UNIVERSIDADE FEDERAL DE SANTA CATARINA
Centro de Ciências Físicas e Matemáticas
Curso de Licenciatura em Matemática

Construção do Corpo dos Números Reais

Autora: Cinthia Marques Vieira Andretti
Orientador: Prof. Dr. Oscar Ricardo Janesch
Florianópolis
Fevereiro 2008

Cinthia Marques Vieira Andretti

Construção do Corpo dos Números Reais

Trabalho acadêmico de graduação apresentado
à disciplina Trabalho de Conclusão de Curso II,
do Curso de Matemática - Habilitação Licenciatura,
do Centro Ciências Físicas e Matemáticas da
Universidade Federal de Santa Catarina

Professora: Carmem Suzane Comitre Gimenez

Florianópolis
Fevereiro 2008

Agradecimentos

Agradeço a Deus, por ter me dado forças e colocado pessoas maravilhosas no meu caminho que tornaram esse trabalho menos árduo.

Agradeco à minha mãe e ao meu noivo, Rodrigo Kloppel, pela paciência, amor e pelas inúmeras palavras e gestos de incentivo, sem os quais nada teria sido possível. Eles foram além de essenciais, indispensáveis durante esta caminhada.

São muitos os amigos que merecem ser lembrados, alguns apenas passaram, mas aqueles que ficaram, Monique Müller Lopes Rocha e Marcos Teixeira Alves, o meu muito obrigada.

Construção do Corpo dos Números Reais
por
Cinthia Marques Vieira Andretti

Esta monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº 02/CMM/08.

_____
Profª Carmem Suzane Comitre Gimenez
Professora da disciplina

Banca Examinadora:

_____
Prof. Dr. Oscar Ricardo Janesch (Orientador)

_____
Prof. Dr. Gustavo Adolfo Torres Fernandes da Costa (UFSC)

_____
Prof. Ms. Rubens Starke (UFSC)

Sumário

Introdução

Neste trabalho construiremos o corpo dos números reais, representado por $\mathbb{R}$. Para atingir este objetivo o texto foi dividido em três capítulos.

No primeiro capítulo recordaremos conceitos de álgebra relativos a grupos, anéis e corpos ordenados.

A teoria dos Anéis é um dos principais assuntos do vasto campo da Álgebra abstrata. A origem da Álgebra remonta aos babilônios e o seu desenvolvimento percorreu um longo caminho que não pretendemos retraçar aqui, mas que teve um momento importante no século XVI com os matemáticos da chamada Escola de Bolonha, que se ocuparam da resolução das equações algébricas do terceiro e do quarto grau. Em seguida Bombelli deu um passo decisivo introduzindo o simbolismo apropriado para as operações permitindo a manipulação de expressões e fórmulas. Importante para o desenvolvimento da teoria foi o estudo dos anéis de inteiros algébricos iniciado por Gauss e desenvolvido por Kronecker, Dirichlet e Hilbert no final do século XIX, início do século XX. Finalmente a noção abstrata de anel foi introduzida na segunda década do século XX.

No segundo capítulo veremos conceitos de cálculo relacionados com seqüências, para isso será necessário relembrar alguns conceitos como supremo e ínfimo.

O terceiro e último capítulo constrói o corpo dos números reais usando os conceitos estabelecidos nos dois primeiros capítulos.

Vários matemáticos do século XIX cuidaram da contrução dos números reais, dentre eles Richard Dedekind, Karl Weierstrass, Charles Méray e Georg Cantor. Mas as teorias dos números reais que permeneceram foram a de Dedekind e a de Cantor.

Richard Dedekind estudou em Göttingen, onde foi aluno de Gauss e Dirichlet. Em 1858 tornou-se professor em Zurique.

Ele conta que do início de sua carreira em 1858, quando teve de ensinar Cálculo Diferencial, percebeu a falta de uma fundamentação adequada para os números reais. E é também ele mesmo quem conta que foi buscar inspiração para

a sua contrução dos números reais na antiga e engenhosa teoria das proporções de Eudoxo.

A definição de Eudoxo associa, a cada par de grandezas, digamos (A, B), dois conjuntos de pares (m, n) de números naturais: o conjunto E ("E"de esquerda) dos pares para os quais $mB < nA$ e o conjunto D ("D"de direita) dos pares para os quais $mB > nA$.

Inspirando-se na definição de Eudoxo, Dedekind notou que o procedimento do sábio grego leva a uma separação dos números racionais em dois conjuntos. Assim, qualquer número racional r efetua um "corte"ou separação de todos os demais números no conjunto "E"dos números menores que r e no conjunto "D"dos números maiores do que r. O próprio número r pode ser incluído como o maior elemento de E ou o menor elemento de D.

Mas, além desses "cortes", há outros, como exemplifica o clássico caso de $\sqrt{2}$. O processo de encontrar a raiz quadrada de 2 conduz à separação dos números racionais em dois conjuntos: o conjunto E das raízes quadradas aproximadas por falta (aí incluídos o zero e os racionais negativos), e o conjunto D das raízes aproximadas por excesso. Só que agora esse corte não tem elemento de separação. No modo de ver de Dedekind, o número irracional $\sqrt{2}$ deve ser criado como elemento de separação entre os conjuntos desse corte.

Dedekind generaliza esse procedimento, primeiro definindo corte de maneira geral, no conjunto $\mathbb{Q}$ dos números racionais.

Corte de Dedekind, ou, simplesmente, *corte*, é todo par (E, D) de conjuntos não vazios de números racionais, cuja união seja $\mathbb{Q}$, e tais que todo elemento de E seja menor que todo elemento de D.

Dedekind observa que a existência de cortes sem elementos de separação no conjunto $\mathbb{Q}$ dos números racionais é a expressão aritmética da descontinuidade de $\mathbb{Q}$, ao passo que, com a adjunção dos novos elementos - os números irracionais - obtemos o conjunto $\mathbb{R}$ dos números reais, que ao contrário de $\mathbb{Q}$, é agora um "contínuo numérico", pois os irracionais vêm preencher as "lacunas" de descontinuidade então existentes em $\mathbb{Q}$.

Mas não basta apenas juntar a $\mathbb{Q}$ os novos elementos para obter $\mathbb{R}$. Este conjunto precisa ter a estrutura que dele se espera. Daí termos de definir nele as operações usuais de adição, multiplicação, etc., e a relação de ordem. E devemos fazer isso de maneira a podermos provar as propriedades usuais desses números que já conhecemos e usamos desde o ensino fundamental. Mais ainda, de maneira que essas definições não conflitem, mas preservem, as mesmas noções já existentes no conjunto $\mathbb{Q}$.

Ao leitor que tiver interesse em ver a contrução do corpo $\mathbb{R}$ dos números reais, de acordo com Dedekind, consulte Geraldo Ávila, Análise Matemática Para Licenciatura.

Vamos considerar agora a construção dos números reais feita por Cantor.

Georg Cantor ($1845-1918$) nasceu em São Petersburgo, onde viveu até 1856, quando sua família transferiu-se para o sul da Alemanha. Doutorou-se pela Universidade de Berlim, onde foi aluno de Weierstrass, de quem teve grande influência em sua formação matemática. Toda sua carreira profissional desenvolveu-se em Halle, para onde tranferiu-se logo que terminou seu doutorado em Berlim.

Como no método de Dedekind, também no de Cantor partimos do pressuposto de que já estamos de posse dos números racionais, com todas as suas propriedades. Começamos definindo *seqüência de Cauchy*, também chamada de seqüência fundamental. Observe que existem pelo menos tantas seqüências de Cauchy quantos são os números racionais, pois qualquer que seja o número racional r, a seqüêcia constante $(r_n) = (r, r, r, ...)$ é de Cauchy. Dentre as seqüências de Cauchy, algumas são convergentes, como essas seqüências constantes e uma infinidade de outras mais. Mas há também uma infinidade de seqüências de Cauchy que não convergem (para um número racional), como a seqüência das aproximações decimais por falta de $\sqrt{2}$,

$$(r_n) = (1, 1.4, 1.41, 1.414, 1.4142, ...).$$

Como se vê, essa seqüência não converge por não existir ainda os números chamados "irracionais". Para criá-los, podemos simplesmente postular que toda "seqüência de cauchy (de números racionais) converge". Feito isso teremos de mostrar como esses novos números se juntam aos antigos (os racionais) de forma a produzir um corpo ordenado completo. E nesse trabalho teríamos de provar que diferentes seqüências definem o mesmo número irracional.

Por causa disso torna-se mais conveniente primeiro juntar em uma mesma classe todas as seqüências que terão um mesmo limite, para depois construir a estrutura de corpo. Fazemos isso definindo, no conjunto das seqüências de Cauchy, uma "relação de equivalência". Essa relação distribui as seqüências de Cauchy em classes de seqüências equivalentes, de tal maneira que duas seqüências pertencem a uma mesma classe se, e somente se, elas são equivalentes.

Exporemos neste trabalho a construção feita por Cantor. com todos os detalhes. Este processo pode ser estendido, com ligeiras modificações, para um espaço métrico e também para a contrução do corpo dos números p-ádicos. Muitas questões em teoria de números são melhor atacadas estudando-as módulo p para todos os primos p. Isto leva à construção dos números p-ádicos. Este campo de estudo é chamado análise local e emerge da teoria algébrica de números.

Capítulo 1

Anéis e Corpos Ordenados

O objetivo deste capítulo é desenvolver os principais resultados sobre anéis e corpos ordenados. Também trataremos com homomorfismos e isomorfismos ordenados.

Grosseiramente falando, uma estrutura algébrica ordenada é um conjunto A, munido de uma estrutura algébrica, com uma relação de ordem em A que é compatível com as operações da estrutura algébrica. Por este motivo, introduziremos os anéis ordenados a partir de grupos ordenados, pois grupos ordenados formam a estrutura algébrica ordenada mais simples que existe.

Iniciaremos recordando a definição de grupo e fixando algumas notações.

1.1 Grupos Ordenados

Definição 1.1. Diz-se que uma operação $*$, sobre um conjunto G, define uma **estrutura de grupo** sobre G se, e somente se, os seguintes axiomas são verificados:

(G_1) $(x * y) * z = x * (y * z)$; $\forall\, x, y, z \in G$ (a operação $*$ é associativa).

(G_2) $\exists\, 1_G \in G$ tal que $x * 1_G = 1_G * x = x$; $\forall\, x \in G$ (existência de elemento neutro para a operação $*$).

(G_3) $\forall\, x \in G, \exists\, x' \in G$ tal que $x * x' = x' * x = 1_G$ (existência de inverso).

Se a operação $*$ de um grupo G satisfaz o axioma:

(G_4) $\forall\, x, y \in G, x * y = y * x$ (a operação $*$ é comutativa),

diremos que G é um **grupo comutativo** ou **abeliano**.

Observação 1.1. Normalmente indica-se a operação do grupo G usando um ponto "$\cdot$". Diremos então que $(G, \cdot)$ é grupo multiplicativo. Neste caso, o elemento neutro de G é denotado por 1 e o inverso de $a \in G$ é denotado por a^{-1}. Quando

o grupo G é abeliano, indicaremos sua operação por " $+$" , e diremos que $(G,+)$ é grupo aditivo. Neste caso, o elemento neutro é denotado por 0 e o simétrico de $a \in G$ é denotado por $-a$.

Abaixo apresentaremos as definições de múltiplo (em grupos aditivos) e potências (em grupos multiplicativos).

Definição 1.2. Sejam $(G,+)$ um grupo, $a \in G$ e $n \in \mathbb{Z}$:

$$na = \begin{cases} 0 & , \quad \text{se } n = 0. \\ a + a + ... + a & , \quad n \text{ vezes quando } n > 0. \\ -(a + a + ... + a) & , \quad -n \text{ vezes quando } n < 0. \end{cases}$$

Definição 1.3. Sejam $(G,\cdot)$ um grupo, $a \in G$ e $n \in \mathbb{Z}$:

$$a^n = \begin{cases} 1_G & , \quad \text{se } n = 0. \\ a \cdot a \cdot ... \cdot a & , \quad n \text{ vezes quando } n > 0. \\ (a \cdot a \cdot ... \cdot a)^{-1} & , \quad -n \text{ vezes quando } n < 0. \end{cases}$$

A partir de agora definiremos ordens parciais e totais em um grupo G.

Definição 1.4. O grupo $(G,\cdot)$ é **ordenado** quando está definida uma relação $\leq$ sobre G que satisfaz, para quaisquer elementos a, b, c de G:

(O_1) $a \leq a$.

(O_2) $a \leq b$ e $b \leq a \Longrightarrow a = b$.

(O_3) $a \leq b$ e $b \leq c \Longrightarrow a \leq c$.

(OA') $a \leq b \Longrightarrow ac \leq bc$ e $ca \leq cb$.

Note que os axiomas (O_1), (O_2), (O_3) dizem que "$\leq$" é relação de ordem em G, e que o axioma (OA') assegura que esta relação de ordem é compatível com a operação do grupo G.

Notação: O grupo G com operação "$\cdot$" e ordenado pela ordem $\leq$ é denotado por $(G,\cdot,\leq)$.

Observação 1.2. Um grupo ordenado também é chamado de grupo **parcialmente ordenado**.

Definição 1.5. Um grupo ordenado $(G,+,\leq)$ é chamado grupo **totalmente ordenado** quando satisfaz o axioma:

(O_4) $\forall\, a, b \in G, a \leq b$ ou $b \leq a$.

Note que um grupo totalmente ordenado nada mais é que um grupo, com uma relação de ordem total, que é compatível com a operação do grupo.

Definição 1.6. Dizemos que um grupo $(G, \cdot)$ é **ordenável**, quando existe uma relação de ordem total em G, que torna $(G, \cdot, \leq)$ um grupo totalmente ordenado.

Neste trabalho, estamos interessados em **grupos abelianos totalmente ordenados**. Por isso, passaremos a usar a notação aditiva. Ressaltamos que quando a operação do grupo é comutativa, o axioma (OA') pode ser escrito como:

(OA) $a \leq b \Longrightarrow a + c \leq b + c$.

Portanto, um grupo abeliano totalmente ordenado é um grupo G, com uma relação de ordem $\leq$, que satisfaz para todo a, b, c em G as seguintes condições:

(G_1) $(a + b) + c = a + (b + c)$.

(G_2) $\exists\, 0 \in G$ tal que $0 + a = a + 0 = a$.

(G_3) $\forall\, a \in G$, $\exists\, (-a) \in G$ tal que $a + (-a) = (-a) + a = 0$.

(G_4) $a + b = b + a$.

(O_1) $a \leq a$.

(O_2) $a \leq b$ e $b \leq a \Longrightarrow a = b$.

(O_3) $a \leq b$ e $b \leq c \Longrightarrow a \leq c$.

(O_4) $a \leq b$ ou $b \leq a$.

(OA) $a \leq b \Longrightarrow a + c \leq b + c$.

Observação 1.3. Sejam $\leq$ uma relação de ordem em G e $a, b \in G$. Escreveremos $a < b$, para indicar que $a \leq b$ e $a \neq b$.

Exemplo 1.1. Seja $(G, \cdot)$ um grupo qualquer. A relação

$$a \text{ “}\leq\text{” } b \Longleftrightarrow a = b$$

torna $(G, \cdot, \leq)$ um grupo ordenado.

De fato, como $(G, \cdot)$ é grupo e a igualdade é uma relação de ordem, basta verificar o axioma (OA'). Mas isso é óbvio, pois de $a, b, c \in G$ temos:
$a = b \Longrightarrow ac = bc$ e $ca = cb$.

Exemplo 1.2. O único grupo totalmente ordenado pela ordem

$$a \text{ “}\leq\text{” } b \Longleftrightarrow a = b$$

é o grupo trivial $G = \{e\}$.

Basta observar que a relação de igualdade só é uma relação de ordem total em um conjunto unitário.

Exemplo 1.3. O grupo abeliano $(\mathbb{Z}, +)$ é totalmente ordenado pela ordem usual de $\mathbb{Z}$. Note que o axioma (OA) é apenas uma propriedade aritmética da adição de números inteiros.

Em função do exemplo acima, é natural perguntar se os grupos abelianos $(\mathbb{Z}_n, +)$ são ordenáveis. Veremos mais tarde que a resposta é não.

A partir de grupos abelianos totalmente ordenados podemos construir um novo grupo abeliano totalmente ordenado, fazendo produto cartesiano. Faremos isso na próxima proposição. Iniciaremos com um lema sobre relação de ordem em produto cartesiano.

Lema 1.1. Sejam G_1 um conjunto com uma relação de ordem $\leq_1$ e G_2 um conjunto com uma relação de ordem $\leq_2$. Então:

$(a_1, a_2) \leq (b_1, b_2) \iff (a_1 <_1 b_1)$ ou $(a_1 = b_1$ e $a_2 \leq_2 b_2)$

é uma relação de ordem em $G_1 \times G_2$. Além disso, se $\leq_1$ e $\leq_2$ são ordens totais então $\leq$ é uma ordem total.

Demonstração.

• $(a_1, a_2) \leq (a_1, a_2)$

Como $a_1 = a_1$ e $a_2 \leq a_2$ segue que $(a_1, a_2) \leq (a_1, a_2)$.

• $(a_1, a_2) \leq (b_1, b_2)$ e $(b_1, b_2) \leq (a_1, a_2) \Longrightarrow (a_1, a_2) = (b_1, b_2)$

$(a_1, a_2) \leq (b_1, b_2) \Longrightarrow (a_1 <_1 b_1)$ ou $(a_1 = b_1$ e $a_2 \leq_2 b_2)$

$(b_1, b_2) \leq (a_1, a_2) \Longrightarrow (b_1 <_1 a_1)$ ou $(b_1 = a_1$ e $b_2 \leq_2 a_2)$

1^o caso: $a_1 <_1 b_1$ e $b_1 <_1 a_1$

Este caso não pode ocorrer, pois $<_1$ é relação de ordem em G_1. De fato,

$a_1 <_1 b_1 \Longrightarrow a_1 \leq_1 b_1$ e $a_1 \neq b_1$

$b_1 <_1 a_1 \Longrightarrow b_1 \leq_1 a_1$ e $b_1 \neq a_1$

como $a_1 \leq_1 b_1$ e $b_1 \leq_1 a_1$ e $\leq_1$ é relação de ordem, segue que $a_1 = b_1$. Absurdo.

2^o caso: $a_1 <_1 b_1$ e $b_1 = a_1$ e $b_2 \leq_2 a_2$

As condições $a_1 <_1 b_1$ e $b_1 = a_1$ não podem ocorrer simultaneamente.

