KLEBER CUSTÓDIO

INTRODUÇÃO AO ESTUDO DOS CORPOS ORDENADOS

Santo André, 2015

UNIVERSIDADE FEDERAL DO ABC

CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO

KLEBER CUSTÓDIO

INTRODUÇÃO AO ESTUDO DOS CORPOS ORDENADOS

Orientador: Prof. Dr. Vinicius Cifú Lopes

Dissertação de mestrado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Mestre.

ESTE EXEMPLAR CORRESPONDE A VERSÃO FINAL DA DISSERTAÇÃO
DEFENDIDA PELO ALUNO KLEBER CUSTÓDIO,
E ORIENTADA PELO PROF. DR. VINICIUS CIFÚ LOPES.

SANTO ANDRÉ, 2015

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Custódio, Kleber
Introdução ao Estudo dos Corpos Ordenados / Kleber Custódio. — 2015.

69 fls.

Orientador: Vinicius Cifú Lopes

Dissertação (Mestrado) — Universidade Federal do ABC, Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Santo André, 2015.

1. Corpo. 2. Estrutura algébrica. 3. Corpo ordenado. I. Lopes, Vinicius Cifú. II. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, 2015. III. Título.

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017
profmat@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Kleber Custodio, realizada em 16 de novembro de 2015:

Prof.(a) Dr.(a) **Vinicius Cifú Lopes** (UFABC) – Presidente

Prof.(a) Dr.(a) **Daniel Miranda Machado** (UFABC) – Membro Titular

Prof.(a) Dr.(a) **Hugo Luiz Mariano** (USP) – Membro Titular

Prof.(a) Dr.(a) **Sinue Dayan Barbero Lodovici** (UFABC) – Membro Suplente

Prof.(a) Dr.(a) **Francisco Miraglia Neto** (USP) – Membro Suplente

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, _____de _____ de 20___.

Assinatura do autor: _____

Assinatura do orientador: _____

À minha família pelo apoio e incentivo.

AGRADECIMENTOS

Agradeço,

Primeiramente, a Deus que me propiciou a vida, a saúde e as demais condições necessárias à minha jornada até este momento.

À minha mãe que sempre me incentivou.

Aos meus amigos do Mestrado Profissional que sempre colaboraram com a minha aprendizagem e aprimoramento.

Aos professores da UFABC pela atenção desprendida e por compartilharem os seus saberes comigo.

Ao meu orientador professor Vinicius Cifú Lopes pelas valiosas sugestões.

Aos professores da banca de avaliação: Daniel Miranda Machado, Hugo Luis Mariano e Vinicius Cifú Lopes.

Aos funcionários da UFABC que sempre foram muito gentis e atenciosos para com as minhas solicitações.

À SBM e a UFABC pela realização do programa.

À CAPES pelo suporte financeiro.

RESUMO

O objetivo deste trabalho é apresentar uma introdução ao estudo de uma classe de estruturas algébricas denominadas corpos, utilizando linguagem e exemplos acessíveis aos estudantes do ensino básico. No início, coloca-se a importância da álgebra axiomática, para em seguida desenvolver a noção de estruturas algébricas e a definição de corpo. Esta é apresentada com axiomas, que são utilizados para deduzir algumas das propriedades dos corpos. Posteriormente, são apresentados alguns casos de corpos que aparecem na literatura matemática. Destaque é dado aos corpos munidos de uma ordem linear e sua semelhança com o corpo dos números reais e também são tratados alguns conceitos que possuem papéis relevantes no estudo dos corpos.

Palavras-chave: corpo, estrutura algébrica, corpo ordenado.

ABSTRACT

Our goal is to introduce a class of algebraic structures called fields, using examples in a way suitable to high school students. Firstly, we show the importance of axiomatic algebra, and then develop the notion of algebraic structures and fields. In turn, axioms are used to define fields and to deduce some further properties. Later, we present some examples of fields that appear in the mathematical literature. Emphasis is given to fields provided with a linear order and their similarity to the real line, and some concepts that are relevant for the study of fields are also treated.

Keywords : field, algebraic structure, ordered field.

CONTEÚDO

Introdução 1

1 NOÇÕES DE ESTRUTURAS ALGÉBRICAS E CORPOS 5

1.1 Estruturas Algébricas 5

1.2 Corpo 6

1.3 Dedução de propriedades dos corpos a partir dos axiomas 8

1.4 Exemplos de corpos 13

2 DEFINIÇÕES E EXEMPLOS DE ALGUNS CORPOS 17

2.1 Corpo dos inteiros módulo primo 17

2.2 Característica de um corpo 22

2.3 Corpo algebricamente fechado 23

2.4 Relações de ordem 24

2.5 Corpo ordenado 26

3 CLASSES DE CORPOS ORDENADOS 32

3.1 Majorante e minorante, máximo e mínimo, supremo e ínfimo 32

3.2 Corpo arquimediano 36

3.3 Corpo ordenado completo 37

3.4 Corpo formalmente real 41

3.5 Corpo real fechado 43

3.6 Corpo de funções racionais dos reais e infinitésimos 46

Conclusão 50

A APÊNDICE A 51

A.1 Noções de Estruturas Algébricas de Anéis 51

A.2 Definições e exemplos de alguns tipos de Anéis 52

Bibliografia 55

INTRODUÇÃO

A Álgebra sempre teve como campos de trabalho o estudo das operações, regras de cálculo e procedimentos para solução de equações, sendo este último um dos principais problemas da Álgebra.

Uma significativa mudança na forma de trabalhar com a Álgebra e com a Matemática ocorreu durante os séculos XVIII e XIX quando os avanços nas teorias de números e conjuntos, e, também nas notações, colocaram as condições para que a Álgebra se tornasse axiomática.

A partir do momento que a Álgebra torna-se axiomática, propriedades de operações algébricas podem ser estudadas sem especificar o conjunto ou elementos sobre os quais a operação é realizada, tampouco é necessário definir o método de cálculo que será empregado para obter o resultado da operação. Esse trabalho de álgebra completamente axiomático é realizado da seguinte forma: coloca-se como hipótese um conjunto de propriedades e passa-se a verificar a sua validade para determinada operação, então tudo que é deduzido a partir dessa hipótese também vale para a operação.

Esse conjunto de propriedades a ser verificado sobre determinada operação é a chamada teoria algébrica que, atualmente, desempenha papel central na Matemática, pois caracteriza, classifica, permite uma previsibilidade de resultados, enfim, coloca uma organização teórica básica em diferentes ramos da Matemática.

Um universo sujeito a operações e relações é uma estrutura, em que a teoria pode ou não valer.

Considerando a importância dessas estruturas algébricas abstratas na Matemática do ensino básico e superior, será abordada ao longo desse trabalho uma classe particular dessas estruturas denominada de corpo.

Ao longo desse estudo básico das estruturas algébricas dos corpos o leitor perceberá que diversas propriedades, conceitos e exemplos aqui tratados estão presentes nos conteúdos do ensino fundamental e médio, e que uma base mais sólida dessas propriedades, conceitos e exemplos pode colaborar com a aprendizagem do estudante e com a prática pedagógica do professor do ensino básico.

A apresentação dos conteúdos desse trabalho e as bibliografias utilizadas para pesquisa em cada seção estão elencadas abaixo:

Introdução; bibliografia: Fernandes; Ricou (2004, p. 9-12) e Milies (2004, p. 3-13, 39-46).

O capítulo 1, que tem o objetivo de definir corpos, traz na:

- seção 1.1, a definição de estruturas algébricas de uma forma simples e objetiva; bibliografia: Castrucci (1969, p. 101-109), Fernandes; Ricou (2004, p. 9-12), e Milies (2004, 39-46).

- seção 1.2, a definição de corpo a partir dos axiomas que são válidos para essa estrutura nas operações de adição (+) e multiplicação (.); bibliografia: Fernandes; Ricou (2004, p. 32-38), Garcia; Lequain (2010, p. 7-11), Hefez (2002, vol. 1, p. 132-135) e Monteiro (1978, p. 178-179).

- seção 1.3, algumas das propriedades de corpo deduzidas a partir dos axiomas de corpo; bibliografia: Domingues; Iezzi (2003, p.211-213, 223-225), Fernandes; Ricou (2004, 32-39), Hefez (2002, vol. 1, 132-135), Lopes (2015, p. 33-37), Marques (2005, p. 10-15) e Monteiro (1978 p. 178-180).

- seção 1.4, alguns exemplos de corpo; bibliografia: Castrucci (1969, p. 107-109), Fernandes; Ricou (2004, p. 37), Garcia; Lequain (2010, p. 10), Marques (2005, p. 15) e Monteiro (1978, cap. 4 e 5).

O capítulo 2, que tem como objetivo estudar alguns casos de corpos e suas propriedades e, também, outras definições necessárias ao estudo desses corpos, traz na:

- seção 2.1, as considerações básicas sobre módulo e classes residuais e as condições que levam um conjunto de inteiros módulo p, p primo, a ser um corpo; bibliografia: Domingues; Iezzi (2003, 133-136), Fernandes; Ricou (2004, p. 115-124), Garcia; Lequain (2010, p. 11-14), Hefez (2002, vol. 1, p. 116-122), Hefez (2006, p. 53-63), Lipschutz (1972, p. 388-389), Marques (2005, p. 7-15), Monteiro (1978, p. 180-184) e Shokranian (2010, p. 39-56).

- seção 2.2, a propriedade denominada de característica de um corpo que aparece em várias proposições e teoremas dos corpos; bibliografia: Domingues; Iezzi (2003, p. 252-253), Fernandes; Ricou (2004, p. 91), Griese (2015, p. 1), Hefez (2002, vol. 1, p. 143-144), Marques (2005, p. 16), Monteiro (1978, p. 210), Polizeli (2007, p. 4) e Shokranian (2010, p. 96).

- seção 2.3, a definição e alguns exemplos de corpos algebricamente fechados; bibliografia: Hefez (2002, vol. 1, cap. 9), Lipschutz (1972, p. 398), Monteiro (1978, p. 268-272, 435-443) e Polizeli, (2007, p. 13-14).

- seção 2.4, as relações de ordem utilizando as notações de teoria dos conjuntos; bibliografia: Almay (1975, p. 24-25), Castrucci (1969, p. 79), Guidorizzi (1987, Vol. 1, p. 6-7), Lopes (2015, p. 37) e Monteiro (1978, p. 22-25).

- seção 2.5, a apresentação de corpos ordenados utilizando os axiomas de ordem e depois por meio do cone positivo, e a seguir é mostrado que as duas definições equivalem; bibliografia: Domingues; Iezzi (2003, p. 276-277), Martin (2010, p. 388-391), Monteiro (1978, p. 227-231) e Souza (2013, p. 32-33).

O capítulo 3, que tem como objetivo estudar a classe dos corpos ordenados e as definições e conceitos necessários para estudo deste tema, traz na:

- seção 3.1, os conceitos que permitem enunciar a propriedade da completude, tais como: majorante e minorante, máximo e mínimo, supremo e ínfimo; bibliografia: Almay (1975, p. 30-36), Dutra (2014, p. 53-59), Guidorizzi (1987, vol. 1, p. 20-29), Lima; Carvalho; Wagner; Morgado (2012. vol. 1, p. 67-76), Lopes (2015, p. 40-46) e Monteiro (1978, p. 25-27, 234-255).

- seção 3.2, a definição e exemplos de corpos arquimedianos; bibliografia: Hefez (2002, vol. 1, p. 154-155), Monteiro (1978, p. 228-229), e Souza (2013, p. 35).

- seção 3.3, o conceito de corpo ordenado completo, exemplos e contraexemplos com breves comentários; bibliografia: Dutra (2014, p. 53-59), Fernandes; Ricou (2004, p. 186-192), Hefez (2002, vol. 1, p. 166-176), Lima (2007, p. 78-83, 126), Lopes (2015, p. 40-45), Monteiro (1978, p. 228, 233-255) e Souza (2013, p. 34-36).

- seção 3.4, uma busca de ordem a partir das propriedades da adição e multiplicação dos corpos reais, que leva à introdução do conceito de corpo formalmente real; bibliografia: Endler (2012, p. 1-2), Fernandes; Ricou (2004, p. 397-404), Griese (2015, p. 1-3), Lang (2002, p. 447-457), Martin (2010, p. 391-392) e Polizeli (2007, p. 3-10).

- seção 3.5, apresenta a definição e exemplos de corpos reais fechados; bibliografia: Guidorizzi (1987, vol. 1, p. 458), Lang (2002, p. 447-457), Martin (2010, p. 393-397), Panek; Rocio (2006, p. 100-101), Prestel (2009, cap. 3), Prestel; Delzell (2011, cap. 1) e Polizeli (2007, p. 10-14).

- seção 3.6, o anel de funções polinomiais e o corpo de funções racionais $\mathbb{R}(X)$ sobre $\mathbb{R}$, o que possibilita chegar à definição de infinitésimos; bibliografia: Domingues; Iezzi

(2003, p. 282-289), Fernandes; Ricou (2004, p. 126-149), Hefez (2002,vol. 2, p. 7-32), Martin (2010, p. 390) e Monteiro (1978, p. 280-311).

O apêndice A, que tem como objetivo abordar alguns detalhes da estrutura algébrica denominada de anel, pois em diversos compêndios de Matemática os corpos são definidos a partir dessas estruturas, traz na:

- seção A.1, a definição da estrutura de anel a partir de axiomas; bibliografia: Fernandes; Ricou (2004, p. 32-35), Garcia; Lequain (2010, p. 7-9), Hefez (2002, vol. 1, p. 23-24) e Monteiro (1978, p. 168-169).

- seção A.2, definições e exemplos dos casos mais comuns de anéis; bibliografia: Castrucci (1969, p. 105-106), Domingues; Iezzi (2003, p. 218-223), Fernandes; Ricou (2004, p. 39-41), Garcia; Lequain (2010, p. 9-17), Hefez (2002, vol. 1, p. 26-31) e Monteiro (1978, p. 175-178).

1

NOÇÕES DE ESTRUTURAS ALGÉBRICAS E CORPOS

Neste capítulo será abordado o conceito de estruturas algébricas que foi decisivo para que se construísse a abordagem axiomática da Álgebra e, também, será destacada para estudo uma classe de estruturas algébricas particulares denominadas corpos. Esta classe de estruturas algébricas é de grande relevância para as definições de Matemática, sendo corpo a estrutura algébrica onde se estuda as quatro operações fundamentais $(+, -, ., /)$ dos números reais na educação básica e, também, é o conceito que aparece nas definições dos conjuntos dos números racionais, reais, complexos, entre outras.

Durante o desenvolvimento do trabalho serão utilizados os conceitos e simbologia de conjuntos, relações e funções de uso corrente em Matemática. O leitor interessado em rever esses temas poderá encontrá-los na Biblioteca Digital do Profmat na tese de dissertação de mestrado de Dutra (2014).

1.1 Estruturas Algébricas

Os casos mais simples de estruturas algébricas podem ser colocados da seguinte forma:

Considere uma ou mais aplicações do tipo $f: A \times A \to A$, sobre um conjunto A, e o trabalho de verificação se f satisfaz, ou não, determinado conjunto de axiomas.

A estrutura algébrica consiste do domínio A e da operação f; ela pode ou não satisfazer os axiomas propostos, isto é, eles valem ou não na estrutura.

De acordo com o conjunto de axiomas que a estrutura satisfaça, ela pertencerá a uma determinada classe de estruturas algébricas. Esse conjunto de axiomas também é chamado de teoria.

Observe que nada foi afirmado sobre o conjunto ou os elementos do conjunto porque o que vai diferenciar as classes de estruturas algébricas umas das outras é a teoria que a estrutura atende. Obviamente, a escolha de um número menor de axiomas leva a uma classe de estruturas algébricas mais abrangente que engloba diversos exemplos concretos. Por outro lado, a escolha de um grupo maior de axiomas restringe o número de exemplos concretos abordados pela teoria. Portanto, um dos trabalhos da Álgebra é definir classes de estruturas algébricas, levando em consideração a sua utilidade e a existência de casos concretos e teóricos que se enquadrem na teoria.

Entre as diversas classes de estruturas algébricas que estão definidas em Álgebra, é destacada para estudo, nesse trabalho, a estrutura algébrica chamada de corpo que aparece em diversas definições Matemáticas. Esta estrutura satisfaz um grupo de axiomas verificados para duas operações binárias: adição (+) e multiplicação (.) sobre um conjunto K, como será visto a seguir.

