provar que $J_v = \{x \in B_v,\ x = 0 \text{ ou } x^{-1} \notin B_v\}$. Seja $x \in J_v$. Para $x \neq 0$, $v(x^{-1}) = -v(x) < 0$ implica que $x^{-1} \notin B_v$. Por outro lado, seja $x \in B_v$, $x \neq 0$ e $x^{-1} \notin B_v$. Assim, $-v(x) = v(x^{-1}) < 0$ implica que $x \in J_v$. □

A cada valorização v do anel de divisão D associamos o anel de valorização total e invariante B_v de D. Para termos uma correspondência bem definida, trabalheremos com classes de valorizações. Para isso usamos a definição abaixo.

Definição 2.5.2 *Sejam u e v valorizações de D. Dizemos que $u \sim v$ (u é equivalente a v) quando $B_u = B_v$.*

É fácil ver que $\sim$ é uma relação de equivalência.

Denotamos por $[v]$ a classe de equivalência da valorização v. Assim, temos uma aplicação bem definida

$$\begin{array}{rcl} \psi : \{[v];\ v \text{ valorização de } D\} & \longrightarrow & \{B;\ B \text{ anel de valorização total e invariante de } D\} \\ [v] & \longmapsto & B_v \end{array}$$

Mostraremos que ψ é bijetora, isto é, existe uma correspondência $1-1$ entre anéis de valorização totais e invariantes do anel de divisão D e classes de valorizações de D. Para isso construiremos a inversa ϕ de ψ.

Seja B um anel de valorização total e invariante do anel de divisão D. A construção do grupo Γ_B, que faremos a seguir, é bastante semelhante à construção do grupo G, vista na Seção 2 do Capítulo 1. No entanto, faremos a construção completa visando destacar o fato que a possível falta de comutatividade não prejudica os cálculos devido à invariância de B.

Considere o conjunto

$$\Gamma_B = \{xB;\ x \in D^*\}$$

onde a igualdade é definida por $xB = yB \Leftrightarrow xy^{-1} \in U(B)$. Logo, $xB = yB \Leftrightarrow yB = xB$.

Como B é invariante, $xB = Bx$, para todo $x \in D^*$. Definindo

$$\begin{array}{rcl} + : \Gamma_B \times \Gamma_B & \longrightarrow & \Gamma_B \\ (xB, yB) & \longmapsto & (xy)B \end{array}$$

e supondo $x_1B = x_2B$ e $y_1B = y_2B$, temos $x_1B + y_1B = x_1y_1B = x_1y_2B = x_1By_2 = x_2By_2 = x_2y_2B = x_2B + y_2B$, e assim a operação $+$ está bem definida em Γ_B. Observe que B invariante implica que a operação acima é exatamente o produto $xByB$. Também, $(\Gamma_B, +)$ é grupo com elemento neutro $B = 1B$ e o simétrico de $xB \in \Gamma_B$ é $x^{-1}B$. Decorre de ([D$_2$], §2, Proposition 4), que Γ_B é abeliano. Além disso, $U(B)$ é subgrupo normal de D^* e $\Gamma_B \simeq \frac{D^*}{U(B)}$. De fato, se $\alpha \in D^*$, então $\alpha U(B)\alpha^{-1} \subseteq \alpha B\alpha^{-1} = B$ e assim, $\alpha \in U(B)$. Ainda mais, a aplicação $\varphi : \frac{D^*}{U(B)} \longrightarrow \Gamma_B$, dada por $\varphi(xU(B)) = xB$ é um isomorfismo de grupos.

Dados $xB, yB \in \Gamma_B$, definimos a relação de ordem

$$xB \leq yB \Leftrightarrow yB \subseteq xB.$$

Vamos mostrar que essa relação é de ordem total em Γ_B. Temos que $y^{-1}x \in D^*$. Daí $y^{-1}x \in B$ ou $x^{-1}y \in B$. Se $y^{-1}x \in B$ então $y^{-1}xB \subseteq B$ implica em $xB \subseteq yB$. Analogamente, $x^{-1}y \in B$ implica em $yB \subseteq xB$.

Definimos agora a aplicação

$$\begin{array}{rcl} v : D & \longrightarrow & \Gamma_B \cup \{\infty\} \\ 0 & \longmapsto & \infty \\ x & \longmapsto & xB,\ x \neq 0 \end{array}$$

Observe que $v|_{D^*} : D^* \longrightarrow \Gamma_B$ é um homomorfismo sobrejetor de grupos e $Ker(v) = \{x \in D^*;\ xB = 1B\} = U(B)$ e assim temos novamente $\frac{D^*}{U(B)} \simeq \Gamma_B$.

De forma análoga à prova da Proposição 1.2.1, demonstra-se a próxima proposição.

Proposição 2.5.1 *Seja B um anel de valorização total e invariante do anel de divisão D. Com a notação estabelecida acima, temos que:*

(a) v é uma valorização de D;

(b) $B_v = B$;

Definimos agora

$$\begin{aligned} \phi : \{B;\ B \text{ anel de valorização total e invariante de } D\} &\longrightarrow \{[v];\ v \text{ valorização de } D\} \\ B &\longmapsto [v] \end{aligned}$$

onde v é a valorização associada à B.

Mostraremos a seguir que ϕ é a inversa da aplicação

$$\begin{aligned} \psi : \{[v];\ v \text{ valorização de } D\} &\longrightarrow \{B;\ B \text{ anel de valorização total e invariante de } D\} \\ [v] &\longmapsto B_v \end{aligned}$$

Teorema 2.5.2 *Existe uma correspondência biunívoca entre anéis de valorização totais e invariantes do anel de divisão D e classes de valorizações de D.*

Demonstração

Pelo visto acima, basta provar que $\psi(\phi(B)) = B$ e $\phi(\psi[v]) = [v]$.

Claro que $\psi(\phi(B)) = \psi([v])$, com $B_v = B$ pelo item (b) da Proposição 2.5.1. Mas $\psi([v]) = B_v$. Portanto $\psi(\phi(B)) = B$. Por outro lado, $\phi(\psi[v]) = \phi(B_v)$. Mas $\phi(B_v) = [w]$, com $B_w = B_v$, novamente aplicamos o item (b) da Proposição 2.5.1. Por definição, $B_v = B_w$ implica que $v \sim w$, isto é, $[v] = [w]$. Portanto, $\phi(\psi[v]) = \phi(B_v) = [w] = [v]$. $\square$

Exemplo 2.8 Seja A um subanel do anel de divisão D. Se A também é um anel de divisão então é fácil ver que a restrição à A de uma valorização em D é uma valorização em A.

Exemplo 2.9 Vamos explicitar neste exemplo a valorização dos quatérnios racionais $\mathbb{H}$ que corresponde ao anel de valorização total e invariante $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$, onde $\alpha = \frac{1}{2}(1 + i + j + k)$. Definimos

$$\begin{aligned} w : \mathbb{H} &\longrightarrow \mathbb{Q} \cup \{\infty\} \\ 0 &\longmapsto \infty \\ a &\longmapsto \tfrac{1}{2} v_2(N(a)) \end{aligned}$$

onde v_2 é a 2-ádica valorização de $\mathbb{Q}$ e $N(a)$ é a norma de $a \in \mathbb{H}$. Note que $w|_{\mathbb{Q}} = v_2$. De fato, se $a \in \mathbb{Q}^*$, então

$$w(a) = \tfrac{1}{2}v_2(N(a)) = \tfrac{1}{2}v_2(a^2) = \tfrac{1}{2}(v_2(a) + v_2(a)) = v_2(a).$$

Assim, $B_w \cap \mathbb{Q} = \{x \in \mathbb{Q};\ v_2(x) \geq 0\} = \mathbb{Z}_{(2)}$. Decorre de ([BrG$_1$], Section 1, Corollary), que $\tilde{V}_{(2)}$ é o único anel de valorização total e invariante que estende $\mathbb{Z}_{(2)}$. Portanto $B_w = \tilde{V}_{(2)}$.

Para ver que w é de fato um valorização, observamos que as condições

- $w(a) = \infty \Leftrightarrow a = 0$,

- $w(ab) = w(a) + w(b)$,

são claramente satisfeitas. Para mostrar que $w(a+b) \geq min\{w(a), w(b)\}$, há muitas contas para fazer. Porém, isso está provado indiretamente em [W$_2$].

Exemplo 2.10 Seja D um anel de divisão. Temos que $D[x]$ é um domínio não necessariamente comutativo. É trabalhoso, porém não difícil, mostrar que $D[x]$ é um domínio de Ore à direita e à esquerda. Conseqüentemente, $D[x]$ admite anel quociente clássico que será um anel de divisão denotado por $D(x)$. Seja $p(x) \in D(x)$. Escrevendo $p(x) = x^k \hat{p}(x)$, com $k \in \mathbb{Z}$ e

$$\hat{p}(x) = \frac{a_0 + a_1x + \ldots + a_nx^n}{b_0 + b_1x + \ldots + b_mx^m}, \quad a_0, b_0 \neq 0,$$

definimos a aplicação

$$\begin{array}{rcl} w : D(x) & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ 0 & \longmapsto & \infty \\ p(x) & \longmapsto & k \end{array}$$

A aplicação w define uma valorização de $D(x)$ em $\mathbb{Z} \cup \{\infty\}$. De fato,

- $w(p(x)) = \infty \Leftrightarrow p(x) = 0$;

- $w(p(x)q(x)) = w(x^k\hat{p}(x)x^r\hat{q}(x)) = w(x^{k+r}\hat{p}(x)\hat{q}(x)) = k + r = w(p(x)) + w(q(x))$;

- $w(p(x) + q(x)) = w(x^k\hat{p}(x) + x^r\hat{q}(x)) = w(x^{min\{k,r\}}\hat{f}(x)) \geq min\{k, r\} = min\{w(p(x)), w(q(x))\}$.

Observação 2.15 Não abordaremos os places para o caso específico de um anel de divisão. Esse assunto aparecerá como caso particular, no próximo capítulo, no estudo de places em anéis artinianos simples. O motivo para isso é que antes da definição de place em anéis artinianos simples, apresentada por Dubrovin em 1982, nenhuma definição de place em anéis de divisão produziu resultados que estendessem os obtidos em corpos.

Capítulo 3

Valorização em Anéis Artinianos Simples

A inexistência do Teorema da Extensão para anéis de valorização totais em anéis de divisão, demonstrada na Seção 3 do Capítulo 2, sugere que a definição proposta por Schilling pode não ser a melhor extensão do conceito de anel de valorização de um corpo. Contudo, como vimos na Seção 1 do Capítulo 2, alguns resultados relevantes são estendidos. Logo, é razoável esperar que uma definição de anel de valorização em anéis de divisão produza uma classe de subanéis que contenha os anéis de valorização totais.

Uma definição consistente para anéis de valorização não comutativos foi apresentada em 1984 por Dubrovin em [D_1]. Na introdução deste artigo, e também no prefácio do livro [MMU], vemos que o estudo para o caso não comutativo de Anéis de Dedekind, Anéis Semihereditários, Anéis de Bezout e Anéis de Cadeia, requeria o análogo do conceito de anéis de valorização de corpos não apenas para anéis de divisão, mas para anéis artinianos simples. É exatamente para essa categoria de anéis que Dubrovin definiu os *anéis de valorização não comutativos* ([D_1], §1, Definition 6), que atualmente são denominados *anéis de valorização de Dubrovin.*

Neste capítulo veremos que a definição de anéis de valorização de Dubrovin generaliza as definições anteriores e é bem sucedida na generalização de diversos resultados. Iniciaremos com o estudo dos anéis artinianos simples e provaremos as principais propriedades dos anéis de valorização de Dubrovin. Na Seção 3 vamos definir place para anéis artinianos simples e relacionar essa definição com os anéis de valorização de Dubrovin. Finalmente na quarta seção estudaremos as funções valorização sobre anéis artinianos simples.

3.1 Anéis Artinianos Simples

Nesta primeira seção veremos resultados sobre anéis artinianos simples que utilizaremos no desenvolver deste capítulo. Entre esses resultados destaca-se o Teorema de Wedderburn-Artin. Veremos também a equivalência entre as definições de *álgebras centrais simples de dimensão finita* e *anéis artinianos simples de dimensão finita sobre o centro.* Fizemos essa observação em função de que muitos trabalhos citam uma ou outra definição para tratar da mesma estrutura.

Lembramos a seguir a definição de anel simples e listamos alguns fatos à respeito deles.

Definição 3.1.1 *Seja $A \neq \{0\}$ um anel com unidade. Dizemos que A é um anel simples quando seus únicos ideais bilaterais são $\{0\}$ e A.*

Observação 3.1 Todo anel de divisão (corpo inclusive) é um anel simples.

Observação 3.2 Seja A um anel com unidade e comutativo. Para que A seja simples, é necessário e suficiente que A seja corpo. De fato, a suficiência é um caso particular da observação anterior e para provar a necessidade, consideremos $x \in A^*$. Como A é simples, segue que $xA = A$ e daí $1 = xa$ para algum $a \in A$. Portanto A é corpo.

Observação 3.3 Seja A um anel com unidade. Não é difícil mostrar que para todo elemento não nulo $a \in A$, o conjunto $AaA := \left\{ \sum_{i=1}^{n} r_i a s_i;\ r_i, s_i \in A,\ n \in \mathbb{N} \right\}$ é um ideal bilateral de A. Assim, se A é simples, $AaA = A$. Também verifica-se facilmente que essa condição é suficiente para que A seja simples.

Observação 3.4 Sabemos que $J(A)$ é um ideal bilateral próprio do anel com unidade A. Assim, se A é anel simples, $J(A) = \{0\}$.