3^o caso: $a_1 = b_1$ e $a_2 \leq_2 b_2$ e $b_1 <_1 a_1$

Análogo ao caso anterior.

4^o caso: $a_1 = b_1$ e $a_2 \leq_2 b_2$ e $b_1 = a_1$ e $b_2 \leq_2 a_2$.

Como $\leq_2$ é relação de ordem em G_2, segue de $a_2 \leq_2 b_2$ e $b_2 \leq_2 a_2$ que $a_2 = b_2$. Portanto $a_1 = b_1$ e $a_2 = b_2$, isto é, $(a_1, a_2) = (b_1, b_2)$.

• $(a_1, a_2) \leq (b_1, b_2)$ e $(b_1, b_2) \leq (c_1, c_2) \Longrightarrow (a_1, a_2) \leq (c_1, c_2)$

$(a_1, a_2) \leq (b_1, b_2) \Longrightarrow (a_1 <_1 b_1)$ ou $(a_1 = b_1$ e $a_2 \leq_2 b_2)$

$(b_1, b_2) \leq (c_1, c_2) \Longrightarrow (b_1 <_1 c_1)$ ou $(b_1 = c_1$ e $b_2 \leq_2 c_2)$

1^o caso: $a_1 <_1 b_1$ e $b_1 <_1 c_1$

Segue que $a_1 \leq_1 b_1$ e $b_1 \leq_1 c_1$. Como $\leq_1$ é uma relação de ordem em G, temos $a_1 \leq_1 c_1$. Note que não pode ocorrer $a_1 = c_1$, pois neste caso teríamos $a_1 <_1 b_1$ e $b_1 <_1 a_1$. Vimos anteriormente que isso é absurdo.

Portanto $a_1 <_1 c_1$, que leva a $(a_1, a_2) \leq (c_1, c_2)$.

2^o caso: $a_1 <_1 b_1$ e $b_1 = c_1$ e $b_2 \leq_2 c_2$

Segue que $a_1 <_1 c_1$ e portanto $(a_1, a_2) \leq (c_1, c_2)$.

3^o caso: $a_1 = b_1$ e $a_2 \leq_2 b_2$ e $b_1 <_1 c_1$

Análogo ao caso anterior.

4^o caso: $a_1 = b_1$ e $a_2 \leq_2 b_2$ e $b_1 = c_1$ e $b_2 \leq_2 c_2$

Segue que $a_1 = c_1$ e $a_2 \leq_2 c_2$. Isso leva a $(a_1, a_2) \leq (c_1, c_2)$.

Admita agora que $\leq_1$ e $\leq_2$ são ordens totais. Devemos mostrar que:

$$\text{se } (a_1, a_2), (b_1, b_2) \in G_1 \times G_2,$$

$$\text{então } (a_1, a_2) \leq (b_1, b_2) \text{ ou } (b_1, b_2) \leq (a_1, a_2).$$

Como $a_1, b_1 \in G_1$ temos $a_1 \leq_1 b_1$ ou $b_1 \leq_1 a_1$.

Como $a_2, b_2 \in G_2$ temos $a_2 \leq_2 b_2$ ou $b_2 \leq_2 a_2$.

1^o caso: $a_1 \leq_1 b_1$ e $a_2 \leq_2 b_2$

Se $a_1 <_1 b_1$ então $(a_1, a_2) \leq (b_1, b_2)$.

Se $a_1 = b_1$, usamos o fato de $a_2 \leq_2 b_2$, para concluir que $(a_1, a_2) \leq (b_1, b_2)$.

2^o caso: $a_1 \leq_1 b_1$ e $b_2 \leq_2 a_2$

Se $a_1 <_1 b_1$ então $(a_1, a_2) \leq (b_1, b_2)$.

Se $a_1 = b_1$, usamos $b_2 \leq_2 a_2$, para obter $(b_1, b_2) \leq (a_1, a_2)$.

3^o caso: $b_1 \leq_1 a_1$ e $a_2 \leq_2 b_2$

Se $b_1 <_1 a_1$ então $(b_1, b_2) \leq (a_1, a_2)$.

Se $b_1 = a_1$, usamos $a_2 \leq_2 b_2$, para obter $(a_1, a_2) \leq (b_1, b_2)$.

4^o caso: $b_1 \leq a_1$ e $b_2 \leq_2 a_2$

Se $b_1 <_1 a_1$ então $(b_1, b_2) \leq (a_1, a_2)$.

Se $b_1 = a_1$, usamos $b_2 \leq_2 a_2$, para obter $(b_1, b_2) \leq (a_1, a_2)$.

■

Proposição 1.1. Sejam $(G_1, +_1, \leq_1)$ e $(G_2, +_2, \leq_2)$ grupos abelianos totalmente ordenados. Então $(G_1 \times G_2, +, \leq)$ é grupo abeliano totalmente ordenado, quando definimos

$$(a_1, b_1) + (a_2, b_2) = (a_1 +_1 a_2, b_1 +_2 b_2).$$

Demonstração. Pelo lema anterior temos que $\leq$ é relação de ordem em $G_1 \times G_2$. Um resultado simples de Teoria de Grupos assegura que $(G_1 \times G_2)$ é grupo abeliano. Resta verificar o axioma (OA), isto é, mostrar que

$$\text{se } (a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2 \text{ e } (a_1, a_2) \leq (b_1, b_2),$$
$$\text{então } (a_1, a_2) + (c_1, c_2) \leq (b_1, b_2) + (c_1, c_2).$$

$(a_1, a_2) \leq (b_1, b_2) \Longrightarrow (a_1 <_1 b_1)$ ou $(a_1 = b_1$ e $a_2 \leq_2 b_2)$

1^o caso: $a_1 <_1 b_1$

Segue que $a_1 \leq_1 b_1$ e $a_1 \neq b_1$. Como $(G_,+_1, \leq_1)$ é grupo abeliano totalmente ordenado e $c_1 \in G_1$ temos:

$$a_1 +_1 c_1 \leq b_1 +_1 c_1 \text{ e } a_1 + c_1 \neq b_1 + c_1 \Longrightarrow a_1 +_1 c_1 < b_1 +_1 c_1$$
$$\Longrightarrow (a_1, a_2)+(c_1, c_2) \leq (b_1, b_2)+(c_1, c_2).$$

2^o caso: $a_1 = b_1$ e $a_2 \leq_2 b_2$

Como $(G_2, +_2, \leq_2)$ é grupo abeliano totalmente ordenado e $c_2 \in G_2$ temos:

$a_2 +_2 c_2 \leq b_2 +_2 c_2$.

De $a_1 = b_1$ tiramos $a_1 +_1 c_1 = b_1 +_1 c_1$.

Isso garante que $(a_1, a_2) + (c_1, c_2) \leq (b_1, b_2) + (c_1, c_2)$.

■

Corolário 1.1. *O grupo abeliano* $(\mathbb{Z} \times \mathbb{Z}, +)$ *é totalmente ordenado.*

Demonstração. Vimos no Exemplo 1.3 que $(\mathbb{Z}, +)$ é grupo abeliano totalmente ordenado. Assim basta aplicar a proposição anterior.

■

Agora estudaremos propriedades dos grupos abelianos totalmente ordenados.

Lema 1.2. Num grupo abeliano totalmente ordenado $(G, +, \leq)$ as seguintes propriedades são equivalentes:

(i) $a < b$

(ii) $a + c < b + c, \forall\, c \in G$

(iii) $-b < -a$

(iv) $a - b < 0$

(v) $0 < b - a$

Demonstração.
• $(i) \implies (ii)$ Se $a < b$ então $a \leq b$ e $a \neq b$. De $a \leq b$ vem por (OA) que, $a + c \leq b + c$. Como $a \neq b$ temos $a + c \neq b + c$.
Logo, $a + c < b + c$.

• $(ii) \implies (iii)$ Como a ordem é total devemos ter $-b < -a$ ou $-b \geq -a$, sendo que estes casos se excluem mutuamente.
Suponha que $-b \geq -a$.

Por (OA), $-b + b \geq -a + b \implies 0 \geq -a + b$
$\implies 0 + a \geq -a + b + a$.

Por (G_4), $0 + a \geq -a + a + b$.
Por (G_1), $0 + a \geq (-a + a) + b$.
Por (G_3) e (G_2), $a \geq b$.
Por (OA), $a + c \geq b + c$. Contradição!

• $(iii) \implies (iv)$ Se $-b < -a$ podemos dizer que $-b \leq -a$ e $-b \neq -a$.

Por (OA), $a - b \leq a - a$.
Por (G_2), $a - b \leq 0$.

Suponha que $a - b = 0$.

Por (G_2), $a - b = a + (-a)$.
Por (OA), $(-a) + a - b = (-a) + a + (-a) \implies -b = -a$.

Contradição. Logo, $a - b < 0$.

• $(iv) \Longrightarrow (v)$ Se $a - b < 0$ podemos dizer que $a - b \leq 0$ e $a - b \neq 0$.

Por (OA), $a - b + (-a) \leq -a$.
Por (G_4), $a + (-a) + (-b) \leq -a$.
Por (G_2), $-b \leq -a$.
Por (OA), $-b + b \leq -a + b$.
Por (G_2), $0 \leq -a + b$.
Por (G_4), $0 \leq b - a$.

Note que não podemos ter $b - a = 0$, pois isso implicaria por (A_4) e (OA), respectivamente, que:

$$\begin{aligned} b - a = b + (-b) &\Longrightarrow -b + b - a + a = -b + b - b + a \\ &\Longrightarrow 0 = -b + a \\ &\Longrightarrow 0 = a - b. \end{aligned}$$

Chegamos em um absurdo. Logo $0 < b - a$.

• $(v) \Longrightarrow (i)$ Se $0 < b - a$ podemos dizer que $0 \leq b - a$ e $0 \neq b - a$.

Por (OA), $a \leq b - a + a$.
Por (G_2), $a \leq b$.

Suponha que $b = a$.

Por (OA) e (G_2) temos:

$$b - a = a - a \Longrightarrow b - a = 0.$$

Contradição. Logo, $a < b$.

■

Observação 1.4. Fazendo $b = 0$, segue do Lema 1.2 $(i) \Longleftrightarrow (v)$ que

$$a < 0 \Longleftrightarrow 0 < -a.$$

Observação 1.5. Fazendo $a = 0$, segue do Lema 1.2 $(i) \Longleftrightarrow (iv)$ que

$$0 < b \Longleftrightarrow -b < 0.$$

Corolário 1.2. *Num grupo abeliano totalmente ordenado $(G, +, \leq)$, as seguintes propriedades são equivalentes:*

(i) $a \leq b$

(ii) $a + c \leq b + c, \forall\, c \in G$

(iii) $-b \leq -a$

(iv) $a - b \leq 0$

(v) $0 \leq b - a$

Demonstração. Imediato do Lema 1.2.

■

Observação 1.6. De forma análoga as observações anteriores, usamos o Corolário 1.2 para obter:

• $a \leq 0 \iff 0 \leq -a$.

• $0 \leq b \iff -b \leq 0$.

Lema 1.3. Para todo elemento a de um grupo abeliano totalmente ordenado $(G, +, \leq)$ e para todo número inteiro n, temos:

(i) se $0 < n$ e se $0 < a$, então $0 < na$.

(ii) se $0 < n$ e se $a < 0$, então $na < 0$.

(iii) se $n < 0$ e se $0 < a$, então $na < 0$.

(iv) se $n < 0$ e se $a < 0$, então $0 < na$.

Demonstração.

(i) Indução sobre n.

• Para $n = 1$.

$n.a = 1.a = a > 0$, por hipótese.

• Hipótese de indução: $ka > 0$ para k fixo, $k > 1$.

• Tese de indução:$(k + 1).a > 0$.

$(k + 1).a = ka + a$

Pela hipótese de indução e pelo Corolário 1.2 temos:

$ka + a > 0 + a = a > 0$.

Logo, por transitividade, $(k + 1).a > 0$.

(ii) Indução sobre n.

• Para $n = 1$.

$n.a = 1.a = a < 0$, por hipótese.

• Hipótese de indução: $ka < 0$ para k fixo, $k > 1$.

• Tese de indução:$(k + 1).a < 0$.

$(k + 1).a = ka + a$

Pela hipótese de indução e pelo Corolário 1.2 temos:

$ka + a < 0 + a = a < 0$.

Logo, por transitividade, $(k + 1).a < 0$.

(iii) Se $n < 0$ temos por (OA),

$n + (-n) < 0 + (-n) \Longrightarrow 0 < -n$.

Então por (i) temos $(-n)a > 0$. Porém, de acordo com a Definição 1.2, $(-n)a = -na$.

Como $-na > 0$, segue da Observação 1.5 que $na < 0$.

(iv) $n < 0 \Longrightarrow -n > 0$.

$a < 0 \Longrightarrow -a > 0$.

Por (i) temos que $(-n)(-a) > 0$. Basta provar que $(-n).(-a) = na$.

Usando a definição temos:

• $(-n).(-a) = (-a) + (-a) + ... + (-a)$, $-n$ vezes.

• $n.a = -(a + a + a + ... + a)$, $-n$ vezes.

Como as expressões acima coincidem, concluímos que $(-n).(-a) = na$.

■

Corolário 1.3. *Para todo número inteiro não nulo n e para todo elemento não nulo a, de um grupo abeliano totalmente ordenado G, tem-se $na \neq 0$.*

Demonstração. Como $n \neq 0$ e $a \neq 0$ temos, pelo Lema 1.3, que $na \neq 0$.

■

Corolário 1.4. *Sejam G um grupo abeliano totalmente ordenado e $a \in G$. Se $0 < a$ e se m e n são números inteiros tais que $m \leq n$, então $ma \leq na$. Além disso, se $m < n$ temos $ma < na$.*

Demonstração.
$m \leq n \Longrightarrow n - m \geq 0$.

Temos dois casos: $n - m > 0$ ou $n - m = 0$.

(i) Se $n - m = 0$ temos por definição que $(m - n) \cdot a = 0$.

$$(n - m).a = 0 \Longrightarrow na - ma = 0$$
$$\Longrightarrow na = ma.$$

(ii) Se $n - m > 0$ temos pelo Lema 1.3 que $(n - m) \cdot a > 0$.

$$(n - m).a > 0 \Longrightarrow na - ma > 0$$
$$\Longrightarrow ma < na.$$

Portanto, $ma \leq na$.

Se $m < n$ temos $ma < na$, pela parte (ii) da demonstração acima.

■

Corolário 1.5. *Sejam G um grupo abeliano totalmente ordenado e $a \in G$. Se $a < 0$ e se m e n são números inteiros tais que $m \leq n$ então $na \leq ma$. Além disso, se $m < n$ então $na < ma$.*

Demonstração.
$m \leq n \Longrightarrow n - m \geq 0$.

Temos dois casos: $n - m > 0$ ou $n - m = 0$.

(i) Se $n - m = 0$ temos por definição que $(n - m) \cdot a = 0$.

$$(n - m).a = 0 \Longrightarrow na - ma = 0$$
$$\Longrightarrow na = ma.$$

(ii) Se $n - m > 0$ temos pelo Lema 1.3 que $(n - m) \cdot a < 0$.

$$(n - m).a < 0 \Longrightarrow na - ma < 0$$
$$\Longrightarrow na < ma.$$

Portanto, $na \leq ma$.

Se $m < n$ temos $na < ma$, pela parte (ii) da demonstração acima.

■

Proposição 1.2. Sejam a e b dois elementos de um grupo abeliano totalmente ordenado G tais que $a < b$ e seja n um número inteiro. As seguintes afirmações são verdadeiras:

(i) se $0 < n$, então $na < nb$.

(ii) se $n < 0$, então $nb < na$.

Demonstração.

(i) Como $a < b$ segue do Lema 1.2 que $a - b < 0$. Desde que $n > 0$, usamos o Lema 1.3 para obter:

$$\begin{aligned} n(a-b) < 0 &\Longrightarrow na - nb < 0 \\ &\Longrightarrow na < nb. \end{aligned}$$

(ii) Como $a < b$ segue do Lema 1.2 que $a - b < 0$. Desde que $n < 0$, usamos o Lema 1.3 para obter:

$$\begin{aligned} n(a-b) > 0 &\Longrightarrow na - nb > 0 \\ &\Longrightarrow nb < na. \end{aligned}$$

■

Corolário 1.6. *Sejam a e b dois elementos de um grupo abeliano totalmente ordenado G tais que $a \leq b$ e seja n um número inteiro. As seguintes afirmações são verdadeiras:*

(i) se $0 < n$, então $na \leq nb$.

(ii) se $n < 0$, então $nb \leq na$.

Demonstração.

(i) Se $a = b$ então $na = nb$.

Se $a < b$, segue da Proposição 1.2 que $na < nb$.

Portanto, $na \leq nb$.

(ii) Se $a = b$ então $na = nb$.

Se $a < b$, segue da Proposição 1.2 que $nb < na$.

Portanto, $nb \leq na$.

■

Veremos a seguir uma caracterização dos grupos abelianos totalmente ordenados.

Definição 1.7. Diz-se que um elemento a, de um grupo abeliano totalmente ordenado G, é **positivo** (respectivamente, negativo) se, e somente se, $0 \leq a$ (respectivamente, $a \leq 0$). Se a é positivo (respectivamente, negativo) e se $a \neq 0$, diremos que a é **estritamente positivo** (respectivamente, estritamente negativo).

De acordo com a definição acima, o elemento neutro $0 \in G$, é positivo e negativo. Como a relação $\leq$ é anti-simétrica, vemos que 0 é o único elemento de G com tal propriedade.

Notação: Sejam G um grupo abeliano e $A, B \subseteq G$. Usaremos as notações:

- $A + B = \{a + b; a \in A \text{ e } b \in B\}$.
- $-A = \{-a; a \in A\}$.

Teorema 1.1. *Se G é um grupo abeliano totalmente ordenado e se P é o conjunto de todos elementos positivos de G, então valem as seguintes propriedades:*

(I) $P + P \subset P$*;*

(II) $P \bigcap (-P) = \{0\}$*;*

(III) $P \bigcup (-P) = G$*.*

Além disso, se G é um grupo abeliano e se P é uma parte do conjunto G que satisfaz as condições (I), (II), (III), então existe uma única relação de ordem total $\leq$ em G, compatível com a adição, tal que P seja o conjunto de todos os elementos positivos da ordem $\leq$.

Demonstração.