1.2 Corpo

Seja K um conjunto onde estão definidas duas operações binárias: adição $(+)$ e multiplicação $(.)$ e duas constantes 0 e 1, com $0 \neq 1$. A estrutura algébrica $(K, +, ., 0, 1)$ é um corpo em relação a essas duas operações se, e somente se, atender o seguinte conjunto de axiomas:

a) Axiomas da Adição

A1 – Associatividade

A adição é associativa, ou seja, para $\forall\, x, y, z \in K$ tem-se $(x + y) + z = x + (y + z)$.

A2 – Comutatividade

A adição é comutativa, ou seja, para $\forall\, x, y \in K$ tem-se $x + y = y + x$.

A3 – Existência do Elemento Neutro da adição

O elemento 0 é um elemento neutro para a adição, ou seja, para $\forall\, x \in K$ tem-se $x + 0 = x = 0 + x$.

Obs: Será verificado na propriedade 1 da seção 1.3 que o elemento neutro da adição é único.

A4 – Existência do Elemento Oposto na adição

A adição admite elementos opostos: para um elemento genérico x é indicado por $-x$, ou seja, para $\forall\, x \in K$ tem-se que $\exists\, (-x) \in K$, tal que, $x + (-x) = 0 = (-x) + x$.

b) Axiomas da Multiplicação.

M1 – Associatividade

A multiplicação é associativa, ou seja, para $\forall\, x, y, z \in K$ tem-se $(x.y).z = x.(y.z)$.

M2 – Comutatividade

A multiplicação é comutativa, ou seja, para $\forall\, x, y \in K$ tem-se $x.y = y.x$.

M3 – Existência do Elemento Neutro da multiplicação

O elemento 1 é um elemento neutro para a multiplicação, chamado de unidade, ou seja, para $\forall\, x \in K$ tem-se $x.1 = x = 1.x$.

Obs: Será verificado na propriedade 12 da seção 1.3 que o elemento neutro da multiplicação é único.

M4 – Existência do Elemento Inverso na multiplicação

A multiplicação possui elementos inversos para elementos não nulos, para um elemento genérico x é indicado por x^{-1}, ou seja, para $\forall\, x \in K - \{0\}$ tem-se que $\exists x^{-1} \in K$ tal que $x.x^{-1} = 1 = x^{-1}.x$.

c) Axioma da Distributividade da multiplicação em relação à adição

DM - A multiplicação é distributiva em relação à adição, ou seja, para $\forall\, x, y, z \in K$ tem-se $x.(y + z) = x.y + x.z$.

Os axiomas acima definem um corpo comutativo.

Excluindo-se o axioma M2 (Comutatividade da multiplicação), dos axiomas de corpo comutativo dados acima, obtém-se uma definição mais geral de corpo que passa a ser chamada de corpo não comutativo ou anel de divisão.

Ao longo desse trabalho será utilizada a denominação corpo para corpo comutativo e quando for o caso de corpo não comutativo será explicitado que se trata desse caso.

Em relação à notação de corpo, quando não houver dúvidas que se trata de um corpo e de quais são as operações $(+)$ e $(.)$, será utilizada como notação apenas K ao invés de $(K, +, ., 0, 1)$.

1.3 Dedução de propriedades dos corpos a partir dos axiomas

Os axiomas de corpo permitem demonstrar diversas propriedades sobre as operações da definição de corpo e até definir outras operações. A seguir são destacadas algumas propriedades provadas a partir dos axiomas de corpo, e que são empregadas na Matemática desde o ensino básico. Vale ressaltar que, além das que estão listadas abaixo, podem ser provadas outras propriedades.

1) O elemento neutro da operação de adição, normalmente denominado de 0, é único.

Demonstração: Caso se admitam dois elementos nulos para a operação de adição 0 e 0^***,** então:
$0 + 0^* = 0$ (porque 0^* é elemento neutro);
$0 + 0^* = 0^*$ (porque 0 é elemento neutro);
conclui-se, portanto, que: $0^* = 0$. ■

2) O oposto, também chamado de simétrico aditivo, de cada elemento de K é único.

Demonstração: Caso um elemento $x \in K$ possua dois simétricos aditivos indicados por y e y', tal que: $x + y = 0$ e $y' + x = 0$, logo:
$y' = y' + 0 = y' + (x + y) = (y' + x) + y = 0 + y = y \Rightarrow y' = y$,
portanto, o elemento simétrico de x é único, e, normalmente, representa-se por $-x$. ■

3) Quaisquer que sejam $x, y \in K$, tem-se: $-(-x) = x$.

Demonstração: O simétrico de x é $-x$, de acordo com o axioma A4 da definição de corpo, então, note que x realiza o papel de oposto de $-x$, que pela propriedade anterior é único, veja:
I) $x + (-x) = 0$
II) $-(-x) + (-x) = 0$
Observando as equações I e II, conclui-se que $-(-x) = x$. ■

4) Para quaisquer que sejam a, x e $y \in K$ se $a + x = a + y$, então, $x = y$ (lei do cancelamento da adição ou lei do corte da adição).

Demonstração: Some o elemento $-a$, simétrico de a, aos dois lados da igualdade acima, como segue:

$(-a) + a + x = (-a) + a + y \Leftrightarrow ((-a) + a) + x = ((-a) + a) + y \Leftrightarrow 0 + x = 0 + y$
$\Leftrightarrow x = y$. ■

5) Dados a e $b \in K$ existe um único elemento $x \in K$ tal que $b + x = a$.

Verificação: Tomando $x = a + (-b)$, tem-se:
Existência: $b + x = x + b \Rightarrow (a + (-b)) + b = = a + ((-b) + b) = a + 0 = a$.
Unicidade: $b + x = a = b + y \Rightarrow x = y$ (Aqui fez-se uso da propriedade do cancelamento da adição.)

Esse elemento $x \in K$ indicado por $a - b$ e é chamado de diferença entre a e b. Veja:

$x = a - b = a + (-b)$

Portanto, fica definida sobre K a operação $(a, b) \longmapsto a - b$ chamada subtração, para a qual valem as igualdades:

$b + (a - b) = a,\ 0 - a = -a$ e $a - a = 0$.

6) Existe o múltiplo de $x \in K$ em relação a um inteiro n.

$0.x = 0$

$(k + 1).x = kx + x$ e $(-k).x = -(kx)$ onde $k \in \mathbb{N}$.

Como todo $x \in K$ é simetrizável para a adição são válidas as fórmulas colocadas abaixo. Para a primeira fórmula foi feito um detalhamento e para as demais, apenas, citado o respectivo axioma de corpo que a torna válida:

- $n(-x) = -(nx) = (-n)x$

Veja que:

$$n \cdot (-x) = \underbrace{(-x) + \ ... + (-x)}_{n \text{ vezes}} = \underbrace{(-1).(x + \ ... + x)}_{n \text{ vezes}} = -(nx)$$

onde já se fez uso da propriedade 11 a seguir.

Pode-se também mostrar que:

- $m(nx) = (mn)x = n(mx)$
- $(m + n)x = mx + nx$
- $n(x + y) = nx + ny$

para quaisquer que sejam os elementos $x, y \in K$ e os números inteiros m e n, por argumentos semelhantes de contagem. Nota-se que não necessariamente $\mathbb{Z} \subset K$, mas obtém-se uma função $\mathbb{Z} \to K$ via $n \mapsto n.1$ (não necessariamente injetora).

7) Propriedade distributiva da multiplicação em relação à subtração.

Para $\forall\, x, y, z \in K$ tem-se que:

$x.(y - z) = x.y - x.z$ e $(y - z).x = y.x - z.x$

Demonstração: De acordo com a definição de diferença e a distributividade da multiplicação em relação à adição que é válida para um corpo, tem-se:

$xy = x[z + (y - z)] = xz + x(y - z)$,

portanto, $x(y - z) = (xy) - (xz)$.

A demonstração da propriedade distributiva para a segunda sentença é semelhante a esta que foi demonstrada para a primeira sentença. ■

Com base nisso, pode-se concluir a convenção usual que os produtos devem ser efetuados em primeiro lugar e a seguir as diferenças.

8) Lei do cancelamento da multiplicação.

Para $\forall\, x, y, z \in K$ e $x \neq 0$ tem-se:

$x.y = x.z \Rightarrow y = z.$

Demonstração: $xy = xz \implies x^{-1}(xy) = x^{-1}(xz) \implies (x^{-1}x)y = (x^{-1}x)z \implies 1y = 1z \implies y = z$. ■

9) O elemento neutro da adição (zero) é absorvente na multiplicação.

Para $\forall\, x \in K$, tem-se $x.0 = 0 = 0.x$

Demonstração: Para $\forall\, x,\ a \in K$ e de acordo com a propriedade 7, distributividade da multiplicação para a diferença, tem-se:

$$x.0 = x(a - a) = (x.a) - (x.a) = 0$$

e $$0.x = (a - a)x = (a.x) - (a.x) = 0.$$ ■

10) Um corpo K não possui divisores de zero.

O fato do corpo K não possuir divisores de zero é facilmente provado com base nos axiomas de corpo, porém, para um melhor detalhamento e compreensão será definido divisor

de zero de um conjunto, abaixo, para, em seguida, ser feita a demonstração que um corpo não possui divisores de zero. Veja:

Definição: Os elementos a e b, não nulos, de um anel $(A, +, ., 0)$ serão chamados divisores de zero se, e somente se, $a.b = 0$.
Observação: A estrutura algébrica chamada de anel está definida no apêndice A.

Demonstração: Admita por absurdo que $\exists\, a, b \in K - \{0\}$ e $a.b = 0$, ou seja, a e b são divisores de zero que pertencem ao corpo K.

Multiplicando por a^{-1} ambos os membros da equação e usando a propriedade associativa da multiplicação e a propriedade 9, tem-se:
$a.b = 0 \Longrightarrow a^{-1}(ab) = a^{-1}(0) \Longrightarrow (a^{-1}a)b = 0 \Longrightarrow b = 0,$
mas isso é um absurdo, pois inicialmente foi admitido: $b \neq 0$.

Conclui-se, portanto, que o corpo K não admite divisores de zero. ■

11) Regra dos sinais na multiplicação.

Para $\forall\, x, y \in K$, tem-se:
$(-x)y = -(xy) = x(-y)$ e $(-x)(-y) = xy.$

Demonstração: De acordo com o que foi desenvolvido nas propriedades 4, 5, 7 e 9 tem-se:

$$(-x)y = (0 - x)y = (0.y) - (xy) = 0 - (xy) = -(xy),$$

$$x(-y) = x(0 - y) = (x.0) - (xy) = 0 - (xy) = -(xy),$$

e

$$(-x)(-y) = -[x(-y)] = -[-(xy)] = xy\ .$$ ■

12) O elemento neutro da multiplicação é único.

Demonstração: Suponha que existam duas unidades no corpo K e que sejam representadas por 1 e $1'$. Pela definição de unidade do axioma M2 de corpo tem-se que:
$1.1' = 1$ e $1.1' = 1'$,
logo: $1 = 1'$. ■

13) O inverso multiplicativo é único.

Demonstração: Suponha que o elemento $a \neq 0$ possua dois inversos multiplicativos b e c, $ab = 1$ e $ac = 1$, então: $ab = ac$ e tem-se pela propriedade 8 que $b = c$. ■
Usualmente a notação do inverso multiplicativo de um elemento x é feita por x^{-1}.

Observações:

I) Note que $x.x^{-1} = 1 \neq 0$.

II) $x, y \neq 0 \Rightarrow x.y \neq 0$ e $(x.y)^{-1} = x^{-1}.y^{-1}$.

III) $(x^{-1})^{-1} = x$ e $(-x)^{-1} = -(x^{-1})$.

14) Para todo $x, y \in K$ com $x \neq 0$ existe y/x que será chamado de quociente e é igual a $y.x^{-1}$.

15) Para todo x e $y \in K$, com $x \neq 0$, existe um único elemento $z \in K$ tal que $x.z = y$.

Demonstração:

Existência: $\forall\, x \in K - \{0\}$ possui inverso em K, que pode ser representado por x^{-1} e $x^{-1} \neq 0$. Por outro lado a multiplicação é fechada em K. Então, tem-se que existe $y.x^{-1}$ para $x, y \in K$ com $x \neq 0$, que será chamado de quociente de y por x e representado da seguinte forma y/x.

Unicidade: para x, y e $z \in K$ com $x \neq 0$, vem que $x.z = y = x.z' \Rightarrow x^{-1}.(x.z) = = x^{-1}.(x.z') \Rightarrow 1.z = 1.z' \Rightarrow z = z'$. ■

16) A operação acima definida será chamada de divisão e entre as propriedades que atende destacam-se as seguintes:

Para os elementos a, b, c, e d do corpo K, com $b \neq 0$ e $d \neq 0$, tem-se que:

I) $\frac{a}{b} = \frac{c}{d}$, se, e somente se, $ad = bc$

II) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, note que $b.d \neq 0$, de acordo com a obs. II da propriedade 13.

III) $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$, note que $-b \neq 0$, pois $-b = 0 \Rightarrow b + 0 = 0 \Rightarrow b = 0$

IV) $\left(\frac{a}{b}\right).\left(\frac{c}{d}\right) = \frac{ac}{bd}$

V) $\frac{a}{b} = 0$ se, e somente se, $a = 0$

VI) $\frac{a}{1} = a$

VII) $\left(\frac{b}{d}\right)^{-1} = \frac{d}{b}$

A seguir será realizada a demonstração de algumas propriedades e comentado como proceder na demonstração das demais:

I) De $\frac{a}{b} = \frac{c}{d}$ vem que $ab^{-1} = cd^{-1}$ e então $ad = (ab^{-1})(bd) = (cd^{-1})(bd) = bc$. ■

II) Tem-se, de acordo com a observação II da propriedade 13, que $\frac{a}{b} + \frac{c}{d} =$

$= ab^{-1} + cd^{-1} = (ad)(b^{-1}d^{-1}) + (bc)(b^{-1}d^{-1}) = (ad)(bd)^{-1} + (bc)(bd)^{-1} =$

$= (ad + bc)(bd)^{-1} = \frac{ad+bc}{bd}$. ■

III) Essa propriedade pode ser demonstrada pela regra de sinais da multiplicação e $(-b)^{-1} = -(b^{-1})$.

IV) Tem-se que $\frac{a}{b}.\frac{c}{d} = ab^{-1}.cd^{-1} = (ac)(b^{-1}d^{-1}) = (ac)(bd)^{-1} = \frac{ac}{bd}$. ■

V) Considerando a propriedade de um corpo não admitir divisores de zero e o fato do zero ser absorvente na multiplicação, tem-se que: $\frac{a}{b} = ab^{-1} = 0$, mas $b \neq 0 \Rightarrow a = 0 \Rightarrow a.b^{-1} = 0$. ■

VI) Pelos axiomas do elemento neutro da multiplicação e do inverso multiplicativo, tem-se que: $(1)^{-1} = 1$, pois $1.1 = 1 = 1.(1)^{-1} \Rightarrow 1 = 1^{-1}$. Então: $\frac{a}{1} = a.(1)^{-1} = a.1 = a$. ■

VII) Pode ser demonstrada com o auxílio do axioma do inverso multiplicativo.

Note que $(-b).b^{-1} = -(b.b^{-1}) = b.(-b^{-1}) \Rightarrow (-b).(-b^{-1}) = = b.b^{-1} = 1 \Rightarrow$ (unicidade do inverso) $(-b)^{-1} = -b^{-1}$.

Então tem-se, pela unicidade do inverso multiplicativo, que $(\frac{b}{d})^{-1} = (b.d^{-1})^{-1} = b^{-1}.(d^{-1})^{-1} = b^{-1}.d = d.b^{-1} = \frac{d}{b}$. ■

Com base nos axiomas de corpo e nas propriedades é possível concluir que um corpo é uma estrutura algébrica fechada para as operações de adição, subtração, multiplicação e divisão, não possui divisores de zero e atende a lei do cancelamento da multiplicação.

1.4 Exemplos de corpos

A seguir, serão colocados alguns exemplos e contraexemplos de corpos. Outros exemplos serão apresentados no próximo capítulo.