Observação 3.5 Se o anel com unidade A é simples, então o seu centro $Z(A)$ é corpo. Para verificar isso observamos inicialmente que se $a \in Z(A)$ e existe $a^{-1} \in A$, então $a^{-1} \in Z(A)$. De fato, se $x \in A$, temos que $a^{-1}x = a^{-1}(xa)a^{-1} = xa^{-1}$. Agora, seja a um elemento não nulo em $Z(A)$. Então $aA = Aa = A$, pois A é simples e $a \in Z(A)$. Logo, existe $b \in A$ tal que $1 = ab = ba$. Portanto, $Z(A)$ é corpo.

Recordamos agora a condição das cadeias descendentes (ascendentes), com a qual vamos relembrar a definição de anel artiniano (noetheriano).

Definição 3.1.2 *Seja E um conjunto parcialmente ordenado.*

(a) *O conjunto E satisfaz a condição das cadeias descendentes (CCD) quando toda cadeia em E da forma $x_1 \geq x_2 \geq \cdots$ é estacionária, isto é, existe $n_0 \in \mathbb{N}$ tal que $n \geq n_0$ implica em $x_n = x_{n_0}$;*

(b) *O conjunto E satisfaz a condição das cadeias ascendentes (CCA) quando toda cadeia em E da forma $x_1 \leq x_2 \leq \cdots$ é estacionária, isto é, existe $n_0 \in \mathbb{N}$ tal que $n \geq n_0$ implica em $x_n = x_{n_0}$.*

Definição 3.1.3 *Seja A um anel com unidade.*

(a) *O anel A é artiniano à esquerda (à direita) quando o conjunto dos ideais à esquerda (à direita) de A, ordenado por inclusão, satisfaz a CCD;*

(b) *o anel A é noetheriano à esquerda (à direita) quando o conjunto dos ideais à esquerda (à direita) de A, ordenado por inclusão, satisfaz a CCA.*

Finalmente, o anel A é artiniano (noetheriano) quando é artiniano (noetheriano) à esquerda e à direita. Um anel artiniano (noetheriano) à esquerda não é, necessariamente, artiniano (noetheriano) à direita. Exemplos disso podem ser vistos em ([L], p. 22).

Utilizaremos posteriormente o fato que um anel com unidade A, artiniano à direita (à esquerda), é também um anel noetheriano à direita (à esquerda), como pode ser visto em ([Go], pp. 138,145).

Veremos agora a equivalência entre a definição de álgebra central simples de dimensão finita e anel artiniano simples de dimensão finita sobre o centro.

Definição 3.1.4 *Seja R um anel comutativo. Dizemos que A é uma $R-$álgebra (ou simplesmente uma álgebra) se $(A, +, .)$ é um anel, $(A, +, *)$ é um $R-$módulo e $(r * x).y = r * (x.y) = (x * r).y$, para todos $x, y \in A$ e para todo $r \in R$. Dizemos ainda que A é uma álgebra central, quando R é o centro do anel A e A é uma álgebra simples quando o anel A é um anel simples.*

É claro que se B é subanel comutativo do anel A então A é $B-$álgebra. Em particular, A é $Z(A)-$álgebra.

Vimos que o centro de um anel simples é um corpo. Assim, para um anel simples Q ou para uma $R-$álgebra simples Q, podemos falar na dimensão de Q visto como $Z(Q)-$espaço vetorial. Denotamos isso por $[Q : Z(Q)]$.

Proposição 3.1.1 *Seja Q um anel com unidade. São equivalentes:*

(i) Q é uma álgebra central simples de dimensão finita;

(ii) Q é um anel artiniano simples de dimensão finita sobre seu centro.

Demonstração

$(ii) \Rightarrow (i)$ É imediato.

$(i) \Rightarrow (ii)$ Por hipótese, temos que Q é um anel simples, um $Z(Q)-$espaço vetorial e $n = [Q : Z(Q)] < \infty$. Provaremos que Q é anel artiniano à direita. Para esquerda é análogo. Consideremos $I_1 \supseteq I_2 \supseteq \cdots$ uma cadeira descendente de ideais à direita de Q. Para todo $i \in \{1, 2, \cdots\}$, I_i é um subespaço vetorial de Q e I_{i+1} é subespaço vetorial de I_i. Logo, $[I_{i+1} : Z(Q)] \leq [I_i : Z(Q)] \leq [Q : Z(Q)] = n$. Desde que $I_i = I_{i+1}$ se, e somente se, $[I_i : Z(Q)] = [I_{i+1} : Z(Q)]$, não podemos ter cadeia estrita de ideais à direita com mais de n elementos. Logo, $I_1 \supseteq I_2 \supseteq \cdots$ é estacionária e Q é artiniano à direita. $\square$

Note que em $(i) \Rightarrow (ii)$ da proposição acima verificamos que se Q é um anel simples de dimensão finita sobre seu centro, então Q é anel artiniano.

Pela Proposição 3.1.1, podemos trabalhar indistintamente com anéis artinianos simples de dimensão finita sobre seu centro ou álgebras centrais de dimensão finita.

Num anel artiniano (à direita ou à esquerda), para provar a inversibilidade de um elemento, basta verificar que esse elemento é inversível à esquerda ou à direita, conforme prova a próxima proposição.

Proposição 3.1.2 *Seja Q um anel artiniano à direita (à esquerda). Se $a, b \in Q$ e $ab = 1$, então $ba = 1$.*

Demonstração

Consideremos o endomorfismo de $Q-$módulos à direita $\varphi : Q \longrightarrow Q$, definido por $\varphi(x) = ax$. Vamos provar que φ é um isomorfismo. Claro que φ é sobrejetor, pois $ab = 1$. Note que $Ker(\varphi) \subseteq Ker(\varphi^2) \subseteq \cdots$ é uma cadeia ascendente de ideais à direita de Q. Como Q é artiniano à direita, temos que Q é noetheriano à direita e portanto, existe $n \in \mathbb{N}$, tal que $Ker(\varphi^n) = Ker(\varphi^{n+1})$. Seja $u \in Ker(\varphi)$. Como φ^n é sobrejetora, existe $v \in Q$, tal que $u = \varphi^n(v)$. Logo, $0 = \varphi(u) = \varphi^{n+1}(v)$ e segue que $v \in Ker(\varphi^{n+1}) = Ker(\varphi^n)$, isto é, $u = \varphi^n(v) = 0$. Logo, φ é injetiva. Como $\varphi(1 - ba) = 0$, temos que $1 = ba$. $\square$

Proposição 3.1.3 *Se Q é um anel artiniano à direita (à esquerda), então Q é seu próprio anel quociente clássico à direita e à esquerda.*

Demonstração

Assumindo que Q é anel artiniano à direita, pela definição de anel quociente clássico à direita (Definição 2.1.4), nota-se facilmente que basta mostrar que todo elemento regular de Q é inversível em Q. Considerando $x \in Q^*$, temos a cadeia descendente de ideais à direita $xQ \supseteq x^2Q \supseteq \cdots$ Por hipótese, existe $n \in \mathbb{N}$, tal que $x^n = x^{n+1}y$, para algum $y \in Q$, o que implica que $xy = 1$, provando assim que x é inversível à direita em Q. Pela proposição anterior, x também é inversível à esquerda em Q e portanto é inversível. Assim, Q é seu próprio anel quociente clássico à direita e à esquerda. Analogamente, se Q é anel artiniano à esquerda, prova-se que Q é seu próprio anel quociente clássico à direita e à esquerda. $\square$

Observe que da proposição anterior conclui-se que $U(Q) = Q^*$.

O próximo teorema e seu corolário são os principais resultados sobre a estrutura de um anel artiniano simples. Uma demonstração detalhada destes fatos pode ser vista em ([F], §4)

Lembre que $M_n(R)$ denota o anel das matrizes quadradas de ordem n sobre o anel R.

Teorema 3.1.1 (Teorema de Wedderburn-Artin) *Qualquer anel artiniano à esquerda simples é isomorfo à um anel de matrizes $M_n(D)$, para um anel de divisão D e um inteiro $n \geq 1$. Reciprocamente, se D é um anel de divisão e $n \geq 1$ é um número inteiro, então $M_n(D)$ é anel artiniano à esquerda simples.*

O Teorema de Wedderburn-Artin também pode ser enunciado para anéis artinianos à direita simples e daí decorre imediatamente o seguinte corolário.

Corolário 3.1.1 *Seja R um anel com unidade. São equivalentes:*

(i) *R é artiniano à esquerda simples;*

(ii) *R é artiniano à direita simples;*

(iii) $R \simeq M_n(D)$*, onde D é um anel de divisão e* $n \geq 1$ *é um inteiro.*

Em função do corolário não é necessário mencionarmos o adjetivo *à esquerda* ou *à direita* quando nos referirmos à anéis artinianos simples.

Na seqüência veremos mais fatos a respeito dos anéis artinianos simples. Utilizaremos estes resultados nas próximas seções.

Teorema 3.1.2 *Seja Q um anel artiniano simples de dimensão finita sobre o centro e seja R um subanel maximal de Q tal que Q é o anel quociente clássico para R.*

(a) *Todo ideal unilateral de R é principal;*

(b) $\frac{R}{J(R)}$ *é isomorfo ao anel de matrizes quadradas $M_n(D)$, para algum $n \in \mathbb{N}$ e para algum anel de divisão D.*

Demonstração

([Re], Theorem 18.7, p. 179). □

Corolário 3.1.2 *Seja Q um anel artiniano simples de dimensão finita sobre seu centro.*

(a) *Todo ideal unilateral de Q é principal;*

(b) $Q \simeq M_n(D)$ *para um anel de divisão D e um inteiro $n \geq 1$.*

Demonstração

Basta tomar $R = Q$ no teorema anterior. □

Conforme veremos na seqüência, a restrição de dimensão finita sobre o centro não é essencial para o item (a) do corolário anterior. Para isso, precisaremos das definições seguintes.

Definição 3.1.5 *Seja R um anel com unidade. O $R-$módulo M é semi-simples quando todo submódulo é um somando direto, isto é, se N é um submódulo de M, existe outro submódulo P de M, tal que $M = N \oplus P$.*

Definição 3.1.6 *O anel Q é semi-simples à esquerda quando o módulo à esquerda Q é semi-simples.*

Assim, podemos dizer que Q é anel semi-simples à esquerda quando todo ideal à esquerda é somando direto.

Analogamente define-se semi-simplicidade à direita. O anel Q é dito semi-simples se for semi-simples à direita e à esquerda.

Se Q é anel artiniano simples, segue de ([F], §4, Teorema 4.10), que Q é semi-simples.

Lema 3.1.1 *Seja Q um anel artiniano simples. Se I é ideal unilateral de Q, então I é principal.*

Demonstração

Pelo visto acima, I é somando direto de Q. Assim, existe um ideal à esquerda J tal que $Q = I \oplus J$. Daí, $1 = a + b$, com $a \in I$ e $b \in J$. Vamos mostrar que $I = Qa$. Claro que $Qa \subseteq I$. Agora, seja $x \in I$. Temos que $1 - a = b$, com $a \in I$ e $b \in J$. Assim, $x - xa = xb$. Daí decorre que $xb \in I \cap J = \{0\}$. Portanto, $x = xa \in Qa$. $\square$

3.2 Anéis de Valorização de Dubrovin

Apresentaremos nesta seção a definição de anel de valorização de Dubrovin e estudaremos os principais resultados que ela produz. Como será observado, esses resultados generalizam os vistos nos capítulos anteriores.

Definição 3.2.1 *Um subanel R de um anel artiniano simples Q é um anel de valorização de Dubrovin de Q quando:*

(a) O anel $\frac{R}{J(R)}$ é artiniano simples;

(b) Dado $q \in Q \setminus R$, existem $r_1, r_2 \in R$ tais que $qr_1, r_2q \in R \setminus J(R)$.

Observamos que a Proposição 2.1.4 garante que o Radical de Jacobson $J(R)$ é um ideal bilateral do anel com unidade R. Assim, o quociente $\frac{R}{J(R)}$ da definição acima está bem definido.

Observamos ainda que um subanel R do anel artiniano simples Q é um anel de valorização de Dubrovin de Q se, e somente se, existe um ideal bilateral I de R, tal que

R/I é um anel artiniano simples, e para cada $q \in Q \setminus R$, existem $r_1, r_2 \in R$ tais que $qr_1, r_2q \in R \setminus I$. Neste caso, como poder ser viso em ([D$_1$], §1, Proposition 3), segue que $I = J(R)$.

A Proposição 1.1.2 afirma que os ideais de um anel de valorização de um corpo estão totalmente ordenados por inclusão. Na Seção 1 do Capítulo 2, vimos que é válida a ordenação total no conjunto dos ideais à esquerda (à direita, bilaterais) de um anel de valorização total de um anel de divisão. Para um anel de valorização de Dubrovin de um anel artiniano simples de dimensão finita sobre o centro é garantida a ordenação total apenas no conjunto dos ideais bilaterias, conforme ([D$_1$], §2, Theorem 4) e ([W$_3$], §1, 1.4). Na verdade, a inclusão é uma relação de ordem num conjunto ainda maior, os $R-$ideais, conforme a Definição ([D$_1$], §2, Definition 1).

Comparando a definição de anel de valorização de Dubrovin com a definição de anel de valorização de um corpo (Definição 1.1.1), ou com a definição de anel de valorização total de um anel de divisão (Definição 2.1.1), não é imediato perceber que a definição de Dubrovin estende as anteriores. Faremos uma prova deste fato, com a ajuda dos lemas abaixo.