(I) $P + P \subset P$

Sejam $a, b \in P$, então $a \geq 0$ e $b \geq 0$.

Por (OA), $a + b \geq 0 + b = b \geq 0$.

Por (O_3), $a + b \geq 0$.

Logo, $a + b \in P$.

(II) $P \bigcap (-P) = \{0\}$

Temos pela Definição 1.7 que se $a \in P$ então $a \geq 0$, e se $b \in (-P)$ então $b \leq 0$.

$$x \in P \bigcap (-P) \Longrightarrow x \in P \text{ e } x \in -P$$
$$\Longrightarrow x \geq 0 \text{ e } x \leq 0.$$

Então por (O_2), $x = 0$.

(III) $P \bigcup (-P) = G$

Claro que $P \bigcup (-P) \subseteq G$, pois $P \subseteq G$ e $(-P) \subseteq G$.

Seja $a \in G$. Como $\leq$ é ordem total temos $a \leq 0$ ou $0 \leq a$. Segue que $a \in (-P)$ ou $a \in P$. Portanto $a \in P \bigcup (-P)$.

Suponha agora que G seja grupo abeliano e que exista $P \subseteq G$ satisfazendo as condições (I), (II) e (III).

Defina em G a relação:

$$a \leq b \Longleftrightarrow b - a \in P.$$

Afirmação: A relação acima é relação de ordem.

• Reflexiva (O_1): É imediato, pois $a - a = 0$ e $0 \in P$ em virtude de (II).

• Anti-simétrica (O_2): Se $a \leq b$ e se $b \leq a$ temos, respectivamente, $b - a \in P$ e $a - b \in P$. Note que $(a - b) = -(b - a)$, logo, $a - b \in (-P)$, de onde vem, por (II), $a - b = 0$, ou seja, $a = b$.

• Transitiva (O_3): Se $a \leq b$ e se $b \leq c$, temos $b - a \in P$ e $c - b \in P$. Da condição (I) resulta que:

$$(b - a) + (c - b) \in P \Longrightarrow c - a \in P$$
$$\Longrightarrow a \leq c.$$

Devemos também verificar que $\leq$ define uma relação de ordem total, ou seja, provar (O_4).

• (O_4): Sejam a e b dois elementos quaisquer de G e consideremos a diferença $a - b$.

Conforme a condição (III) temos $a - b \in P$ ou $a - b \in (-P)$.

Se $a - b \in P$ temos $b \leq a$.

Se $a - b \in (-P)$ temos $b - a \in P$, ou seja, $a \leq b$.

Falta verificar que a relação $\leq$ é compatível com a operação do grupo, isto é, falta provar (OA).

• (OA): Sejam a, b e c elementos quaisquer de G e suponhamos que $a \leq b$.

$a \leq b \Longrightarrow b - a \in P$

$\Longrightarrow (b + c) - (a + c) = b - a \in P$

$\Longrightarrow a + c \leq b + c$.

Note que o conjunto P é formado pelos elementos positivos de G. De fato,

$$a \in P \Longleftrightarrow a - 0 \in P \Longleftrightarrow 0 \leq a.$$

Finalmente, vamos provar a unicidade da ordem.

Seja R uma relação de ordem total em G, compatível com a adição de G, tal que P é o conjunto dos elementos positivos de G segundo a ordem R. Isto é,

$$P = \{a \in G; 0Ra\}.$$

Pelo Corolário 1.2 temos:

$aRb \Longleftrightarrow 0R(b - a) \Longleftrightarrow b - a \in P$.

Mas havíamos definido a relação

$$b - a \in P \Longleftrightarrow a \leq b.$$

Segue que $aRb \Longleftrightarrow a \leq b$.

Portanto as relações R e $\leq$ coincidem.

■

Corolário 1.7. *Um grupo abeliano G é ordenável se, e somente se, existe uma parte P, do conjunto G, que satisfaz as condições (I), (II) e (III).*

Demonstração. É imediato do teorema anterior.

■

Exemplo 1.4. O subconjunto $P = \mathbb{N}$ do grupo abeliano $\mathbb{Z}$ dos números inteiros satisfaz as condições (I), (II) e (III) do Teorema 1.1. Portanto, define uma ordem total $\leq$, sobre $\mathbb{Z}$, pondo-se

$$a \leq b \Longleftrightarrow b - a \geq 0.$$

Além disso, esta ordem é compatível com a adição:

$$a \leq b \text{ e } c \in \mathbb{Z} \Longrightarrow a + c \leq b + c.$$

Analogamente, o subconjunto $P = -\mathbb{N}$ também satisfaz as condições (I), (II) e (III). Portanto, obtém-se uma outra ordem total, compatível com a adição, pondo-se

$$aRb \Longleftrightarrow b - a \text{ é o oposto de um números natural.}$$

Podemos completar o que foi visto acima mostrando que os únicos subconjuntos P, de $\mathbb{Z}$, que satisfazem as condições (I), (II) e (III) são $\mathbb{N}$ e $-\mathbb{N}$.

Com efeito, conforme (III) temos $1 \in P$ ou $1 \in -P$.

Se $1 \in P$ temos, por (II), que $\mathbb{N} \subset P$. Suponha, por absurdo, $\mathbb{N} \neq P$.

$$\begin{aligned} \mathbb{N} \neq P &\Longrightarrow \exists\, b \in P \text{ tal que } b \notin \mathbb{N} \\ &\Longrightarrow b = -a, \text{ com } a \in \mathbb{N} \\ &\Longrightarrow b \in P \bigcap (-P) = \{0\} \\ &\Longrightarrow b = 0, \end{aligned}$$

contradição, pois $b \notin \mathbb{N}$.

Analogamente, se $1 \in -P$ conclui-se que $P = -\mathbb{N}$.

Em resumo, o grupo abeliano $\mathbb{Z}$ dos números inteiros só pode ser ordenado de dois modos obtendo-se, então, a ordem habitual e sua oposta.

O exemplo a seguir mostra uma outra forma de se obter o resultado do Corolário 1.1.

Exemplo 1.5. Consideremos o conjunto $G = \mathbb{Z} \times \mathbb{Z}$ e coloquemos, por definição, $(a, b) + (c, d) = (a + c, b + d)$ quaisquer que sejam (a, b) e (c, d) em G. É fácil verificar que esta operação define uma estrutura de grupo abeliano sobre $\mathbb{Z} \times \mathbb{Z}$.

Indiquemos por P o subconjunto de $\mathbb{Z} \times \mathbb{Z}$ formado por todos os pares (a, b) tais que $0 < a$ e b qualquer, ou $a = 0$ e $0 \leq b$, onde $\leq$ é a ordem habitual do grupo aditivo $\mathbb{Z}$.

Vamos verificar as condições (I), (II) e (III) para o subconjunto P.

(I): Sejam (a, b) e $(c, d) \in P$.

$(a, b) \in P \Longrightarrow (0 < a$ e b qualquer) ou $(a = 0$ e $0 \leq b)$.

$(c, d) \in P \Longrightarrow (0 < c$ e d qualquer) ou $(c = 0$ e $0 \leq d)$.

1^o caso: $0 < a$, b qualquer, $0 < c$ e d qualquer.

$(a, b) + (c, d) = (a + c, b + d)$.

Por (OA) e (O_3) temos:

$0 < a$ e $0 < c \Longrightarrow 0 < a + c$.

Logo, $(a + c, b + d) \in P$.

2^o caso: $0 < a$, b qualquer, $c = 0$ e $0 \leq d$.

Por (G_2), $a + c = a + 0 = a > 0$.

Logo, $(a + c, b + d) \in P$.

3^o caso: $a = 0$, $0 \leq b$, $0 < c$ e d qualquer.

Análogo ao caso anterior.

4^o caso: $a = 0$, $0 \leq b$, $c = 0$ e $0 \leq d$.

$a + c = 0 + 0 = 0$ e $0 \leq b + d$,

por (OA) e (O_3).

Logo, $(a + c, b + d) \in P$.

(II): Seja $(a, b) \in P \bigcap (-P)$.

$(a, b) \in P \Longrightarrow (0 < a$ e b qualquer) ou $(a = 0$ e $0 \leq b)$.

$(a, b) \in (-P) \Longrightarrow (a < 0$ e b qualquer) ou $(a = 0$ e $b \leq 0)$.

1^o caso: $0 < a$, b qualquer, $a < 0$ e b qualquer.

Não podem ocorrer simultanenamente $0 < a$ e $a < 0$.

2^o caso: $0 < a$, b qualquer, $a = 0$ e $b \leq 0$.

Não podem ocorrer simultanenamente $0 < a$ e $a = 0$.

3^o caso: $a = 0$, $0 \leq b$, $a < 0$ e b qualquer.

Análogo ao caso anterior.

4^o caso: $a = 0$, $0 \leq b$, $a = 0$ e $b \leq 0$.

$0 \leq b$ e $b \leq 0 \Longrightarrow b = 0$,

por (O_2).

Logo, $(a, b) = (0, 0)$.
Portanto, $P \bigcap (-P) = \{(0, 0)\}$.

(III): Seja $(a, b) \in G$.

Se $a = 0$ e $0 \leq b$ então $(a, b) \in P$.

Se $a = 0$ e $b < 0$ então $(a, b) \in (-P)$.

Se $0 < a$ e b qualquer então $(a, b) \in P$.

Se $a < 0$ e b qualquer então $(a, b) \in (-P)$.

Logo, $P \bigcup (-P) = G$.

Portanto, pelo Teorema 1.1, $\mathbb{Z} \times \mathbb{Z}$ é um grupo ordenado pela ordem $\leq$, definido por

$$\begin{aligned}(a, b) \leq (c, d) &\iff (c, d) - (a, b) \in P \\ &\iff (c - a, d - b) \in P \\ &\iff c - a > 0 \text{ ou } (c - a = 0 \text{ e } d - b \geq 0) \\ &\iff a < c \text{ ou } (a = c \text{ e } b \leq d).\end{aligned}$$

Exemplo 1.6. Os grupos abelianos $(\mathbb{Z}_n, +)$ não são ordenáveis.

De acordo com o Corolário 1.7, basta verificar que $\mathbb{Z}_n$ não possui subconjunto que satisfaça as condições (I), (II) e (III).

Suponha que $\mathbb{Z}_n$ possua subconjunto P satisfazendo (I), (II) e (III).

Se P contém um gerador de $(\mathbb{Z}_n, +)$, segue da condição (I) que $P = \mathbb{Z}_n$. Então $(-P) = \mathbb{Z}_n$ e isso contradiz (II). Portanto P não pode conter gerador de $\mathbb{Z}_n$.

Como $\overline{1}$ e $\overline{n-1}$ são geradores de $(\mathbb{Z}_n, +)$, segue de (III) que

$\overline{1}, \overline{n-1} \in (-P)$. Mas

- $\overline{1} \in (-P) \Longrightarrow -\overline{1} = \overline{n-1} \in P$
- $\overline{n-1} \in (-P) \Longrightarrow \overline{1} \in P$.

Isso diz que P possui gerador de $(\mathbb{Z}_n, +)$. Absurdo.

Portanto, não existe subconjunto P que satisfaça as condições (I), (II) e (III).

Veremos a seguir uma generalização do Teorema 1.1.

Teorema 1.2. *Seja G um grupo abeliano.*

(a) Se $(G, +, \leq)$ é parcialmente ordenado, então o conjunto P dos elementos positivos de G satisfaz:

(I) $P + P \subset P$.

(II) $P \bigcap (-P) = \{0\}$.

(b) Se $P \subseteq G$ satisfaz (I) e (II), então existe uma única relação de ordem em G, compatível com a adição de G, tal que P é o conjunto dos elementos positivos desta ordem.

(c) A ordem obtida em (b) é total se, e somente se, P também satisfaz a condição (III).

Demonstração.

(a) Demonstração análoga a do Teorema 1.1.

(b) Defina em G a relação:

$$a \leq b \Longleftrightarrow b - a \in P.$$

A demonstração, de que a relação acima é relação de ordem é análoga àquela feita no Teorema 1.1.

Falta provar a unicidade. Seja R uma relação de ordem em G, compatível com a adição de G, tal que P é o conjunto dos elementos positivos de G segundo a ordem R. Isto é,

$$P = \{a \in G; 0Ra\}.$$

Pelo Corolário 1.2 temos:

$aRb \Longleftrightarrow 0R(b - a) \Longleftrightarrow b - a \in P$.

Mas havíamos definido a relação

$$b - a \in P \Longleftrightarrow a \leq b.$$

Segue que $aRb \Longleftrightarrow a \leq b$.

Portanto as relações R e $\leq$ coincidem.

(c) Se a ordem é total então para todo $a \in G$ temos:

$a \leq 0$ ou $a \geq 0 \Longrightarrow a \in -P$ ou $a \in P$.

Portanto, $P \bigcup (-P) = G$.

Reciprocamente, suponha que valha a condição (III).

Dados $a, b \in G$ temos $a - b \in G$, e então

$$a - b \in P \text{ ou } a - b \in (-P) \Longrightarrow 0 \leq a - b \text{ ou } a - b \leq 0$$
$$\Longrightarrow b \leq a \text{ ou } a \leq b.$$

Portanto, a ordem $\leq$ é ordem total.

■

Exemplo 1.7. Considere o grupo abeliano $\mathbb{Z}$ dos números inteiros e tome P como o conjunto dos números naturais pares. Podemos verificar usando o teorema anterior, que P define uma ordem parcial sobre $\mathbb{Z}$.

Vamos demonstrar a afirmação acima.
Sejam a e b em P. Podemos escrever $a = 2x$ e $b = 2y$; $x, y \in \mathbb{N}$.

(I) $P + P \subset P$

$2x + 2y = 2(x + y) \in P$, por definição.

(II) $P \bigcap (-P) = \{0\}$

$a \in P \bigcap (-P) \Longrightarrow a \in P$ e $a \in (-P)$.

$a \in P \Longrightarrow a = 2x$, $x \in \mathbb{N}$ e

$a \in (-P) \Longrightarrow a = 2y$, $y \in (-\mathbb{N})$

Então temos $2x = 2y \Longrightarrow x = y$.

Logo, $x \in \mathbb{N} \bigcap (-\mathbb{N}) = \{0\}$. Como $a = 2x$ e $x = 0$ temos $a = 0$.

Segue do Teorema 1.2 que $P = \{2x; x \in \mathbb{N}\}$ define em $\mathbb{Z}$ a relação de ordem

$$a \leq b \Longleftrightarrow b - a \in P.$$

Note que esta ordem não é total. De fato, para ser total deveríamos ter $\mathbb{Z} = P \bigcup (-P)$. Mas isso não é verdade pois $3 \in \mathbb{Z}$, mas $3 \notin P$ e $3 \notin (-P)$.

Existe uma categoria especial de grupos abelianos totalmente ordenados, que usaremos posteriormente, são os grupos abelianos totalmente ordenados arquimedianos.

Definição 1.8. Diz-se que um grupo abeliano totalmente ordenado $(G, +, \leq)$ é **grupo arquimediano** se, e somente se, a ordem $\leq$ satisfaz o seguinte axioma:

(AA) quaisquer que sejam a e b em G, se $0 < a$ e $0 < b$ então existe um número natural n tal que $b < na$.

Exemplo 1.8. O grupo abeliano $\mathbb{Z}$ dos números inteiros, com a ordem usual, é arquimediano, pois se a e b são dois inteiros tais que $0 < a < b$, temos $b < (b + 1)a$.

Exemplo 1.9. O grupo ordenado $\mathbb{Z} \times \mathbb{Z}$, definido no Exemplo 1.5, não é arquimediano, pois, por exemplo, temos $(0, 0) < (0, 1) < (1, 1)$ e no entanto $n(0, 1) = (0, n) < (1, 1)$ para todo $n \in \mathbb{N}^*$.

Teorema 1.3. *Se $(G, +, \leq)$ é um grupo arquimediano e se a e b são dois elementos estritamente positivos, então existe um único número natural não nulo m tal que $(m - 1)a \leq b < ma$.*

Demonstração. Consideremos o conjunto S de todos os números naturais não nulos n tais que $b < na$.

De acordo com o axioma de Arquimedes S é não vazio, logo, existe $m = \min S$ e temos $m \neq 0$ e $b < ma$.

Se $m = 1$, temos $0.a = 0 < b < a$.

Se $m > 1$, teremos $m > 0$ e $m - 1 \notin S$, portanto, $(m - 1)a \leq b < ma$.

Finalmente, seja $m' \in \mathbb{N}^*$ tal que $(m' - 1)a \leq b < m'a$.

Se $m < m'$, temos $m \leq m' - 1$, portanto, em virtude do Corolário 1.4, resulta que $ma \leq (m' - 1)a$, de onde vem, $ma \leq b$, contra a definição do inteiro m.

Analogamente, chega-se a uma contradição no caso em que se supõe $m' < m$.

Portanto, $m' = m$.

■

Proposição 1.3. Se $(G, +, \leq)$ é um grupo arquimediano e se a e b são dois elementos quaisquer de G, com $a \neq 0$, então existe um número inteiro n tal que $b < na$.

Demonstração.
Se $b < a$, tome $n = 1$. Assim podemos assumir $a \leq b$.
Se $a = b < 0$, tome $n = -1$. Então $b < 0 < na$.
Se $a = b > 0$, tome $n = 2$. Então $b = a < a + a = na$.
Se $b = 0$ e $a > 0$, tome $n = 1$.
Se $b = 0$ e $a < 0$, tome $n = -1$. Então $0 = b < na$.
Portanto, podemos assumir $a < b$ e $a \neq 0 \neq b$. Vamos analisar os casos:

(i) $a > 0$ e $b > 0$.

(ii) $a < 0$ e $b > 0$.

(iii) $a < 0$ e $b < 0$.

(i) É imediato do Teorema 1.3 .

(ii) Se $a < 0$ então $-a > 0$. Dessa forma basta usar o item anterior.

(iii) Temos $a < 0$ e $b < 0$. Além disso, temos que $a < b$.
Tome então $n = -1$, assim $b < 0 < na = -1a$.

■

A relação de ordem de um grupo abeliano ordenado permite que se estabeleça o conceito de módulo que gera algumas propriedades importantes.

Definição 1.9. Chama-se **valor absoluto** (ou módulo) de um elemento a, de um grupo totalmente ordenado G, ao elemento $|a|$ definido por :

$$|a| = \begin{cases} a & , \text{ se } 0 \leq a. \\ -a & , \text{ se } a < 0. \end{cases}$$

Notemos que a definição acima pode ser posta sob a forma

$$|a| = \max\{a, -a\}.$$

Por exemplo, $|1| = 1$, $|0| = 0$ e $|-1| = 1$.