Exemplos:

1) São corpos os conjuntos: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2})$, pois é possível verificar a validade dos axiomas de corpo em cada um desses conjuntos.

Obs.: Os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ usuais em Matemática são construídos na teoria de conjuntos, alguns detalhes dessas construções podem ser encontrados em Monteiro (1978, cap. 4 e 5).

Para ilustrar melhor o fato que esses conjuntos atendem a teoria dos corpos, será mostrado a seguir que o conjunto $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2},\ \ a\ , b \in \mathbb{Q}\}$ satisfaz todos os axiomas de corpo, ou seja, é um corpo. Serão utilizadas as propriedades de $\mathbb{Q}$ e $\mathbb{R}$, para tanto.

Considere que $a, b, c, d, g, h \in \mathbb{Q}$, logo:

a) $\mathbb{Q}(\sqrt{2})$ é fechado para a adição e a multiplicação, veja:

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$, como $a + c \in \mathbb{Q}$ e $b + d \in \mathbb{Q}$, logo $\mathbb{Q}(\sqrt{2})$ é fechado para a adição.

$(a + b\sqrt{2})\ .\ (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, como $(ac + 2bd) \in \mathbb{Q}$ e $(ad + bc) \in \mathbb{Q}$, logo $\mathbb{Q}(\sqrt{2})$ é fechado para a multiplicação.

b) A multiplicação e a adição são comutativas, porque esses são números reais.

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2})$

$(a + b\sqrt{2}).(c + d\sqrt{2}) = (c + d\sqrt{2}).(a + b\sqrt{2})$

c) A adição e a multiplicação admitem elemento neutro, respectivamente, o zero e o um, novamente porque $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Veja:

$(a + b\sqrt{2}) + 0 = (a + b\sqrt{2})$

$(a + b\sqrt{2}).1 = (a + b\sqrt{2})$

Note que: $0 = (0 + 0\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$ e

$1 = (1 + 0\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$

d) A adição e a multiplicação são associativas, novamente porque $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$:

Sejam: $q_1 = a + b\sqrt{2}$, $q_2 = c + d\sqrt{2}$ e $q_3 = g + h\sqrt{2}$, então, é válido na adição $(q_1 + q_2) + q_3 = q_1 + (q_2 + q_3)$ e na multiplicação, é válido $(q_1.q_2).q_3 = q_1.(q_2.q_3)$.

e) Todo elemento na adição admite oposto e na multiplicação todo elemento não nulo admite inverso. Veja:

Seja o elemento $(a + b\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$,

I) o oposto de $a + b\sqrt{2}$ é $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}$, que pertence a $\mathbb{Q}(\sqrt{2})$. Veja a seguir o desenvolvimento algébrico:

$$(a + b\sqrt{2}) + (-a) + (-b)\sqrt{2} = (a - a) + (b - b)\sqrt{2} = 0 + 0\sqrt{2} = 0.$$

II) o inverso de $(a + b\sqrt{2})$ é $\left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$, sendo que $a + b\sqrt{2} \neq 0 \Rightarrow a \neq 0$ ou $b \neq 0$ (isto está detalhados nas duas observações abaixo) $\Rightarrow a^2 \neq 2b^2$ porque $a, b \in \mathbb{Q}$ e $\sqrt{2} \notin \mathbb{Q}$. Veja a seguir o desenvolvimento algébrico:

$$(a + b\sqrt{2}).\left[\left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}\right] =$$

$$= \left(\frac{a^2}{a^2-2b^2}\right) + \left(\frac{-ab}{a^2-2b^2}\right)\sqrt{2} + \left(\frac{ab}{a^2-2b^2}\right)\sqrt{2} + 2\left(\frac{-b^2}{a^2-2b^2}\right) =$$

$$= \frac{a^2-2b^2}{a^2-2b^2} = 1.$$

Obs. 1: $a + b\sqrt{2} \neq 0 \Leftrightarrow a \neq 0$ ou $b \neq 0$, com $a, b \in \mathbb{Q}$. Como $a = -(b\sqrt{2})$ ocorre só no caso que $a = -b = 0 = b$.

Obs. 2: Se $a \neq 0$ ou $b \neq 0 \Rightarrow a^2 - 2b^2 \neq 0$. Então ocorre 3 casos:

(1) $a \neq 0$ e $b = 0 \Rightarrow a^2 - 2b^2 = a^2 > 0$

(2) $a = 0$ e $b \neq 0 \Rightarrow a^2 - 2b^2 = -2b^2 < 0$

(3) $a \neq 0$ e $b \neq 0$ e $a^2 - 2b^2 = 0 \Rightarrow \sqrt{2} = \left|\frac{a}{b}\right| \in \mathbb{Q} \Rightarrow$ absurdo.

f) Distributividade da multiplicação em relação a adição, porque são números reais.

Sejam: $q_1 = a + b\sqrt{2}$, $q_2 = c + d\sqrt{2}$ e $q_3 = g + h\sqrt{2}$, então, é válida a propriedade distributiva $(q_1).(q_2 + q_3) = (q_1).(q_2) + (q_1).(q_3)$.

Aqui vale observar que, em algumas demonstrações (a, c, e) foi preciso verificar que $\mathbb{Q}(\sqrt{2})$ continha os números construídos, enquanto em outras (b, d, f) usou-se o fato de que essas propriedades já valem em um corpo maior $\mathbb{R}$, que contém todos os números envolvidos.

Aqui será deixada, para o professor do ensino médio, uma sugestão para generalizar um pouco isto:

Veja que se $\sqrt{n} \notin \mathbb{Q}$ então $\mathbb{Q}(\sqrt{n})$ é corpo.

2) Não são corpos os conjuntos $\mathbb{N}$ e $\mathbb{Z}$.

No caso de $\mathbb{N}$ seus elementos não possuem simétrico, exceto 0, para a adição e na multiplicação o único elemento que admite inverso multiplicativo é o 1.

No caso de $\mathbb{Z}$ apenas dois de seus elementos possuem inverso multiplicativo 1 e -1.

2

DEFINIÇÕES E EXEMPLOS DE ALGUNS CORPOS

Neste capítulo será verificado que à medida que se acrescentam mais axiomas na definição de corpo, outros corpos que recebem nomes específicos são gerados. Dentre os corpos que são gerados dessa forma foram destacados para estudo os seguintes: o corpo dos inteiros módulo primo, corpo algebricamente fechado e corpo ordenado. Algumas definições que ajudam a fundamentar o estudo desses corpos também são abordadas, tais como: característica de um corpo e relação de ordem.

2.1 Corpo dos inteiros módulo um primo

O conjunto dos inteiros módulo um primo é um corpo, embora o conjunto dos números inteiros não seja um corpo (exemplo 2 da seção 1.4). Para compreender essa ideia são necessários alguns conceitos de aritmética, tais como congruência módulo um inteiro e classes residuais, colocados a seguir.

Definição: No conjunto dos inteiros $\mathbb{Z}$ diz-se que x é côngruo a y módulo n, se a diferença $x - y$ é divisível por n. Indica-se por $x \equiv y \bmod n$.

Exemplo:

$8 \equiv 2 \bmod 3$, pois 3 divide $(8 - 2)$, representando simbolicamente tem-se $3|(8 - 2)$.

Antes de mostrar que uma relação de equivalência em $\mathbb{Z}$ é definida por $x \equiv y \bmod n$, será definido, abaixo, relação de equivalência.

Definição: Uma relação R sobre um conjunto E é uma **relação de equivalência** se, e somente se, é reflexiva, transitiva e antissimétrica.

As propriedades citadas na definição de relação de equivalência são as seguintes:

E1: Propriedade reflexiva: $\forall\, x \in E$, tem-se xRx.

E2: Propriedade simétrica: $\forall\, x, y \in E$, se xRy, então yRx.

E3: Propriedade transitiva: $\forall\, x, y, z \in E$, se xRy e se yRz, então xRz.

Agora de posse do conceito de relação de equivalência pode-se observar que uma relação de equivalência em $\mathbb{Z}$ é definida por $x \equiv y \bmod n$, veja:

I) $x \equiv x \bmod n$ (propriedade reflexiva).

II) $x \equiv y \bmod n \implies y \equiv x \bmod n$ (propriedade simétrica).

III) $x \equiv y \bmod n,\ y \equiv z \bmod n \implies x \equiv z \bmod n$ (propriedade transitiva).

Definição: A classe residual módulo n do elemento a de $\mathbb{Z}$ é o conjunto:

$$\bar{a} = \{x \in \mathbb{Z} : x \equiv a \bmod n\}$$

Como para todo $x \in \mathbb{Z}$ tem-se pelo algoritmo de Euclides que $x = qn + r$ para únicos $q, n, \in \mathbb{Z}$ e $0 \leq r < n$, então, $x \equiv r \bmod n$ e os diferentes restos (r) obtidos pela divisão dos números de $\mathbb{Z}$ por um dado número n pertencem cada um a sua respectiva classe de equivalência módulo n.

O conjunto das classes de equivalência de $\mathbb{Z}$ módulo n será representado por $\mathbb{Z}_n$ e para cada uma das classes de equivalência será adotado como representante um dos possíveis restos: $\overline{r_i}$. Assim:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

Exemplificando numericamente para o conjunto das classes de $\mathbb{Z}_5$ e $\mathbb{Z}_6$, tem-se:

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ e $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Continuando a exemplificação numérica para as classes $\overline{r_i}$ de $\mathbb{Z}_5$ tem-se:

$\bar{0} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

$\bar{1} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$

$\bar{2} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$

$\bar{3} = \{\ldots, -7, -2,\ 3,\ 8, 13, \ldots\}$

$\bar{4} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

Pode-se observar no exemplo que a união de todos os elementos das classes residuais módulo n, para um dado n, forma o conjunto dos inteiros $\mathbb{Z}$ e que, por outro lado, sobre o conjunto de todas as classes residuais módulo n $(\mathbb{Z}_n)$, podem ser definidas as operações de:

- Adição: $\bar{a} + \bar{b} = \overline{a + b}$

- Multiplicação: $\bar{a}.\bar{b} = \overline{a.b}$

Estas operações estão bem definidas, pois o resultado $\overline{a+b}$ independe dos representantes a e b escolhidos para $\bar{a}$ e $\bar{b}$. Veja:

Se $a \equiv a'$ e $b \equiv b'$, então $a - a' = qn$ e $b - b' = xn$, donde $(a+b) - (a'+b') = (q+x)n$ e vem $a + b \equiv a' + b'$. (Analogamente para o produto.). Então o resultado de $\bar{a} + \bar{b}$ é o mesmo de $\overline{a'} + \overline{b'}$, e o de $\bar{a}.\bar{b}$ é o mesmo de $\overline{a'}.\overline{b'}$.

Exemplo:

Para exemplificar numericamente essas operações, abaixo, são colocadas as tábuas de adição e multiplicação de $\mathbb{Z}_5$ e $\mathbb{Z}_6$, respectivamente, veja:

Tábuas de adição e multiplicação de $\mathbb{Z}_5$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Tábuas de adição e multiplicação de $\mathbb{Z}_6$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Essas tábuas são como a tabuada escolar que é ensinada na educação básica e servem para mostrar os resultados das operações. Por exemplo, nas tábuas de $\mathbb{Z}_5$ para as classes $\bar{2}$ e $\bar{1}$, temos: $\bar{2} + \bar{1} = \bar{3}$ e $\bar{2}.\bar{1} = \bar{2}$.

Pela observação das tábuas de adição e multiplicação de $\mathbb{Z}_5$ e $\mathbb{Z}_6$ conclui-se que:

- o conjunto $\mathbb{Z}_5$ é um corpo, pois verifica todos os axiomas de corpo.
- o conjunto $\mathbb{Z}_6$ não é um corpo, pois não verifica o axioma M4 (existência do inverso multiplicativo), e, também, não são válidas as propriedades 8 (Lei do cancelamento da multiplicação) e 9 (Um corpo não possui divisores de zero), pois $\overline{2}.\overline{3} = \overline{0}$ e $\overline{3}.\overline{4} = \overline{0}$ e $\overline{2} \neq \overline{0}$, $\overline{3} \neq \overline{0}$ e $\overline{4} \neq \overline{0}$.

Os axiomas de corpo para os inteiros módulo n, que serão enunciados a seguir, não precisam de demonstração, pois valem nos inteiros para os representantes das classes residuais, com exceção do axioma M4, que não vale, em geral.

Axiomas da adição:

A1 (Associatividade) $\left(\bar{a} + \bar{b}\right) + \bar{c} = \bar{a} + \left(\bar{b} + \bar{c}\right)$

A2 (Comutatividade) $\bar{a} + \bar{b} = \bar{b} + \bar{a}$

A3 (Existência do elemento neutro) $\bar{a} + \overline{0} = \bar{a}$ para todo $\bar{a} \in \mathbb{Z}$

A4 (Existência do oposto) dado $\bar{a}$ existe $\bar{b}$ tal que $\bar{a} + \bar{b} = \overline{0}$

Axiomas da multiplicação:

M1 (Associatividade) $\left(\bar{a}.\bar{b}\right).\bar{c} = \bar{a}.(\bar{b}.\bar{c})$

M2 (Comutatividade) $\bar{a}.\bar{b} = \bar{b}.\bar{a}$

M3 (Existência do elemento neutro) $\bar{a}.\overline{1} = \bar{a}$ para todo $\bar{a} \in \mathbb{Z}$

M4 (Existência do elemento inverso) para qualquer $\bar{a} \in \mathbb{Z} - \{0\}$ existe $\bar{b}$ tal que $\bar{a}.\bar{b} = \overline{1}$

Axioma da distributividade da Multiplicação em relação a adição

DM (distributividade da multiplicação) $\bar{a}.\left(\bar{b} + \bar{c}\right) = \overline{ab} + \overline{ac}$

Considerando os exemplos numéricos $\mathbb{Z}_5$ e $\mathbb{Z}_6$ e os axiomas de corpo enunciados acima para as classes residuais é possível perceber que a verificação do axioma de corpo M4 (Existência do elemento inverso na multiplicação), e das propriedades 8 (Lei do cancelamento da multiplicação) e 10 (Um corpo não possui divisores de zero) da seção 1.3 são determinantes para que um conjunto de inteiros módulo n seja um corpo ou não.

A seguir são definidas as condições que levam um corpo de resíduos módulo n a atender o axioma M4 e, portanto, as propriedades 8 e 9.

O seguinte teorema dá uma condição para que um elemento $\bar{a}$ de $\mathbb{Z}_n$ não seja divisor de zero, ou em outras palavras seja regular para a multiplicação.

Teorema: Um elemento $\bar{a}$ de um conjunto de resíduos módulo n, $\mathbb{Z}_n$ $(n > 1)$, é um divisor de zero se, e somente se, $mdc\ (a,n) = d > 1$.

Demonstração: Considere que se $\bar{a} \neq 0$ e que $n \nmid a$ (n não divide a), e seja $\bar{b} \neq 0$ tal que $\overline{ab} = 0$, de onde vem que $ab = qn$ e consequentemente que $n|ab$ (n divide ab). A seguir serão analisados os dois casos: $d = 1$ e $d > 1$.

1º caso: Se o $mdc\ (a,n) = d = 1$, então, pelo teorema de Euclides tem-se que se o $mdc\ (a,n) = 1$ e $n|(ab) \Rightarrow n|b$. Portanto, $\bar{b} = 0$, e conclui-se que se a e n forem primos entre si, $\bar{a}$ não é um divisor de zero, ou seja, $\bar{a}$ é regular para a multiplicação.

2º caso: Se o $mdc\ (a,n) = d > 1$, então, a e n não são primos entre si. Então, d é um fator comum de a e n e tem-se: $a = a_1 d$ e $n = n_1 d$. Veja que $1 \leq n_1 < n$, logo, $\overline{n_1} \neq \bar{0}$ e, por outro lado, $\bar{a}.\overline{n_1} = \overline{an_1} = \overline{a_1 d\ n_1} = \overline{a_1 n} = \bar{0}$. Portanto, conclui-se que $\bar{a}$ é um divisor de zero se a e n não forem primos entre si. ■

Levando em consideração a demonstração acima o seguinte corolário pode ser enunciado:

Corolário: Um elemento $\bar{a} \in \mathbb{Z}_n$ $(n > 1)$ é invertível se, e somente se, a e n são primos entre si.