Lema 3.2.1 *Se R é um anel de valorização de Dubrovin do anel artiniano simples Q, então $J(R)$ é seu único ideal bilateral maximal.*

Demonstração

Seja M um ideal bilateral maximal de R. É fácil ver que $\frac{M+J(R)}{J(R)}$ é ideal bilateral de $\frac{R}{J(R)}$ que é anel artiniano simples. Logo, $M + J(R) = R$ ou $M + J(R) = J(R)$. No primeiro caso obtemos $m \in M$ e $r \in J(R)$ tais que $1 = m + r$. Vimos na Proposição 2.1.4 que $r \in J(R)$ implica que $1 - xr$ é inversível, para todo $x \in R$. Assim, para $x = 1$, vem que $m = 1 - r \in U(R)$, contradizendo o fato de ser $M \neq R$. Portanto, só resta $M + J(R) = J(R)$ e disso decorre que $M = J(R)$. $\square$

Note que o Lema 3.2.1 é o análogo da Proposição 1.1.5 e do Corolário 2.1.1.

Para cada anel com unidade R, sabemos que $J(R)$ é ideal bilateral próprio de R. Assim, $J(R)$ não contém elementos inversíveis à direita e elementos inversíveis à esquerda. Segue que $J(R) \subseteq R \setminus U(R)$. Tomando complementar em relação a R vem que $U(R) \subseteq R \setminus J(R)$. No entanto, diferente do que ocorre quando R é um anel de valorização total ou anel de valorização de um corpo, no caso em que R é um anel de valorização de Dubrovin não temos em geral a igualdade $J(R) = R \setminus U(R)$, (ou equivalentemente $U(R) = R \setminus J(R)$) como veremos após a Proposicão 3.2.3. Essa igualdade vale quando R é um anel comutativo, conforme afirma o lema seguinte.

Lema 3.2.2 *Seja R um anel de valorização de Dubrovin de Q. Se R é comutativo, então $R \setminus U(R) = J(R)$.*

Demonstração

Seja $x \in R \setminus U(R)$. Como $x \notin U(R)$, então $Rx = xR$ está contido num ideal bilateral maximal. Pelo Lema 3.2.1 devemos ter $xR \subseteq J(R)$. Logo, $R \setminus U(R) = J(R)$, ou equivalentemente, $R \setminus J(R) = U(R)$. $\square$

A próxima proposição mostra que a definição de anel de valorização de Dubrovin estende aos anéis artinianos simples o conceito de anel de valorização de um corpo.

Proposição 3.2.1 *Seja Q um corpo e R um subanel de Q. São equivalentes:*

(i) *O anel R é um anel de valorização de Q;*

(ii) *O anel R é um anel de valorização de Dubrovin de Q.*

Demonstração

$(i) \Rightarrow (ii)$ Pela Proposição 1.1.5, $J(R)$ é ideal maximal de R. Logo, $\frac{R}{J(R)}$ é corpo, provando a condição (a) da Definição 3.2.1. Seja agora $q \in Q \setminus R$. Então $q^{-1} \in R$ e tomamos $r_1 = r_2 = q^{-1} \in R$, obtendo $qr_1 = r_2q = 1 \in R \setminus J(R)$.

$(ii) \Rightarrow (i)$ Seja $q \in Q \setminus R$. Por hipótese, existe $r \in R$ tal que $qr \in R \setminus J(R)$. Do Lema 3.2.2 vem que $qr \in U(R)$. Logo, $q^{-1} = r(qr)^{-1} \in R$ e R é anel de valorização do corpo Q.

$\square$

A classe dos anéis de valorização de Dubrovin também engloba os anéis de valorização totais, conforme a proposição seguinte.

Proposição 3.2.2 *Seja Q um anel de divisão e R um subanel de Q. Se R é anel de valorização total de Q, então R é anel de valorização de Dubrovin de Q.*

Demonstração

Pelo Corolário 2.1.1 e Proposição 2.1.5, $J(R)$ é ideal bilateral maximal de R e $J(R) = R \setminus U(R)$. Seja $\bar{x} \in \frac{R}{J(R)}$, $\bar{x} \neq \bar{0}$, isto é, $x \notin J(R)$. Assim, $x \in U(R)$. Então $\bar{y} = x^{-1} + J(R) \in \frac{R}{J(R)}$ e $\bar{x}\bar{y} = \bar{y}\bar{x} = \bar{1}$. Decorre que $\frac{R}{J(R)}$ é anel de divisão e portanto é anel artiniano simples. Isso mostra a condição (a) da Definição 3.2.1. Para provar a condição (b) basta proceder analogamente à prova de $(i) \Rightarrow (ii)$ da proposição anterior. $\square$

Exemplo 3.1 Para cada número primo p, $\mathbb{Z}_{(p)} = \{ab^{-1};\ a, b \in \mathbb{Z},\ p \nmid b\}$ é um anel de valorização de Dubrovin de $\mathbb{Q}$, já que $\mathbb{Z}_{(p)}$ é anel de valorização de $\mathbb{Q}$.

Exemplo 3.2 O anel $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$, com $\alpha = \frac{1}{2}(1 + i + j + k)$, é um anel de valorização de Dubrovin de $\mathbb{H}$, já que é total em $\mathbb{H}$.

A proposição abaixo completa a relação entre anéis de valorização de Dubrovin e anéis de valorização totais de um anel de divisão.

Proposição 3.2.3 *Seja R um anel de valorização de Dubrovin do anel de divisão Q. São equivalentes:*

(i) R é anel de valorização total de Q;

(ii) $R \setminus U(R) = J(R)$;

(iii) $\frac{R}{J(R)}$ é anel de divisão;

$(i) \Rightarrow (ii)$ Veja a Proposição 2.1.5.

$(ii) \Rightarrow (iii)$ Seja $\bar{0} \neq \bar{x} \in \frac{R}{J(R)}$. Segue que $x \notin J(R) = R \setminus U(R)$. Assim, basta proceder analogamente à prova da Proposição 3.2.2.

$(iii) \Rightarrow (i)$ Seja $q \in Q \setminus R$. Como R é anel de valorização de Dubrovin de Q, existem $r_1, r_2 \in R$ tais que $qr_1, r_2q \in R \setminus J(R)$. Por hipótese, $\frac{R}{J(R)}$ é anel de divisão. Assim, existem $\alpha, \beta \in R$ tais que $\alpha(qr_1) = (qr_1)\alpha = 1 = \beta(r_2q) = (r_2q)\beta$. Decorre que $1 = q(r_1\alpha) = (\beta r_2)q$, o que implica em $q^{-1} \in R$. Portanto R é anel de valorização total de Q. $\square$

Como era esperado, pela inexistência de um Teorema da Extensão para anéis de valorização totais, existem anéis de valorização de Dubrovin de um anel de divisão que não são totais. Os exemplos que aparecem nos artigos sobre o assunto são os subanéis

$V_{(p)} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)}i + \mathbb{Z}_{(p)}j + \mathbb{Z}_{(p)}k$ do anel de divisão $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, onde p é um número primo diferente de 2. Pelo Teorema 2.4.2, sabemos que $V_{(p)}$ não é total em $\mathbb{H}$. Assim, para $p \neq 2$, decorre da proposição anterior que $V_{(p)} \setminus J(V_{(p)}) \nsubseteq U(V_{(p)})$, isto é, existe $x \in V_{(p)}$ tal que $x \notin J(V_{(p)}) \cup U(V_{(p)})$. A prova de que $V_{(p)}$ é anel de valorização de Dubrovin é feita indiretamente. Veja por exemplo ([W_1], §1, Example (c)), ([Br], §3) e ([BrG_2], §2). Faremos uma prova disso na Proposição 3.2.4.

No caso $p = 2$, o subanel $V_{(2)} = \mathbb{Z}_{(2)} + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$ não é anel de valorização de Dubrovin de $\mathbb{H}$, pois de acordo com ([W_1], §1, Example (c)), $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$ é o único anel de valorização de Dubrovin R de $\mathbb{H}$ tal que $R \cap \mathbb{Q} = \mathbb{Z}_{(2)}$.

Uma caracterização dos anéis de valorização de Dubrovin pode ser obtida através dos anéis de Bezout.

Definição 3.2.2 *Um anel de Bezout à direita é um anel R tal que todo ideal à direita finitamente gerado é principal.*

Um anel de Bezout à esquerda define-se analogamente. Um anel que é anel de Bezout à direita e à esquerda é chamado anel de Bezout.

Note que se R é anel de valorização do corpo $\mathbb{K}$, então R é anel de Bezout pela Proposicão 1.1.4. A Proposição 2.1.2 garante que no caso de R ser um anel de valorização total do anel de divisão D, R é um anel de Bezout.

Teorema 3.2.1 *Seja R um subanel do anel artiniano simples Q. São equivalentes:*

(i) *R é anel de valorização de Dubrovin de Q;*

(ii) *$\frac{R}{J(R)}$ é anel artiniano simples, R é anel de Bezout e Q é o anel quociente clássico para R.*

Demonstração

Veja ([D_1], §1, Theorem 4) ou ([Br], §3, Theorem 5). □

Uma prova para o fato de que $V_{(p)}$, $p \neq 2$, é anel de valorização de Dubrovin de $\mathbb{H}$ pode ser obtida combinando o teorema anterior com o Teorema 3.1.2.

Proposição 3.2.4 *Se p é um número primo diferente de 2, então $V_{(p)} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)}i + \mathbb{Z}_{(p)}j + \mathbb{Z}_{(p)}k$ é um anel de valorização de Dubrovin de $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$.*

Demonstração

Claro que $V_{(p)}$ é subanel de $\mathbb{H}$, todo elemento regular de $V_{(p)}$ tem inverso em $\mathbb{H}$ e $\{mn^{-1};\ m,n \in V_{(p)},\ n \neq 0\} \subseteq \mathbb{H}$. Por outro lado, dado $h = \frac{a_1}{a_2} + \frac{b_1}{b_2}i + \frac{c_1}{c_2}j + \frac{d_1}{d_2}k \in \mathbb{H}$, podemos escrever $h = mn^{-1}$, onde $m = a_1b_2c_2d_2 + b_1a_2c_2d_2i + c_1a_2b_2d_2j + d_1a_2b_2c_2k$ e $n = a_2b_2c_2d_2$. Logo, $h \in \{mn^{-1};\ m,n \in V_{(p)},\ n \neq 0\}$ e $\mathbb{H}$ é anel quociente clássico à direita para $V_{(p)}$. Notando que no desenvolvimento acima o elemento n comuta com m, podemos facilmente provar que $\mathbb{H}$ é também anel quociente clássico à esquerda para $V_{(p)}$. Também provamos na Proposição 2.4.1 que $V_{(p)}$, $p \neq 2$ é subanel maximal de $\mathbb{H}$. Como $\mathbb{H}$ é anel de divisão com centro $\mathbb{Q}$ e $[\mathbb{H} : \mathbb{Q}] = 4$, aplicamos o Teorema 3.1.2 para concluir que todo ideal de $V_{(p)}$ é principal e que $\frac{V_{(p)}}{J(V_{(p)})} \simeq M_n(D)$, onde D é um anel de divisão. Assim, $\mathbb{H}$ é o anel quociente clássico para $V_{(p)}$, $V_{(p)}$ é anel de Bezout, pois seus ideais unilaterais são principais e $\frac{V_{(p)}}{J(V_{(p)})}$ é anel artiniano simples, pois $\frac{V_{(p)}}{J(V_{(p)})} \simeq M_n(D)$, que é anel artiniano simples pelo Teorema de Wedderburn-Artin. Segue do Teorema 3.2.1 que para $p \neq 2$, $V_{(p)}$ é anel de valorização de Dubrovin de $\mathbb{H}$. $\square$

Se V é um anel de valorização do corpo $\mathbb{K}$ e $\mathbb{L}$ é um subcorpo de $\mathbb{K}$, sabemos que $V \cap \mathbb{L}$ é anel de valorização de $\mathbb{L}$. Esse resultado é estendido para anéis artinianos simples conforme a proposição seguinte.

Proposição 3.2.5 *Seja R um anel de valorização de Dubrovin do anel artiniano simples Q. Então:*

(a) $Z(R) = R \cap Z(Q)$;

(b) $Z(R)$ é anel de valorização do corpo $Z(Q)$.

$$\begin{tikzcd}[arrows=dash]
Q \arrow[d] \arrow[dr] & \\
Z(Q) \arrow[dr] & R \arrow[d] \\
& Z(R)
\end{tikzcd}$$

Demonstração

(a) Claro que $R \cap Z(Q) \subseteq Z(R)$. Seja agora $x \in Z(R)$. Dado $q \in Q$, usamos o Teorema 3.2.1 para escrever $q = mn^{-1}$, com $m \in R$ e $n \in R^*$, pois Q é o anel quociente clássico

de R. Agora, $xqn = xm = mx = mn^{-1}nx = qnx = qxn$. Como $n \in R^*$, e Q é o anel quociente clássico de R, temos que $n \in U(Q)$. Logo, $xq = qx$ e $x \in Z(Q) \cap R$.
(b) Seja $q \in Z(Q)$, $q \neq 0$. Suponha que $q \notin Z(R) = R \cap Z(Q)$. Vamos mostrar que $q^{-1} \in Z(R)$. Temos que $q^{-1} \in Z(Q)$ e então resta mostrar que $q^{-1} \in R$. Como $q \in Z(Q)$ e $q \notin R \cap Z(Q)$ temos que $q \in Q \setminus R$. Desde que R é anel de valorização de Dubrovin de Q, existe $r \in R$ tal que $qr \in R \setminus J(R)$. Assim, $RqrR$ é ideal bilateral de R que não está contido em $J(R)$, que por sua vez, é o único ideal bilateral maximal de R. Conforme observamos após a Definição 3.2.1, os ideias bilaterias de R estão totalmente ordenados por inclusão. Portanto, concluímos que $RqrR = R$. Assim, existem $\alpha, \beta \in R$ tais que $1 = \alpha(qr)\beta$. Como $q \in Z(Q)$, $1 = q(\alpha r\beta) = (\alpha r\beta)q$, com $\alpha r\beta \in R$, isto é, $q^{-1} = \alpha r\beta \in R$.
$\square$

Observe que no caso de $Q = \mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ e $R = V_{(p)} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)}i + \mathbb{Z}_{(p)}j + \mathbb{Z}_{(p)}k$, com p um número primo diferente de 2, decorre da proposição que $Z(V_{(p)}) = V_{(p)} \cap Z(\mathbb{H}) = V_{(p)} \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ e $Z(V_{(p)}) = \mathbb{Z}_{(p)}$ é anel de valorização do corpo $Z(Q) = \mathbb{Q}$. Para $p = 2$, o mesmo vale para o anel $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)}i + \mathbb{Z}_{(2)}j + \mathbb{Z}_{(2)}k$, com $\alpha = \frac{1}{2}(1+i+j+k)$.