Teorema 1.4. *Num grupo abeliano totalmente ordenado G, valem as seguintes propriedades:*

(i) $0 \leq |a|$ *para todo a em G e* $|a| = 0$ *se, e somente se,* $a = 0$.

(ii) $|-a| = |a|$, *para todo a em G.*

(iii) $-|a| \leq a \leq |a|$, *para todo a em G.*

(iv) se $0 \leq a$ *e se* $x \in G$ *é tal que* $-a \leq x \leq a$, *então* $|x| \leq a$.

(v) $|x + y| \leq |x| + |y|$, *quaisquer que sejam x e y em G.*

Demonstração.

(i) • $0 \leq |a|$ para todo a em G

Se $a \geq 0$ então $|a| = a$, por definição. Logo, por transitividade, temos $|a| \geq 0$.

Se $a < 0$ então $|a| = -a$. Por (OA), temos $-a > 0$. Logo, $|a| > 0$.

• $|a| = 0 \iff a = 0$.

$(\Longrightarrow)$ Suponha $a \neq 0$.

$a > 0 \Longrightarrow |a| = a > 0$. Absurdo.

$a < 0 \Longrightarrow |a| = -a > 0$. Absurdo.

$(\Longleftarrow)$ Se $a = 0$, então por definição $|a| = |0| = 0$.

(ii) $|-a| = |a|$, para todo a em G.

• Se $a \geq 0$ então por (OA), $-a \leq 0$. Logo, $|a| = a$ e $|-a| = -(-a) = a$, o que resulta em $|a| = |-a|$.

• Se $a \leq 0$ então por (OA), $-a \geq 0$. Logo, $|a| = -a$ e $|-a| = -a$, o que resulta em $|a| = |-a|$.

(iii) $-|a| \leq a \leq |a|$, para todo a em G.

• Se $a \geq 0$ então $|a| = a$. Podemos dizer, em particular, que $a \leq |a|$.
Como $|a| \geq 0$, então $-|a| \leq 0$. Ficamos com:

$-|a| \leq 0 \leq a \leq |a| \Longrightarrow -|a| \leq a \leq |a|$.

• Se $a < 0$, temos que:

$a < 0 < |a| \Longrightarrow a < |a|$.

Podemos dizer, em particular, que $a \leq |a|$. Além disso, temos que:

$|a| = -a \Longrightarrow -|a| = a \Longrightarrow -|a| \leq a$.

Logo, $-|a| \leq a \leq |a|$.

(iv) se $0 \leq a$ e se $x \in G$ é tal que $-a \leq x \leq a$, então $|x| \leq a$.

Se $x \geq 0$, então $|x| = x \leq a$.

Se $x < 0$, então $|x| = -x$. Mas, por hipótese, $-a \leq x$ o que implica que $-x \leq a$. Logo, $|x| \leq a$.

(v) $|x + y| \leq |x| + |y|$, quaisquer que sejam x e y em G.

Somando membro a membro as desigualdades

$-|x| \leq x \leq |x|$ e $-|y| \leq y \leq |y|$,

obtemos:

$-(|x| + |y|) \leq x + y \leq |x| + |y|$,

logo de (iv), segue que $|x + y| \leq |x| + |y|$.

■

Proposição 1.4. Para todo número inteiro n e para todo elemento x de um grupo abeliano totalmente ordenado G temos $|nx| = |n| \cdot |x|$.

Demonstração. Temos quatro casos, são eles:

(i) $n \geq 0$ e $x \geq 0$.

(ii) $n < 0$ e $x < 0$.

(iii) $n \geq 0$ e $x < 0$.

(iv) $n < 0$ e $x \geq 0$.

(i) Como $n \geq 0$ e $x \geq 0$ temos por definição,

$|n| = n$ e $|x| = x$.

Temos também pelo Lema 1.3 que $nx \geq 0$ então $|nx| = nx$.

Logo $|n| \cdot |x| = n \cdot x = |nx|$.

(ii) Como $n < 0$ e $x < 0$ temos por definição,

$|n| = -n$ e $|x| = -x$

Temos novamente pelo Lema 1.3 que $nx > 0$ então $|nx| = nx$. Ficamos com,

$|n| \cdot |x| = (-n) \cdot (-x) = nx = |nx|$.

(iii) Como $n \geq 0$ e $x < 0$ temos

$|n| = n$ e $|x| = -x$

Sabemos que $n \cdot x < 0$, ou seja, $|nx| = -nx$.

Logo $|n| \cdot |x| = (-n) \cdot x = |nx|$.

(iv) Análogo ao item (iii).

■

Proposição 1.5. Se a e b são dois elementos quaisquer de um grupo abeliano totalmente ordenado G, então $||a| - |b|| \leq |a - b|$.

Demonstração.
1^o caso: $a \geq 0$ e $b \geq 0$ então $|a| = a$ e $|b| = b$. Assim

$||a| - |b|| = |a - b| \leq |a - b|$.

2^o caso: $a \leq 0$ e $b \leq 0$ então $|a| = -a$ e $|b| = -b$. Assim

$$\begin{aligned} ||a| - |b|| &= |(-a) - (-b)| \\ &= |-a + b| \\ &= |(-1) \cdot (a - b)| \\ &= |-1| \cdot |a - b| \leq |a - b|. \end{aligned}$$

3^o caso: $a \geq 0$ e $b < 0$ então $|a| = a$ e $|b| = -b$. Assim

$||a| - |b|| = |a - (-b)| = |a + b|$.

Gostaria de provar que $|a + b| \leq |a - b|$.

Pelo Teorema 1.4, $|a + b| \leq |a| + |b| = a - b$.

Como $a \geq 0$ e $b < 0$ temos $b < a$, ou seja, $0 < a - b$. Portanto, $|a - b| = a - b$.

Logo, $|a + b| \leq |a - b|$.

4^o caso: $a < 0$ e $b \geq 0$. Demonstração análoga a anterior.

■

Na próxima secção estudaremos uma estrutura algébrica munida de duas operações, os anéis.

1.2 Anéis Ordenados

Definição 1.10. Um conjunto não vazio A é um **anel** em relação às operações binárias de adição $(+)$ e multiplicação $(\cdot)$ desde que, para arbitrários $a, b, c \in A$, as seguintes propriedades sejam verificadas:

(A_1) $(a + b) + c = a + (b + c)$ (a operação $(+)$ é associativa).

(A_2) $a + b = b + a$ (a operação $(+)$ é comutativa).

(A_3) $\exists\, 0_A \in A$ tal que $a + 0_A = a$ (existe elemento neutro para a operação $(+)$).

(A_4) $\forall\, a \in A$, $\exists\, (-a) \in A$ tal que $a + (-a) = 0_A$ (todo elemento tem simétrico aditivo).

(M_1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (a operação $(\cdot)$ é associativa).

(M_2) $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributividade de $(\cdot)$ à esquerda de $(+)$).

(M_3) $(b + c) \cdot a = b \cdot a + c \cdot a$ (distributividade de $(\cdot)$ à direita de $(+)$).

Nas condições expostas acima dizemos que a terna ordenada $(A, +, \cdot)$ é um anel.

Por abuso de linguagem é comum dizer-se apenas que A é um anel para expressar o conceito agora introduzido. Isto naturalmente pressupõe que as duas operações tenham sido fixadas "a priori".

Definição 1.11. O anel $(A, +, \cdot)$ é **anel comutativo** quando:

(M_4) $a \cdot b = b \cdot a$; $\forall\, a, b \in A$.

Definição 1.12. O anel $(A, +, \cdot)$ é **anel com unidade** quando:

(M_5) $\exists\, 1_A \in A$ tal que $a \cdot 1_A = 1_A \cdot a = a$, $\forall\, a \in A$.

Definição 1.13. O anel $(A, +, \cdot)$ é **anel sem divisores de zero** quando:

(M_6) $a, b \in A$ e $a \cdot b = 0 \Longrightarrow a = 0$ ou $b = 0$.

Definição 1.14. Um **domínio** (domínio de integridade ou anel de integridade) é um anel comutativo, com unidade e sem divisores de zero.

Exemplo 1.10. São exemplos clássicos de domínios:
• Anel dos inteiros $(\mathbb{Z}, +, \cdot)$.
• Anel dos racionais $(\mathbb{Q}, +, \cdot)$.

• Anel dos reais $(\mathbb{R}, +, \cdot)$.
• Anel dos complexos $(\mathbb{C}, +, \cdot)$.

Exemplo 1.11. Para cada $n \in \mathbb{Z}$, o conjunto $n\mathbb{Z} = \{n \cdot q \setminus q \in \mathbb{Z}\}$, é anel em relação à adição e à multiplicação usuais de $\mathbb{Z}$. Note que $n\mathbb{Z}$ é comutativo, sem divisores de zero, mas não tem unidade, exceto quando $n = 1$.

Exemplo 1.12. $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a, b, c, d \in \mathbb{R} \right\}$, com as operações usuais de matrizes é anel não comutativo, com divisores de zero e com unidade.

Proposição 1.6. As seguintes afirmações são verdadeiras para um anel qualquer.

(i) O elemento neutro da adição é único.

(ii) O elemento neutro da multiplicação é único.

(iii) O simétrico de um elemento é único.

Demonstração.

(i) O elemento neutro da adição é único.

De fato, sejam α e α' elementos neutros para a adição. Como α' é neutro temos que

$\alpha = \alpha' + \alpha$

e, como α é neutro temos que

$\alpha' = \alpha + \alpha'$.

Por (A_2) temos então que

$\alpha' = \alpha + \alpha' = \alpha' + \alpha = \alpha$.

Logo $\alpha' = \alpha$.

(ii) O elemento neutro da multiplicação é único.

A demonstração acima devidamente adaptada nos fornece o resultado.

(iii) O simétrico de um elemento $a \in G$ é único.

De fato, se a' e a'' são dois simétricos de a, então por (A_2) e (A_1) temos que

$a'' = 0 + a'' = (a' + a) + a'' = a' + (a + a'') = a' + 0 = a'$.

■

Observação 1.7. Usaremos o símbolo 0 para denotar o elemento neutro da adição que será chamado de zero.

Observação 1.8. Usaremos o símbolo 1 para denotar o elemento neutro da multiplicação que será chamado de unidade ou apenas de um.

A proposição a seguir traz propriedades de simétricos em um anel qualquer. Usaremos estes resultados na demonstração do Teorema 1.6.

Proposição 1.7. Sejam A um anel qualquer e $a, b \in A$. Então:

(i) $a(-b) = (-a)b = -ab$.

(ii) $(-a).(-b) = ab$.

Demonstração.

(i) Note que:

$0 = a.0 = a.(b - b) = ab + a(-b)$.

Isso assegura que o simétrico de ab é $a(-b)$. Portanto, $-ab = a(-b)$.

Analogamente verifica-se que $-ab = (-a)b$.

(ii) Usando (i) temos:

$(-a)(-b) = -(a(-b)) = -(-(ab))$.

Como $ab - ab = 0$, concluímos que o simétrico de $-ab$ é ab. Isto é, $-(-ab) = ab$.

Portanto, $(-a)(-b) = -(-ab) = ab$.

■

Ao se definir um novo ente matemático é necessário que se estabeleça quando dois representantes deste ente são considerados iguais. É o que faremos agora em relação a anéis. Para isto há a necessidade de algumas definições.

Definição 1.15. Sejam A e A' dois anéis e seja f uma função do conjunto A no conjunto A'. Diz-se que f é um **homomorfismo** do anel A no anel A' se, e somente se, são válidas as seguintes condições:

(1) $f(a + b) = f(a) + f(b)$.

(2) $f(a \cdot b) = f(a) \cdot f(b)$, quaisquer que sejam a, b $\in A$.

Exemplo 1.13. Sejam $A = \mathbb{Z}$ e $B = \mathbb{Z} \times \mathbb{Z}$, $f : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ definida por $f(x) = (x, 0)$, $\forall x \in \mathbb{Z}$. f é homomorfismo porque

$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$ e

$f(x \cdot y) = (x \cdot y, 0) = (x, 0) \cdot (y, 0) = f(x) \cdot f(y)$.

Exemplo 1.14. Considere a função $f : \mathbb{Z} \longrightarrow A$, onde A é um anel, definida por $f(n) = 1_A n$. f é homomorfismo porque

$f(m) + f(n) = 1_A m + 1_A n = 1_A(m + n) = f(m + n)$ e

$f(m) \cdot f(n) = (1_A m) \cdot (1_A n) = 1_A(m(1_A n)) = m(n1_A) = 1_A(mn) = f(mn)$.

Definição 1.16. Se f é um homomorfismo de A em A' e se f é uma função injetora, diremos que f é um **monomorfismo** de A em A' ou que f é um homomorfismo injetor de A em A'.

Exemplo 1.15. O homomorfismo $f : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ dado por $f(x) = (x, 0)$, $\forall\, x \in \mathbb{Z}$, é monomorfismo pois

$f(x) = f(y) \Longrightarrow (x, 0) = (y, 0) \Longrightarrow x = y$.

Existe uma forma alternativa para verificar se um homomorfismo f é monomorfismo. Para apresentá-la, introduziremos o conceito a seguir.

Definição 1.17. Seja $f : A \longrightarrow B$ um homomorfismo de anéis, chamamos de **núcleo** (ou kernel) de f o conjunto $N(f) = \{a \in A; f(a) = 0\}$.

Exemplo 1.16. Seja $f : \mathbb{Z} \longrightarrow A$ definida por $f(n) = 1_A n$. Vimos no Exemplo 1.14 que f é um homomorfismo. Tomando-se $A = \mathbb{Z}$, o homomorfismo f é a função idêntica de $\mathbb{Z}$ e seu núcleo se reduz a $\{0\}$.

Exemplo 1.17. Seja $f : \mathbb{Z} \longrightarrow A$ definida por $f(n) = 1_A n$. Vimos no Exemplo 1.14 que f é um homomorfismo. Seja $m > 1$ e tomemos $A = \mathbb{Z}_m$.

Neste caso, o homomorfismo f é definido por $f(n) = \overline{1} \cdot n = \overline{n}$ e seu núcleo é $m\mathbb{Z}$ como vemos abaixo:

$N(f) = \{a \in \mathbb{Z}; f(a) = \overline{0}\} = \{a \in \mathbb{Z}; a \cdot \overline{1} = \overline{0}\} = \{a \in \mathbb{Z}; \overline{a} = \overline{0}\} = m\mathbb{Z}$.

Proposição 1.8. Seja $f : A \longrightarrow B$ um homomorfismo. São equivalentes:

(i) f é monomorfismo

(ii) $N(f) = \{0\}$.

Demonstração.

• $(i) \Longrightarrow (ii)$

$$\begin{aligned} f(0) = 0 &\Longrightarrow 0 \in N(f) \\ &\Longrightarrow \{0\} \subseteq N(f). \end{aligned}$$

$$\begin{aligned} x \in N(f) &\Longrightarrow f(x) = 0 = f(0) \\ &\Longrightarrow x = 0, \end{aligned}$$

por f ser monomorfismo. Ficamos com $x \in \{0\}$, ou seja, $N(f) \subseteq \{0\}$.

Logo, $N(f) = \{0\}$.

• $(ii) \Longrightarrow (i)$ Suponhamos $f(x) = f(y)$. Então:

$$\begin{aligned} f(x) = f(y) &\Longrightarrow f(x) - f(y) = 0 \\ &\Longrightarrow f(x - y) = 0 \\ &\Longrightarrow x - y = 0 \\ &\Longrightarrow x = y. \end{aligned}$$

Logo, f é monomorfismo.

■

Observação 1.9. Note que o Exemplo 1.15 pode ser feito utilizando a proposição acima, ou seja, mostrando que o $N(f) = \{0\}$.

$N(f) = \{m \in \mathbb{Z}; f(m) = (m, 0) = (0, 0)\} = \{0\}$.

Definição 1.18. Se f é um homomorfismo de A em A' e se f é uma função sobrejetora, diremos que f é um **epimorfismo** de A em A' ou que f é um homomorfismo sobrejetor de A em A'.

Exemplo 1.18. $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(x, y) = x$, $\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}$, é um homomorfismo sobrejetor uma vez que

$f((x, y) + (x', y')) = f(x + x', y + y') = x + x' = f(x, y) + f(x', y')$,

$f((x, y) \cdot (x', y')) = f(x \cdot x', y \cdot y') = x \cdot x' = f(x, y) \cdot f(x', y')$.

Dado $x \in \mathbb{Z}$, tome $(x, 0) \in \mathbb{Z} \times \mathbb{Z}$, então $f(x, 0) = x$.

Logo, f é um homomorfismo sobrejetor.

Definição 1.19. Se f é um homomorfismo de A em A' e se f é uma função bijetora, diremos que f é um **isomorfismo** de A em A' ou que f é um homomorfismo bijetor de A em A'.

Observação 1.10. Um homomorfismo de A em A também é denominado *endomorfismo* de A. Um isomorfismo de A em A é chamado *automorfismo* de A.

A existência de um isomorfismo entre dois anéis implica que os dois anéis, mesmo que tenham elementos distintos e que as operações neles definidas também sejam diferentes, algebricamente têm a mesma estrutura. Por esta razão, a existência de um isomorfismo entre dois anéis é utilizada para definir igualdade de anéis: dois anéis são iguais quando eles são isomorfos.

Baseados no Exemplo 1.16 e no Exemplo 1.17 daremos a seguinte definição.

Definição 1.20. Chama-se **característica** de um anel comutativo A, com elemento unidade $1_A \neq 0$, ao único número natural m tal que $m\mathbb{Z}$ seja o núcleo do homomorfismo $f : \mathbb{Z} \longrightarrow A$ definido por $f(n) = 1_A \cdot n$.

Dessa forma, o anel A tem característica zero se, e somente se , 0 é o único número inteiro tal que $1_A \cdot n = 0$. Por outo lado, o anel A tem característica $m > 0$ se, e somente se, m é o menor número natural não nulo tal que $1_A \cdot m = 0$.

Observação 1.11. O Exemplo 1.16 e o Exemplo 1.17 nos mostram, respectivamente, que o anel $\mathbb{Z}$ dos números inteiros tem característica zero e o anel $\mathbb{Z}_m$ ($m > 1$), dos inteiros módulo m, tem característica m.