Com o corolário e o teorema de Bézout, abaixo:

Teorema de Bézout: Dados dois inteiros a, n, não nulos, existem x e y tais que $ax + ny = mdc(a,n)$.

Então tem-se que:

$mdc\ (a,n) = 1 \Rightarrow \exists\ x, y$ e como $ax + ny = 1 \Rightarrow ax \equiv 1 \bmod n \Rightarrow \bar{a}.\bar{x} = \bar{1}$.

$mdc\ (a,n) > 1 \Rightarrow \bar{a}$ é divisor de $\bar{0}\ \Rightarrow \bar{a}$ não é invertível .

Conforme já foi exposto, se a e n são primos entre si, logo, pelas propriedades de m.d.c. da Aritmética, que pode ser visto em Hefez (2006, p. 53 - 63), existem números inteiros r e s tais que $ra - sn = 1$, de onde vem, $\bar{r}\bar{a} = 1$, ou seja, $\bar{a}$ é invertível. Reciprocamente, se $\bar{a}.\bar{b} = 1$, então $n|(ab - 1)$, donde $ab = 1 + nq$ e $ab + (-q)n = 1 \Rightarrow$ $\Rightarrow mdc\ (a,n)|1 \Rightarrow mdc\ (a,n) = 1$. ■

Com isso mostra-se que qualquer elemento a de uma classe de resíduos módulo n de $\mathbb{Z}_n$ que for coprimo com n atende as propriedades 8 e 10 e o axioma M4 de corpo.

Como o que se quer definir são as condições para que $\mathbb{Z}_n$ seja um corpo, então, tem-se que todos os elementos não nulos de $\mathbb{Z}_n$ deverão ser classes de números relativamente primos com n, o que obriga n a ser um número primo. Veja que existem duas possibilidades para n:

I) Se $n > 1$ não é primo, $\mathbb{Z}_n$ não é um corpo porque tem divisores próprios de zero, pois $n = ab$ e, portanto, existe $\bar{a}.\bar{b} = 0$, com $\bar{a} \neq 0$ e $\bar{b} \neq 0$.

II) Se $n > 1$, for primo, e $\bar{a} \neq 0$, então, $mdc(a,n) = 1$ e $\bar{a}$ é invertível, pois $mdc(a,n) \in \{1,n\}$ e $mdc(a,n)|a$. Logo, $\bar{a} \neq 0 \Rightarrow n \nmid a \Rightarrow mdc(a,n) = 1$.

Portanto, o seguinte teorema foi demonstrado:

Teorema: O conjunto $\mathbb{Z}_n$ dos inteiros módulo n é um corpo se, e somente se, n é um número primo. ■

O conjunto $\mathbb{Z}_n$ dos inteiros módulo n, com n primo, é um corpo finito, mas não é o único caso de corpo finito. Outro exemplo interessante de corpo finito é o corpo de Galois $GF(p^k)$, sendo um corpo para cada potência p^k, com p primo e $k > 0$ que pode ser visto em Fernandes (2004, p. 205).

2.2 Característica de um corpo

A característica de um corpo é o menor número natural não nulo (n) que multiplicado pela unidade do corpo (1) é igual a zero.

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

Quando não houver um número natural n tal que $n \cdot 1 = 0$, diz–se que a característica do corpo K é zero.

A definição acima permite enunciar o seguinte teorema:

Teorema: A característica de um corpo é 0 ou um número primo.

Demonstração:

Se não existe n inteiro positivo tal que $n \cdot 1 = 0$, então a característica do corpo é zero.

Se existe n inteiro positivo, tal que $n \cdot 1 = 0$, denote por n o menor inteiro positivo, então a característica do corpo é n. Para provar que n é primo, admita por absurdo que n não é primo, então $n = a.b$, com a e b inteiros maiores que 1, logo:

$n \cdot 1 = 0 \Rightarrow (a.b).1 = 0 \Rightarrow (a.b).1^2 = 0 \Rightarrow (a.1).(b \cdot 1) = 0 \Rightarrow a.1 = 0$ ou $b.1 = 0$.

Veja que a conclusão contraria o fato de n ser o menor inteiro positivo tal que $n.1 = 0$. Portanto, n é primo. ■

É fácil ilustrar a definição de característica com exemplos, veja:

Exemplos:

1) Os conjuntos $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2})$ são corpos que têm característica zero, pois nesses corpos não existe $n \in \mathbb{N} - \{0\}$, tal que $n \cdot 1 = 0$. Nota-se que $\mathbb{Z}$ e $\mathbb{Q}$ podem ser vistos dentro de todo corpo de característica 0, porque a função $n \mapsto n.1$ é injetora.

2) O conjunto $\mathbb{Z}_5$ dado no item de corpos módulo p, com p primo, é um exemplo de corpo que tem característica diferente de zero. Pela tábua da multiplicação é possível concluir que existe $n.1 = 0$, no corpo $\mathbb{Z}_5$. Veja que 5 é o menor número natural não nulo que é côngruo a zero. Portanto, quando 5 que pertence a classe $\bar{0}$ de $\mathbb{Z}_5$ é multiplicado pela unidade $\bar{1}$ do conjunto $\mathbb{Z}_5$, tem-se que $5.\bar{1} = \bar{0}$, ou seja, $n = 5$.

De acordo com o que foi exposto sobre o corpo dos inteiros módulo p e a definição de característica o seguinte teorema pode ser enunciado:

Teorema: O corpo dos inteiros módulo p $(\mathbb{Z}_p)$, sendo p primo, possui característica p.

A demonstração desse teorema pode ser feita tomando como base o exemplo 2 e o teorema anterior.

2.3 Corpo algebricamente fechado

Um corpo K é algebricamente fechado se, e somente se, há pelo menos uma raiz em K para todo polinômio não constante de $K[X]$. Mostra-se que, então, todo polinômio de $K[X]$ fatora-se completamente nesse anel (a definição e algumas exemplos de anéis encontram-se no apêndice A).

A seguir, algumas considerações sobre corpos algebricamente fechados são colocadas nos exemplos.

Exemplos:

1) Não são algebricamente fechados os corpos $\mathbb{Q}$ e $\mathbb{R}$, pois o polinômio $X^2 + 1$ não possui raiz real. De fato, em vista da ordem, $x^2 + 1 > 0$ para todo x. De forma similar, será visto que os corpos ordenados (como definidos a seguir) também não são algebricamente fechados.

2) O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado, o que constitui o Teorema Fundamental da Álgebra, cuja demonstração pode ser vista em Monteiro (1978, p. 434 - 443).

3) Um corpo algebricamente fechado K não é finito, pois se $a_1,\ a_2, \ldots, a_n$ forem os únicos elementos de K, o polinômio $(X - a_1).(X - a_2) \ldots (X - a_n) + 1$ não terá nenhuma raiz em K.

2.4 Relações de ordem

Para o estudo de corpo ordenado convém antes rever o que são: relação de ordem, ordem total e ordem estrita.

Em Matemática uma relação de ordem permite comparar dois elementos de um conjunto e ordená-los segundo um critério, além disso, é interessante que a relação de ordem seja compatível com as operações do conjunto, pois fornecerá condições adicionais de previsão dos resultados das operações. A seguir são colocadas as definições de relação de pré-ordem e de ordem.

Definição: Uma relação S sobre um conjunto E é uma **relação de pré-ordem** sobre E se, e somente se, é reflexiva e transitiva.

Definição: Uma relação R sobre um conjunto E é uma **relação de ordem** se, e somente se, é reflexiva, transitiva e antissimétrica.

As propriedades citadas nas definições são as seguintes:

O1: Propriedade reflexiva: $\forall\ x \in E$, tem-se xRx.

O2: Propriedade antissimétrica: $\forall\, x, y \in E$, se xRy e se yRx, então $x = y$.

O3: Propriedade transitiva: $\forall\, x, y, z \in E$, se xRy e se yRz, então xRz.

Observe que é utilizada a mesma notação de teoria dos conjuntos, que coloca o nome da relação entre os nomes dos elementos relacionados. É a mesma postura usada habitualmente em $x \leq y$.

Portanto, uma estrutura ordenada é dada por um par ordenado (E, R), onde R é uma ordem sobre o conjunto E, ou seja, E é um conjunto ordenado pela ordem R. Depois de fixada a ordem R sobre E, diz-se, simplesmente, que E é um conjunto ordenado.

Colocamos a seguir a definição de uma relação de ordem total e em seguida a de ordem estrita.

Definição: Uma relação de ordem R sobre um conjunto E é uma **relação de ordem total** se, e somente se, atende a propriedade da totalidade.

O4: Propriedade da totalidade: $\forall\, x, y \in E$, tem-se xRy ou yRx.

Quando um conjunto E atender a uma ordem total R, será dito que o conjunto E é totalmente ou linearmente ordenado pela ordem R, ou seja, a ordem R é uma ordem total ou linear sobre E.

Definição: Seja o conjunto E ordenado pela relação R, uma relação R^* será chamada de **ordem estrita** sobre E, se para $x, y \in E$ for válida xR^*y se, e somente se, xRy e $x \neq y$.

É possível verificar que a ordem estrita R^*satisfaz as seguintes condições:

O1': $\forall x \in E$ tem-se que não é válido xR^*x;

O2': $\forall\, x, y \in E$, se xR^*y , então não é válido yR^*x;

O3: $\forall\, x, y, z \in E$, se xR^*y e se yR^*z, então xR^*z.

É interessante observar que: se a ordem R for total, para uma ordem estrita R^* associada a R, a condição O4 poderá ser enunciada sob a forma da lei da tricotomia:

O4': $\forall\, x, y \in E$, tem-se que xR^*y, ou $x = y$, ou yR^*x.

Para indicar uma relação de ordem, em geral, o símbolo $\leq$ é empregado, então: $a \leq b$ significa que "a é menor ou igual a b".

A ordem estrita $<$ é associada à ordem $\leq$, então $a < b$ significa que "a é estritamente menor que b", ou seja, $a \leq b$ e $a \neq b$.

Existe também a notação oposta de $\leq$ indicada por $\geq$, então, para a situação acima $a \leq b$, tem-se, consequentemente, que $b \geq a$ significa que "b é maior ou igual a a".

Obviamente, a notação oposta da ordem estrita $<$ é indicada por $>$, então: $b > a$ significa que "b é estritamente maior que a".

2.5 Corpo ordenado

Um corpo K será chamado de corpo ordenado se existir uma relação de ordem total que permita verificar quando um elemento é maior que outro, e que seja compatível com as operações de adição e multiplicação da definição de corpo.

Um corpo K ordenado possui os elementos neutros da adição e da multiplicação, respectivamente, 0 e 1, e $0 < 1$, pois num corpo $0 \neq 1$ e $0 \leq 1^2 = 1$ devido ao fato (verificado a seguir) os quadrados serem sempre não negativos.

Se um corpo K é ordenado pela relação binária $\leq$, então, ele atende as seguintes propriedades, para $a, b, c \in K$:

(0) Sempre $a \leq a$ (reflexão).

(1) Se $a \leq b$ e $b \leq a$, então $a = b$ (antissimetria).

(2) Se $a \leq b$ e $b \leq c$, então $a \leq c$ (transitividade).

(3) Dados $a, b \in K$, ou $a \leq b$ ou $b \leq a$ (totalidade).

(4) Se $a \leq b$, então $a + c \leq b + c$.

(5) Se $a \leq b$ e $0 \leq c$ então $ac \leq bc$, e se $c \leq 0$ então $bc \leq ac$.

Uma ordem total sobre o corpo K é estabelecida pelos quatro primeiros axiomas e os dois últimos axiomas estabelecem a compatibilidade das operações de adição e multiplicação com a ordem estabelecida.

Outra forma de definir corpo ordenado $(K, \leq)$ é a partir do conjunto P dos elementos não negativos de K, sendo $P = \{x \in K: 0 \leq x\}$ chamado de o cone positivo de K. Veja a seguir a definição de corpo ordenado a partir do cone positivo.

Definição: Um corpo K é ordenado se o cone positivo $P \subset K$, verifica os seguintes axiomas:

(P0) $P \cap (-P) = \{0\}$

Define-se $-P = \{-x : x \in P\}$

(P1) $P \cup (-P) = K$

(P2) $P + P \subset P$

Por definição $P + P = \{x + y : x, y \in P\}$

(P3) $P.P \subset P$

Por definição $P.P = \{x.y : x, y \in P\}$

Teorema: As duas definições que foram dadas para corpo ordenado se equivalem e demonstraremos isso a seguir.

Demonstração: A condição P0 vem diretamente da definição do cone positivo P sobre o corpo K; P1 resulta do fato que a ordem $\leq$ é total; P2 resulta da soma de desigualdades; P3 resulta do produto de desigualdades.

Agora será demonstrada a recíproca.

Veja que o cone positivo do corpo K satisfaz as condições P0, P1, P2 e P3 e define uma relação de ordem $\leq$ sobre K, da seguinte forma: para $a, b \in K$, vale $a \leq b$ se, e somente se, $b - a \in P$. Desse modo, $a < b$ se, e somente se, $b - a \in P - \{0\}$. Consequentemente, a notação $a \in P$ é equivalente a dizer que $0 \leq a$ ou que $a \geq 0$ e a notação $a \leq b$ é usada para $b - a \in P$.

A verificação que esta relação satisfaz as condições que foram enunciadas na definição anterior de corpo ordenado dada com base na relação binária $\leq$ será feita a seguir:

(0) Sempre $a \leq a$ (reflexão).

Essa propriedade é imediata pelo axioma P0, pois $a - a = 0 \in P$.

(1) Se $a \leq b$ e $b \leq a$, então $a = b$ (antissimetria).

Pelo axioma P0, suponha que $b - a \in P$ e $a - b \in P$, como $b - a = -(a - b)$, tem-se que, $a - b \in -P$, logo $a - b \in -P \cap P$, o que acarreta que $a - b = 0$, ou seja, $a = b$.

(2) Se $a \leq b$ e $b \leq c$, então $a \leq c$ (transitividade).

Tem-se que $a \leq b$ e $b \leq c$, então $(b - a), (c - b) \in P$. Pelo axioma P2 vale $(b - a) + (c - b) \in P$, ou seja, $(c - a) \in P$, portanto, $a \leq c$.

(3) Dados $a, b \in K$, ou $a \leq b$ ou $b \leq a$ (totalidade).

Tem-se pelo axioma P1 que $a - b \in P$ ou $a - b \in -P$. Se $a - b \in P$ então $b \leq a$ e se $a - b \in -P$ então $a \leq b$.

(4) Se $a \leq b$, então $a + c \leq b + c$, para todo $c \in K$.

Se $a, b, c \in K$ e supondo $a \leq b$ tem-se que $b - a \in P$, e considerando que $c + (-c) = 0$ vem $b - a = (b + c) - (a + c) \in P \Rightarrow a + c \leq b + c$, aqui usou-se o axioma P2.

(5) Se $a \leq b$ e $0 \leq c$ então $ac \leq bc$, e se $c \leq 0$ então $bc \leq ac$.

Tem-se que $a \leq b$, $b - a \in P$, então:

se $0 \leq c$, tem-se $c \in P$. Logo: $(b - a).c \in P \Rightarrow bc - ac \in P \Rightarrow ac \leq bc$, aqui foi utilizado o axioma P3. ■

Nota-se que se tem duas construções: a partir da ordem $\leq$ obtemos o cone $P_{\leq}$ e a partir do cone P obtemos a ordem $\leq_P$. Percebe-se que uma é inversa da outra, de modo que $\leq_{(P_{\leq})} = \leq$ e $P_{(\leq_P)} = P$.

Com base no que foi exposto, sobre corpo ordenado e o cone positivo P do corpo ordenado, o seguinte lema pode ser enunciado:

Lema: O cone positivo P de um corpo ordenado K é fechado para a adição e a multiplicação, $-1 \notin P$, e para todo $x \in K$ tem-se que $x^2 \in P$.

Demonstração:

1) O fato do cone positivo P do corpo K ser fechado para a adição e a multiplicação decorre diretamente da definição de corpo e de cone positivo.

2) o fato de $-1 \notin P$ pode ser mostrado da seguinte forma:

Como $1 = 1^2 \in P$ e $1 \neq 0$ temos que $1 \in P$ e que $-1 \in -P$, logo, $-1 \notin P$. Caso contrário $1 \in P \cap (-P) = \{0\}$ e $1 = 0$ (absurdo).