O chamado *Teorema da Extensão* para anéis de valorização de Dubrovin é uma espécie de recíproca da proposição anterior.

Teorema 3.2.2 (Teorema da Extensão) *Seja Q um anel artiniano simples de dimensão finita sobre $Z(Q)$. Se V é um anel de valorização do corpo $Z(Q)$ então existe um anel de valorização de Dubrovin R de Q tal que $R \cap Z(Q) = V$.*

$$\begin{tikzcd}
Q \arrow[d, dash] \arrow[dr, dash, dotted] & \\
Z(Q) \arrow[dr, dash] & R \arrow[d, dash, dotted] \\
 & V
\end{tikzcd}$$

Observação 3.6 A primeira prova para o Teorema da Extensão foi apresentada também por Dubrovin num artigo posterior ([D_2], §3, Theorem 2 and Theorem 3) em 1985.

Observação 3.7 Uma nova prova foi apresentada por Brungs e Gräter em 1990. Veja ([BrG_2], §3, Theorem 3.8). Essa prova, segundo seus autores, está baseada na prova de Dubrovin mas difere em pontos essenciais, pois evita argumento de transfinitude.

Observação 3.8 O enunciado do Teorema da Extensão deixa claro que duas restrições são impostas. A saber, Q deve ter dimensão finita sobre seu centro e obtem-se apenas extensões de anéis de valorização do centro de Q.

Observação 3.9 Não é conhecido até hoje, se a hipótese de Q ter dimensão finita sobre seu centro é essencial para o Teorema da Extensão.

Observação 3.10 O Teorema da Extensão só vale para obter extensões de anéis de valorização do centro de Q. O seguinte contra-exemplo pode ser visto em ([BrG$_2$], §1) e ([W$_1$], §2). Se $Q = \mathbb{H}$, então $Z(Q) = \mathbb{Q}$. O anel de valorização $\mathbb{Z}_{(5)}$ de $\mathbb{Q}$ tem duas extensões no corpo $\mathbb{Q}[\,i\,]$, mas nenhuma dessas extensões pode ser estendida a um anel de valorização de Dubrovin de $\mathbb{H}$.

O Teorema da Correspondência, visto anteriormente em suas versões para corpos e anéis de divisão, também é estendido aos anéis artinianos simples. Sua demonstração pode ser vista em ([D$_1$], §2, Corollary).

Lembramos que um ideal P de um anel não necessariamente comutativo Q é primo quando $P \neq Q$ e se A e B são ideais de Q tais que $AB \subseteq I$, então $A \subseteq P$ ou $B \subseteq P$.

Teorema 3.2.3 (Teorema da Correspondência) *Seja Q que um anel artiniano simples de dimensão finita sobre o centro e R um anel de valorização de Dubrovin de Q. Então*

(a) *Se $R \subseteq R' \subseteq Q$, então R' é anel de valorização de Dubrovin de Q e $J(R')$ é ideal primo de R. Ainda mais, $\frac{R}{J(R')}$ é anel de valorização de Dubrovin de $\frac{R'}{J(R')}$;*

(b) *Existe uma correspondência biunívoca entre ideias primos de R e sobreanéis de R em Q.*

Para concluir esta seção listamos outros resultados sobre os anéis de valorização de Dubrovin.

Seja Q um anel artiniano simples com centro $Z(Q)$, $[Q : Z(Q)] < \infty$ e R um anel de valorização de Dubrovin de Q.

- Se $e^2 = e \in R$, então eRe é anel de valorização de Dubrovin de eQe ([D$_1$], §1, Theorem 7).

- $M_n(R)$ é anel de valorização de Dubrovin de $M_n(Q)$.

- A aplicação $R' \longmapsto R' \cap Z(Q)$ é uma bijeção, que preserva a inclusão, entre sobreanéis de R em Q e sobreanéis de $R \cap Z(Q)$ em $Z(Q)$ ([D_2], §2, Theorem 1 (1)).

Outros resultados podem ser encontrados em [D_1], [D_2] e [W_3].

3.3 Places e Anéis de Valorização de Dubrovin

Na Seção 3 do primeiro capítulo definimos places sobre corpos e como principal resultado vimos que dado um corpo $\mathbb{K}$, existe uma correspondência biunívoca entre classes de places sobrejetores de $\mathbb{K}$ e os anéis de valorização de $\mathbb{K}$.

Em analogia com esse fato, vamos utilizar a definição de place em anéis artinianos simples, proposta por Dubrovin em [D_1], para mostrar que dado um anel artiniano simples Q, existe uma correspondência biunívoca entre classes de places de Q e os anéis de valorização de Dubrovin de Q.

Essa correspondência decorrerá do Teorema 3.3.1 ([D_1], §1, Proposition 3) cuja demonstração é o objetivo principal desta seção. Essa proposição estabalecerá a maneira de se obter um anel de valorização de Dubrovin de um anel artiniano simples Q, a partir de um place definido sobre Q, e reciprocamente, mostrará que dado um anel de valorização de Dubrovin R do anel artiniano simples Q, é possível definir um place sobre Q, cujo anel de valorização de Dubrovin seja R.

Trabalhamos para que os resultados desta seção sejam independentes da Seção 2 deste capítulo para, em consonância com a teoria de valorização em corpos, mostrar que a teoria de valorização sobre anéis artinianos simples também pode ser abordada, desde seu início, através do estudo dos places.

Para estender o conceito de place para anéis artinianos simples, vamos denotar a união do símbolo ∞ ao anel artiniano simples Q por $\tilde{Q} = Q \cup \{\infty\}$.

Convencionamos

(1) $a + \infty = \infty + a = \infty$, $\forall\ a \in Q$;

(2) $c.\infty = \infty.c = \infty$, $\forall\ c \in U(Q)$.

Note que não estão definidos $\infty + \infty$, $c.\infty$ e $\infty.c$ para $c \notin U(Q)$, o que inclui o caso $\infty.\infty$.

Decorre de (2) que $-\infty = \infty$, já que $-1 \in U(Q)$.

Definição 3.3.1 *Um place à direita de um anel artiniano simples Q sobre um anel artiniano simples D é uma aplicação sobrejetiva $f : \tilde{Q} \longrightarrow \tilde{D}$ tal que, dados $x, y \in \tilde{Q}$, tem-se*

(*a*) *Se $f(x) + f(y)$ está definido, então $x + y$ está definido e $f(x + y) = f(x) + f(y)$;*

(*b*) *Se $f(x)f(y)$ está definido, então xy está definido e $f(xy) = f(x)f(y)$;*

(*c*) *Para todo $q \in Q$ tal que $f(q) = \infty$, existe $r \in Q$ tal que $f(r) \neq \infty$ e $f(qr) \neq \infty, 0$.*

Um place à esquerda é definido analogamente substituindo a condição $f(qr) \neq \infty, 0$ do item (c) por $f(rq) \neq \infty, 0$. Um place à direita e à esquerda é chamado um *place* de Q em D.

A seguinte proposição apresenta propriedades de um place. Sua demonstração não oferece dificuldades e é análoga à demonstração da Proposição 1.3.1.

Proposição 3.3.1 *Sejam Q e D anéis artinianos simples e $f : \tilde{Q} \longrightarrow \tilde{D}$ um place.*

(*i*) *$f(1) = 1$, $f(0) = 0$ e $f(\infty) = \infty$;*

(*iii*) *$f(-x) = -f(x)$, para todo $x \in \tilde{Q}$;*

No próximo teorema relacionamos places com anéis de valorização de Dubrovin. Para isso serão necessários um lema e uma proposição preliminares.

Seja R um anel com unidade e X um subconjunto de R. Definimos os conjuntos

$$r_R(X) = \{r \in R;\ Xr = 0\} \quad \text{e} \quad \ell_R(X) = \{r \in R;\ rX = 0\}$$

Chamamos $r_R(X)$ e $\ell_R(X)$ respectivamente de anulador à direita e anulador à esquerda de X em R. Não é difícil verificar que $r_R(X)$ é ideal à direita de R e $\ell_R(X)$ é ideal à esquerda de R.

Lema 3.3.1 *Se Q é um anel artiniano simples e $x \in Q$, então $\ell_Q(r_Q(x)) = Qx$.*

Demonstração

Para provar a inclusão $Qx \subseteq \ell_Q(r_Q(x))$, consideremos $\alpha = qx \in Qx$ e $\beta \in r_Q(x)$. Assim, $\alpha\beta = qx\beta = 0$ implica que $\alpha \in \ell_Q(r_Q(x))$. Agora provaremos que $\ell_Q(r_Q(x)) \subseteq Qx$. Conforme vimos antes do Lema 3.1.1, Q é semi-simples. Assim, existe um ideal à esquerda I de Q, tal que $Q = Qx \oplus I$. Pelo Lema 3.1.1, todos os ideais unilaterais de Q são principais, e daí $Q = Qx \oplus Qy$, para algum $y \in Q$. Temos que $1 = a + b$, com $a \in Qx$ e $b \in Qy$. Afirmamos que $Qx = Qa$ e $a^2 = a$. Claro que $Qa \subseteq Qx$, pois $a \in Qx$. Por outro lado, seja $u \in Qx$. Temos que $1 - a = b$ implica em $ub = u - ua$. Nessa igualdade, note que o lado esquerdo está em Qy e o lado direito está em Qx. Logo, $ub \in Qx \cap Qy = \{0\}$. Portanto, $ub = 0$ e assim, $u = ua \in Qa$, para todo $u \in Qx$. Logo, $Qx = Qa$. Finalmente, fazendo $u = a$, temos $a = a^2$. Agora seja $s \in \ell_Q(r_Q(x))$. Então $s\lambda = 0$ para todo $\lambda \in r_Q(x)$. Mas $1 - a \in r_Q(x)$, pois $x = qa$ e $qa(1 - a) = qa - qa^2 = 0$ implica em $qa(1 - a) = 0$, isto é, $x(1 - a) = 0$. Logo, $s(1 - a) = 0$, e daí $s = sa \in Qa = Qx$. □

Proposição 3.3.2 *Sejam R um subanel do anel artiniano simples Q e $\mathfrak{M}$ um ideal bilateral maximal de R. Se para cada $q \in Q \setminus R$ existem $r_1, r_2 \in R$ tais que $qr_1, r_2q \in R \setminus \mathfrak{M}$, então $1 + \mathfrak{M} \subseteq U(R)$.*

Demonstração

Vamos provar inicialmente que $1 + \mathfrak{M} \subseteq Q^*$. Seja $m \in \mathfrak{M}$. Note que

$$\ell_Q(1 + m) \subseteq \ell_Q(1 + m)^2 \subseteq \cdots .$$

Além disso, é fácil ver que $\ell_Q(x)$ é ideal à esquerda de Q, para todo $x \in Q$. Como Q é artiniano, então pela observação após a Definição 3.1.3, Q é noetheriano. Portanto, a cadeia acima é estacionária, isto é, existe $n \in \mathbb{N}$ tal que $\ell_Q(1 + m)^m = \ell_Q(1 + m)^n$, para todo $m \geq n$. Como $(1 + m)^n$ é a soma do elemento 1 com produtos que envolvem $m \in \mathfrak{M}$ e $\mathfrak{M}$ é ideal bilateral, temos que $(1 + m)^n = 1 + m_0$, para algum $m_0 \in \mathfrak{M}$. Assim,

$$\ell_Q(1 + m_0) = \ell_Q(1 + m)^n = \ell_Q(1 + m)^{n+1} = \cdots = \ell_Q(1 + m)^{2n} = \ell_Q(1 + m_0)^2.$$