Definição 1.21. Seja A um anel comutativo com elemento unidade $1_A \neq 0$ e suponhamos que esteja definida uma ordem total $\leq$ sobre o conjunto A. Diz-se que esta ordem é compatível com a estrutura de anel definida sobre o conjunto A ou, simplesmente, que A é um **anel ordenado** pela ordem $\leq$ se, e somente se, são válidos os seguintes axiomas

(OA) $\forall\, a, b, c \in A,$ se $a \leq b,$ então $a + c \leq b + c$.

(OM) $\forall\, a, b, c \in A,$ se $a \leq b$ e $0 \leq c$ então $ac \leq bc$.

Se A é anel comutativo com elemento unidade e se estiver fixada, sobre o conjunto A, uma ordem total $\leq$ que satisfaz os axiomas (OA) e (OM) diremos, simplesmente, que A, é um anel ordenado suprimindo-se, portanto, a referência à ordem total fixada sobre o conjunto A e ao fato que esta ordem satisfaz os axiomas (OA) e (OM).

Observação 1.12. Apesar de haver a restrição $0 \leq c$ no axioma (OM), costuma-se dizer que a ordem $\leq$ é compatível com a multiplicação.

Observação 1.13. Se A é um anel ordenado pela ordem $\leq$, então é imediato que $(A, +, \leq)$ é um grupo abeliano ordenado, portanto, num anel ordenado valem as propriedades enunciadas na secção 1.1 relativas à adição.

Definição 1.22. Seja A um anel comutativo com unidade $1_A \neq 0$. Dizemos que A é **ordenável**, quando existe uma relação de ordem total $\leq$ em A, que satisfaz os axiomas (OA) e (OM).

Teorema 1.5. *Todo anel comutativo ordenado tem característica zero.*

Demonstração. Seja A um anel ordenado. Considere o homomorfismo $f : \mathbb{Z} \longrightarrow A$, tal que $f(n) = 1_A \cdot n$.

$n \in N(f) \iff n \cdot 1_A = 0$.

Como $(A, +, \leq)$ é grupo abeliano totalmente ordenado e $1_A \in A$ usamos o Corolário 1.3 para concluir que $n = 0$. Portanto,

$$\begin{aligned} n \in N(f) &\iff n \cdot 1_A = 0 \\ &\iff n = 0. \end{aligned}$$

Segue que A tem característica zero.

■

Definição 1.23. Sejam A um anel com unidade e $a \in A$. Definimos:

$a^0 = 1_A$

$a^n = a \cdot ... \cdot a$, n vezes quando $n \in \mathbb{N}^*$.

Veremos a seguir algumas propriedades da ordem, relativas aos produtos, e só consideraremos o caso em que o anel ordenado não admita divisores próprios do zero. Portanto, daqui por diante só consideraremos anéis de integridade ordenados.

Teorema 1.6. *Num anel de integridade ordenado A valem as seguintes propriedades:*

(1) Regra dos sinais:

- *(a) se $0 < a$ e se $0 < b$, então, $0 < ab$.*
- *(b) se $a < 0$ e $b < 0$, então $0 < ab$.*
- *(c) se $a < 0$ e $b > 0$, então, $ab < 0$.*
- *(d) se $0 < ab$, então $0 < a$ e $0 < b$ ou $a < 0$ e $b < 0$.*
- *(e) se $ab < 0$, então $0 < a$ e $b < 0$ ou $a < 0$ e $0 < b$.*

(2) $0 \leq a^2$ para todo a em A e $0 < a^2$ para todo $a \neq 0$; em particular, o elemento unidade de A é estritamente positivo.

(3) Se a é inversível, então a e a^{-1} são ambos estritamente positivos ou estritamente negativos.

(4) $|ab| = |a| \cdot |b|$.

Demonstração.

(1) (a) $0 < a \Longrightarrow 0 \leq a$ e $a \neq 0$.
$0 < b \Longrightarrow 0 \leq b$ e $b \neq 0$.

Por (OM) temos:

$0 \cdot b \leq a \cdot b \Longrightarrow 0 \leq ab$.

Note que não podemos ter $ab = 0$ já que $a, b \neq 0$ e A é anel de integridade (sem divisores de zero).
Logo, $0 < ab$.

(b) Pelo Lema 1.2 temos:
$a < 0 \Longrightarrow -a > 0$ e
$b < 0 \Longrightarrow -b > 0$.

Por (a) temos:

$(-a) \cdot (-b) > 0 \Longrightarrow ab > 0$.

(c) De $a < 0$ temos $-a > 0$. Então por (a),

$$\begin{aligned}(-a) \cdot b > 0 &\Longrightarrow -ab > 0 \\ &\Longrightarrow ab < 0.\end{aligned}$$

(d) Se $0 < a$, podemos dizer que $0 \leq a$.
Suponha, por absurdo, que $b \leq 0$, então por (OM),

$a.b \leq a.0 = 0$,

contradição. Outro caso é análogo.

(e) Se $0 < a$, podemos dizer que $0 \leq a$.
Suponha, por absurdo, que $0 \leq b$, então por (OM),

$0.b \leq a.b \Longrightarrow 0 \leq a.b$,

contradição! O caso $a < 0$ é análogo.

(2) $0 \leq a^2, \forall\, a \in A$.

$a > 0 \Longrightarrow a.a = a^2 > 0$, por $(1)(a)$.
$a < 0 \Longrightarrow a.a = a^2 > 0$, por $(1)(b)$.
$a = 0 \Longrightarrow a.a = 0.0 = 0$.

De qualquer forma, temos $a^2 \geq 0$. Além disso, fica claro que se $a \neq 0$, então $a^2 > 0$.

Como $1_A \neq 0$ temos, em particular, que $1_A = 1_A \cdot 1_A = (1_A)^2 > 0$.

(3) a é inversível $\Longrightarrow (a > 0$ e $a^{-1} > 0)$ ou $(a < 0$ e $a^{-1} < 0)$.

Se $a > 0$ temos $a.a^{-1} = 1_A > 0$ por (2). Então por $(1)(d)$, $a^{-1} > 0$.
Se $a < 0$ temos $a.a^{-1} = 1_A > 0$ por (2). Então por $(1)(d)$, $a^{-1} < 0$.

(4) $|ab| = |a|.|b|$

• $a \geq 0$ e $b \geq 0$

Por $(1)(a)$ temos $ab \geq 0$. Então $|ab| = ab$.
De $a \geq 0$ temos $|a| = a$. Da mesma forma $|b| = b$.
Então ficamos com $|ab| = a.b = |a|.|b|$.

• $a < 0$ e $b < 0$

Por $(1)(b)$ temos $ab \geq 0$. Então $|ab| = a.b$.
De $a < 0$ temos $|a| = -a$. Da mesma forma $|b| = -b$.
Então ficamos com $|ab| = a.b = (-a).(-b) = |a|.|b|$.

• $a \geq 0$ e $b < 0$

Por $(1)(c)$ temos $ab \leq 0$. Então $|ab| = -a.b$.
De $a \geq 0$ temos $|a| = a$. De $b < 0$ temos $|b| = -b$.
Então ficamos com $|ab| = -a.b = a.(-b) = |a|.|b|$.

• $a < 0$ e $b \geq 0$

Análogo ao caso anterior.

■

Proposição 1.9. Num anel de integridade ordenado A valem as seguintes propriedades:

(i) se $0 < a$, então $0 < a^n$ para todo número natural n.

(ii) se $a < 0$, então $0 < a^{2n}$ e $a^{2n+1} < 0$ para todo número natural n.

Demonstração.

(i) Temos que provar que se $0 < a$, então $0 < a^n$.

Por indução sobre n.

• Para $n = 0$ temos $a^0 = 1_A$, por definição. Como $1_A > 0$, pelo Teorema 1.6, temos que $a^0 > 0$.

• Hipótese de indução: para k fixo, $k > 0$ temos $0 < a^k$.

• Tese de indução: $0 < a^{k+1}$.

$a^{k+1} = a^k.a > 0$.

(ii) Pelo Teorema 1.6 (2) temos que $a^2 > 0$, pois $a \neq 0$.

Segue de (i) que $(a^2)^n > 0$, isto é, $a^{2n} > 0$.

Como $a^{2n} > 0$ e $a < 0$, aplicamos a Regra dos Sinais para concluir que $a^{2n+1} = a^{2n} \cdot a < 0$.

■

Notação: Sejam A um anel e P um subconjunto de A. Usaremos a notação:

$$PP = \{ab \in A; a, b \in P\}.$$

Teorema 1.7. *Se A é um anel de integridade ordenado e se P é o conjunto dos elementos positivos de A, então temos:*

(I) $P + P \subset P$.

(II) $P \bigcap (-P) = \{0\}$.

(III) $P \bigcup (-P) = A$.

(IV) $PP \subset P$.

Além disso, se A é um anel de integridade e se P é uma parte do conjunto A que satisfaz as condições (I), (II), (III) e (IV), então existe uma única ordem total $\leq$, sobre A, compatível com a adição e a multiplicação, tal que P seja o conjunto de todos os elementos positivos pela ordem $\leq$.

Demonstração.
(I), (II) e (III)

Como A é ordenado temos que $(A, +, \leq)$ é grupo abeliano totalmente ordenado.

Além disso, P é o conjunto dos elementos positivos de $(A, +, \leq)$.

Segue do Teorema 1.1 que P satisfaz as condições (I), (II) e (III).

(IV) $PP \subset P$

Sejam $a, b \in P$. Então $0 \geq a$ e $0 \geq b$. Por (OM) temos:

$0.b \leq a.b \Longrightarrow 0 \leq a.b$.

Seja A um anel de integridade e suponhamos que exista uma parte P, do conjunto A, que satisfaça as condições (I), (II), (III) e (IV).

Pelo Teorema 1.1, aplicado ao grupo $(A, +, \leq)$, existe uma única ordem $\leq$, compatível com a adição, tal que P seja o conjunto dos elementos positivos por esta ordem.

Pela Definição 1.22 basta verificar (OM). Mas o axioma (OM) é de verificação imediata por (IV).

■

Corolário 1.8. *Um anel de integridade A é ordenável se, e somente se existe uma parte P, de A, satisfazendo as condições (I), (II), (III) e (IV).*

Demonstração. É imediato do teorema anterior.

■

Teorema 1.8. *A ordem habitual dos números inteiros é a única ordem total compatível com a estrutura de anel definida sobre $\mathbb{Z}$.*

Demonstração. O subconjunto $P = \mathbb{N}$ do anel $\mathbb{Z}$ dos números inteiros satisfaz as condições (I), (II), (III) e (IV) do Teorema 1.7, logo, $\mathbb{Z}$ é um anel ordenável. Note que esta ordem é a ordem usual dos números inteiros:

$$a \leq b \Longleftrightarrow b - a \in \mathbb{N}.$$

Sejam R uma ordem total definida sobre $\mathbb{Z}$ compatível com a adição e a multiplicação e, P o conjunto dos elementos positivos pela ordem R, isto é:

$$P = \{a \in \mathbb{Z}; 0Ra\}.$$

Vamos provar que $P = \mathbb{N}$.

Por indução temos:

• $1 \in P$, pelo Teorema 1.6.

• Suponha k fixo, $k > 1$ tal que $k \in P$ então $0Rk$.

• Gostaria de provar que $k+1 \in P$.

$k \in P$ e $1 \in P \Longrightarrow 0Rk$ e $0R1$
$\Longrightarrow (0+1)R(k+1)$
$\Longrightarrow 1R(k+1)$
$\Longrightarrow k+1 \in P$.

Portanto $n \in P$, para todo n natural não nulo.

Note que $0 \in P$, logo, $\mathbb{N} \subset P$. Falta provar que $P \subset \mathbb{N}$. Suponha por absurdo, que isso não ocorra, então existe $b \in P$ tal que

$b \notin \mathbb{N} \Longrightarrow b \in (-\mathbb{N})$

pois $\mathbb{Z} = \mathbb{N} \bigcup -\mathbb{N}$. Temos então $b = -a$, $a \in \mathbb{N}$.

$b = -a \Longrightarrow b \in -P$.

Mas então $b \in P \bigcap (-P) = \{0\}$, de onde vem que $b = 0$.

Chegamos dessa forma a uma contradição, pois $0 \in \mathbb{N}$. Logo a ordem R coincide com a ordem habitual dos números inteiros.

■

Definição 1.24. Sejam $(A, +, \cdot)$ um anel e $A' \subseteq A$, $A' \neq \{\}$. Dizemos que A' é **subanel** de A quando A' é um anel com as operações de A, isto é:

(i) $x, y \in A' \Longrightarrow x + y \in A'$ e $x \cdot y \in A'$.

(ii) $(A', +, \cdot)$ é anel.

Definição 1.25. Seja A' um subanel de A. Se $1_A \in A'$, dizemos que A' é **subanel unitário** de A.

Proposição 1.10. Sejam A um anel e A' um subconjunto de A. Temos que A' é um subanel unitário de A se, e somente se, as seguintes condições são satisfeitas:

(i) $1 \in A'$.

(ii) quaisquer que sejam $a, b \in A'$, temos que $a - b \in A'$ e $a \cdot b \in A'$.

Demonstração.
($\Longrightarrow$) É imediato da definição.

($\Longleftarrow$) Como $1 \in A'$, segue que

$0 = 1 - 1 \in A'$.

Se $a \in A'$, então $-a = 0 - a \in A'$.

Sejam agora a e b elementos de A', logo $-b \in A'$ e conseqüentemente

$a + b = a - (-b) \in A'$.

Como $a \cdot b \in A'$ e as demais propriedades que definem um anel são verificadas em A' pois o são em A, temos que A' é um subanel de A.

■

Teorema 1.9. *Seja A um anel comutativo com elemento unidade $1_A \neq 0$. Então o conjunto de todos os múltiplos inteiros de 1_A*

$$1_A \cdot \mathbb{Z} = \{m \cdot 1_A; m \in \mathbb{Z}\}$$

é o menor subanel unitário de A.

Demonstração. Seja A um anel comutativo com elemento unidade $1_A \neq 0$.

Claro que $1_A \in 1_A \cdot \mathbb{Z}$.

Sejam $m \cdot 1_A$, $n \cdot 1_A \in 1_A \cdot \mathbb{Z}$.

Como

$$m \cdot 1_A - n \cdot 1_A = (m - n) \cdot 1_A \in 1_A \cdot \mathbb{Z}$$

e

$$m \cdot 1_A \cdot n \cdot 1_A = (mn) \cdot 1_A \in 1_A \in 1_A \cdot \mathbb{Z}$$

segue da Proposição 1.10 que $1_A \cdot \mathbb{Z}$ é subanel unitário de A. Falta provar que é o menor.

Seja A' um subanel unitário de A. Logo, $1_A \in A'$.

Dado $m \in \mathbb{Z}$, temos:

• se $m = 0$ então $m \cdot 1_A = 0 \in A'$.

• se $m > 0$ então $m \cdot 1_A = 1_A + ... + 1_A \in A'$.

• se $m < 0$ então $m \cdot 1_A = -(1_A + ... + 1_A) \in A'$.

Portanto, $m \cdot 1_A \subseteq A'$.

■

Teorema 1.10. *Se A é um anel comutativo com elemento unidade $1_A \neq 0$ e se A tem característica zero, então o menor subanel unitário de A é isomorfo ao anel $\mathbb{Z}$ dos números inteiros.*

Demonstração. Consideremos a função $f : \mathbb{Z} \longrightarrow 1_A \cdot \mathbb{Z}$, definida por $f(n) = 1_A \cdot n$.

• Para f ser homomorfismo devemos ter:

(1) $f(a+b) = f(a) + f(b)$.

(2) $f(ab) = f(a).f(b)$.

Sejam m, $n \in \mathbb{Z}$:

(1) $f(m+n) = 1_A \cdot (m+n) = 1_A \cdot m + 1_A \cdot n = f(m) + f(n)$.

(2) $f(m.n) = 1_A \cdot (mn) = (m1_A).(n1_A) = f(m) \cdot f(n)$.

• Para f ser epimorfismo devemos ter f sobrejetora, ou seja, $Im(f) = 1_A \cdot \mathbb{Z}$.

$Im(f) = \{f(x); x \in \mathbb{Z}\} = \{1_A \cdot x; x \in \mathbb{Z}\} = 1_A \cdot \mathbb{Z}$.

• Para f ser monomorfismo devemos ter f injetora. Pela Proposição 1.8 devemos ter $N(f) = \{0\}$. Como A tem característica zero,

$N(f) = \{x \in \mathbb{Z}; f(x) = 0\} = \{x \in \mathbb{Z}; 1_A \cdot x = 0\} = \{0\}$,

logo, f é injetora.

■

Definição 1.26. Sejam $(A, +, \cdot, \leq)$ e $(A', +, \cdot, \leq)$ dois anéis de integridade ordenados e f uma função do conjunto A no conjunto A'. Diz-se que f é um **isomorfismo ordenado** de A em A' se, e somente se, f satisfaz as seguintes condições:

(1) f é um isomorfismo do anel A no anel A'.

(2) quaisquer que sejam a e b em A, tem-se $a \leq b$ se, e somente se, $f(a) \leq f(b)$.

Teorema 1.11. *O menor subanel unitário $1_A \cdot \mathbb{Z}$, de um anel de integridade ordenado A, é ordenadamente isomorfo ao anel $\mathbb{Z}$ dos números inteiros.*

Demonstração. Pelo Teorema 1.5, o anel de integridade ordenado tem característica zero. Então, pelo Teorema 1.9, temos que $1_A \cdot \mathbb{Z}$ é o menor subanel unitário de A. Aplicando agora o Teorema 1.10, temos que $1_A \cdot \mathbb{Z}$ é isomorfo ao anel $\mathbb{Z}$ dos números inteiros.

O isomorfismo é $f : \mathbb{Z} \longrightarrow 1_A \cdot \mathbb{Z}$, $f(n) = 1_A \cdot n$.

Basta provar que $1_A \cdot \mathbb{Z}$ é ordenadamente isomorfo ao anel $\mathbb{Z}$. Então pela Definição 1.26 devemos ter para quaisquer m e n em $\mathbb{Z}$, $m \leq n$ se, e somente se, $f(m) \leq f(n)$.

($\Longrightarrow$) Sejam $m, n \in \mathbb{Z}$ tais que $m \leq n$.

Como $n - m \geq 0$, temos por definição que $(n-m) \cdot 1_A \geq 0$. Assim:

$0 \leq (n-m) \cdot 1_A = n \cdot 1_A - m \cdot 1_A \Longrightarrow m \cdot 1_A \leq n \cdot 1_A \Longrightarrow f(m) \leq f(n)$.