3) O fato de que para todo $x \in K$ tem-se que $x^2 \in P$ pode ser mostrado da seguinte forma:

Se $x \in P$, então, $-x \in -P$ e, portanto,

$xx = x^2 \in P$

e $(-x)(-x) = xx = x^2 \in P$ (válido pela regra de sinais, e por $a \leq b$ e $b \leq a$, então $a - b \in P \cap (-P)$).

Logo $x^2 \in P$, para qualquer que seja $x \in K$. ■

A seguir será feita uma observação interessante a respeito de uma pré-ordem própria.

Pré-ordem própria: Se, para $P \subseteq K$, forem válidas as propriedades: P2, P3, $-1 \notin P$, e todo quadrado pertencer a P, então a relação $a \leq b$ para $(b - a) \in P$ é uma pré-ordem sobre K.

Abaixo, se encontram destacadas as propriedades de ordem relativas ao produto válidas num corpo ordenado K. Elas são consequências dos novos axiomas de corpo ordenado.

1) Regra de sinais (2º tipo):

a) se $0 < a$ e $0 < b$, então $0 < ab$;

b) se $a < 0$ e $b < 0$, então $0 < ab$;

c) se $a < 0$ e $0 < b$, então $ab < 0$.

Comparando essas regras de sinais com as propriedades da seção 1.3, em particular com a propriedade 11 e 6, pode-se observar que essas novas regras de sinais do 2º tipo são compatíveis com as que foram colocadas na propriedade 11. Veja:

a) é compatível com a definição de multiplicação e com a propriedade 6 e11, pois se for colocado que x e $y \in P \subset K$ então $xy = (-x)(-y)$ e tem-se a compatibilidade com a regra de sinais do 2º tipo. Veja: se $0 < x$ e $0 < y$, então $0 < xy$.

b) é compatível com a propriedade 11, pois se for colocado x e $y \in P \subset K$ então $(-x)(-y) = xy$ e tem-se a compatibilidade com a regra de sinais do 2º tipo. Veja: se $-x < 0$ e $-y < 0$, então $0 < (-x)(-y) = xy$.

c) é compatível com a propriedade 11da seção 1.3, pois se for colocado que x e $y \in P \subset K$ então $(-x)y = -(xy) = x(-y)$ e tem-se a compatibilidade com a regra de sinais do 2º tipo. Veja: se $-x < 0$ e $0 < y$, então $(-x)y = -(xy) = x(-y) < 0$.

2) $0 \leq a^2$ para qualquer $a \in K$, e $0 < a^2$ para qualquer $a \in K - \{0\}$.

3) Se $a \neq 0$, então a e a^{-1} são ambos estritamente positivos ou estritamente negativos.

Use, para tanto, que: $a^{-1}.a^2 = a$, com $a^2 > 0$.

4) Se $0 < a < 1$, então $1 < a^{-1}$ e se $1 < a$, então $0 < a^{-1} < 1$.

5) Se $0 < a < b$, então $0 < b^{-1} < a^{-1}$ e se $a < b < 0$, então $b^{-1} < a^{-1} < 0$.

Proposição: Um corpo ordenado K tem característica zero.

Demonstração: Seja um corpo ordenado K com elemento unidade 1, e um número natural $n \neq 0$. Como $0 < 1$ e em virtude da regra de sinais da adição tem-se: $0 < n.1 = \underbrace{1 + \cdots + 1}_{n \text{ vezes}}$, portanto, a característica de um corpo ordenado K é zero. ■

Exemplos:

1) O corpo $\mathbb{Q}$ dos números racionais é ordenado, e a ordenação é única, a partir da ordem usual em $\mathbb{Z}$.

Para demonstrar a afirmação acima serão utilizadas as propriedades de quociente de um corpo (propriedade 14 da seção 1.3) e as definições de corpo ordenado e de cone positivo de um corpo.

O cone positivo P do conjunto dos números racionais $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}\ e\ b \in \mathbb{Z}^*\}$, onde $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, é formado por todas as frações a/b (a e b em $\mathbb{Z}$ e $b \neq 0$), tal que $0 \leq ab$ em $\mathbb{Z}$. Para que a fração $a/b \in P$ ela não depende da sua representação. Veja que se $a/b = c/d$ e se $0 \leq ab$ então $0 \leq cd$.

Agora, para fazer a verificação dos axiomas P0, P1, P2 e P3 do cone positivo em $\mathbb{Q}$, considere dois elementos x e y do cone positivo P de $\mathbb{Q}$, tais que $x = \frac{a}{c}$ e $y = \frac{b}{c}$, com $a, b, c \in \mathbb{Z}$ e $c \neq 0$. Então:

(P0) $P \cap (-P) = 0$

Se $x \in P \cap (-P)$, então $x \in P$ e $-x \in P$, como $x = \frac{a}{c}$ tem-se que $0 \leq ac$ e para $-x = \frac{-a}{c}$ tem-se $0 \leq (-a)c$, logo $ac \leq 0$, então $ac = 0$, usando-se as propriedades de ordem em $\mathbb{Z}$. Como $c \neq 0$, então $a = 0$, logo $x = 0$.

(P1) $P \cup (-P) = \mathbb{Q}$

O que se quer mostrar é que $x \in P \cup (-P)$. Se $0 \leq ac$ então $\frac{a}{c} \in P$; se $ac \leq 0$, então, $(-a)$c ≥ 0 e $\frac{-a}{c} \in P$, ou seja, $x \in -P$.

(P2) $P + P \subset P$

Sejam $x, y \in P$, como $x = \frac{a}{c}$ e $y = \frac{b}{c}$, podemos assumir isto pois se $x = \frac{a'}{u}$ e $y = \frac{b'}{v} \Rightarrow x = \frac{a'v}{uv}$ e $y = \frac{b'u}{uv}$, então, tem-se que $x + y = \frac{a}{c} + \frac{b}{c} = \frac{a+b}{c} \in P$ porque $ac \geq 0$ e $bc \geq 0$ implicam $(a + b)c \geq 0$.

(P3) $P.P \subset P$

Sejam $x, y \in P$, como $x = \frac{a}{c}$ e $y = \frac{b}{c}$, então, tem-se que $x.y = \frac{a}{c}.\frac{b}{c} = \frac{a.b}{c^2} \in P$ porque $ac \geq 0$ e $bc \geq 0$ implicam $(a.b)c^2 \geq 0 \Rightarrow xy \geq 0$.

2) O corpo $\mathbb{C}$ dos números complexos, $\mathbb{C} = \{a + bi: a, b \in \mathbb{R}\}$ com $i = \sqrt{-1}$, não é ordenável, pois se fosse existiria um cone positivo $P \subseteq \mathbb{C}$ e ocorreria que: $i \in P$ ou $-i \in P$. Logo: $i^2 = (-i)^2 = -1 \in P$, mas isso é absurdo, pois $-1 \notin P$. Portanto, o corpo $\mathbb{C}$ não pode ser ordenado com ordem total compatível com $(+)$ e $(.)$.

3

CLASSES DE CORPOS ORDENADOS

Neste capítulo serão estudadas algumas classes de corpos ordenados, tais como: corpo arquimediano, corpo ordenado completo, corpo formalmente real, corpo real fechado e o corpo de funções racionais dos reais. Ao longo do capítulo, também, são colocados conceitos e definições necessários para fundamentar esses estudos e que permitem enunciar a propriedade da completude, tais como: majorante e minorante, máximo e mínimo, supremo e ínfimo.

3.1 Majorante e minorante, máximo e mínimo, supremo e ínfimo

O objetivo dessa seção é introduzir os conceitos que permitem enunciar a propriedade de completude que, por sua vez, pode ser utilizada para diferenciar $\mathbb{R}$ de $\mathbb{Q}$.

Definição: Diz-se que uma parte A não vazia de um conjunto E, ordenado pela ordem $\leq$, é majorada se, e somente se, existe $b \in E$, tal que $x \leq b$ para todo x em A.

Na definição acima A é dito majorado ou limitado superiormente e todo elemento $b \in E$ que atende a definição é chamado de limitante superior ou majorante de A.

Definem-se, da mesma forma, as noções de conjunto minorado ou conjunto limitado inferiormente, minorante ou limitante inferior.

Um conjunto A é dito limitado se for limitado inferiormente e superiormente.

Definição: Seja A um conjunto ordenado pela ordem $\leq$. Diz-se que um elemento $m \in A$ é um **máximo** de A (respectivamente **mínimo** de A) se, e somente se, m é um **majorante** de A (respectivamente **minorante** de A). Note, aqui, que m deve ser elemento de A.

Proposição: Se existir o máximo de A, então este máximo é único. Veja:

Demonstração: Admita que $m\ e\ m'$ são máximos de A, então: $m \leq m'$ pois m' é majorante de A e $m \in A$, analogamente, $m' \leq m$, pois m é majorante de A e $m' \in A$, portanto, devido à propriedade antissimétrica: $m = m'$. ■

Da mesma forma tem-se que: se m é mínimo de A, então este mínimo é único.

A notação do máximo de A será feita por máx (A) e do mínimo de A por mín (A).

Exemplos:

1) No subconjunto D dos números reais, dado pelo intervalo $[-2,0]$, tem-se:
mín $(D) = -2$ e máx $(D) = 0$.

2) No subconjunto $F =]-1,4]$ dos números reais, tem-se:
não existe mínimo em F e máx $(F) = 4$.

3) O subconjunto dos números reais dado por $]-1,6[$ não possui mínimo, nem máximo.

Aqui vale a pena notar: I) a diferença substancial do que se segue com o conteúdo do Ensino Médio e II) que será dado valor ao papel de -1 e 6 no exemplo 3.

Definição: Seja A um subconjunto não vazio de um conjunto E ordenado pela ordem $\leq$. Diz-se que um elemento $m \in E$ é o **supremo** de A (respectivamente **ínfimo** de A) se, e somente se, tal m é o **menor majorante** de A (respectivamente **maior minorante** de A).

A notação do supremo de A será feita por sup (A) e do ínfimo de A por ínf (A). Então:

sup $(A) =$ mín $\{x \in E : x$ é majorante de $A\}$

ínf $(A) =$ máx $\{x \in E : x$ é minorante de $A\}$

Para um conjunto ilimitado superiormente e inferiormente, ou seja, que não tem mínimo, nem máximo, usam-se para indicação de ínfimo e supremo, respectivamente, $-\infty$ e $+\infty$.

Exemplos:

1) Se $H = \{x \in \mathbb{R} : x = \frac{1}{n},\ n \in \mathbb{N} - \{0\}\}$, então:

H não possui mínimo e tem ínf $(H) = 0$.

H possui máx $(H) = 1$ e sup $(H) =$ máx $(H) = 1$.

2) No conjunto dos números naturais, $\mathbb{N}$ tem-se:

$\mathbb{N}$ possui mín $(\mathbb{N}) = 0$ e ínf $(\mathbb{N}) = 0$.

$\mathbb{N}$ não possui máximo e $\sup(\mathbb{N}) = +\infty$.

3) No subconjunto dos números reais, $F =]-2,4]$, tem-se que:

F não possui mínimo e tem ínf $(F) = -2$.

F possui máx $(F) = 4$ e $\sup(F) = $ máx $(F) = 4$.

Pelo que foi exposto as seguintes proposições podem ser colocadas:

Proposição: Sejam $A \subset E$, $A \neq \emptyset$ e $m \in E$. Então: $m = $ máx $(A) \Leftrightarrow m = \sup(A)$ e $m \in A$.

Proposição: Sejam $A \subset E$, $A \neq \emptyset$ e $m \in E$. Então: $m = $ mín $(A) \Leftrightarrow m = $ ínf (A) e $m \in A$.

Outra propriedade que possui papel relevante em vários teoremas do cálculo, e é de vital importância na definição dos números reais, que é um corpo ordenado completo, é a propriedade do supremo, definida a seguir:

Propriedade do Supremo: Todo subconjunto de números reais, não vazio e majorado, possui supremo.

Outras duas propriedades relevantes para o cálculo são consideradas consequências da propriedade do supremo e serão enunciadas a seguir:

Propriedade de Arquimedes: Um conjunto A é arquimediano se para dois elementos quaisquer $x, y \in A$, $x, y > 0$, existe pelo menos um número natural n tal que $nx > y$.

Demonstração: Considere o conjunto $D = \left\{n \in \mathbb{N} : n \leq \frac{y}{x}\right\}$. Agora serão analisadas as possibilidades: $D = \emptyset$ e $D \neq \emptyset$.

Se $D = \emptyset$, então $n > \frac{y}{x}$ para qualquer $\forall\, n \in \mathbb{N}$, e tem-se que $nx > y$.

Se $D \neq \emptyset$, então $\frac{y}{x}$ é um limitante superior de D, ou seja, D é limitado superiormente. Assim, existe um número real p que é o supremo de D, e existe um número natural n_0, tal que $n_0 > p \Rightarrow n_0 \notin D \Rightarrow n_0 > \frac{y}{x} \Rightarrow n_0 x > y$. ■

Aqui, fez-se uso do fato de todo real (p) estar abaixo de um natural n_0, ou seja, $\mathbb{N}$ não é limitado superiormente. Isso será provado no Exemplo 1, a seguir.

Como já foi afirmado a propriedade arquimediana pode ser considerada uma

consequência da propriedade do supremo, porém, ela não é equivalente à propriedade do supremo. Portanto, não é necessário que o conjunto admita a propriedade do supremo para ser arquimediano.

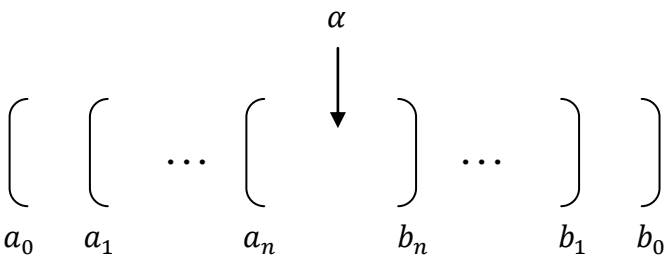
O exemplo abaixo ajuda a compreender melhor essa ideia.

Exemplo:

1) Considere válido o axioma do supremo. Agora será provado que o conjunto $\mathbb{N}$ não tem majorante. Por absurdo, admita $\mathbb{N}$ limitado superiormente, logo existe $\sup(\mathbb{N}) = s$, $s \in \mathbb{R}$. Como $\mathbb{N}$ é não vazio, existe um $n \in \mathbb{N}$, tal que $n > s - 1$, porque $s - 1 < s$ que é supremo, logo $n + 1 > s \Rightarrow s$ não é um majorante de $\mathbb{N}$, ou seja, $n + 1$ é um majorante de $\mathbb{N}$ o que é um absurdo, pois $n + 2 \in \mathbb{N}$. Logo, $\mathbb{N}$ não é limitado superiormente e, portanto, vale a propriedade arquimediana.

Propriedade dos intervalos encaixantes: Em $\mathbb{R}$**,** numa sequência de intervalos fechados $[a_0, b_0] \supset [a_1, b_1] \supset [a_2, b_2] \supset \ldots \supset [a_n, b_n] \supset \cdots$ existe um número real α que pertence a todos os intervalos da sequência, ou seja, $a_n \leq \alpha \leq b_n$, para $\forall\, n \in \mathbb{N}$.

Esquematicamente tem-se:



Em símbolos a propriedade dos intervalos encaixantes pode ser escrita como:

Sejam os intervalos $I_n = [a_n, b_n]$, para $n \in \mathbb{N}$, que satisfaçam:

$I_0 \supset I_1 \supset I_2 \supset \ldots$, então tem-se que: $\bigcap_{n=0}^{\infty} I_n \neq \emptyset$.

Demonstração: Seja $A = \{a_n : n \in \mathbb{N}\}$, não vazio e limitado superiormente, pois cada b_n é um majorante de A. Pela propriedade do supremo, existe um $\alpha \in \mathbb{R}$, tal que $\alpha = \sup(A)$. Então $a_n \leq \alpha$ para qualquer $n \in \mathbb{N}$, e também $\alpha \leq b_n$ para qualquer $n \in \mathbb{N}$ porque α é o menor majorante de A, logo $a_n \leq \alpha \leq b_n$. Portanto, α pertence à intersecção de todos os intervalos fechados I_n. ■

Observação: Pode-se concluir que $\bigcap_{n=0}^{\infty} I_n$ é formada por um único elemento se for admitida a hipótese que $b_n - a_n \longrightarrow 0$.