Logo, $\ell_Q(1 + m_0) = \ell_Q(1 + m_0)^2$. Pelo Lema 3.1.1, temos que os ideais unilaterais de Q

são principais. Segue que

$$\ell_Q(1+m_0) = \ell_Q(1+m_0)^2 = Qu \qquad (1)$$

para algum $u \in Q$. Agora suponha $q \in r_Q(1+m_0)$ e $q \in Q \setminus R$. Por hipótese, existe $r \in R$ tal que $qr \in R \setminus \mathfrak{M}$. Assim, $0 = (1+m_0)q = (1+m_0)qr$ implica em $qr + m_0qr = 0$, donde $qr \in \mathfrak{M}$, o que é uma contradição. Logo, $r_Q(1+m_0) \subseteq R$. Assim, se $\alpha \in r_Q(1+m_0)$, temos que $\alpha \in R$ e $(1+m_0)\alpha = 0$, implicando em $\alpha + m_0\alpha = 0$. Decorre que $\alpha \in \mathfrak{M}$. Logo, $r_Q(1+m_0) \subseteq \mathfrak{M}$. Analogamente, prova-se que $\ell_Q(1+m_0) \subseteq \mathfrak{M}$. O produto $\ell_Q(1+m_0)r_Q(1+m_0)$ do ideal à esquerda $\ell_Q(1+m_0)$ com o ideal à direita $r_Q(1+m_0)$ é um ideal bilateral do anel simples Q. Como

$$\ell_Q(1+m_0)r_Q(1+m_0) \subseteq \mathfrak{M} \subsetneqq R \subseteq Q,$$

segue da simplicidade de Q que

$$\ell_Q(1+m_0)r_Q(1+m_0) = \{0\}. \qquad (2)$$

Seja $q \in \ell_Q(1+m_0)$. Por (2), $q(r_Q(1+m_0)) = 0$ e daí $q \in \ell_Q(r_Q(1+m_0))$. De (1), temos que $Qu \subseteq \ell_Q(1+m_0)$. Também $\ell_Q(1+m_0) \subseteq \ell_Q(r_Q(1+m_0))$. Pelo Lema 3.3.1, temos que $\ell_Q(r_Q(1+m_0)) = Q(1+m_0)$. Desta forma, $u = q(1+m_0)$ e $u \in \ell_Q(1+m_0)$. Segue que $0 = u(1+m_0) = q(1+m_0)^2$, o que implica que $q \in \ell_Q(1+m_0)^2 = \ell_Q(1+m_0)$. Logo, $q(1+m_0) = 0$, isto é, $u = 0$. Assim $0 = \ell_Q(1+m_0)$, o que implica em dizer que $1+m_0$ é regular à esquerda em Q. Analogamente $1+m_0$ é regular à direita. Portanto, $1+m_0$ é regular em Q. Finalmente, se $a \in Q$ e $(1+m)a = 0$, temos $0 = (1+m)a = (1+m)^{n-1}(1+m)a = (1+m)^n a = (1+m_0)a$ e assim, $a = 0$, pois $1+m_0 \in Q^*$. Provamos desta forma que $1+m$ é regular à direita em Q. Da mesma maneira, $1+m$ é regular à esquerda em Q. Isso conclui a prova de que $1+\mathfrak{M} \subseteq Q^*$. Agora, dado $m \in \mathfrak{M}$, temos que $1+m \in 1+\mathfrak{M} \subseteq Q^*$. Lembrando que $Q^* = U(Q)$, temos que $1+m$ tem inverso $(1+m)^{-1} \in Q$. Se $(1+m)^{-1} \notin R$, então $[(1+m)^{-1}-1] \in Q \setminus R$ e aplicando a hipótese, obtemos $s \in R$ tal que $[(1+m)^{-1}-1]s = r \in R \setminus \mathfrak{M}$. Multiplicando a última igualdade por $1+m$ à esquerda, $s-(1+m)s = (1+m)r$ implica em $-ms = r+mr$, donde concluímos que $r \in \mathfrak{M}$, o que é uma contradição. Logo, $(1+m)^{-1} \in R$, isto é, $1+\mathfrak{M} \subseteq U(R)$. $\square$

Provaremos agora o principal resultado desta seção, seguindo a demonstração original de Dubrovin ([D_1], §1, Proposition 3).

Teorema 3.3.1 *Sejam Q e D anéis artinianos simples.*

(a) Se f é um place de Q em D, então $R_f := \{q \in Q : f(q) \neq \infty\}$ é um anel de valorização de Dubrovin de Q e $f|_{R_f} : R_f \longrightarrow D$ é um homomorfismo de anéis com núcleo $\mathfrak{M}_{R_f} := \{q \in Q : \ f(q) = 0\} = J(R_f)$. Reciprocamente,

(b) Se R é um subanel de Q e $\mathfrak{M}_R$ é um ideal bilateral de R tal que $\frac{R}{\mathfrak{M}_R}$ é artiniano simples, e se para $q \in Q \setminus R$ existem $r_1, r_2 \in R$ tais que $qr_1, r_2q \in R \setminus \mathfrak{M}_R$, então a aplicação

$$\begin{aligned} f : \tilde{Q} &\longrightarrow \tilde{B} \\ a &\longmapsto \bar{a}, \quad \text{se } a \in R \\ a &\longmapsto \infty, \quad \text{se } a \notin R \end{aligned}$$

é um place de Q em $B = \frac{R}{\mathfrak{M}_R}$ tal que $R_f = R$. Além disso, $\mathfrak{M}_R = J(R)$.

Demonstração

Afirmação 1: R_f é um subanel de Q.

Prova Sejam $a, b \in R_f$. Desde que $f(a) \neq \infty$ e $f(b) \neq \infty$, temos que $f(a)f(b)$ está definido, e como f é place, ab também está definido e $f(ab) = f(a)f(b) \in D$. Logo, $ab \in Q$. Além disso, $f(a)+f(-b)$ está definido implica que $a-b$ está definido e $f(a-b) = f(a)+f(-b) = f(a)-f(b) \in D$. Segue que $a-b \in R_f$ e R_f é subanel de Q.

Afirmação 2: Dado $q \in Q \setminus R_f$, existem $r_1, r_2 \in R_f$, tais que $qr_1, r_2q \in R_f \setminus J(R_f)$.

Prova Temos que $f(q) = \infty$. Como f é place à direita e à esquerda, existem $r_1, r_2 \in Q$ tais que $f(r_2q) \neq \infty, 0$; $f(qr_1) \neq \infty, 0$; $f(r_1) \neq \infty$; $f(r_2) \neq \infty$. Assim,

- $f(r_1) \neq \infty \neq f(r_2) \Rightarrow r_1, r_2 \in R$;
- $f(qr_1) \neq \infty \neq f(r_2q) \Rightarrow qr_1, r_2q \in R_f$;
- $f(qr_1) \neq 0 \neq f(r_2q) \Rightarrow qr_1, r_2q \notin \mathfrak{M}_{R_f}$.

Afirmação 3: $\mathfrak{M}_{R_f} := \{q \in Q : \ f(q) = 0\}$ é ideal bilateral maximal de R_f e $\frac{R_f}{\mathfrak{M}_{R_f}} \simeq D$. Além disso, $\mathfrak{M}_{R_f} = J(R_f)$.

Prova Seja $\hat{f} : R_f \longrightarrow D$, $\hat{f} = f|_{R_f}$. Provaremos que $\hat{f}$ é um homomorfismo sobrejetivo de anéis. É claro que $\hat{f}(1) = f(1) = 1$. Se $a, b \in R_f$, então $\hat{f}(a) = f(a) \neq \infty$, $\hat{f}(b) = f(b) \neq \infty$, $a + b \in R_f$ e $ab \in R_f$. Logo, $f(a) + f(b)$ e $f(a)f(b)$ estão definidos e $\hat{f}(a + b) = f(a + b) = f(a) + f(b) = \hat{f}(a) + \hat{f}(b)$. Analogamente, $\hat{f}(ab) = \hat{f}(a)\hat{f}(b)$. Para provar a sobrejetividade, tome $d \in D$. Como f é sobrejetiva, existe $u \in \tilde{Q}$ tal que $f(u) = d$. Assim $u \in R$, pois $d \in D$. Logo, $\hat{f}(u) = f(u) = d$. Note agora que $Ker(\hat{f}) = \{q \in R_f;\ f(q) = 0\} = \{q \in Q;\ f(q) = 0\} = \mathfrak{M}_{R_f}$. Isso mostra que $\mathfrak{M}_{R_f}$ é ideal bilateral de R_f e pelo Teorema dos Homomorfismos, $\frac{R_f}{\mathfrak{M}_{R_f}} \simeq D$. Decorre que $\frac{R_f}{\mathfrak{M}_{R_f}}$ é anel artiniano simples e assim seus únicos ideais bilaterais são os triviais. Aplicando o Segundo Teorema dos Homomorfismos, temos que $\mathfrak{M}_{R_f}$ é ideal bilateral maximal de R_f. Da Afirmação 2 e da Proposição 3.3.2 decorre que $1 + \mathfrak{M}_{R_f} \subseteq U(R)$. Agora, o Lema 2.1.2 diz que $\mathfrak{M}_{R_f} = J(R_f)$, o que conclui a prova da afirmação.

Já vimos que $\frac{R_f}{\mathfrak{M}_{R_f}}$ é anel artiniano simples e $\mathfrak{M}_{R_f} = J(R_f)$, o que implica que $\frac{R_f}{J(R_f)}$ é anel artiniano simples. Esse fato, junto com a Afirmação 2, assegura que R_f é anel de valorização de Dubrovin de Q, o que conclui a prova da parte (a) do teorema.

Para provar a parte (b) vamos demonstrar que valem as condições (a), (b) e (c) da definição de place para a aplicação $f : \tilde{Q} \longrightarrow \tilde{D}$ definida no enunciado do teorema.

(a) Sejam $x, y \in \tilde{Q}$ tais que $f(x) + f(y)$ esteja definido. Provaremos que $x + y$ está definido e $f(x + y) = f(x) + f(y)$. Temos que $f(x) \neq \infty$ ou $f(y) \neq \infty$, o que implica em $x \in R$ ou $y \in R$. Caso x e y estejam em R, então $x + y$ está definido e $x + y \in R$. Assim, $f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y)$. Pode ocorrer também que $x \in R$ e $y \notin R$ ou ainda $y \in R$ e $x \notin R$. Basta analisar o primeiro caso e o segundo será análogo. Temos que $x \in R$ implica em $x \neq \infty$ e assim $x + y$ está definido. Note que neste caso $x + y \notin R$, pois caso contrário, $x = r - y \in R$, para algum $r \in R$. Desta maneira, $f(x + y) = \infty = \bar{x} + \infty = f(x) + f(y)$.

(b) Sejam $x, y \in \tilde{Q}$ tais que $f(x)f(y)$ esteja definido. Provaremos que xy está definido e que $f(xy) = f(x)f(y)$. Basta analisarmos dois casos:

$$f(x) \neq \infty \neq f(y) \qquad \text{e} \qquad f(x) \in U(D) \text{ e } f(y) = \infty.$$

No primeiro caso, $x, y \in R$ implica em xy definido e $xy \in R$. Assim, $f(xy) = \overline{xy} = \bar{x}\bar{y} = f(x)f(y)$. No segundo caso, $f(x) \in U(D)$ implica em $f(x) \neq \infty$ e assim, $f(x) = \bar{x}$ e $x \in R$. Mostraremos que $x^{-1} \in R$. Como $f(x) \in U(D)$, sabemos que existe $u \in R$ tal

que $f(u) \in D$ e $f(x)f(u) = 1$, isto é, $\bar{x}\bar{u} = \bar{1} = 1 + \mathfrak{M}_R$. Daí, $\overline{xu - 1} = \bar{0} = \mathfrak{M}_R$ e assim $xu \in 1+\mathfrak{M}_R$. Pela Proposição 3.3.2, $1+\mathfrak{M}_R \in U(R)$. Logo, existe $r \in R$ tal que $xur = 1$, isto é, $x^{-1} \in R$. Portanto, $x \in U(R)$. Temos que $f(y) = \infty$. Para $y = \infty$ temos que xy está definido e $xy = \infty$, o que implica em $f(xy) = \infty = f(x)\infty = f(x)f(y)$. Para $y \in Q \setminus R$, também temos que xy está definido. Observe que $xy \in Q \setminus R$, pois $xy \in R$ implica em $x^{-1}(xy) = y \in R$. Assim, $f(xy) = \infty = f(x)\infty = f(x)f(y)$.
(c) Dado $q \in Q$ tal que $f(q) = \infty$, temos que $q \in Q \setminus R$. Por hipótese, existem $r_1, r_2 \in R \subseteq Q$ tais que $qr_1, r_2q \in R \setminus \mathfrak{M}_R$, isto é, existem $r_1, r_2 \in Q$ tais que $f(r_1) \neq \infty$ e $f(r_2) \neq \infty$ e $f(qr_1) \neq 0, \infty$ e $f(r_2q) \neq 0, \infty$. Resta demonstrar que $\mathfrak{M}_R = J(R)$. A Proposição 3.3.1 garante que $1 + \mathfrak{M}_R \subseteq U(R)$. Pelo Lema 2.1.2, $\mathfrak{M}_R = J(R)$. $\square$

Seja Q um anel artiniano simples. No conjunto dos places definidos sobre Q, definimos a relação de equivalência

$$f_1 \sim f_2 \Leftrightarrow R_{f_1} = R_{f_2},$$

que será utilizada para provar o seguinte corolário:

Corolário 3.3.1 *Seja Q um anel artiniano simples. Existe uma correspondência biunívoca entre anéis de valorização de Dubrovin de Q e classes de places de Q.*

Demonstração

Definimos

$$\begin{array}{rcl} \psi : \{[f];\ f \text{ place sobre } Q\} & \longrightarrow & \{R;\ R \text{ anel de valorização de Dubrovin de } Q\} \\ [f] & \longmapsto & R_f \end{array}$$

Pelo item (a) do Teorema 3.3.1, temos que de fato $\psi([f])$ é um anel de valorização de Dubrovin de Q. É fácil ver que ψ está bem definida e é injetora, pois

$$\psi([f_1]) = \psi([f_2]) \Leftrightarrow R_{f_1} = R_{f_2} \Leftrightarrow f_1 \sim f_2 \Leftrightarrow [f_1] = [f_2].$$