($\Longleftarrow$) Seja agora $m, n \in \mathbb{Z}$ tais que $f(m) \leq f(n)$.

Então $m \cdot 1_A \leq n \cdot 1_A$, isto é, $(m-n) \cdot 1_A \leq 0$.

Suponha, por absurdo, que $m - n > 0$.

Segue da definição de múltiplo em A que

$(m-n) \cdot 1_A = 1_A + ... + 1_A > 0$. Absurdo!

Logo, $m - n \leq 0$, e portanto $m \leq n$.

■

Nesta última secção trabalharemos com um tipo particular de estrututa algébrica, os corpos. É importante frisar que os corpos são anéis de integridade onde todo elemento não nulo é inversível.

1.3 Corpos Ordenados

Definição 1.27. Um anel $(A, +, \cdot)$ é um **corpo** quando é anel comutativo, com unidade e satisfaz:

(M_7) $a \in A, a \neq 0 \Longrightarrow \exists\, a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1_A$.

Proposição 1.11. Em um corpo o elemento inverso é único.

Demonstração. De fato, se a' e a'' são dois inversos de a, então temos que:

$a' = a' \cdot 1 = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = 1 \cdot a'' = a''$.

■

Exemplo 1.19. São corpos: $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

Exemplo 1.20. $\mathbb{Z}$ não é corpo pois somente 1 e -1 são inversíveis em $\mathbb{Z}$.

Definição 1.28. Seja K um corpo e suponhamos que esteja definida uma ordem total $\leq$ sobre o conjunto K. Diz-se que esta ordem é compatível com a estrutura de corpo definida sobre o conjunto K, ou que K é um **corpo ordenado** pela ordem $\leq$ se, e somente se, estão satisfeitas os axiomas (OA) e (OM) da Definição 1.21.

Se K é um corpo e se estiver fixada, sobre o conjunto K, uma ordem total $\leq$ que satisfaz os axiomas (OA)e (OM) diremos, simplesmente que K é um corpo ordenado suprimindo-se portanto, a referência à ordem total fixada sobre o conjunto K e ao fato que esta ordem satisfaz os axiomas (OA) e (OM). Diremos que um corpo K é **ordenável** se, e somente se , existe uma ordem total, sobre o conjunto K, que satisfaz os axiomas (OA) e (OM).

Conforme a definição acima, se $(K, +, \cdot, \leq)$ é um corpo ordenado, então $(K, +, \cdot, \leq)$ é um anel de integridade ordenado. Portanto, são verdadeiras em K as propriedades estabelecidas na secção anterior para os anéis de integridade ordenados. Completaremos o Teorema 1.6 acrescentando algumas propriedades que derivam do fato que todo elemento não nulo de K é inversível.

Teorema 1.12. *Num corpo ordenado K valem as seguintes propriedades:*

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

(2) Se $0 < a < 1_K$, então $1_K < a^{-1}$ e se $1_K < a$, então $0 < a^{-1} < 1_K$, onde 1_K indica o elemento unidade de K.

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

(4) $|a^{-1}| = |a|^{-1}$, para todo $a \neq 0$.

(5) $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$, quaisquer que sejam a e b em K, com $b \neq 0$.

Demonstração.

(1) $a \cdot a^{-1} = 1_K > 0$

- Se $a > 0$ então pela regra dos sinais, como $1_K > 0$ devemos ter $a^{-1} > 0$.
- Se $a < 0$ então pela regra dos sinais, como $1_K > 0$ devemos ter $a^{-1} < 0$.

(2) • Se $0 < a < 1_K$ então $1_K < a^{-1}$

Como $a > 0$ temos $a^{-1} > 0$, por (1).

Por (OM) temos $a \cdot a^{-1} < 1_K \cdot a^{-1}$. Portanto $1_K < a^{-1}$.

• Se $1_K < a$ então $0 < a^{-1} < 1_K$

Como $1_K > 0$ temos, por transitividade, $a > 0$.

$a > 0 \Longrightarrow a^{-1} > 0$, por (1).

Por (OM) temos: $1_K \cdot a^{-1} < a \cdot a^{-1} \Longrightarrow a^{-1} < 1_K$

$\Longrightarrow 0 < a^{-1} < 1_K$.

(3) • Se $0 < a < b$ então $0 < b^{-1} < a^{-1}$

Por (1) temos:

$0 < a \Longrightarrow 0 < a^{-1}$ e
$0 < b \Longrightarrow 0 < b^{-1}$.

Por (OM) ficamos com:

$$\begin{aligned} 0 < a < b &\Longrightarrow 0 \cdot b^{-1} < a \cdot b^{-1} < b \cdot b^{-1} \\ &\Longrightarrow 0 < a \cdot b^{-1} < 1_K \\ &\Longrightarrow 0 < a^{-1} \cdot a \cdot b^{-1} < a^{-1} \cdot 1_K \\ &\Longrightarrow 0 < 1_K \cdot b^{-1} < a^{-1} \\ &\Longrightarrow 0 < b^{-1} < a^{-1}. \end{aligned}$$

• Se $a < b < 0$ então $b^{-1} < a^{-1} < 0$

Por (1) temos:

$a < 0 \Longrightarrow a^{-1} < 0$ e
$b < 0 \Longrightarrow b^{-1} < 0$.

Pelo Lema 1.2 temos:

$a^{-1} < 0 \Longrightarrow 0 < -a^{-1}$ e
$b^{-1} < 0 \Longrightarrow 0 < -b^{-1}$.

Por (OM) ficamos com:

$$\begin{aligned} a < b < 0 &\Longrightarrow -a \cdot b^{-1} < -b \cdot b^{-1} < 0 \\ &\Longrightarrow -a \cdot b^{-1} < -1_K < 0 \\ &\Longrightarrow a^{-1} \cdot a \cdot b^{-1} < a^{-1} \cdot 1_K < 0 \\ &\Longrightarrow b^{-1} < a^{-1} < 0. \end{aligned}$$

(4) $|a^{-1}| = |a|^{-1}$

$$\begin{aligned} 1_K &= a \cdot a^{-1} \\ |1_K| &= |a \cdot a^{-1}| \\ 1_K &= |a| \cdot |a^{-1}|, \end{aligned}$$

pelo Teorema $1.6\ (4)$.

Segue que o inverso de $|a|$ é $|a^{-1}|$, isto é, $|a|^{-1} = |a^{-1}|$.

(5) $\left|\dfrac{a}{b}\right| = \dfrac{|a|}{|b|}$

$$\left|\frac{a}{b}\right| = |a \cdot b^{-1}|$$
$$= |a| \cdot |b^{-1}| \text{ (pelo Teorema } 1.6\ (4))$$
$$= |a| \cdot |b|^{-1} \text{ (pelo item anterior)}$$
$$= \frac{|a|}{|b|}$$

■

Definição 1.29. Diz-se que um conjunto não vazio K, totalmente ordenado pela ordem $\leq$, é **denso** se, e somente se, quaisquer que sejam a e b em K, com $a < b$, existe $c \in K$ tal que $a < c < b$. Um subconjunto K_0, de K, é **totalmente denso** em K (ou, simplesmente, é denso em K) se, e somente se, quaisquer que sejam a e b em K, com $a < b$, existe c_0 em K_0 tal que $a < c_0 < b$.

Teorema 1.13. *Se K é um corpo ordenado pela ordem $\leq$, então o conjunto K é denso pela mesma ordem.*

Demonstração. Mostraremos que se a e b são dois elementos quaisquer de K e se $a < b$ então $\exists\, c \in K$ tal que $a < c < b$, onde

$$c = (2 \cdot 1_K)^{-1} \cdot (a + b)$$

Notemos inicialmente que 1_K e $2 \cdot 1_K$ são estritamente positivos, pelo Teorema 1.6. Novamente pelo Teorema 1.6 temos que $(2 \cdot 1_K)^{-1}$ é estritamente positivo.

De $a < b$ resulta por (OA) que:

$$a + a < a + b \Longrightarrow (2 \cdot 1_K)a < a + b.$$

De $a < b$ também obtemos:

$$a + b < b + b \Longrightarrow a + b < (2 \cdot 1_K)b.$$

Multiplicando as desigualdades por $(2 \cdot 1_K)^{-1}$ e usando (OM), vem que:

$$a < (2 \cdot 1_K)^{-1} \cdot (a + b)$$

e

$$(2 \cdot 1_K)^{-1} \cdot (a + b) < b.$$

Portanto $a < (2 \cdot 1_K)^{-1} \cdot (a + b) < b$.

■

Corolário 1.9. *O conjunto P^* dos elementos estritamente positivos de um corpo ordenado K não tem mínimo.*

Demonstração. Suponha que $b \in P^*$ é mínimo para P^*. Então $b \in K$ e $b > 0$.
Tome $a = 0 \in K$.
Pelo teorema anterior, existe $c \in K$ tal que $a < c < b$.
Segue que $c \in K$ e $c > 0$. Assim $c \in P^*$. Isso contradiz a minimalidade de b.
Portanto P^* não tem mínimo.

■

Definição 1.30. Diz-se que um corpo ordenado $(K, +, \cdot, \leq)$ é **arquimediano** se, e somente se, o grupo ordenado $(K, +, \leq)$ é arquimediano.

Para verificar que um dado corpo ordenado K é arquimediano, basta comparar os elementos estritamente positivos de K com elemento unidade 1_K, conforme o teorema seguinte.

Teorema 1.14. *Um corpo ordenado K é arquimediano se, e somente se, para todo elemento estritamente positivo a de K, existe um número natural n tal que $a < n \cdot 1_k$.*

Demonstração.

($\Longrightarrow$) Se o corpo K é arquimediano então de acordo com a Definição 1.8,

quaisquer que sejam a e b em K, se $0 < a$ e $0 < b$ então $\exists\, n \in \mathbb{N}$ tal que $b < na$.

Sejam a, $1_K \in K$, $0 < a$.

Pelo Teorema 1.6 temos $0 < 1_K$.

Como K é arquimediano existe $n \in \mathbb{N}$ tal que $a < n \cdot 1_K$.

($\Longleftarrow$) Suponha agora que seja válida a seguinte condição:

$$\forall\, a \in K, a > 0, \exists\, n \in \mathbb{N} \text{ tal que } a < n \cdot 1_K. \ (*)$$

Vamos provar que K é arquimediano.

Consideremos dois elementos quaisquer de K, a e b, tais que $0 < a < b$.

Temos dois casos, $1_K \leq a$ ou $a < 1_K$.

(i) $1_K \leq a$

Como $b \in K$ e $b > 0$, segue de $(*)$ que existe $n \in \mathbb{N}$ tal que $b < n \cdot 1_K$.

Temos também pelo Corolário 1.4 que

$$n \cdot 1_K \leq n \cdot a \Longrightarrow b < n \cdot 1_k \leq n \cdot a$$
$$\Longrightarrow b < n \cdot a.$$

(ii) Pelo Teorema 1.12 temos

$a < 1_K \Longrightarrow 1_K < a^{-1}$.

Por hipótese existe $n \in \mathbb{N}$ tal que $a^{-1} < n \cdot 1_K$.

Por (OM),

$a \cdot a^{-1} < n \cdot a \Longrightarrow 1_K < n \cdot a$.

Portanto, de acordo com o caso anterior, existe $p \in \mathbb{N}$ tal que

$b < p \cdot (na) = (pn) \cdot a$.

■

Corolário 1.10. *Se a é um elemento estritamente positivo de um corpo arquimediano K , então existe um número natural não nulo n tal que $(n \cdot 1_K)^{-1} < a$.*

Demonstração. Pelo Teorema 1.6, se $0 < a$ então $0 < a^{-1}$.

Pelo Teorema anterior, $\exists n \in \mathbb{N}^*$ tal que $a^{-1} < n \cdot 1_K$.

Note que:

• pela Regra dos Sinais, como $n > 0$ e $1_K > 0 \Longrightarrow n \cdot 1_K > 0$;

• e pelo Teorema 1.6, $(n \cdot 1_K)^{-1} > 0$.

Por (OM) temos

$$(n \cdot 1_K)^{-1} \cdot a^{-1} < (n \cdot 1_K)^{-1} \cdot (n \cdot 1_K) = 1_K \Longrightarrow (n \cdot 1_K)^{-1} \cdot a^{-1} \cdot a < 1_K \cdot a$$
$$\Longrightarrow (n \cdot 1_K)^{-1} < a.$$

■

Definição 1.31. Sejam K um corpo e $B \subseteq K$. Se B é um corpo com as operações de K , dizemos que B é um **subcorpo** de K. $B \subseteq K$ é subcorpo de K quando:

(1) B é subanel de K.

(2) B tem unidade.

(3) $b \in B, b \neq 0 \Longrightarrow b^{-1} \in B$.

Definição 1.32. Todo corpo que admite um único subcorpo é denominado **corpo primo**.

Teorema 1.15. *O corpo primo K_0, de um corpo ordenado arquimediano K, é totalmente denso em K.*

Demonstração. Sejam a e b dois elementos quaisquer de K e suponhamos que $a < b$.

Precisamos mostrar que $\exists x \in K_0$ tal que $a < x < b$. Para isso distinguiremos quatro casos.

(i) $a = 0$.

Conforme o Corolário 1.10 temos:

$\exists n \in \mathbb{N}^*$ tal que $a < (n \cdot 1_k)^{-1} < b$.

Basta escolher $x = (n \cdot 1_k)^{-1}$.

(ii) $0 < a < b$.

$a < b \Longrightarrow b - a > 0$. Em virtude do Corolário 1.10

$\exists n \in \mathbb{N}^*$ tal que $(n \cdot 1_K)^{-1} < b - a$.

Como K é arquimediano, existe de acordo com o Teorema 1.3, um único número natural não nulo m tal que

$(m-1)(n \cdot 1_K)^{-1} \leq a < m(n \cdot 1_K)^{-1}$.

Portanto,

$$\begin{aligned} a < m(n \cdot 1_K)^{-1} &= (m \cdot 1_K) \cdot (n \cdot 1_K)^{-1} \\ &= [(m-1) \cdot 1_K + 1_K] \cdot (n \cdot 1_K)^{-1} \\ &= (m-1) \cdot (n \cdot 1_K)^{-1} + (n \cdot 1_K)^{-1} < a + (b-a) = b. \end{aligned}$$

Basta escolher $x = (m \cdot 1_k) \cdot (n \cdot 1_K)^{-1}$.

(iii) $a < 0 < b$.

Neste caso, tome $x = 0$.

(iv) $a < b < 0$.

Temos $0 < -b < -a$, logo de acordo com (ii) , existe $x \in K_0$ tal que $-b < x < -a$, de onde vem, $a < -x < b$, com $-x \in K_0$.

■

Terminaremos esta secção estudando o problema do prolongamento da ordem definida sobre um anel de integridade ordenado ao seu corpo de frações.

Definição 1.33. Sejam A e A' dois conjuntos tais que $A \subset A'$ e sejam R e R' relações de ordem definidas, respectivamente sobre A e A'. Diz-se que R' é um **prolongamento** de R se, e somente se, é válida a seguinte condição:

quaisquer que sejam a e b em A, tem-se aRb se, e somente se, $aR'b$.

Notemos que se R' e total, então R também é total.

Interessa-nos examinar a definição acima no caso em que A' seja um anel de integridade ordenado pela ordem R' e A seja um sub-anel unitário, de A', ordenado pela ordem R. Indicamos por P (respectivamente, P') o conjunto dos elementos de A (respectivamente, A') que são positivos pela ordem R (respectivamente, R'), isto é,

$$P = \{x \in A; 0Rx\} \text{ e } P' = \{x' \in A'; 0R'x'\}.$$

Com estas notações, demonstraremos o teorema seguinte.

Teorema 1.16. *A ordem R' é um prolongamento da ordem R se, e somente se, $P \subset P'$; neste caso, tem-se $P = P' \bigcap A$.*

Demonstração.

($\Longrightarrow$) Suponhamos que R' seja um prolongamento de R e seja x um elemnto qualquer de A.

$x \in P \Longrightarrow 0Rx \Longrightarrow 0R'x \Longrightarrow x \in P'$.

Portanto, $P \subset P'$.

($\Longleftarrow$) se $P \subset P'$ e se x e y são dois elementos quaisquer de A, temos

$xRy \Longleftrightarrow 0R(y-x) \Longleftrightarrow 0R'(y-x) \Longleftrightarrow xR'y$.

Portanto, R' é um prolongamento de R.

Falta provar que $P = P' \bigcap A$.

• $P \subset P' \bigcap A$

É imediato pois $P \subset P'$ e $P \subset A$.

• $P' \bigcap A \subset P$

Suponha que $P \neq P' \bigcap A$. Logo, existe $a \in P' \bigcap A$ tal que $a \notin P$.

De $A = P \bigcup (-P)$ e $a \notin P$ resulta $a = -b$ com $b \in P$. Logo, $a \in (-P')$ e como $a \in P'$ temos $a = 0$, contra o fato que $a \notin P$.

Portanto, $P = P' \bigcap A$.

■

O teorema acima nos mostra que o problema do prolongamento da ordem R, definida sobre A, a uma ordem total R' definida sobre A' e compatível com a estrutura de anel de A', resume-se em determinar um subconjunto P', de A', que satisfaça as condições (I), (II), (III), (IV) e $P \subset P'$.

Mostraremos agora que um domínio de integridade gera de maneira natural um corpo. Para isto, seja A um domínio de integridade e consideremos o conjunto

$$B = \{(a, b) \in AXA; b \neq 0\}.$$

Se definirmos em B a relação $(a, b) \sim (a', b')$ se, e somente se, $a \cdot b' = a' \cdot b$, teremos uma relação de equivalência.

Evidentemente, $a \cdot a = a \cdot a$, ou seja, $\sim$ é reflexiva.

Como $a' \cdot b = a \cdot b'$, temos que $\sim$ é simétrica.

Para verificar a transitividade, suponhamos que $(a, b) \sim (a', b')$ e $(a', b') \sim (a'', b'')$. Devemos provar que $(a, b) \sim (a'', b'')$.

$(a, b) \sim (a', b') \Longrightarrow a \cdot b' = a' \cdot b$.

$(a', b') \sim (a'', b'') \Longrightarrow a' \cdot b'' = a'' \cdot b'$.