Exemplo:

1) A expansão decimal do número real $\sqrt{3}$ é dada por 1,732050808... . A propriedade dos intervalos encaixantes e a observação que foi feita pode mostrar que essa expansão decimal de $\sqrt{3}$ leva a um único número. Veja:

$\sqrt{3} \in [1,2]$

$\sqrt{3} \in \left[1 + \frac{7}{10}, 1 + \frac{8}{10}\right]$

$\sqrt{3} \in \left[1 + \frac{7}{10} + \frac{3}{10^2}, 1 + \frac{7}{10} + \frac{4}{10^2}\right]$

$\sqrt{3} \in \left[1 + \frac{7}{10} + \frac{3}{10^2} + \frac{2}{10^3}, 1 + \frac{7}{10} + \frac{3}{10^2} + \frac{3}{10^3}\right]$

$\sqrt{3} \in \left[1 + \frac{7}{10} + \frac{3}{10^2} + \frac{2}{10^3} + \frac{0}{10^4}, 1 + \frac{7}{10} + \frac{3}{10^2} + \frac{2}{10^3} + \frac{1}{10^4}\right]$

$\vdots$

Observe que a expansão decimal corresponde a uma sequência de intervalos encaixantes com comprimento 10^{-n} tendendo a zero quando n tende ao infinito, que, por sua vez, garantem que o número em questão existe e é único.

3.2 Corpo arquimediano

Um corpo ordenado K, com elemento unidade 1, é arquimediano se, e somente se, para todo elemento estritamente positivo $a \in K$, existe um número natural $n \neq 0$ tal que $a < n1$.

Exemplo:

1) O conjunto dos números racionais $\mathbb{Q}$ é um corpo arquimediano.

Na seção 2.5 já foi mostrado que $\mathbb{Q}$ é um corpo ordenado, então basta mostrar a arquimedianidade, o que será feito a seguir.

Seja $d \in \mathbb{Q}$ um número racional estritamente positivo, então $d = \frac{m}{n}$ e $m, n \in \mathbb{N} - \{0\}$, e pode-se tomar $m + 1 \in \mathbb{Q}$, de modo que $\frac{m}{n} < m + 1$, ou seja, $\mathbb{Q}$ é arquimediano de acordo com a definição de corpo arquimediano. ■

3.3 Corpo ordenado completo

Definição: Um corpo ordenado K é *completo* se todo subconjunto não vazio e majorado de K admite supremo em K.

Como será visto a respeito de $\mathbb{Q}$, não é necessário que um corpo ou um conjunto atenda a propriedade do supremo para ser arquimediano. No entanto, como apresentado na seção 3.1, da propriedade do supremo decorre a arquimedianidade, ou seja, se o corpo atende a propriedade do supremo é um corpo arquimediano. Logo, a seguinte proposição pode ser enunciada:

Proposição: Se um corpo é ordenado completo, ele é um corpo arquimediano.

Demonstração: Se K é um corpo ordenado completo, então K admite a propriedade do supremo e todo subconjunto limitado superiormente de K admite supremo. Então, para um subconjunto não vazio limitado superiormente $S \subset K$, existe $\sup(S) = s$. Para verificar que K é arquimediano tome $S = \{n.1 : n \in \mathbb{N}, a \in K \text{ e } n.1 \leq a\}$ e veja as duas possibilidades abaixo:

- se $S = \emptyset$ então $\forall n \ \ a < n.1$;

- se $S \neq \emptyset$, como a é majorante de S, existe $s = \sup S$, donde $s - 1 < n.1$ para algum $n \ \Rightarrow s < (n+1).1 \ \Rightarrow (n+1).1 \notin S \Rightarrow (n+1).1 > a.$■

Como a propriedade do supremo permitiu enunciar a propriedade dos intervalos encaixantes e numa análise mais rigorosa é possível verificar que elas se equivalem pode-se enunciar a seguinte proposição:

Proposição: Todo corpo ordenado completo é arquimediano e satisfaz a propriedade dos intervalos encaixantes.

Demonstração: Na proposição anterior mostrou-se que o corpo K ordenado completo é arquimediano, então resta mostrar que o corpo ordenado completo arquimediano admite a propriedade dos intervalos encaixantes. Então, considere:

Uma sucessão de intervalos fechados I_n em K tal que $I_{n+1} \subset I_n$ e $I_n = [a_n, b_n]$ para todo número natural n; neste caso, tem-se $a_n \leq b_n$ e é imediato que a sucessão (a_n) é crescente e majorada por qualquer b_n, e esta sucessão possui $\sup(a_n) = a \in I_n$. Então,

$a_n \leq a \leq b_n$ para qualquer $n \in \mathbb{N}$ porque também todo b_n é majorante dos a_n, logo $a \leq b_n$. Portanto, a pertence a intersecção de todos os intervalos fechados I_n, de K. ■

Exemplos:

1) O corpo $\mathbb{Q}$ é ordenado, mas não é completo porque não atende a propriedade do supremo ou os intervalos encaixantes. Para mostrar isso mais claramente considere o subconjunto $S \subset \mathbb{Q}$, tal que $S = \{s \in \mathbb{Q} : 0 < s \text{ e } s^2 < 2\} =]0, \sqrt{2}[\cap \mathbb{Q}$ e $T \subset \mathbb{Q}$, tal que $T = \{t \in \mathbb{Q} : t > 0 \text{ e } t^2 > 2\} =]\sqrt{2}, +\infty[\cap \mathbb{Q}$. Como a ordem em $\mathbb{Q}$ é densa, se existir $\sup S \in \mathbb{Q}$ teria que valer $(\sup S)^2 = 2$ e se existir um $\text{ínf}\, T \in \mathbb{Q}$ teria que valer que $(\inf T)^2 = 2$. Contudo, sabemos que não existe um número racional cujo quadrado seja igual a 2.

Antes de iniciar a demonstração será colocado e demonstrado um teorema sobre a ordem densa de um corpo ordenado K:

Teorema: Se K é um corpo ordenado pela ordem $\leq$, então o conjunto K é denso pela mesma ordem, isto é, se $a, b \in K$ e $a < b$, então existe $x \in K$ tal que $a < x < b$.

Demonstração: Se $a, b \in K$ e $a < b$, então $a < \frac{a+b}{2} < b$.

I) De $a < b \Rightarrow a + a < a + b \Rightarrow 2a < a + b \Rightarrow a < \frac{a+b}{2}$

II) De $a < b \Rightarrow a + b < b + b \Rightarrow a + b < 2b \Rightarrow \frac{a+b}{2} < b$

Agora será dado prosseguimento a demonstração do exemplo 1.

Demonstração:

A) O conjunto S não possui elemento máximo em $\mathbb{Q}$. Considere $s \in S$, agora tomando um número racional $r < 1$ tal que $0 < r < \frac{2-s^2}{2s+1}$. Veja que $s + r \in S$. Com efeito, de $r < 1$ segue-se que $r^2 < r$. Da outra desigualdade que r satisfaz segue-se que $r(2s + 1) < 2 - s^2$. Consequentemente, que $(s + r)^2 = s^2 + 2sr + r^2 < s^2 + 2sr + r = s^2 + r(2s + 1) < s^2 + 2 - s^2 = 2$, e assim dado qualquer $s \in S$ existe um número maior, $s + r \in S$.

B) O conjunto T não possui elemento mínimo em $\mathbb{Q}$. De fato, dado qualquer $t \in T$, tem-se que $t > 0$ e $t^2 > 2$. Logo, se pode obter um número racional r tal que $0 < r < \frac{t^2-2}{2t}$. Então $2rt < t^2 - 2$ e daí $(t - r)^2 = t^2 - 2tr + r^2 > t^2 - 2tr > 2$. Note também que $r < \frac{t}{2} - \frac{1}{t}$, donde $r < t$, isto é $t - r$ é positivo. Assim, dado $t \in T$, pode-se obter $t - r \in T$, e $t - r < t$.

C) Se $s \in S$ e $t \in T$, então $s < t$. Tem-se que $s^2 < 2 < t^2$ e, portanto, $s^2 < t^2$, consequentemente, $s < t$, pois s e t são positivos.

Usando os itens A, B e C é possível mostrar que em $\mathbb{Q}$ não existem $\sup S$ e $\text{ínf } T$.

Supondo que exista $a = \sup S$ e $a > 0$. Esse supremo não poderia ser $a^2 < 2$, pois $a \in S$, e então a seria o elemento máximo de S, que não existe por A. Por outro lado não poderia ser $a^2 > 2$, pois isto faria $a \in T$, mas devido ao item B, T não possui elemento mínimo em $\mathbb{Q}$.

Assim, se existisse $a = \sup S$, deverá ser $a^2 = 2$, o que contraria o lema de Pitágoras, logo não existe supremo de S em $\mathbb{Q}$, e com isso mostrou-se que $\mathbb{Q}$ não é completo.

2) O corpo $\mathbb{R}$ é ordenado e completo.

De fato o corpo $\mathbb{R}$ é um corpo ordenado completo, pois verifica a propriedade do supremo, a propriedade dos intervalos encaixantes e é arquimediano.

3) $\mathbb{R}$ é o único corpo ordenado e completo, a menos de isomorfismos.

Para esclarecer essa colocação, primeiro será visto de forma sucinta as definições de homomorfismo e isomorfismo para, em seguida, mostrar que na teoria dos corpos ordenados completos todos os seus modelos são isomórficos.

Definição: Dados dois corpos K e K' munidos, respectivamente, das operações e relações $+$, $.$, $<$, e $\oplus$, $\odot$, $\prec$, uma função $f: K \to K'$ é um homorfismo se, e somente se, $f(a+b) = f(a) \oplus f(b)$ e $f(a.b) = f(a) \odot f(b)$ para qualquer $a, b \in K$ e ainda $f(a) \prec f(b)$ para $a < b$ em K. Usa-se então os mesmos símbolos $+$, $.$, $<$.

Se f é bijetora, então f é um isomorfismo.

Na teoria dos corpos ordenados completos todos os seus modelos são isomórficos a $(\mathbb{R}, +, ., <)$, ou seja, a teoria dos corpos ordenados completos é categórica.

Para mostrar isso, considere dois corpos ordenados completos K e K', como corpos ordenados completos têm característica zero, pode-se admitir que $\mathbb{Q} \subseteq K, K'$. Veja também que para qualquer $x \in K$, existe uma sequência de racionais que converge para x: por exemplo, em $\mathbb{R}$, a sequência das expansões decimais finitas que aproximam x. Veja:

Dado $x \in K$, tome $x_0 = \sup\{r \in \mathbb{Q} : r \leq x\}$, então $\forall n \in \mathbb{N}\ \exists\, r_n \in \mathbb{Q} \cap \left]x_0 - \frac{1}{n}, x_0\right]$ (por propriedade do supremo) e obtemos $\lim r_n = x_0$. Note que $x_0 \leq x$ pela definição de

supremo. Para mostrar $x = x_0$, utiliza-se a arquimedianidade para construir racionais entre x_0 e x caso $x_0 < x$, levando a um absurdo.

Observe que quaisquer duas sequências de racionais, construídas por arquimedianidade, com mesmo limite em K devem ter o mesmo limite em K', isso porque a diferença entre elas converge para zero.

Então esta função está bem definida: $\Phi: K \to K'$, $\Phi(x)$ é o limite em K' de uma sequência de racionais que converge para x em K.

Agora será mostrado que Φ é um isomorfismo que fixa $\mathbb{Q}$:

I) Φ fixa $\mathbb{Q}$: se $r \in \mathbb{Q}$, a sequência constante r converge para r em K e K', logo $\Phi(r) = r$. Todo isomorfismo faz isso, bastando que fixe 0 e 1. Veja:

$$\Phi\left(\frac{m}{n}\right) = \frac{\Phi(m)}{\Phi(n)} = \frac{\Phi(1 + \cdots + 1)}{\Phi(1 + \cdots + 1)} = \frac{\Phi(1) + \cdots + \Phi(1)}{\Phi(1) + \cdots + \Phi(1)} = \frac{m\,\Phi(1)}{n\,\Phi(1)} = \frac{m}{n}$$

II) Φ preserva $+, ., <$: isso segue das propriedades de limites. No caso de $a, b \in K$, $a < b$, tomamos $q_1, q_2 \in \mathbb{Q}$, $a < q_1 < q_2 < b$. Temos então $n_0 \geq 0$ de modo que as sequências de racionais $r_n \to a$, $s_n \to b$ respeitam, para $n > n_0$, $r_n < q_1 < q_2 < s_n$ (em K e K', pois são todos racionais). Então $\lim r_n \leq q_1 < q_2 \leq \lim s_n$, donde $\Phi(a) < \Phi(b)$

III) Φ é injetor: por um argumento semelhante ao que mostra sua boa definição: se $x < y$ em K existe $q \in \mathbb{Q}$ tal que $x < q < y \Rightarrow \Phi(x) < \Phi(q) = q < \Phi(y)$

IV) Φ é sobrejetor: dado $y \in K'$, tome uma sequência de racionais convergindo para y, ou seja, é uma sequência de Cauchy. Se x é o limite dessa sequência em K, então $\Phi(x) = y$.

Obs.: Uma sequência de números reais é dita sequência de Cauchy se cumpre a seguinte condição: dado um número real arbitrário $\varepsilon > 0$, pode-se obter $n_0 \in \mathbb{N}$ tal que $m > n_0$ e $n > n_0$ implica $|x_m - x_n| < \varepsilon$.■

A construção do corpo ordenado completo $\mathbb{R}$, em geral, é feita usando-se os cortes de Dedekind como pode ser vista em Pontes (2014), ou por classes de equivalência de sequências de Cauchy, como pode ser vista em Monteiro (1978, p. 256 - 268). Ao final das construções, ambas as representações de $\mathbb{R}$ são isomórficas.

3.4 Corpo formalmente real

A teoria dos corpos formalmente reais foi desenvolvida por Émil Artin e Otto Schreier para demonstrar o décimo sétimo problema de Hilbert, proposto em 1.900. O enunciado desse problema é mostrar que: se uma expressão polinomial com números reais retorna sempre valores maiores ou iguais a zero, então essa expressão pode ser representada como uma soma de quadrados de funções racionais, ou seja, frações de polinômios.

Artin e Schreier demonstraram esse teorema para polinômios e funções racionais sobre um corpo formalmente real, mas cujos argumentos são elementos do seu fecho real. Portanto, a demonstração do teorema se aplica ao caso de $\mathbb{R}$ que é um corpo formalmente real e é o seu próprio fecho real.

A seguir será analisada a questão da ordem no corpo formalmente real, tendo como ponto de partida a busca de propriedades da adição e multiplicação que possam substituir a relação de ordem, e tomando como referência as propriedades dos números reais, então a seguinte consideração sobre corpo formalmente real pode ser colocada:

O conjunto dos números reais $\mathbb{R}$ atende a seguinte propriedade algébrica:
sejam $x_1, x_2, \dots, x_n \in \mathbb{R}$, então: $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$, se, e somente se, $x_1 = x_2 = \cdots = x_n = 0$.

O corpo que admite essa propriedade dos números reais será chamado de corpo formalmente real e a definição desse tipo de corpo pode ser enunciada da seguinte forma:

Definição: Um corpo K é formalmente real se

$$\sum_{i=0}^{m} x_i^2 = 0 \Rightarrow x_i = 0, \qquad 1 \leq i \leq m$$

A proposição a seguir coloca uma maneira equivalente de enunciar a definição:

Proposição: O corpo K é formalmente real se, e somente se, -1 não pode ser expresso como uma soma de quadrados de elementos de K.

Demonstração:

I) Se $\sum_{i=1}^{m} x_i^2 = -1$, $x_i \in K$, então $\sum_{i=1}^{m} x_i^2 + 1^2 = 0$, de modo que K não pode ser formalmente real.

II) Se K não for formalmente real, pode-se escrever $\sum_{i=0}^{m} x_i^2 = 0$, $x_i \in K$ e assumindo $x_1 \neq 0$, então dividindo tudo por x_1^2, vem $1 + \sum_{i=2}^{m} \frac{x_i^2}{x_1^2} = 0$, donde $\sum_{i=2}^{m} \left(\frac{x_i}{x_1}\right)^2 = -1$. ■

Proposição: Se um corpo K é formalmente real, então a sua característica é zero.