Também ψ é sobrejetora, pois dado R um anel de valorização de Dubrovin de Q, define-se $D = \frac{R}{\mathfrak{M}_R}$ e

$$\begin{array}{rcl} f : \tilde{Q} & \longrightarrow & \tilde{D} \\ a & \longmapsto & \bar{a}, \quad \text{se } a \in R \\ a & \longmapsto & \infty, \ \text{se } a \in \tilde{Q} \setminus R \end{array}$$

e pelo item (b) do Teorema 3.3.1, f é um place de Q em D, tal que $R_f = R$. $\square$

Exemplo 3.3 Da Proposição 3.2.4, sabemos que $V_{(p)}$, $p \neq 2$, é anel de valorização de Dubrovin do anel $\mathbb{H}$ dos quatérnios racionais. Pelo Teorema 3.3.1, a aplicação

$$\begin{array}{rcl} f : \tilde{\mathbb{H}} & \longrightarrow & \frac{V_{(p)}}{J(V_{(p)})} \cup \{\infty\} \\ x & \longmapsto & \bar{x},\ x \in V_{(p)} \\ x & \longmapsto & \infty,\ x \in \tilde{\mathbb{H}} \setminus V_{(p)} \end{array}$$

é um place do anel artiniano simples $\mathbb{H}$ no anel artiniano simples $\frac{V_{(p)}}{J(V_{(p)})}$. O anel de valorização de Dubrovin correspondente a $[f]$ é $R_f = \{x \in \mathbb{H};\ f(x) \neq \infty\} = \{x \in \mathbb{H};\ x \in V_{(p)}\} = V_{(p)}$

Exemplo 3.4 Da mesma forma que no exemplo anterior, a aplicação

$$\begin{array}{rcl} f : \tilde{\mathbb{H}} & \longrightarrow & \frac{\tilde{V}_{(2)}}{J(\tilde{V}_{(2)})} \cup \{\infty\} \\ x & \longmapsto & \bar{x},\ x \in \tilde{V}_{(2)} \\ x & \longmapsto & \infty,\ x \in \tilde{\mathbb{H}} \setminus \tilde{V}_{(2)} \end{array}$$

é um place do anel artiniano simples $\mathbb{H}$ no anel artiniano simples $\frac{\tilde{V}_{(2)}}{J(\tilde{V}_{(2)})}$. O anel de valorização de Dubrovin correspondente à $[f]$ é $\tilde{V}_{(2)}$.

3.4 Funções Valorização em Anéis Artinianos Simples

Vimos na Seção 2 do Capítulo 1 o conceito de valorização num corpo $\mathbb{K}$. Estudamos suas principais propriedades e obtivemos uma correspondência biunívoca entre classes de valorizações e anéis de valorização de $\mathbb{K}$. Generalizamos esses fatos na Seção 5 do Capítulo 2, abordando as valorizações definidas sobre um anel de divisão D. Vimos que existe uma correspondência biunívoca entre os anéis de valorização totais e invariantes de D e classes de valorizações de D.

Nesta seção definiremos valorização para um anel artiniano simples. Veremos que esse conceito generaliza os anteriores e estudaremos as propriedades desta classe de valorizações.

Também vamos obter um mecanismo para construção de exemplos de valorizações em anéis artinianos simples de dimensão finita sobre seu centro. Como objetivo principal apresentaremos uma correspondência biunívoca entre uma classe especial de valorizações definidas sobre o anel artiniano simples Q e os anéis de valorização de Dubrovin de Q que satisfazem a uma condição específica.

Vamos considerar Γ um grupo abeliano totalmente ordenado pela relação $\leq$ e $\Gamma \cup \{\infty\}$ a união do símbolo ∞ ao grupo Γ com as mesmas convenções vistas anteriormente.

A definição abaixo foi apresentada por Morandi em ([Mo], §2, Definition 2.1) e foi motivada pelo exemplo que expomos na seqüência.

Definição 3.4.1 *Seja Q um anel artiniano simples. Dizemos que $w : Q \longrightarrow \Gamma \cup \{\infty\}$ é uma valorização de Q se as seguintes condições são satisfeitas:*

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

(b) $w(x) = \infty \Leftrightarrow x = 0$;

(c) $w(xy) \geq w(x) + w(y),\ \forall\ x, y \in Q$;

(d) $w(x + y) \geq min\{w(x), w(y)\},\ \forall\ x, y \in Q$;

(e) $w(Q) = w(st(w)) \cup \{\infty\}$, *onde* $st(w) = \{x \in Q^*;\ w(x^{-1}) = -w(x)\}$.

Exemplo 3.5 Seja $Q = M_n(D)$ um anel artiniano simples, onde D é anel de divisão, e $v : D \longrightarrow \Gamma \cup \{\infty\}$ uma valorização de D. Uma maneira natural de estender v à Q é definir:

$$\begin{array}{rcl} w : Q & \longrightarrow & \Gamma \cup \{\infty\} \\ (d_{ij}) & \longmapsto & min_{i,j}\{v(d_{ij})\} \end{array}$$

Vamos identificar D com o conjunto $\{(a_{ij}) \in M_n(D);\ a_{ii} = d \text{ e } a_{ij} = 0 \text{ para } i \neq j\}$. Assim, é fácil ver que $w|_D = v$. A função w satisfaz as condições da Definição 3.4.1. Para verificar essa afirmação, consideremos $x = (x_{ij})$, $y = (y_{ij}) \in Q$.

(a) Como $v(-1) = 0$, temos que $w(-1) = 0$.

(b) $w(x) = \infty \Leftrightarrow min_{i,j}\{v(x_{ij})\} = \infty \Leftrightarrow x_{ij} = 0, \forall\ i, j \Leftrightarrow x = 0$.

(c) Denotamos $xy = (u_{ij})$, com $u_{ij} = \sum_{k=1}^{n} x_{ik}y_{kj}$. Assim,

$w(xy) = min_{i,j}\{v(u_{i,j})\} \geq min_{i,j}\{min_k\{v(x_{ik}y_{kj})\}\} = min_{i,j}\{min_k\{v(x_{ik})+v(y_{kj})\}\}$

$\geq min_k\{v(x_{ik})\} + min_k\{v(y_{kj})\} = min_{i,k}\{v(x_{ik})\} + min_{j,k}\{v(y_{kj})\} = w(x) + w(y)$.

(d) $w(x + y) = min_{i,j}\{v(x_{ij} + y_{ij})\} \geq min_{i,j}\{min\{v(x_{ij}), v(y_{ij})\}\}$

$= min\{min_{i,j}\{v(x_{ij})\}, min_{i,j}\{v(y_{ij})\}\} = min\{w(x), w(y)\}$.

(e) Claro que $w(st(w)) \cup \{\infty\} \subseteq w(Q)$. Agora seja $y \in w(Q)$. Então existe $x = (x_{ij}) \in Q$ tal que $y = w(x) = min_{i,j}\{v(x_{ij})\} = v(x_{rs})$, para algum par $r, s \in \{1, 2, \cdots, n\}$. Se $y = \infty$, a prova é imediata. Assumindo $y \neq \infty$, temos $v(x_{rs}) \neq \infty$ o que implica em $x_{rs} \neq 0$. Escolhendo $z = (z_{ij})$, com $z_{ii} = x_{rs}$ e $z_{ij} = 0$ para $i \neq j$, temos que $z \in Q^*$. Como $w(z) = min\{v(0), v(x_{rs})\} = v(x_{rs})$ e $w(z^{-1}) = min\{v(0), v(x_{rs}^{-1})\} = v(x_{rs}^{-1}) = -v(x_{rs}) = -w(z)$, temos que $y = w(z) \in w(st(w))$.

Observação 3.11 Observando novamente que a Definição 3.4.1 foi motivada pelo exemplo acima, vemos que uma valorização em $Q = M_n(D)$ sempre pode ser construída a partir de uma valorização do anel de divisão D.

Observação 3.12 Para uma valorização $v : D \longrightarrow \Gamma \cup \{\infty\}$, onde D é um corpo ou um anel de divisão, vimos nas Definições 1.2.1 e 2.5.1, que não se fazia necessário exigir que $v(-1) = 0$, pois isso decorria de $v(1) = 0$, que por sua vez, era conseqüência da igualdade $v(xy) = v(x) + v(y)$. Também o item (e) da Definição 3.4.1 era imediato, já que para uma valorização v definida sobre um anel de divisão D (corpo inclusive), vimos no item (c) do Lema 2.5.1, que $v(x^{-1}) = -v(x)$, para todo $x \in D^*$. Logo, $st(v) = D^*$.

Observação 3.13 A diferença marcante entre a Definição 3.4.1 e as definições de valorização sobre corpos ou anéis de divisão é a desigualdade descrita no item (c), que aparece devido à necessidade de tratar com os possíveis divisores de zero de Q.

Seja Q um anel artiniano simples. Da mesma maneira que uma valorização definida sobre um corpo ou um anel de divisão, uma valorização $w : Q \longrightarrow \Gamma \cup \{\infty\}$ sempre pode ser considerada uma aplicação sobrejetora. Para isso, provaremos que $G = w(Q \setminus \{0\})$ é um subgrupo totalmente ordenado de Γ, e assim, podemos trocar Γ por G. Claro que G é totalmente ordenado, uma vez que $G \subseteq \Gamma$ e Γ é totalmente ordenado. Sejam $a, b \in G$,

$a = w(x)$, $b = w(y)$. Pelo item (e) da Definição 3.4.1, podemos escolher x e y tais que $w(x^{-1}) = -w(x)$ e $w(y^{-1}) = -w(y)$. Como $xy^{-1} \in Q \setminus \{0\}$ e $a - b = w(x) - w(y) = w(x) + w(y^{-1})$, o item (a) do lema abaixo mostra que $a - b = w(xy^{-1}) \in G$, e portanto G é um subgrupo de Γ.

Lema 3.4.1 *Seja Q um anel artiniano simples, $w : Q \longrightarrow \Gamma \cup \{\infty\}$ uma valorização de Q.*

(a) Se $x \in st(w)$ e $y \in Q$, então $w(xy) = w(yx) = w(x) + w(y)$;

(b) $w(1) = 0$;

(c) $w(-x) = w(x)$, para todo $x \in Q$;

(d) $st(w)$ é um subgrupo de Q^* e $w : st(w) \longrightarrow \Gamma$ é um homomorfismo.

Demonstração

(a) $w(y) = w(x^{-1}xy) \geq w(x^{-1}) + w(xy) = -w(x) + w(xy) \geq -w(x) + w(x) + w(y) = w(y)$. Logo, $w(x) + w(y) \geq w(xy) \geq w(x) + w(y)$. Portanto, $w(xy) = w(x) + w(y)$. Analogamente, prova-se que $w(yx) = w(x) + w(y)$.

(b) Como $w((-1)^{-1}) = w(-1) = 0 = -w(-1)$, temos que $-1 \in st(w)$. Assim, $w(1) = w((-1)(-1)) = w(-1) + w(-1) = 0$.

(c) $w(-x) = w(-1x) = w(-1) + w(x) = w(x)$.

(d) Sejam $a, b \in st(w)$. Temos que $w(a^{-1}) = -w(a)$ implica em $-w(a^{-1}) = w(a)$, isto é, $a^{-1} \in st(w)$. Agora, pelo item (a), $w((ab)^{-1}) = w(b^{-1}a^{-1}) = w(b^{-1}) + w(a^{-1}) = -w(b) - w(a) = -(w(a) + w(b)) = -w(ab)$, o que implica que $ab \in st(w)$. Portanto, $st(w)$ é um subgrupo de Q^* e assim, novamente por (a), $w : st(w) \longrightarrow \Gamma \cup \{\infty\}$ é um homomorfismo de grupos. $\square$

Seja Q um anel artiniano simples e w uma valorização de Q. Se $Q = \mathbb{K}$ é um corpo, a Definição 3.4.1 recai na Definição 1.2.1 e pelo Teorema 1.2.1, $R_w = \{x \in \mathbb{K};\ w(x) \geq 0\}$ é um anel de valorização de $\mathbb{K}$ e $J_w = \{x \in \mathbb{K};\ w(x) > 0\} = J(R_w) = \mathfrak{M}_{R_w} = R_w \setminus U(R_w)$. No Teorema 2.5.1 vimos que se $Q = D$ é um anel de divisão, então R_w é um anel de valorização total e invariante de D e $J_w = J(R_w) = R_w \setminus U(R_w)$ é o único ideal bilateral maximal de R_w. Com a ajuda do lema seguinte saberemos como esses fatos se estendem para um anel artiniano simples qualquer.

Lema 3.4.2 *Se Q é um anel artiniano simples e w é uma valorização de Q, então:*

(a) $R_w := \{x \in Q;\ w(x) \geq 0\}$ *é um subanel de Q;*

(b) $J_w := \{x \in Q;\ w(x) > 0\}$ *é um ideal bilateral próprio de R_w.*

(c) *Se $q \in Q \setminus R_w$, existem $r_1, r_2 \in R_w$ tais que $qr_1, r_2q \in R_w \setminus J_w$.*

Demonstração

(a) Como $w(0) = \infty$ e $w(1) = 0$, temos que $0, 1 \in R_w$. Sejam $a, b \in R_w$. Observe que $w(ab) \geq w(a) + w(b) \geq w(b) \geq 0$, o que implica que R_w é fechado para a multiplicação. Também R_w é fechado para diferenças, pois $w(a-b) = w(a+(-b)) \geq min\{w(a), w(-b)\} = min\{w(a), w(b)\} \geq 0$. Logo, R_w é subanel de Q.