Multiplicando a primeira igualdade por b'' e a segunda por b, obtemos:

$a \cdot b' \cdot b'' = a' \cdot b \cdot b''$ e $a' \cdot b'' \cdot b = a'' \cdot b' \cdot b \Longrightarrow a \cdot b' \cdot b'' = a'' \cdot b' \cdot b.$

$$\Longrightarrow b' \cdot (a \cdot b'' - a'' \cdot b) = 0.$$

Como $b' \neq 0$ e A é um domínio de integridade, $a \cdot b'' = a'' \cdot b$, provando que $(a, b) \sim (a'', b'')$.

A classe de equivalência de um elemento $(a, b) \in B$ será indicada por

$$\frac{a}{b} = \{(x, y) \in B; (x, y) \sim (a, b)\}$$

e o conjunto das classes de equivalência será indicado por K, ou seja,

$$K = \left\{\frac{a}{b}; a, b \in A \text{ e } b \neq 0\right\}.$$

Dessa forma, K será chamado corpo de frações do anel de integridade A.

Teorema 1.17. *Seja $(A, +, \cdot, \leq)$ um anel de integridade e seja K o corpo de frações do anel de integridade A. Nestas condições temos:*

(1) existe uma única ordem total R, sobre o conjunto K, que é prolongamento da ordem $\leq$ e que é compatível com a estrutura de corpo definida sobre K;

(2) o conjunto P' dos elementos positivos de K, pela ordem R, é formado por todas as frações $\frac{a}{b}$ (a e b em A e $b \neq 0$) tais que $0 \leq ab$.

Demonstração. Consideremos o subconjunto P' definido na parte (2) acima e vamos mostrar que P' satisfaz as condições (I), (II), (III), (IV) e $P \subset P'$, onde P indica o conjunto dos elementos positivos de A.

Notemos, inicialmente, que a condição imposta sobre a fração $\frac{a}{b}$ para que esta fração pertença a P' não depende da representação deste elemento, ou seja,

$$\text{se } \frac{a}{b} = \frac{c}{d} \text{ e se } 0 \leq ab, \text{ então temos } 0 \leq cd.$$

Isto é imediato, pois

$ad = bc \Longrightarrow (ab)(cd) = (bc)^2 \Longrightarrow 0 \leq (ab)(cd)$,

como $0 \leq ab$ teremos, conforme a Regra dos sinais, $0 \leq cd$. Esta observação nos permite representar dois elementos dados x e y de P' sob as formas

$$x = \frac{a}{c} \text{ e } y = \frac{b}{c}, \text{ com } a, b, c \text{ em } A \text{ e } c \neq 0. \ (***)$$

A partir de agora sejam x e y representados sob a forma $(***)$.

• (I) $P' + P' \subset P'$

Sejam x e y dois elementos quaisquer de P'.

Por hipótese temos $ac \in P$ e $bc \in P$, logo, $(a+b)c = ac + bc \in P + P \subset P$,

de onde resulta que o elemento $x + y = \frac{a+b}{c}$ pertence a P'.

• (II) $P' \bigcap (-P') = \{0\}$

Seja $x \in P' \bigcap (-P')$ um elemento qualquer. Temos

$x \in P' \Longrightarrow 0 \leq ac$

e

$-x \in P' \Longrightarrow 0 \leq -ac \Longrightarrow ac \leq 0$

Por (O_2), $a = 0$, de onde vem, $x = 0$.

• (III) $P' \bigcup (-P') = K$

Seja x um elemento qualquer de K.

$ac \in A = P \bigcup (-P) \Longrightarrow ac \in P$ ou $ac \in (-P)$.

$ac \in P \Longrightarrow x \in P'$

$ac \in (-P) \Longrightarrow -(ac) = (-a)c \in P \Longrightarrow -x \in P'$.

• (IV) $P'P' \subset P'$

Sejam x e y dois elementos quaisquer de P'. Por hipótese, temos

$ac \in P$ e $bc \in P \Longrightarrow (ac)(bc) = (ab)c^2 \in P$.

Portanto, $xy = \dfrac{ab}{c^2} \in P'$.

• $P \subset P'$

É imediato, pois, todo elemento a de P pode ser representado sob a forma $\dfrac{a}{1}$ e temos $a \cdot 1 = a \in P$, portanto, $a \in P'$.

Fica assim demonstrado que P' satisfaz as condições do Teorema 1.7; portanto, existe uma ordem total R, sobre o conjunto compatível com a estrutura de corpo definida sobre K, tal que $P' = \{x \in K; 0Rx\}$ e como $P \subset P'$ resulta que a ordem R é um prolongamento da ordem $\leq$. Falta, portanto, verificar que a ordem R que satisfaz estas condições é única.

Suponhamos, então, que R_1 seja uma ordem total sobre K satisfazendo as mesmas condições.

Seja $P_1 = \{x \in K; 0R_1x\}$ e notemos que $P_1 \bigcap A = P$. Se x é um elemento qualquer de P_1 representado sob a forma $(***)$, temos

$$\begin{aligned} c^2 \in P \subset P_1 &\Longrightarrow c^2x \in P_1P_1 \subset P_1 \\ &\Longrightarrow ac \in P_1 \bigcap A = P \\ &\Longrightarrow x = \frac{a}{c} \in P' \\ &\Longrightarrow P_1 \subset P'. \end{aligned}$$

Notando-se que $-P_1 \subset -P'$, teremos

$$\begin{aligned} P' &= P' \bigcap K \\ &= P' \bigcap [P_1 \bigcup (-P_1)] \\ &= P_1 \bigcup [P' \bigcap (-P_1)] \subset P_1 \bigcup [P' \bigcap (-P')] = P_1 \bigcup \{0\} = P_1, \end{aligned}$$

logo $P' \subset P_1$ e então $P' = P_1$, ou seja, a ordem R_1 coincide com a ordem R.

■

Teorema 1.18. *Existe uma única ordem total $\leq$, sobre o conjunto $\mathbb{Q}$ dos números racionais, compatível com sua estrutura de corpo; além disso, um número racional $\frac{a}{b}$ (a e b inteiros, $b \neq 0$) é positivo se, e somente se, ab é um número natural.*

Demonstração. De acordo com o teorema anterior, aplicado para o caso particular em que $A = \mathbb{Z}$ e $K = \mathbb{Q}$, concluímos que o corpo $\mathbb{Q}$ dos números racionais é ordenável; além disso, como $\mathbb{Z}$ admite uma única estrutura de anel ordenado (Teorema 1.10) resulta que o corpo $\mathbb{Q}$ só pode ser ordenado de um único modo.

O resultado que $\frac{a}{b}$ é positivo se, e somente se, ab é natural é conseqüência imediata da parte (2) do Teorema anterior.

■

A única ordem definida sobre $\mathbb{Q}$ é chamada ordem habitual dos números racionais e, conforme o Teorema 1.14, sabemos que o corpo $\mathbb{Q}$ é totalmente denso por esta ordem.

Teorema 1.19. *O corpo ordenado dos números racionais é arquimediano.*

Demonstração. Seja a um número racional estritamente positivo sob a forma $\frac{m}{n}$, onde m e n são números naturais não nulos. Note que:

$$\frac{m}{n} < m + 1,$$

pois m e n são números naturais. Logo, em virtude do Teorema 1.14, temos que $\mathbb{Q}$ é um corpo arquimediano.

■

Capítulo 2

Corpos Ordenados Completos

Neste capítulo apresentaremos algumas ferramentas de cálculo que serão utilizadas para a construção do corpo dos números reais.

Iniciaremos estudando o conceito de corpo ordenado completo.

2.1 Supremo e Ínfimo

Definição 2.1. Sejam $(K, \leq)$ conjunto ordenado e $A \subset K$ não vazio.
Dizemos que $x_0 \in A$ é **elemento mínimo** de A, se $x_0 \leq x$, para todo $x \in A$.

Definição 2.2. Sejam $(K, \leq)$ conjunto ordenado e $A \subset K$ não vazio.
Dizemos que $x_0 \in A$ é **elemento máximo** de A, se $x \leq x_0$, para todo $x \in A$.

Exemplo 2.1. $A = \{1, 2, 3\}$
1 é elemento mínimo e 3 é elemento máximo.

Exemplo 2.2. $A = \mathbb{N}$
0 é elemento mínimo.

Exemplo 2.3. $A = \mathbb{Z}$
A não possui elemento máximo, nem mínimo.

Definição 2.3. Sejam $(K, \leq)$ conjunto ordenado e $A \subset K$ não vazio. Dizemos que $x_0 \in K$ é **cota inferior** de A se, $x_0 \leq x$, para todo $x \in A$. Nestas condições A é **limitado inferiormente** ou **minorado**.

Definição 2.4. Sejam $(K, \leq)$ conjunto ordenado e $A \subset K$ não vazio. Dizemos que $x_0 \in K$ é **cota superior** de A se, $x \leq x_0$, para todo $x \in A$. Nestas condições A é **limitado superiormente** ou **majorado**.

Exemplo 2.4. $A = \{1, 2, 3\} \subseteq \mathbb{N}$
0 é cota inferior de A. Para todo n natural, $n \geq 3$ é cota superior de A.
Note que 1 também é cota inferior de A.

Definição 2.5. Sejam $(K, \leq)$ conjunto ordenado e $X \subset K$. Seja

C_s o conjunto das cotas superiores de X e
C_i o conjunto das cotas inferiores de X.

O elemento mínimo de C_s, se existir, é chamado **supremo** de X e o elemento máximo de C_i, se existir é chamado **ínfimo** de X.

Exemplo 2.5. Todo subconjunto finito e não vazio S, de um conjunto totalmente ordenado E, tem supremo e ínfimo que são, respectivamente, o máximo e o mínimo de S.

Exemplo 2.6. O ínfimo do conjunto P^* dos elementos estritamente positivos de um corpo ordenado K é igual a zero. Conforme o Corolário 1.9, este conjunto não tem mínimo. Além disso, P^* não admite supremo, pois este conjunto não é majorado.

Podemos definir supremo e ínfimo de outra maneira. Às vezes, dependendo da situação, torna-se mais conveniente usar uma ou outra definição. Antes de apresentarmos outra definição para supremo será necessário definir conjunto limitado.

Definição 2.6. Um subconjunto S não vazio de um anel ordenado A é **limitado**, se S for limitado inferior e superiormente.

Definição 2.7. Sejam K um corpo ordenado e $X \subset K$. Diz-se que um elemento $s \in K$ é o **supremo** de X se, e somente se, são válidas as seguintes condições:

(a) Para todo $x \in X$, tem-se $x \leq s$;

(b) Se $s' \in K$ é tal que $x \leq s'$ para todo $x \in X$, então $s \leq s'$.

Note que as definições de supremo (Definição 2.5 e Definição 2.7) são equivalentes.

De fato, se $s \in K$ satisfaz a Definição 2.5 então x é limitado superiormente e $x \leq s$, $\forall\, x \in X$, pois s é cota superior de X ($s \in C_s$). Como s é o mínimo de C_s temos $s \leq s'$.

Reciprocamente, sejam K, X e s satisfazendo a Definição 2.7. Como $x \leq s$, $\forall\, x \in X$, temos que $s \in C_s$. Para verificar que s é o mínimo de C_s tome outro elemento $s' \in C_s$. Como $s' \in C_s$ devemos ter $x \leq s'$, $\forall\, x \in X$. Segue da Definição 2.7 que $s \leq s'$. Portanto, $s' = \min X$.

Definição 2.8. Sejam K um corpo ordenado e $X \subset K$. Diz-se que um elemento $i \in K$ é o **ínfimo** de X se, e somente se , são válidas as seguintes condições:

(a) Para todo $x \in X$, tem-se $i \leq x$;

(b) Se $i' \in K$ é tal que $i' \leq x$ para todo $x \in X$, então $i' \leq i$.

De forma análoga ao que fizemos acima, prova-se que as definições de ínfimo (Definição 2.5 e Definição 2.8) são equivalentes.

Teorema 2.1. *Se o conjunto X admite supremo, então este elemento é único.*

Demonstração. Suponha que X tenha dois supremos, s_1 e s_2. Então, pela Definição 2.7, temos:

s_1 é supremo então $\forall x \in X, x \leq s_1$.

s_2 é supremo então $\forall x \in X, x \leq s_2$.

Pela parte (b) da Definição 2.7 temos:

$s_1 \leq s_2$ e $s_2 \leq s_1 \Longrightarrow s_1 = s_2$, por (O_2).

■

Teorema 2.2. *Se o conjunto X admite ínfimo, então este elemento é único.*

Demonstração. Análoga a anterior.

■

Proposição 2.1. Se o conjunto X admite supremo s, então s é máximo de X se, e somente se, $s \in X$.

Demonstração.
$(\Longrightarrow)$ s é máximo de X então $s \in X$, pela Definição 2.2.
$(\Longleftarrow)$ $s \in X$ e s é supremo então,

$\forall x \in X$ tem-se $x \leq s$.

Logo s é máximo de X, por definição.

■

Teorema 2.3. *Se S e S_1 são dois subconjuntos de K tais que $S_1 \subset S$, $S_1 \neq \{\}$ e se S e S_1 admitem supremos, então* $\sup S_1 \leq \sup S$.

Demonstração.
S tem supremo então, $\forall\, x \in S$, $x \leq \sup S$.

S_1 tem supremo então, $\forall\, x' \in S_1$, $x' \leq \sup S_1$.

Suponha, por absurdo, que $\sup S_1 > \sup S$.

$\sup S$ não é cota superior de S_1, pois $\sup S_1$ é a menor cota inferior.

Logo existe $y \in S_1$ tal que $\sup S < y \leq \sup S_1$.

Como $S_1 \subset S$ e $y \in S_1$ temos $y \in S$. Isso diz que $y \in S$ e $\sup S < y$.

Contradição. Portanto, $\sup S_1 \leq \sup S$.

■

Lema 2.1. Um subconjunto não vazio S, de um grupo abeliano totalmente ordenado $(G, +, \leq)$, admite supremo se, e somente se, $-S$ admite ínfimo. Neste caso, tem-se

$$\sup(-S) = -\inf S \text{ e } \inf(-S) = -\sup S.$$

Demonstração.
($\Longrightarrow$) Como S admite supremo, então por definição

$$\forall\, x \in S, x \leq \sup S \Longrightarrow -x \geq -\sup S,$$

pelo Corolário 1.2. Portanto, $-\sup S$ é cota inferior para $-S$.

Seja u outra cota inferior de $-S$. Devemos provar que $u \leq \sup -S$.

$$\begin{aligned} u \text{ cota inferior para } -S &\Longrightarrow u \leq x, \forall\, x \in -S \\ &\Longrightarrow -u \geq -x, \forall x \in S. \end{aligned}$$

Como $\sup S$ é a menor cota superior de S e $-u$ também é cota superior de S, segue que $\sup S \leq -u$. Isso leva a $u \leq -\sup S$.

Portanto, se S tem supremo $\sup S$ então $-S$ tem ínfimo $-\sup S$, isto é, $\inf(-S) = -\sup(S)$.

($\Longleftarrow$) Como $-S$ admite ínfimo, então por definição

$$\forall\, x \in (-S), x \geq \inf(-S) \Longrightarrow -x \leq -\inf(-S),$$

pelo Corolário 1.2. Portanto, $-\inf(-S)$ é cota superior para $-S$.

Seja u outra cota superior de $-S$. Devemos provar que $u \leq -\inf(-S)$.

$$\begin{aligned} u \text{ cota superior para } -S &\Longrightarrow x \leq u, \forall\, x \in -S \\ &\Longrightarrow -x \geq -u, \forall x \in S. \end{aligned}$$

Como $-\inf(-S)$ é a maior cota inferior de S e $-u$ também é cota inferior de S, segue que $-u \leq -\inf(-S)$. Isso leva a $u \leq \inf(-S)$.

Portanto, se S tem ínfimo $\inf S$ então $-S$ tem supremo $-\inf S$, isto é, $\sup(-S) = -\inf(S)$.

■

Proposição 2.2. Sejam A e B dois subconjuntos não vazios de um grupo abeliano totalmente ordenado G e suponhamos que estes conjuntos admitam supremos, então as seguintes igualdades são verificadas:

(i) $\sup(A+B) = \sup A + \sup B$;

(ii) $\sup(A \bigcup B) = \sup\{\sup A, \sup B\}$.

Demonstração.

(i) $a+b = \{x+y; x \in A \text{ e } y \in B\}$.

Sabemos que $x \leq \sup A$ e $\forall\, y \in B$, $\forall\, x \in A$ e $\forall\, y \in B$.

Então por (OA) e (O_3) temos

$x+y \leq \sup A + y$ e $\sup A + y \leq \sup A + \sup B \Longrightarrow x+y \leq \sup A + \sup B$.

Logo $\sup A + \sup B$ é cota superior de $A+B$.

Seja u outra cota superior de $A+B$. Devemos provar que $\sup A + \sup B \leq u$, e então teremos pela Definição 2.8, que $\sup A + \sup B = \sup(A+B)$.

Suponha, por absurdo, que $\sup A + \sup B > u$. Então

$\sup(B) > u - \sup A$,

ou seja, $u - \sup A$ não é cota superior de B.

Logo $\exists\, b \in B$ tal que $u - \sup A < b \leq \sup(B)$

Novamente por (OA) temos que $u - b < \sup(A)$, ou seja,

$u - b$ não é cota superior de A.

Logo $\exists\, a \in A$ tal que $u - b < a \leq \sup(A)$

Então por (OA), $u < a + b \in A + B$. Contradição.

Portanto, $\sup(A+B) = \sup A + \sup B$.

(ii) Seja $x \in A \bigcup B$

Se $x \in A$ temos $x \leq \sup A$

Se $x \in B$ temos $x \leq \sup B$

De modo geral, $x \leq \max\{\sup A, \sup B\} = \sup\{\sup A, \sup B\}$.

Logo, sup $\{\sup A, \sup B\}$ é cota superior de $A \bigcup B$.

Seja u outra cota superior de $A \bigcup B$. Devemos provar que $\sup\{\sup A, \sup B\} \leq u$.

Suponha, por absurdo, que $u < \sup\{\sup A, \sup B\}$. Temos dois casos:

• $\sup\{\sup A, \sup B\} = \sup A$;

• $\sup\{\sup A, \sup B\} = \sup B$.

1^o caso: $u < \sup\{\sup A, \sup B\} = \sup A$

Note que u não é cota superior de A, então $\exists\, a \in A$ tal que $u < a \leq \sup A$.

Como $a \in A$ temos, em particular, que $a \in (A \bigcup B)$. Ficamos com:

$u < a \in A \bigcup B$. Contradição.