Demonstração: Admita que a característica de um corpo K é $p > 0$. Então:
$0 = \underbrace{1^2 + 1^2 + \ldots + 1^2}_{p \text{ parcelas}}$, o que contradiz a definição de corpo formalmente real. ■

O teorema a seguir confirma que essa propriedade captura a noção de ordem.

Teorema: As condições abaixo são equivalentes para um corpo K.

(1) K é um corpo ordenável, isto é existe uma ordem total em K compatível com $+$ e $.$;

(2) K é um corpo formalmente real.

Referência: Teorema 11.1 em Jacobson (1980). Discutem-se abaixo as idéias principais.

(1) Sendo P o cone positivo do corpo ordenado K, então, pelo que foi mostrado na seção 2.5 sobre o cone positivo de um corpo ordenado, tem-se que se $x \in K$, então $x^2 \in P$ e $-1 \notin P$, também tem-se que P é fechado para a soma e o produto, então toda soma de quadrados de P continua em P. Logo, -1 não poderá ser expresso como uma soma de quadrados em K.

(2) Sendo K formalmente real, defina:

$$P_0 = \left\{ \sum_{i=1}^{m} x_i^2 : x_i \in K, 1 \leq i \leq m \right\}$$

Então P_0 verifica todas as condições de pré-ordem própria que foram colocadas na seção 2.5, veja abaixo.

$-1 \notin P_0$, pois é um corpo formalmente real;

qualquer $x \in K$ tem quadrado em P_0;

P_0 é fechado para a soma e para o produto, veja: $\sum_{i=1}^{m} x_i^2 + \sum_{j=1}^{m} y_j^2$ é uma soma de quadrados e $\left(\sum_{i=1}^{m} x_i^2\right).\left(\sum_{j=1}^{m} y_j^2\right) = \sum_{i,j}^{m} x_i^2 y_j^2 = \sum_{i,j}^{m} \left(x_i y_j\right)^2$.

Uma aplicação do lema de Zorn acarreta que existe um cone positivo P, tal que $P_0 \subseteq P$. A respeito desse lema, veja Fernandes; Ricou (2004), Endler (2012) e Lopes (2012), para então acompanhar os cálculos em Jacobson (1980, t. 11.1).

3.5 Corpo real fechado

Os corpos reais fechados são uma subclasse de corpos ordenados que em relação à ordem e as propriedades algébricas tem comportamento igual ao dos números reais. Essa subclasse de corpos ordenados será definida a seguir:

Definição: Um corpo ordenado K é dito real fechado se todo polinômio de grau ímpar em K tem uma raiz em K, e todo elemento positivo de K tem uma raiz quadrada em K.

A seguir será mostrado que $\mathbb{R}$ é um corpo real fechado usando o Teorema do Valor Intermediário, para isso será enunciado o teorema do valor intermediário e logo após proposto e demonstrado que uma função polinomial $p(x)$ com grau ímpar possui raízes em $\mathbb{R}$.

Teorema do valor intermediário: Se $f:[a;\ b] \to \mathbb{R}$ uma função contínua e d um número entre $f(a)$ e $f(b)$. Então existe um número $c \in (a;\ b)$ tal que $f(c) = d$. A demonstração desse teorema pode ser vista em Guidorizzi (1987, p. 458) e requer apenas a completude de $\mathbb{R}$.

Proposição: $\mathbb{R}$ é um corpo real fechado, então $p: \mathbb{R} \to \mathbb{R}$ definida por:

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

com n inteiro e ímpar e $a_n \neq 0$ possui uma raiz em $\mathbb{R}$**.**

Demonstração: As funções polinomiais são funções contínuas logo $p: \mathbb{R} \to \mathbb{R}$ é contínua. Agora, sem perda de generalidade, supondo $a_n > 0$ pode-se escrever:

$$p(x) = x^n \left(a_n + \frac{a_{n-1}}{x} + \ldots, + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n}\right)$$

e assim, tem-se $\lim_{x\to-\infty} p(x) = -\infty$ e $\lim_{x\to+\infty} p(x) = +\infty$, visto que n é um número ímpar. Isso significa que existe $c \in \mathbb{R}$, tal que $p(c) = 0$. ■

Uma proposição interessante que mostra que todo elemento positivo do corpo real fechado $\mathbb{R}$ tem raiz quadrada em $\mathbb{R}$ é:

Proposição: $a \in \mathbb{R}, a > 0 \Rightarrow \exists b$ e $b^2 = a$.

Se $a = 0$ ou $a = 1$, tem-se: $0^2 = 0$ e $1^2 = 1$.
Se $1 < a$, tem-se: para $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ contínua, como $f(1) = 1$, $f(a) = a^2$ e $1 < a < a^2$, então $\exists b$ tal que $f(b) = a$.

Se $1 > a > 0$, tem-se: para $f: \mathbb{R} \to \mathbb{R}, f(x) = x^2$ contínua, como $f(1) = 1$, $f(a) = a^2$ e $1 > a > a^2 > 0$, então $\exists b$ tal que $f(b) = a$.

Proposição: Seja K um corpo ordenado. Então K é real fechado se, e somente se, $K(i)$ é algebricamente fechado.

Essa proposição não será demonstrada e detalhes adicionais sobre ela podem ser vistos em Martin (2010, p. 393-399) e Lang (2002, p. 451-454).

Para entender essa caracterização é preciso explicar o que é $K(i)$. Qualquer que seja K, esse é o menor corpo que estende K - isto é, contém K com as mesmas operações - e contém $i = \sqrt{-1}$. Um possível modo de construí-lo é usando o corpo de frações racionais $K(X)$, que será construído depois, particularmente, para $K = \mathbb{R}$, com a substituição $X = i$ e a regra $i^2 = -1$.

Os corpos reais fechados são os que melhor compartilham as propriedades de $\mathbb{R}$, mas sua teoria extrapola o espaço deste trabalho: uma sugestão é Prestel (2009, cap. 3). Aqui apenas será elucidado o Teorema de Tarski- Seidenberg, isto é, será explicado o seu enunciado:

Teorema: Em um corpo real fechado, toda propriedade pode ser escrita, na linguagem $+, ., 0, 1$ e $\leq$, equivalentemente, sem quantificadores, e todos os corpos reais fechados, assim como $\mathbb{R}$, satisfazem as mesmas propriedades fechadas. (Prestel (2009, p. 24 - 25).)

Para maior clareza será verificado o que significa "propriedade" e "propriedade fechada". Uma propriedade é uma expressão de comprimento finito, com significado preciso, escrita utilizando-se somente estes símbolos:

- Variáveis: x, y, z, x_1, x_2, x_3, ... para os elementos do corpo;
- Constantes: 0 e 1;
- Operações: $+, -, .$;
- Relações binárias $=$ e $<$;
- Parênteses: (e);
- Conectivos lógicos: & ("e"), $\vee$ ("ou"), $\to$ ("implica") e $\neg$ ("não");
- Quantificadores: $\forall$ ("para todo") e $\exists$ ("existe").

Essa definição pode ser melhorada, para o que se indica textos de lógica como Prestel (2009, cap. 1 e 3).

Por exemplo, pode-se escrever a seguinte propriedade:

$P(x,y)$: $\exists z\ (x.x.z + x.y + 1 = 0)$

A partir de $P(x,y)$, também pode-se construir outras propriedades, como $\exists x\ P(x,y)$ e $\forall x \exists y\ P(x,y)$. Esta última é um exemplo de propriedade fechada ou sentença, em que toda variável é quantificada.

São essas propriedades que se utilizam para descrever lugares geométricos como conjuntos de pontos (no plano, no espaço, etc.) que satisfazem propriedades dadas. Por exemplo, com a seguinte propriedade:

$Q(x,y)$: $x.x + y.y = 1 + 1 + 1 + 1$,

o conjunto $\{(x,y) \in \mathbb{R}^2 : Q(x,y)\}$ é a circunferência de centro na origem e raio 2, vista como lugar geométrico.

A seguir, no exemplo, veja o que o teorema de Tarski-Seidenberg fala sobre os lugares geométricos.

Exemplo:

1) Seja $P(x)$ uma propriedade , para um corpo real fechado K. Então $\{x \in K : P(x)\}$ é uma união de um número finito de intervalos. Para demonstrá-lo, usou-se o teorema para assumir que P não tem quantificadores. A seguir, fez-se uso de um resultado de lógica que permite escrever tal P assim:

$$(P_{11}(x)\ \&\ P_{12}(x)\ \&\ \dots) \vee (P_{21}(x)\ \&\ P_{22}(x)\ \&\ \dots) \vee \dots$$

onde cada propriedade $P_{ij}(x)$ é uma equação ou inequação ou desigualdade, ou seja, não tem conectivos ou quantificadores. Olhando com mais atenção a definição de propriedade, é possível ver que $P_{ij}(x)$ pode ser reescrita como:

$$p_{ij}(x) = 0 \text{ ou } p_{ij}(x) \neq 0 \text{ ou } p_{ij}(x) > 0 \text{ ou } p_{ij}(x) \geq 0$$

onde $p_{ij}(x)$ é um polinômio na variável x. Como o polinômio tem um número finito de raízes, o lugar geométrico de $P_{ij}(x)$ é da forma enunciada (entendendo-se um ponto também como intervalo) e as equações de intersecção e união preservam essa forma.

3.6 Corpo de funções racionais dos reais e infinitésimos

Para tratarmos do conceito do corpo de funções racionais convém antes rever a definição de polinômios com uma indeterminada X sobre um corpo $\mathbb{R}$, e para isto será colocada algumas considerações sobre polinômios e indeterminada.

Seja $\mathbb{R}$ o corpo dos reais e X uma indeterminada sobre $\mathbb{R}$, o conjunto $\mathbb{R}[X]$ dos polinômios com coeficientes em $\mathbb{R}$ é formado por polinômios representados na forma usual por:

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X^1 + a_0$$

onde os a_n são os coeficientes em $\mathbb{R}$.

Um polinômio de $\mathbb{R}[X]$ também pode ser representado como uma soma finita: $f = \sum_{i=0}^{n} a_i X^i$, para algum $n \in \mathbb{N}$.

Agora serão colocadas algumas considerações sobre um polinômio f qualquer de $\mathbb{R}[X]$.

- o grau de f é n, se n é o maior inteiro para o qual $a_n \neq 0$, ou seja gr $(f) = n$ se $a_n \neq 0$ e nesse caso o coeficiente a_n é chamado de principal, por ser o coeficiente que acompanha a indeterminada de maior grau.

- se $a_n = 1$, chamamos f de polinômio mônico.

- se todos os coeficientes de f forem nulos, f será um polinômio nulo, $f = 0$.

- um termo qualquer, $a_n X^n$, do polinômio f é chamado de monômio.

Em $\mathbb{R}[X]$ definem-se as operações de adição e multiplicação. Veja:

Sejam: $f(X) = \sum_{i=0}^{n} a_i X^i$ e $g(X) = \sum_{i=0}^{n} b_i X^i$, observe que aqui pode ter a_n ou $b_n = 0$, polinômios quaisquer de $\mathbb{R}[X]$, então:

na adição: $\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{n} b_j X^j = \sum_{i=0}^{n} (a_i + b_i) X^i$

na multiplicação: $(\sum_{i=0}^{n} a_i X^i) . (\sum_{j=0}^{n} b_j X^j) = \sum_{k=0}^{n+n} c_k X^k$ onde $c_k = \sum_{i=0}^{k} a_i . b_{k-i}$

O conjunto $\mathbb{R}[X]$ para as operações acima definidas é comutativo, possui elemento unidade $1 \neq 0$, não possui divisores de zero e atende os seguintes axiomas da definição de corpo (seção 1.2): A1, A2, A3, A4, M1, M2, M3 e DM. Veja:

- o elemento neutro da adição é 0.

- o simétrico do elemento f de $\mathbb{R}[X]$ é $-f$.

- a associatividade e a comutatividade da adição são de verificação imediata.

- o elemento neutro da multiplicação é 1.

- a comutatividade da multiplicação é de verificação imediata.

- a associatividade e a distributividade da multiplicação podem ser verificadas por extenso.

- é interessante notar que $\mathbb{R} \subset \mathbb{R}[X]$, pois todo elemento $a \in \mathbb{R}$ pode ser escrito como $f = 0x^n + 0x^{n-1} + \ldots, + 0x^1 + a$.

- o fato de $\mathbb{R}[X]$ não admitir divisores de zero merece ser detalhado:

Seja f e $g \in \mathbb{R}[X]$, e $f.g = 0$ com $f \neq 0$ e $g \neq 0$, então $\text{gr}(f) + \text{gr}(g) = 0 \Rightarrow \text{gr}(f) = \text{gr}(g) = 0 \Rightarrow f, g$ constantes $\Rightarrow f, g \in \mathbb{R} \Rightarrow f.g = 0$, e isto é um absurdo, pois $\mathbb{R}$ é um corpo, exceto se f ou $g = 0$. ■

Os conjuntos que são comutativos, possuem elemento unidade $1 \neq 0$, não possuem divisores de zero e atendem os seguintes axiomas da definição de corpo (seção 1.2): A1, A2, A3, A4, M1, M2, M3 e DM, satisfazem os axiomas de anel, conforme está definido no apêndice A, e, portanto, o conjunto $\mathbb{R}[X]$ com as operações + e . é um anel.

Pode-se definir a partir de cada polinômio uma função polinomial. Então o conjunto das funções polinomiais com coeficientes em $\mathbb{R}$, pode ser construído a partir dos polinômios de $\mathbb{R}[X]$, e se diz que $f: \mathbb{R} \to \mathbb{R}$ é a função polinomial associada ao polinômio f, inclusive assumindo as mesmas considerações feitas acima para os polinômios, conforme visto em Hefez (2003, vol. 2 , p. 11-12) e Fernandes; Ricou (2004, p. 138-139). O anel de funções polinomiais também será indicado por $\mathbb{R}[X]$, pois são anéis isomorfos.

A partir de $\mathbb{R}[X]$ será construído o seu corpo de frações $\mathbb{R}(X)$, assim como $\mathbb{Q}$ é construído a partir de $\mathbb{Z}$ no ensino básico. Vale observar que assim como $\mathbb{Z} \subset \mathbb{Q}$ tem-se que $\mathbb{R}[X] \subset \mathbb{R}(X)$ e o que se quer definir é:

$$\mathbb{R}(X) = \left\{ \frac{p(X)}{q(X)} : p, q \in \mathbb{R}[X] \,,\ q \neq 0 \right\}$$

A função racional $\frac{p(X)}{q(X)}$ é a classe de equivalência do par $\big(p(X), q(X)\big)$ sob a relação $(p, q) \sim (p_1, q_1) \iff pq_1 = p_1 q$. Note que essa é a definição de fração em $\mathbb{Q}$ quando $p, q, p_1, q_1 \in \mathbb{Z}$.

As operações $+$ e $.$ em $\mathbb{R}[X]$ induzem operações em $\mathbb{R}(X)$, segundo as propriedades de quociente colocadas na propriedade 16 de corpo da seção 1.3, da mesma forma que se faz com $\mathbb{Q}$ a partir de $\mathbb{Z}$. Veja:

Para os elementos $p(X)$, $q(X)$, $r(X)$ e $s(X)$ do anel $\mathbb{R}[X]$, com $q(X) \neq 0$ e $s(X) \neq 0$, tem-se que:

I) $\frac{p(X)}{q(X)} = \frac{r(X)}{s(X)}$, se, e somente se, $p(X)\, s(X) = q(X)\, r(X)$

II) $\frac{p(X)}{q(X)} + \frac{r(X)}{s(X)} = \frac{p(X)\, s(X) + q(X)\, r(X)}{q(X)\, s(X)}$, note que $q(X)\, s(X) \neq 0$.

III) $-\frac{p(X)}{q(X)} = \frac{-p(X)}{q(X)} = \frac{p(X)}{-q(X)}$, note que $-q(X) \neq 0$.

IV) $\left(\frac{p(X)}{q(X)}\right).\left(\frac{r(X)}{s(X)}\right) = \frac{p(X)\ r(X)}{q(X)\, s(X)}$, note que $q(X).\, s(X) \neq 0$.