(b) É fácil ver que J_w é fechado para diferenças e considerando $a \in J_w$ e $b \in R_w$, temos que $w(ab) \geq w(a) + w(b) \geq w(a) > 0$. Logo, $ab \in J_w$. Analogamente, $ba \in J_w$. Observe ainda que $1 \in R_w \setminus J_w$ e portanto J_w é um ideal bilateral próprio de R_w.

(c) Como $q \in Q \setminus R_w$, temos que $w(q) < 0$. Pelo item (e) da Definição 3.4.1, existe $x \in st(w)$ tal que $w(q) = w(x)$. Como $w(x^{-1}) = -w(x) = -w(q)$, temos que $w(x^{-1}) > 0$ e assim, $x^{-1} \in R_w$. Escolhendo $r_1 = r_2 = x^{-1} \in R_w$, segue que $w(qr_1) = w(qx^{-1}) = w(q) - w(x) = 0$, o que implica em $qr_1 \in R_w \setminus J_w$. Analogamente, $r_2q \in R_w \setminus J_w$. □

O lema garante que se R_w/J_w é um anel artiniano simples, então R_w é um anel de valorização de Dubrovin do anel artiniano simples Q, conforme a Definição 3.2.1. Lembre que nesse caso $J_w = J(R_w)$. Enunciaremos esses fatos na próxima proposição.

Nem sempre é válido que R_w/J_w é anel artiniano simples, mesmo impondo-se a condição de Q ter dimensão finita sobre seu centro, conforme o Exemplo 3.7, que apresentaremos após a Proposição 3.4.3.

Definição 3.4.2 *Seja R um subanel do anel artiniano simples Q. O estabilizador de R é o conjunto $st(R) := \{x \in Q^*;\ xRx^{-1} = R\}$.*

Não é difícil verificar que $(st(R), \cdot)$ é subgrupo de $(Q^*, \cdot)$. Caso Q seja um corpo, o subgrupo $st(R)$ é todo o grupo Q^*. Além disso, se Q é um anel de divisão e R é um anel de valorização total e invariante de D, também temos $st(R) = Q^*$.

Outro fato a ser destacado é que sendo w uma valorização do anel artiniano simples Q, temos $st(w) \subseteq st(R_w)$. De fato, para $s \in st(w)$ e $x \in R_w$, temos que $w(sxs^{-1}) =$

$w(s) + w(x) + w(s^{-1}) = w(x) \geq 0$, o que implica em $sR_w s^{-1} \subseteq R_w$. Analogamente, $s^{-1}R_w s \subseteq R_w$ implica em $R_w \subseteq sR_w s^{-1}$. Portanto, $s \in st(R_w)$ e $st(w) \subseteq st(R_w)$.

Agora já podemos demonstrar a seguinte proposição.

Proposição 3.4.1 *Seja w uma valorização do anel artiniano simples Q. Se R_w/J_w é anel artiniano simples, então R_w é anel de valorização de Dubrovin de Q com $J(R_w) = J_w$, e para cada $x \in Q \setminus \{0\}$, existe $\alpha \in st(R_w)$ tal que $R_w x R_w = \alpha R_w$.*

Demonstração

Já vimos que se R_w/J_w é anel artiniano simples, então R_w é anel de valorização de Dubrovin de Q com $J(R_w) = J_w$. Então seja $x \in Q \setminus \{0\}$. Sabemos que existe $\alpha \in st(w)$ tal que $w(x) = w(\alpha)$. Assim, $w(x) + w(\alpha^{-1}) = 0$ implica em $w(x\alpha^{-1}) = 0$, isto é, $x\alpha^{-1} \in R_w \setminus J(R_w)$. Concluímos que $x\alpha^{-1} \in R_w x\alpha^{-1} R_w$ e $x\alpha^{-1} \notin J(R_w)$. Conforme observamos após a Definição 3.2.1, os ideais bilaterias de R_w estão totalmente ordenados por inclusão, assim $J(R) \subsetneqq R_w x\alpha^{-1} R_w$. Pelo Lema 3.2.1, $J(R_w)$ é o único ideal bilateral maximal de R_w. Portanto, $R_w x\alpha^{-1} R_w = R_w$. Agora, como $st(w) \subseteq st(R_w)$, temos que $\alpha \in st(R_w)$, isto é, $\alpha^{-1} R_w = R_w \alpha^{-1}$ e $R_w \alpha = \alpha R_w$. Portanto, $R_w x R_w = \alpha R_w$. □

Pela proposição, dada uma valorização w de Q tal que R_w/J_w é anel artiniano simples, associamos o anel de valorização de Dubrovin R_w de Q.

Da mesma maneira que nos capítulos anteriores, trabalharemos com classes de valorizações de Q. Nosso objetivo é provar que existe uma correspondência biunívoca entre os conjuntos

$\mathcal{W} = \{[w];\ w$ valorização de Q, tal que R_w/J_w é anel artiniano simples$\}$

$\mathcal{R} = \{R;\ R$ anel de valorização de Dubrovin de Q e se $x \in Q \setminus \{0\}$, existe $\alpha \in st(R)$ tal que $RxR = \alpha R\}$.

Definição 3.4.3 *Sejam v e w valorizações de Q. Dizemos que v é equivalente a w ($v \sim w$) quando $R_v = R_w$.*

É fácil provar que $\sim$ é uma relação de equivalência.

Denotando por $[w]$ a classe de equivalência da valorização w, temos a aplicação

$$\begin{aligned} \psi : \mathcal{W} &\longrightarrow \mathcal{R} \\ [w] &\longmapsto R_w \end{aligned}$$

que está bem definida tendo em vista a Proposição 3.4.1. Para verificar que a aplicação ψ é uma bijeção, construiremos a inversa ϕ de ψ. Para isso, dado um anel de valorização de Dubrovin R de Q, tal que para todo $x \in Q \setminus \{0\}$, existe $\alpha \in st(R)$, tal que $RxR = \alpha R$, precisamos construir uma valorização w de Q, tal que $R_w = R$ e $J_w = J(R)$. Iniciaremos construindo o grupo de valores para tal valorização w.

Seja R um anel de valorização de Dubrovin do anel artiniano simples Q. No conjunto

$$\Gamma_R = \{RqR;\ q \in Q \setminus \{0\} \text{ e existe } \alpha_q \in st(R) \text{ tal que } RqR = \alpha_q R\}$$

definimos a operação

$$Rq_1R + Rq_2R = \alpha_{q_1}\alpha_{q_2}R$$

e a relação

$$Rq_1R \leq Rq_2R \Leftrightarrow Rq_2R \subseteq Rq_1R.$$

Observe que $Rq_1R + Rq_2R$ é exatamente o produto $(Rq_1R)(Rq_2R)$, pois $\alpha_{q_1}\alpha_{q_2}R = \alpha_{q_1}R\alpha_{q_2}R = (Rq_1R)(Rq_2R)$.

Lema 3.4.3 *Com a notação estabelecida acima,* $(\Gamma_R, +)$ *é um grupo aditivo, abeliano e totalmente ordenado pela relação* $\leq$*. Mais ainda,* $\Gamma_R \simeq \frac{st(R)}{U(R)}$.

Demonstração

Inicialmente verificaremos que a operação $+$ é fechada em Γ_R e também está bem definida em Γ_B. Temos $Rq_1R+Rq_2R = \alpha_{q_1}\alpha_{q_2}R = R\alpha_{q_1}\alpha_{q_2}R \in \Gamma_R$, pois $\alpha_{q_1}\alpha_{q_2} \in st(R) \subseteq Q\setminus\{0\}$. Isso diz que $+$ é uma operação fechada em Γ_R. Provemos que $+$ está bem definida. Consideremos $Rq_1R = R\hat{q}_1R$ e $Rq_2R = R\hat{q}_2R$. Assim, $\alpha_{q_1}R = \alpha_{\hat{q}_1}R$ e $\alpha_{q_2}R = \alpha_{\hat{q}_2}R$. Dessa forma, para $x \in R$, $\alpha_{q_1}\alpha_{q_2}x = \alpha_{q_1}\alpha_{\hat{q}_2}r = \alpha_{q_1}s\alpha_{\hat{q}_2} = \alpha_{\hat{q}_1}y\alpha_{\hat{q}_2} = \alpha_{\hat{q}_1}\alpha_{\hat{q}_2}z$, com $r, s, y, z \in R$. Dessa maneira, $\alpha_{q_1}\alpha_{q_2}R \subseteq \alpha_{\hat{q}_1}\alpha_{\hat{q}_2}R$. Analogamente, prova-se que $\alpha_{\hat{q}_1}\alpha_{\hat{q}_2}R \subseteq \alpha_{q_1}\alpha_{q_2}R$ e assim, $\alpha_{q_1}\alpha_{q_2}R = \alpha_{\hat{q}_1}\alpha_{\hat{q}_2}R$, isto é, $Rq_1R+Rq_2R = R\hat{q}_1R+R\hat{q}_2R$, o que mostra que a soma está bem definida em Γ_R. Vamos provar que $(\Gamma_R, +)$ é grupo. É fácil ver que o neutro é R. O inverso de $RqR = \alpha R \in \Gamma_R$ é $R\alpha^{-1}R = \alpha^{-1}R$, pois $RqR + R\alpha^{-1}R = \alpha R + \alpha^{-1}R = R$. Claro que $R\alpha^{-1}R \in \Gamma_R$, pois do fato de $st(R)$ ser grupo decorre que $\alpha^{-1} \in st(R)$. De ([D$_2$], §2, Proposition 4), concluímos que Γ_B é abeliano. Segue de ([D$_1$], §2, Theorem 4) que Γ_B é totalmente ordenado por inclusão. Resta demonstrar o isomorfismo $\Gamma_R \simeq$

$\frac{st(R)}{U(R)}$. Note que o quociente está bem definido, pois $U(R)$ é um subgrupo normal de $st(R)$. Consideremos a aplicação $\varphi : \frac{st(R)}{U(R)} \longrightarrow \Gamma_R$, dada por $\varphi(qU(R)) = RqR = qR$. Primeiramente provemos que φ é um homomorfismo. Sejam $q_1, q_2 \in st(R)$. Note que $\varphi(q_1U(R)q_2U(R)) = \varphi(q_1q_2U(R)) = Rq_1q_2R = (Rq_1R)(Rq_2R) = \varphi(q_1U(R)) + \varphi(q_2U(R))$. Afirmamos que $Ker(\varphi) = U(R)$. De fato, $qU(R) \in Ker(\varphi)$ implica em $\varphi(qU(R)) = R$, isto é, $RqR = R$. Como $q \in st(R)$, temos que $RqR = Rq = R$ e assim, $q \in U(R)$. Também φ é sobrejetora, pois dado $RqR \in \Gamma_R$, sabemos que existe $\alpha \in st(R)$ tal que $\alpha R = RqR$. Assim, escolhendo $\alpha U(R) \in \frac{st(R)}{U(R)}$, temos que $\varphi(\alpha U(R)) = R\alpha R = RqR$. Portanto, $\Gamma_R \simeq \frac{st(R)}{U(R)}$. $\square$

Agora utilizaremos o grupo Γ_R construído acima, para definir a aplicação

$$\begin{aligned} w : Q &\longrightarrow \Gamma_R \cup \{\infty\} \\ 0 &\longmapsto \infty \\ 0 \neq x &\longmapsto RxR \end{aligned}$$

Proposição 3.4.2 *A aplicação w é uma valorização de Q com $R_w = R$ e $J_w = J(R)$.*
Demonstração

Verificaremos os itens (a) à (e) da Definição 3.4.1. A prova de (a) e (b) é imediata. Para verificar (c) e (d), consideremos $x, y \in Q$. Se $x + y = 0$, é imediato que $\infty = w(x + y) \geq min\{w(x), w(y)\}$. Vamos supor $x + y \neq 0$ e $w(x) \geq w(y)$. Temos $RxR \subseteq RyR$ e também $x+y \in RyR$. Segue que $R(x+y)R \subseteq RyR$, ou seja, $w(x+y) \geq w(y) = min\{w(x), w(y)\}$. Isso prova o item (d). Como $xy \in (RxR)(RyR)$, temos $RxyR \subseteq (RxR)(RyR)$ e com isso, $w(xy) \geq w(x) + w(y)$, o que prova (c). Resta provar (e), isto é, mostrar que $w(st(w)) \cup \{\infty\} = w(Q)$. A inclusão $w(st(w)) \cup \{\infty\} \subseteq w(Q)$ é óbvia. Para provar a inclusão contrária observemos inicialmente que $w(Q) = w(st(R))$. De fato, se $w(q) \in w(Q)$, temos que $w(q) = RqR = \alpha R$, para algum $\alpha \in st(R)$ e como $w(\alpha) = R\alpha R = \alpha R = w(q)$, temos que $w(q) \in w(st(R))$. Agora, se $s \in st(R)$, então $w(s^{-1}) + w(s) = Rs^{-1}R + RsR = s^{-1}sR = R$ e assim, $w(s^{-1}) = -w(s)$, isto é, $s \in st(w)$. Logo, $st(R) \subseteq st(w)$. Dessa maneira, $w(Q) = w(st(R)) \subseteq w(st(w))$ e concluímos a prova de que w é uma valorização de Q. Finalmente, note que $RxR \subseteq R \Leftrightarrow w(x) \geq w(1) = 0$ implica em $R = \{x \in Q;\ w(x) \geq 0\} := R_w$. Provemos agora que $J(R) = \{x \in Q;\ w(x) > 0\}$. Se $x \in J(R)$, temos que $RxR \subseteq J(R) \subsetneqq R$ implica em $w(x) > 0$. Por outro lado, se $x \in Q$ e $w(x) > 0$, temos que

$x \in R$ e $RxR \subsetneqq R$. Podemos ter $J(R) \subseteq RxR$ ou $RxR \subseteq J(R)$. A primeira possibilidade não ocorre pois $J(R)$ é maximal e $RxR \subsetneqq R$. Só resta $RxR \subseteq J(R)$ e assim $x \in J(R)$. $\square$

Recordemos que

- $\mathcal{W} = \{[w];\ w$ valorização de $Q,$ tal que R_w/J_w é anel artiniano simples$\}$
- $\mathcal{R} = \{R;\ R$ anel de valorização de Dubrovin de Q e se $x \in Q \setminus \{0\}$, existe $\alpha \in st(R)$ tal que $RxR = \alpha R\}$.

Assim, podemos finalmente definir a aplicação

$$\begin{aligned} \phi : \mathcal{R} &\longrightarrow \mathcal{W} \\ R &\longmapsto [w] \end{aligned}$$

onde w é a valorização associada a R. O teorema seguinte afirma que ϕ é a inversa da aplicação

$$\begin{aligned} \psi : \mathcal{W} &\longrightarrow \mathcal{R} \\ [w] &\longmapsto R_w \end{aligned}$$

Teorema 3.4.1 *Seja Q um anel artiniano simples. Existe uma correspondência biunívoca entre as classes de valorizações $[w]$ de Q tais que R_w/J_w é anel artiniano simples e os anéis de valorização de Dubrovin R de Q, tais que dado $x \in Q \setminus \{0\}$, existe $\alpha \in st(R)$ tal que $RxR = \alpha R$.*

Demonstração

Não é difícil verificar que $\psi(\phi(R)) = R$ e $\phi(\psi[w]) = [w]$. $\square$

Teorema 3.4.2 ([MMU] p. 70, Theorem 12.3) *Seja Q um anel artiniano simples de dimensão finita sobre seu centro e seja R um anel de valorização de Dubrovin de Q com $V = Z(R)$. São equivalentes:*

(i) R é integral sobre V;

(ii) Dado $x \in Q \setminus \{0\}$, existe $\alpha \in st(R)$ tal que $RxR = \alpha R$.

Combinando o Teorema 3.4.2 com as Proposições 3.4.2 e 3.4.1, obtemos o seguinte corolário.

Corolário 3.4.1 *Seja Q um anel artiniano simples de dimensão finita sobre seu centro e R um anel de valorização de Dubrovin de Q. Existe uma valorização w em Q tal que $R_w = R$ e $J_w = J(R)$ se, e somente se, R é integral sobre $V = Z(R)$.*

Observe que no caso de Q ser um corpo, tal valorização w sempre existe e é uma valorização no sentido que definimos para corpos, recaindo nos resultados do Capítulo 1.

Em seguida apresentaremos uma proposição que fornece uma ferramenta útil para a construção de valorizações sobre anéis artinianos simples.

Proposição 3.4.3 *Seja Q um anel artiniano simples de dimensão $n < \infty$ sobre seu centro $\mathbb{F}$, $\{a_1 = 1, a_2, \cdots, a_n\}$ uma $\mathbb{F}-$base de Q e $v : \mathbb{F} \longrightarrow \Gamma \cup \{\infty\}$ uma valorização de $\mathbb{F}$. A aplicação*

$$\begin{array}{rcl} w : Q & \longrightarrow & \Gamma \cup \{\infty\} \\ \sum_{i=1}^{n} a_i x_i & \longmapsto & min_i\{v(x_i)\} \end{array}$$

é tal que $w|_{\mathbb{F}} = v$. Também, para que w defina uma valorização em Q é necessário e suficiente que $w(a_i a_j) \geq 0$, para todos $i, j \in \{1, 2, \cdots, n\}$.

Demonstração

Como $a_1 = 1$, é claro que $w|_{\mathbb{F}} = v$. A necessidade é fácil de ser provada, pois se w é uma valorização de Q, vale que $w(xy) \geq w(x) + w(y)$, para todos $x, y \in Q$. Em particular, $w(a_i a_j) \geq w(a_i) + w(a_j) = v(1) + v(1) = 0$. Para provar a suficiência, vamos verificar os itens (a) à (e) da Definição 3.4.1.

(a) Como $v(-1) = 0$, é claro que $w(-1) = 0$.

(b) $v(\sum_{i=1}^{n} a_i x_i) = min_i\{v(x_i)\} = \infty$ se, e somente se, $x_i = 0$, para todo i. Isso equivale a dizer que $\sum_{i=1}^{n} a_i x_i = 0$.

Para o restante consideremos $x, y \in Q$, $x = \sum_{i=1}^{n} a_i x_i$, $y = \sum_{i=1}^{n} a_i y_i$.

(d) Temos que $x+y = \sum_{i=1}^{n} a_i(x_i+y_i)$ e $w(x+y) = min_i\{v(x_i+y_i)\} \geq min_i\{min\{v(x_i), v(y_i)\}\}$ $= min\{min_i\{v(x_i)\}, min_i\{v(y_i)\}\} = min\{w(x), w(y)\}$.

(e) A inclusão $w(st(w)) \cup \{\infty\} \subseteq w(Q)$ é direta. Para a inclusão contrária, tome $w(x) \in w(Q)$. Podemos supor $\infty \neq w(x) = w(\sum_{i=1}^{n} a_i x_i) = min_i\{v(x_i)\}$, o que implica que existe $j \in \{1, 2, \cdots, n\}$ tal que $w(x) = v(x_j)$ e $0 \neq x_j \in \mathbb{F}$. Escolhendo $s = 1x_j \in Q^*$, obtemos $w(s^{-1}) = w(x_j^{-1}) = v(x_j^{-1}) = -v(x_j) = -w(s)$. Portanto, $s \in st(w)$ e $w(s) = w(x)$, o que prova que $w(Q) \subseteq w(st(w)) \cup \{\infty\}$.

(c) Temos que $xy = \sum_{i,j=1}^{n} a_i a_j x_i y_j$. Denotando $a_i a_j = \sum_{r=1}^{n} a_r t_{ijr}$ segue que $min_r\{v(t_{ijr})\} = w(a_i a_j) \geq 0$, e assim $v(t_{ijr}) \geq 0$ para todos $i, j, r \in \{1, 2, \cdots, n\}$.

Também $xy = \sum_{i,j=1}^{n} (\sum_{r=1}^{n} a_r t_{ijr}) x_i y_j = \sum_{r=1}^{n} a_r (\sum_{i,j=1}^{n} t_{ijr} x_i y_j)$. Assim,

$$\begin{aligned} w(xy) &= min_r\{v(\textstyle\sum_{i,j=1}^{n} t_{ijr} x_i y_j)\} \\ &\geq min_r\{min_{i,j}\{v(t_{ijr} x_i y_j)\}\} \\ &= min_r\{min_{i,j}\{v(t_{ijr}) + v(x_i) + v(y_j)\}\} \\ &\overset{(1)}{\geq} min_{i,j}\{v(x_i) + v(y_j)\} \\ &= min_{i,j}\{v(x_i) + v(y_j)\} \\ &= w(x) + w(y). \end{aligned}$$

Observe que utilizamos a hipótese $w(a_i a_j) \geq 0$ na passagem assinalada com (1). Concluímos assim que w é uma valorização de Q. $\square$

Exemplo 3.6 Seja $\mathbb{H}$ a álgebra de divisão dos quatérnios com centro $\mathbb{Q}$ e base $\{a_1 = 1, a_2 = i, a_3 = j, a_4 = k\}$. Consideremos a valorização $p-$ádica $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$. Definimos

$$\begin{aligned} w_p : \mathbb{H} &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ \textstyle\sum_{r=1}^{4} a_r x_r &\longmapsto min_r\{v_p(x_r)\} \end{aligned}$$

Observe que $w_p(a_r a_s) = 0$ para todos $r, s \in \{1, 2, 3, 4\}$ e assim, pela Proposição 3.4.3, w_p é uma valorização de $\mathbb{H}$. Note ainda que $R_{w_p} = \{q \in \mathbb{H};\ w_p(q) \geq 0\} = \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)} i + \mathbb{Z}_{(p)} j + \mathbb{Z}_{(p)} k$. De fato, $q = \sum_{r=1}^{4} a_r x_r \in R_{w_p}$ implica em $w_p(q) = min_r\{v_p(x_r)\} \geq 0$. Isso é equivalente a $v_p(x_r) \geq 0$, para todo $r \in \{1, 2, 3, 4\}$, isto é, $q \in \mathbb{Z}_{(p)} + \mathbb{Z}_{(p)} i + \mathbb{Z}_{(p)} j + \mathbb{Z}_{(p)} k$. Na segunda seção deste capítulo, vimos que para $p \neq 2$, $\mathbb{Z}_{(p)} + \mathbb{Z}_{(p)} i + \mathbb{Z}_{(p)} j + \mathbb{Z}_{(p)} k$ é anel de valorização de Dubrovin de $\mathbb{H}$ e portanto, w_p é uma valorização de $\mathbb{H}$ tal que R_{w_p} é anel de valorização de Dubrovin de $\mathbb{H}$.

Exemplo 3.7 No exemplo anterior, se $p = 2$, temos que w_2 é uma valorização de $\mathbb{H}$. Entretanto, R_{w_2} não é anel de valorização de Dubrovin de $\mathbb{H}$, pois como pode ser visto em ([W$_1$], §1, Example (c)), o anel $\tilde{V}_{(2)} = \mathbb{Z}_{(2)}\alpha + \mathbb{Z}_{(2)} i + \mathbb{Z}_{(2)} j + \mathbb{Z}_{(2)} k$, onde $\alpha = \frac{1}{2}(1 + i + j + k)$, é o único anel de valorização de Dubrovin de $\mathbb{H}$ tal que $\tilde{V}_{(2)} \cap \mathbb{Q} = \mathbb{Z}_{(2)}$. Nesse caso, $\frac{R_{w_2}}{J(R_{w_2})}$ não é anel artiniano simples.

Referências Bibliográficas

[A] Atiyah, M. F. *Introduction al Algebra Commutativa.* Barcelona, Reverte, 1973.

[B] Bagio, D. *Anéis Quocientes Clássicos e Localização Não Comutativa.* Dissertação de Mestrado. Florianópolis, UFSC, 2000.

[Bo] Bourbaki, N. *Commutative Algebra.* Paris, Herman, 1972.

[Br] Brungs, H. H. *Noncommutative Valuation Ring*, Perspectives in Ring Theory, 233 (1988), 105-115.

[BrG_1] Brungs, H.H. and Gräter, J., *Valuation Rings in Finite Dimensional Division Algebras*, J. Algebra, 120, (1989), 90-99.

[BrG_2] Brungs, H.H. and Gräter, J., *Extensions of Valuation Rings in Central Simple Algebras*, Trans. Amer. Math. Soc. 317 (1990), 287-302.

[C] Cohn, P. M. *On Extending Valuation in Division Algebras*, Studia Scient. Math. Hung., 16, (1981), 65-70.

[D_1] Dubrovin, N. I. *Noncommutative Valuation Rings*, Trudy Moskov. Mat. Obshch. 45, (1982) 265-280 (Russia); English transl.: Trans. Moscow Math. Soc. 45 (1984), 273-287.

[D_2] Dubrovin, N. I. *Noncommutative Valuation Rings in Simple Finite Dimensional Algebras Over a Field*, Mat. Sbornik 123 (1984), 496-509. English transl.: Math. USSR Sb, 51 (1985), 493-505.

[E] Endler, O. *Valuation Theory.* New York, Springer-Verlag, 1972.

[F] Ferrero, M. *Notas da XVI Escola de Álgebra*, Universidade de Brasília, Brasília, 2000.

[H] Hasse, H. *Number Theory*. New York, Springer-Verlag, 1980.

[Ha] Herstein, I. N. *Topics in Algebra*. New York, John Wiley & Sons, 1975.

[G] Gonçalves, A. *Introdução à Álgebra*. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 1979.

[Go] Goodearl, K. R. *Ring Theory: Nonsingular Rings and Modules*. Marcel Dekker, New York, 1976.

[L] Lam, T.Y. *A First Course in Noncommutative Rings*. Berlin, Springer-Verlag, 1991.

[MMU] H. Marubayashi, H. Miyamoto e A. Ueda *Non-Commutative Valuation Rings and Semi-Hereditary Orders*. Kluwer, Dordrecht, 1997.

[Mo] Morandi, P. J. *Value Functions on Central Simple Algebras*, Trans. Amer. Math. Soc., 315 (1989), 606-622.

[Re] Reiner, I. *Maximal Orders*. Londres, Academic Press, 1975.

[Ri] Ribenboim, P. *Théorie des Valuations*. Montréal, Presses Univ. Montréal, 1968.

[S] Pierre, S. *Algebraic Theory of Numbers*. Paris, Hermann, 1970.

[Sa] Santos, J. P. O., *Introdução à Teoria dos Números*. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, CNPq, 1998.

[Br] Brungs, H. H. *Noncommutative Valuation Ring*, Perspectives in Ring Theory, 233, (1988), 105-115.

[W_1] Wadsworth, A. R. *Dubrovin Valuation Rings*, Perspectives in Ring Theory, 233, (1988) 359-374.

[W_2] Wadsworth, A. R. *Extending Valuations to Finite Division Algebras*, Proceedings of the Amer. Math. Soc., 98 (1986), 20-22.

[W_3] Wadsworth, A. R. *Dubrovin Valuation Rings and Henselization*, Math. Ann. 283 (1989), 301-328.