V) $\frac{p(X)}{q(X)} = 0$, se, e somente se, $p(X) = 0$.

VI) $\frac{p(X)}{1} = p(X)$, pois $\mathbb{R}[X] \subseteq \mathbb{R}(X)$.

VII) $\left(\frac{p(X)}{q(X)}\right)^{-1} = \frac{q(X)}{p(X)}$, se $p(X) \neq 0$.

A ordem de $\mathbb{Z}$ induz a ordem em $\mathbb{Q}$ ($\frac{a}{b} > 0 \Leftrightarrow ab > 0$), conforme mostrado no exemplo 1 de corpo ordenado na seção 2.5. Analogamente, sendo possível ordenar $\mathbb{R}[X]$ (abaixo), $\mathbb{R}\,(X)$ é um corpo ordenado. Convém observar que há outras formas de ordenar $\mathbb{R}[X]$ além da que será colocada.

Para ordenar $\mathbb{R}[X]$ será definido que $p(X) > 0$, se $p(X) \neq 0$ e o coeficiente principal de $p(X)$, denotado por $\mathrm{cp}(p)$, é positivo em $\mathbb{R}$. Assim se $f(X)$, $g(X) \in \mathbb{R}[X]$, então $f(X) < g(X) \Leftrightarrow \mathrm{cp}\,(g(X) - f(X)) > 0$. Então $\leq$ é uma relação de ordem total em $\mathbb{R}[X]$ e essa ordem, compatível com $+$ e $.$, se transfere para o corpo de frações, $\frac{p(X)}{q(X)} > 0$ em $\mathbb{R}(X) \Leftrightarrow f(X).\, g(X) > 0$ em $\mathbb{R}[X]$.

Veja que nessas condições $\mathbb{R}(X)$ não é arquimediano e não pode ter a propriedade do supremo, pois não existe $n \in \mathbb{N}$, tal que $n.1 > X$.

Observe, que de fato, para qualquer real k, tem-se $X > k$ porque $X - k$ tem coeficiente positivo. Isso coloca X depois de todos os reais, isto é, X é um elemento infinitamente grande em $\mathbb{R}(X)$. Do mesmo modo, se $\varepsilon > 0$ for um real positivo arbitrário, temos $\varepsilon X - 1 > 0$, donde se obtém $\varepsilon > \frac{1}{X}$. Já que $\frac{1}{X}$ também é positivo (porque $X > 0$), concluímos que $\frac{1}{X}$ é um elemento infinitesimal, ou seja, situa-se entre 0 e todos os reais positivos.

Contudo, $\mathbb{R}(X)$ também não é real fechado: de fato, X não tem raiz quadrada. Isso pode ser mostrado assim: se $\left(\frac{f(X)}{g(X)}\right)^2 = X$ então $\big(f(X)\big)^2 = X.\big(g(X)\big)^2$ e o membro esquerdo é polinômio de grau par, enquanto o direito é de grau ímpar, contradição. Desse modo, $\mathbb{R}(X)$ não compartilha todas as propriedades de $\mathbb{R}$. Porém, há corpos reais fechados com infinitésimos, nos quais se demonstram propriedades do Cálculo com ajuda desses elementos e que valem, portanto, em $\mathbb{R}$. Veja, por exemplo, Davis (2005) e Keisler (2012).

CONCLUSÃO

A apresentação da estrutura algébrica de corpo a partir dos axiomas propiciou um campo fértil para a proposta inicial desse trabalho que era colocar parte da álgebra existente nessa classe de estruturas algébricas numa linguagem mais acessível ao ensino básico.

A partir dos axiomas de corpo foi feita a dedução de várias propriedades algébricas dos corpos que, por sua vez, são largamente empregadas no ensino básico e superior de Matemática, mais do que isso, foi possível mostrar que a álgebra envolvida nessas deduções, geralmente, não vai muito além dos fundamentos básicos de álgebra que são trabalhados ao longo do ensino fundamental e médio. Com isso, ficou claro o vínculo natural entre o assunto aqui tratado e a álgebra do ensino básico.

Seguindo por esse caminho e utilizando o vínculo construído foi realizada uma introdução ao estudo de diferentes corpos que são obtidos ao acrescentar mais axiomas à definição inicial de corpo. Esse estudo evidenciou a diferença entre as estruturas algébricas de diferentes corpos, ou seja, a modificação ou admissão de novos axiomas leva a teorias diferentes e consequentemente a estruturas algébricas mais específicas.

Ao longo do estudo dessas teorias de corpos, as demonstrações e exemplos que foram colocados sempre primaram pela utilização dos conceitos de álgebra do ensino básico, e nos casos que necessitaram de definições mais complexas foram escolhidos caminhos que pudessem ser percorridos na sua maior parte com esses conceitos de álgebra do ensino básico.

Enfim, através desse trabalho espera-se colaborar com os estudantes que se encontram na educação básica e pretendem uma formação de nível superior em áreas que utilizam a Matemática. No caso particular do professor do ensino básico espera-se que, embora não seja aconselhável aplicar todo o conteúdo aqui discutido em sala de aula, a base conceitual aqui desenvolvida permita ajudar na construção de estratégias pedagógicas que sejam benéficas para a aprendizagem dos seus alunos.

A

APÊNDICE A

A.1 Noções de Estruturas Algébricas de Anéis

As definições utilizadas na maior parte dos compêndios de álgebra para corpo fazem menção à estrutura algébrica chamada de anel.

Veja a seguir duas dessas definições de corpo:

Definição: Um anel comutativo K com elemento unidade 1, diferente de zero, é um corpo se, e somente se, qualquer que seja $a \in K - \{0\}$, existe a' tal que $a.a' = a'.a = 1$.

Definição: Um corpo é um anel comutativo K, com elemento unidade 1 diferente de zero, sendo todo elemento não nulo de K invertível para a multiplicação.

Como esse tipo de definição é recorrente em álgebra, torna-se interessante definir a estrutura algébrica denominada de anel.

Definição: Um conjunto sobre o qual estão definidas duas operações adição (+) e multiplicação (.), será denominado anel se, e somente se, atender os axiomas A1, A2, A3, A4, M1, e DM da definição de corpo (seção 1.2).

Um anel será representado por $A(+,.)$, ou, simplesmente, por A quando for clara a referência a um anel.

Exemplos:

1) Todos os corpos que foram apresentados ao longo do trabalho são exemplos de anéis.

2) O conjunto dos números inteiros $\mathbb{Z}$ é um exemplo de anel.

3) Os conjuntos de polinômios $\mathbb{Z}[X]$ e $\mathbb{R}[X]$ são anéis.

4) Para cada $n \geq 1$ o conjunto das matrizes quadradas $n \times n$, $M_{n\times n}$, sobre $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ é anel.

A.2 Definições e exemplos de alguns tipos de Anéis

Nesta seção serão abordadas e exemplificadas diferentes estruturas algébricas de anéis que são geradas à medida que se acrescenta mais axiomas na definição de anel.

Anel Comutativo

Definição: O Anel A é comutativo se a operação de multiplicação definida sobre o anel é comutativa.

Em outras palavras o anel é comutativo se atende ao axioma M2 da definição de corpo.

Exemplos:

1) O anel dos polinômios de uma variável X com coeficientes em $\mathbb{R}$, indicado por $\mathbb{R}[X]$ é um exemplo que será um pouco mais detalhado em anel de integridade.

2) O conjunto dos números inteiros pares $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ é um anel comutativo que não possui elemento unidade.

Anel com elemento unidade

O anel A com elemento unidade é aquele que possui o elemento neutro da multiplicação, normalmente, chamado de unidade e indicado por 1.

Em outras palavras é o anel que atende ao axioma M3 dado na definição de corpo.

Exemplos:

1) O conjunto das matrizes quadradas de ordem n fixada $M_n(\mathbb{R})$ é um anel não comutativo com elemento unidade.

Ilustrando com um exemplo numérico do conjunto das matrizes quadradas 2×2, tem-se que:

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ é o elemento neutro da adição, e $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o elemento neutro da multiplicação, ou seja, a unidade na operação de multiplicação é a matriz identidade.

Como: $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} . \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 7 & 11 \end{pmatrix}$ e $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} . \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 6 \\ 7 & 10 \end{pmatrix}$, fica clara a não comutatividade do anel.

2) O conjunto dos números inteiros $\mathbb{Z}$ é um anel comutativo com elemento unidade 1. Veja que $\mathbb{Z}$ é fechado para as operações de adição e multiplicação, e é possível demonstrar que ele atende aos axiomas A1, A2, A3, A4, M1, M2, M3 e DM da definição de corpo (seção 1.2).

Divisores de zero em um anel

Se num anel A, $ab = 0$ e $a, b \neq 0$, então, a é um divisor de zero à esquerda e b um divisor de zero à direita. Caso A seja comutativo, a e b são chamados de divisores de zero.

Exemplos:

1) Os conjuntos de números inteiros módulo n, com $n \in \mathbb{N}$ não primo, são anéis comutativos com elemento unidade e com divisores de zero, conforme mostrado na seção 2.1.

2) O anel de matrizes quadradas 2×2 possui divisores de zero à esquerda e à direita. Veja:

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Domínio de Integridade

Domínio de integridade ou simplesmente domínio é um anel A comutativo com elemento unidade $1 \neq 0$, e sem divisores de zero.

Exemplos:

1) Os corpos são exemplos de domínios de integridade, pois satisfazem as condições de anel e não possuem divisores de zero.

2) O conjunto dos polinômios de uma variável X com coeficientes em $\mathbb{R}$, indicado por $\mathbb{R}[X]$ é um exemplo interessante de anel de integridade. A seguir será mostrado que $\mathbb{R}[X]$ é um anel de integridade:

Considere em $\mathbb{R}[X]$ dois polinômios $f(x) = a_0 + a_1x + \ldots + a_nx^n$ e $g(x) = b_0 + b_1x + \ldots + b_mx^m$, tais que $f(x)g(x) = 0$.

Suponha por absurdo que $f(x)$ e $g(x)$ não são nulos, com $a_n \neq 0$ e $b_m \neq 0$. Como $f(x)g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n+m}x^{n+m}$ tem-se que $c_{n+m} = a_n\, b_m \neq 0$, o que é um absurdo. Logo $f(x)$ ou $g(x)$ é nulo.

3) O anel dos polinômios com coeficientes em $\mathbb{Z}$, é um domínio, usualmente, indicado por $\mathbb{Z}[X]$.

BIBLIOGRAFIA

ALMAY, P. *Elementos de cálculo diferencial e integral*. São Paulo: Kronos, 1975.

CASTRUCCI, B. *Elementos de teoria dos conjuntos.* 3ª edição. São Paulo: Livraria Nobel S. A., 1969.

DOMINGUES, H. H.; IEZZI, G. *Álgebra moderna*. 4ª edição reform.. São Paulo: Atual, 2003.

DAVIS, M. *Applied nonstandard analysis*. Dover Publications, 2005.

DUTRA, W. S. *A construção dos números reais: noções fundamentais e sugestões ao ensino básico*. 2014. 73 f. Dissertação (Mestrado em Matemática) - Departamento de Ciências Exatas e Tecnológicas, Universidade Estadual de Santa Cruz. Ilhéus, 2014.
Disponível em: < http://bit.profmat-sbm.org.br/xmlui/handle/123456789/1178 >.
Acesso em: 04/05/2015.

ENDLER, O. *Teoria dos corpos.* Rio de Janeiro: IMPA, 2012, Publicações matemáticas.
Disponível em: < http://www.impa.br/opencms/pt/biblioteca/pm/PM_19.pdf >.
Acesso em: 21/05/2015.

FERNANDES, R. L.; RICOU, M. *Introdução à álgebra*. Lisboa: IST Press, 2004.

GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. 5ª edição. Rio de Janeiro: IMPA, 2010, Projeto Euclides.

GRIESE, C. *Corpos formalmente reais e reais fechados.* Não publicado. São Paulo, 2015. (Acervo particular do orientador.)

GUIDORIZZI, H. L. *Um curso de cálculo*. 2ª edição. Rio de Janeiro, São Paulo: LTC Livros Técnicos e Científicos Editora Ltda., 1987. Vol. 1.

HEFEZ, A. *Curso de álgebra*. 3ª edição. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2002. Vol. 1. Coleção Matemática Universitária.

HEFEZ, A. *Curso de álgebra*. Versão preliminar. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2003. Vol.2.

HEFEZ, A. *Elementos de aritmética*. 2ª edição. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006. Vol. 1. Textos Universitários.

JACOBSON, N. *Basic algebra II*. San Francisco: W. H. Freeman and Company, 1980.

KEISLER, H. J. *Elementary calculus: an infinitesimal approach*. 3ª ed. Dover Publications, 2012.

LANG, S. *Algebra*. 3ª ed. Massachusetts: Addison-Wesley Publishing Company Inc., 2002.

LIMA, E. L. *Curso de análise*. 12ª edição (segunda impressão). Rio de Janeiro: SBM, 2007. Vol. 1, Projeto Euclides.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. *A matemática do ensino médio*. 10ª edição. Rio de Janeiro: SBM, 2012. Vol. 1.

LIPSCHUTZ, S. *Álgebra linear*. São Paulo: Editora McGraw-Hill do Brasil Ltda., 1972.

LOPES, V. C. *Uma página sobre o lema de Zorn.* 2012.
Disponível em: < http://hostel.ufabc.edu.br/~vinicius/zorn.pdf>.
Acesso em: 30/11/2015.

LOPES, V. C. *Guia de cálculo.* Versão preliminar: UFABC, 1º quad. 2015. Santo André, 2015.
Disponível em: < http://hostel.ufabc.edu.br/~vinicius/guiacalc.pdf>.

Acesso em: 04/05/2015.

MARQUES, C. M. *Introdução à teoria de anéis.* Departamento de Matemática-UFMG, 1999 (rev. 2005).
Disponível em: < http://www.mat.ufmg.br/~marques/Apostila-Aneis.pdf>.
Acesso em: 04/05/2015.

MARTIN, P. A. *Grupos, corpos e teoria de Galois*. São Paulo: Editora Livraria da Física, 2010.

MILIES, C. P. *Breve história da álgebra abstrata*. Instituto de Matemática e Estatística - Universidade de São Paulo. São Paulo, 2004.
Disponível em: < http://www.bienasbm.ufba.br/M18.pdf>.
Acesso em: 04/06/2015.

MONTEIRO, L. H. J. *Elementos de álgebra*. 2ª edição. Rio de Janeiro: Livros Técnicos e Científicos Editora S.A., 1978.

PANEK, L; ROCIO, O. G. *Funções trigonométricas definidas sobre corpos reais fechados.* Boletim da Sociedade Paranaense de Matemática, Maringá, vol.24 nº 1- 2/2006.
Disponível em:<http://periodicos.uem.br/ojs/index.php/BSocParanMat/article/view/7444>.
Acesso: 02/02/2015.

POLIZELI, P.. *Involuções positivas sobre uma álgebra semisimples*. 2007. 79 f. Dissertação (Mestrado em Matemática) - Centro de Ciências Exatas, Universidade Federal do Paraná. Maringá, 2007.

PONTES, K. M. *Existência e unicidade dos números reais via cortes de Dedekind*. 2014. 66 f. Dissertação (Mestrado em Matemática) – Centro de Ciências Exatas e da Natureza, Dep. Matemática, Universidade Federal da Paraíba. João Pessoa, 2014.
Disponível em: < http://bit.profmat-sbm.org.br/xmlui/handle/123456789/1555>.
Acesso em: 04/05/2015.

PRESTEL, A.; DELZELL, C. N. *Mathematical logic and model theory - a brief introduction:* Springer, 2011.

PRESTEL, A. *Model theory for the real algebraic geometer*. Roma, Italia: Instituti Editoriali e Poligrafici Internazionali, 1998.

SHOKRANIAN, S. *Álgebra 1*. Rio de Janeiro: Editora Ciência Moderna Ltda., 2010.

SOUZA, J. S. *Números reais: um corpo ordenado e completo*. 2013. 61 f. Dissertação (Mestrado em Matemática) - Instituto de Matemática e Estatística, Universidade Federal de Goiás. Goiânia, 2013.
Disponível em: < http://bit.profmat-sbm.org.br/xmlui/handle/123456789/529>.
Acesso em: 24/05/2015.