Logo $\sup(A \bigcup B) = \sup\{\sup A, \sup B\}$

O outro caso é análogo ao primeiro.

■

Proposição 2.3. Sejam A e B dois subconjuntos não vazios de um grupo abeleano totalmente ordenado G e suponhamos que estes conjuntos admitam ínfimos, então as seguintes igualdades são verificadas:

(i) $\inf(A + B) = \inf A + \inf B$;

(ii) $\inf(A \bigcup B) = \inf\{\inf A, \inf B\}$.

Demonstração. Análoga a do teorema anterior.

■

Proposição 2.4. Seja A um subconjunto não vazio de um corpo ordenado K e suponhamos que A admita supremo e ínfimo. Então as seguintes propriedades são verificadas:

(i) se $c \in K$ e $0 \leq c$, então $\sup(cA) = c \cdot \sup A$ e $\inf(cA) = c \cdot \inf A$;

(ii) se $c \in K$ e $c \leq 0$, então $\sup(cA) = c \cdot \inf A$ e $\inf(cA) = c \cdot \sup A$.

Demonstração. $c \cdot A = \{c \cdot x; x \in A\}$

(i) $\forall\, x \in A, x \leq \sup A$.

Por (OM), $c \cdot x \leq c \cdot \sup A$.

Note que $c \cdot \sup A$ é cota superior de $c \cdot A$. Seja u outra cota superior de cA. Devemos provar que $c \cdot \sup A \leq u$.

Suponha, por absurdo, que $u < c \cdot \sup A$.

Como $c > 0$ temos $\dfrac{1}{c} > 0$. Então, novamente por (OM),

$\dfrac{1}{c}u < \sup A$, ou seja,

$\dfrac{1}{c}u$ não é cota superior de A.

Logo $\exists\, a \in A$ tal que $\dfrac{1}{c}u < a \leq \sup A$.

Por (OM), $u < c \cdot a \in cA$. Contradição!

Logo $\sup (c \cdot A) = c \cdot \sup A$.

O outro caso é idêntico.

(ii) Análogo ao anterior.

■

A partir de agora temos condições de estudar o que nos propomos no início desta secção.

Definição 2.9. Seja $(G, +, \leq)$ um grupo comutativo totalmente ordenado e suponhamos que o conjunto G tenha mais de um elemento. Dizemos que G é um **grupo ordenado completo** se, e somente se, vale o seguinte axioma (chamado axioma de completividade):

(AC): todo subconjunto de G, não vazio e majorado, admite supremo.

Exemplo 2.7. O grupo ordenado $(\mathbb{Z}, +, \leq)$, onde $\leq$ é a ordem habitual dos números inteiros, é completo, pois todo subconjunto de $\mathbb{Z}$ não vazio e majorado admite máximo.

Teorema 2.4. *Seja $(G, +, \leq)$ um grupo abeliano totalmente ordenado e suponhamos que o conjunto G tenha mais de um elemento. Nestas condições, G é um grupo ordenado completo se, e somente se, todo subconjunto de G, não vazio e minorado, tem ínfimo.*

Demonstração.
($\Longrightarrow$) Seja $X \subseteq G$, $X \neq \{\}$, X minorado.

Como X tem cota inferior temos:

$\exists\, x_0 \in G$ tal que $x_0 \leq x$, $\forall\, x \in X$.

$\exists\, x_0 \in G$ tal que $-x \leq -x_0$, $\forall\, x \in X$.

$\exists\, -x_0 \in (-G) = G$ tal que $-x \leq -x_0$, $\forall\, -x \in (-X)$.

Segue que $-X$ é subconjunto não vazio de G e $-X$ é majorado.

Desde que G é completo, existe $\sup(-X) \in G$.

Pelo Lema 2.1, existe $-inf(X) \in G$. Logo $\inf(X) \in G$.

($\Longleftarrow$) Seja $X \subseteq G$, $X \neq \{\}$, X minorado e $i = \inf(S)$.

Como X tem cota inferior temos:

$\exists\, x_0 \in G$ tal que $x_0 \leq x$, $\forall\, x \in X$.

se $x_0' \in X$ é tal que $x_0' \leq x$ para todo $x \in X$, então $x_0' \leq x_0$, ou seja, x_0 é ínfimo.

se $x_0' \in X$ é tal que $x \leq x_0'$ para todo $x \in X$, então $x_0 \leq x_0'$, ou seja, x_0 é supremo.

Logo, pela Definição 2.9, G é completo.

■

Teorema 2.5. *Todo grupo ordenado completo G é arquimediano.*

Demonstração. Sejam a e b dois elementos quaisquer de G tais que $0 < a < b$ e consideremos o conjunto $S = \{na \in G / n \in \mathbb{N}\}$.

Gostaria de provar que G é arquimediano, isto é, que existe $n \in \mathbb{N}$ tal que $b < na$. Suponha, por absurdo, que $na \leq b$, para todo número natural n, de onde resulta que S é majorado, logo, existe $L = \sup S$.

Note que $L - a < L$. Se $L - a \geq L$, teríamos por (OA)

$$\begin{aligned} L - a - L \geq L - L &\Longrightarrow -a \geq 0 \\ &\Longrightarrow a \leq 0. \end{aligned}$$

Contradição, pois assumimos $0 < a$.

Como $L = \sup S$ temos que L é a menor das cotas superiores. Então existe $p \in \mathbb{N}$ tal que

$L - a < pa \leq L$

$L - a < pa \Longrightarrow L - a + a < pa + a$

$$\Longrightarrow L < (p+1)a \in S.$$

Contradição, pois $L = \sup S$.

■

Definição 2.10. Diz-se que um corpo ordenado $(K, +, \cdot, \leq)$ é **completo** se, e somente se, o grupo ordenado $(K, +, \leq)$ é completo.

Corolário 2.1. *Todo corpo ordenado completo é arquimediano.*

Demonstração. Pela definição anterior temos que K é grupo ordenado completo. Então, pelo teorema anterior, K é arquimediano.

■

Corolário 2.2. *O corpo primo, de um corpo ordenado completo K, é totalmente denso em K.*

Demonstração. Pelo Corolário 2.1 temos que K é arquimediano, então pelo Teorema 1.15 temos que o corpo primo K_0, de K, é totalmente denso em K.

■

Exemplo 2.8. O corpo $\mathbb{Q}$ dos números racionais não é completo.

Consideremos o subconjunto

$$S = \{x \in \mathbb{Q}; 0 \leq x \text{ e } x^2 < 2\}$$

do corpo $\mathbb{Q}$ dos números racionais. É imediato que S é limitado, pois 0 e 2 são, respectivamente, minorante e majorante de S e mais, $0 = \min\ S = \inf\ S$.

Afirmamos que S não admite supremo. De fato, suponhamos por absurdo, que $a \in \mathbb{Q}$ seja o supremo de S. Dessa forma, temos, necessariamente, $0 < a < 2$. Sabemos que não existe um número racional que elevado ao quadrado seja igual a 2. Portanto, podemos distinguir dois casos: $a)\, a^2 < 2$ e $b)\, 2 < a^2$.

a) Consideremos o número racional $a' = \dfrac{4a}{2 + a^2} > 0$.

Temos $(a')^2 = \dfrac{16a^2}{(2 - a^2)^2 + 8a^2} \leq 2$, logo, $(a')^2 < 2$ e então $a' \in S$.

Por outro lado,

$$a^2 < \frac{1}{2}(2 + a^2) < 2 \Longrightarrow \frac{1}{2} < \frac{2}{2 + a^2}$$
$$\Longrightarrow a < \frac{4a}{2 + a^2} = a',$$

o que é absurdo, pois a e a' são elementos de S e a é o supremo de S.

b) $2 < \frac{1}{2}(2+a^2) < a^2 \Longrightarrow \frac{2+a^2}{2a} < a$,

portanto, existe $s \in S$ tal que

$$\frac{2+a^2}{2a} < s \leq a \Longrightarrow \left(\frac{2+a^2}{2a}\right)^2 < s^2 < 2.$$

Por outro lado, temos

$$\left(\frac{2+a^2}{2a}\right)^2 = \frac{(2-a^2)^2+8a^2}{4a^2} \geq 2$$

e chegamos assim a uma contradição.

Nas duas próximas secções introduziremos as definições e resultados básicos sobre as seqüências convergentes e as seqüências fundamentais num corpo ordenado K. Estas secções têm por objetivo demonstrar que existe um corpo ordenado completo, ou seja, que o que foi estabelecido na secção anterior possui exemplos.

É importante salientar que uma definição não pode definir "tudo "e também não pode definir "nada", isto é, devemos ter exemplos e contra exemplos de tal definição.

Iniciaremos recordando o conceito de função.

2.2 Seqüências Convergentes

Definição 2.11. Sejam E e F dois conjuntos e seja $E \,\mathrm{X}\, F$ o produto cartesiano de E por F. Todo subconjunto R de $E \,\mathrm{X}\, F$ é denominado de **relação** de E em F (ou relação entre elementos de E e elementos de F). Se R é uma relação de E em E, isto é, se R é um subconjunto de $E\mathrm{X}\, E$, diz-se simplesmente, que R é uma relação sobre E.

Admitiremos a noção de par ordenado como conceito primitivo. A cada elemento a e a cada elemento b está associado um terceiro elemento indicado por (a,b) e denominado par ordenado, de modo que se tenha $(a,b) = (c,d)$ se, e somente se, $a = c$ e $b = d$.

Definição 2.12. Sejam E e F dois conjuntos e seja f uma relação de E em F, isto é, f é um subconjunto do produto cartesiano de E por F . Diz-se que f é uma **função** de E em F se, e somente se, estiverem verificadas as seguintes condições:

(i) para todo x em E existe um elemento y de F tal que $(x,y) \in f$;

(ii) quaisquer que sejam os elementos x , y_1 , y_2 , com x em E e y_1 , y_2 em F,

$$\text{se } (x, y_1) \in f \text{ e } (x, y_2) \in f, \text{ então } y_1 = y_2.$$

Seja f uma função de um conjunto I num conjunto E. No lugar de indicar a imagem de um elemento $i \in I$ por $x(i)$ também se usa a notação indexada x_i, isto é, põe-se $x(i) = x_i$. Neste caso a função f é indicada por $(x_i)_{i\in I}$ e é chamada família de elementos de E tendo I para conjunto de índices ou família de elementos de E indexada pelo conjunto I. Cada elemento x_i passa a ser denominado termo ou componente de índice i da família $(x_i)_{i\in I}$.

Observação 2.1. Os conceitos de seqüência majorada, minorada e limitada, assim como os conceitos de majorante, minorante, supremo e ínfimo de uma seqüência são definidos através do conjunto dos termos desta seqüência.

Definição 2.13. Uma **seqüência** é uma função

$$\begin{aligned} \mathrm{f} : \mathbb{N} &\longrightarrow \mathbb{R} \\ n &\longmapsto a_n. \end{aligned}$$

Exemplo 2.9. Seqüência constante.

$$\begin{aligned} \mathrm{f} : \mathbb{N} &\longrightarrow \mathbb{R} \\ n &\longmapsto a. \end{aligned}$$

Exemplo 2.10. Seqüência dos números pares.

$$\begin{aligned} \mathrm{f} : \mathbb{N} &\longrightarrow \mathbb{R} \\ n &\longmapsto 2 \cdot n. \end{aligned}$$

Exemplo 2.11. Seqüência dos números ímpares.

$$\begin{aligned} \mathrm{f} : \mathbb{N} &\longrightarrow \mathbb{R} \\ n &\longmapsto 2 \cdot n + 1. \end{aligned}$$

Definição 2.14. Dizemos que uma **seqüência** $(a_n)_{n\in\mathbb{N}}$ é **inferiormente limitada** se, e somente se, $\exists\, A \in \mathbb{R}$ tal que $A \leq a_n$, $\forall\, n \in \mathbb{N}$.

Definição 2.15. Dizemos que uma **seqüência** $(a_n)_{n\in\mathbb{N}}$ é **superiormente limitada** se, e somente se, $\exists\, B \in \mathbb{R}$ tal que $a_n \leq B$, $\forall\, n \in \mathbb{N}$.

Definição 2.16. Dizemos que uma **seqüência** $(a_n)_{n\in\mathbb{N}}$ é **limitada** se, e somente se, $(a_n)_{n\in\mathbb{N}}$ for limitada inferior e superiormente.

Observação 2.2. Decorre imediatamente da Definição 2.14 e da Definição 2.15 que (a_n) será limitada se, e somente se, $|a_n| \leq M$, onde $M = \max\{|A|, |B|\}$.

Exemplo 2.12. $a_n = (-1)^n \cdot n$ é uma seqüência ilimitada.

Exemplo 2.13. $a_n = n$ é uma seqüência limitada inferiormente por 0, ou seja, $0 \leq a_n$.

Exemplo 2.14. $a_n = -n$ é uma seqüência limitada superiormente por 0, ou seja, $a_n \leq 0$.

Exemplo 2.15. $a_n = \dfrac{1}{n}$ é uma seqüência limitada, ou seja, $0 < a_n \leq 1$.

Notação: Seja K um corpo ordenado. Indiquemos por P (respectivamente, P^*) o conjunto dos elementos positivos (respectivamente, estritamente positivos) de K e $S(K)$ o conjunto de todas as seqüências $(a_n)_{n\in\mathbb{N}}$ de elementos de K.

Definindo em $S(K)$ a adição e a multiplicação por:

$$(a_n) + (b_n) = (a_n + b_n)$$

$$(a_n) \cdot (b_n) = (a_n \cdot b_n)$$

é fácil ver que $S(K)$ é um anel comutativo com unidade.

Definição 2.17. Diz-se que uma **seqüência** $(a_n) \in S(K)$ **converge** para um elemento $a \in K$ ou que (a_n) é convergente para a se, e somente se, para todo $\varepsilon \in P^*$ existe $n_0 \in \mathbb{N}$ tal que

$$|a_n - a| < \varepsilon,$$

para todo $n \in \mathbb{N}$, $n > n_0$.

Definição 2.18. Dizemos que a **seqüência** $(a_n)_{n\in\mathbb{N}}$ é **divergente** (ou diverge) se, e somente se, $(a_n)_{n\in\mathbb{N}}$ não for convergente.

Teorema 2.6. *Toda seqüência $(a_n) \in S(K)$ converge, no máximo, para um elemento de K .*

Demonstração. Suponhamos, por absurdo, que (a_n) seja convergente para a e para b, ambos em K , com $a \neq b$. Para todo $\varepsilon \in P^*$, existem números naturais p e q tais que

$$|a_n - a| < \varepsilon \text{ , } \forall\, n > p \text{ e}$$

$$|a_n - b| < \varepsilon \text{ , } \forall\, n > q.$$

Seja $n_0 = \max\{p, q\}$ e escolha $n > n_0$. Então

$$|a - b| = |(a - a_n) + (a_n - b)| \leq |a_n - a| + |a_n - b| < \varepsilon + \varepsilon = 2\varepsilon.$$

Tome $\varepsilon = \dfrac{1}{2}|a - b| \in P^*$, assim

$$|a - b| < 2 \cdot \varepsilon = 2 \cdot \frac{1}{2}|a - b| = |a - b|,$$

contradição.

■

Definição 2.19. Se uma seqüência $(a_n) \in S(K)$ coverge para um elemento a de K, diremos que a é o **limite** desta seqüência e escreveremos

$$a = \lim a_n \text{ ou } a = \lim_{n \longrightarrow +\infty}(a_n).$$

Exemplo 2.16. Toda seqüência constante $(a) \in S(K)$ é convergente e seu limite é a.

Exemplo 2.17. A seqüência $(a_n) \in S(\mathbb{Q})$, definida por $a_n = \dfrac{1}{n+1}$ converge para zero.

Com efeito, para todo número racional estritamente positivo ε existe um número natural n_0 tal que $\dfrac{1}{\varepsilon} < n_0$, pois $\mathbb{Q}$ é arquimediano. Portanto, para todo $n > n_0$, teremos:

$$\left|\frac{1}{n+1} - 0\right| = \frac{1}{n+1} < \frac{1}{n_0} < \varepsilon,$$

logo, $\lim\left(\dfrac{1}{n+1}\right) = 0$.

Exemplo 2.18. A seqüência $\left(\dfrac{1}{2}\right)^n \in S(\mathbb{Q})$é convergente a zero. Com efeito, é fácil verificar que $n + 1 \leq 2^n$, logo $\left(\dfrac{1}{2}\right)^n \leq \left(\dfrac{1}{n+1}\right)$, para todo número natural n. Portanto, de acordo com o Exemplo anterior, tem-se $lim\left(\dfrac{1}{2}\right)^n = 0$.

Exemplo 2.19. A seqüência $(n) \in S(\mathbb{Q})$ não é convergente.

Notação: O conjunto de todas as seqüências limitadas de elementos do corpo ordenado K será indicado por $S_l(K)$ e $S_c(K)$ indicará o conjunto de todas as seqüências convergentes, de elementos do corpo ordenado K.

Pode-se provar $S_l(K)$ é subanel unitário de $S(K)$. A demonstração é uma verificação de propriedades aritméticas de seqüências limitadas.

Daremos a seguir diversas propriedades das seqüências convergentes.

Lema 2.2. $S_c(K) \subset S_l(K)$, isto é, toda seqüência convergente é limitada.

Demonstração. Se $(a_n) \in S_c(K)$ e se $\lim a_n = a$, então dado $1 \in P^*$ existe $p \in \mathbb{N}$ tal que

$$|a_n - a| < 1 \text{ , } \forall n > p.$$

Temos pela Proposição 1.5 que

$$||a_n| - |a|| \leq |a_n - a|.$$

Logo, por (O_3), para todo $n > p$ temos

$$\begin{aligned} ||a_n| - |a|| < 1 &\Longrightarrow -1 < |a_n| - |a| < 1 \\ &\Longrightarrow |a| - 1 < |a_n| < |a| + 1. \end{aligned}$$

Ou seja, (a_n) é limitada para todo $n > p$. Falta garantir para $n \leq p$. Dessa forma, tome $M = \max\{|a_0|, |a_1|, ..., |a_p|, |a| + 1\}$.

Portanto, para todo $n \in \mathbb{N}$, $|a_n| \leq M$, isto é, (a_n) é limitada.

■

Notação: Indicaremos por $S_0(K)$ o conjunto de todas as seqüências de $S_c(K)$, que são convergentes a zero.

Lema 2.3. A seqüência $(a_n) \in S_c(K)$ converge para $a \in K$ se, e somente se, $(a_n - a) \in S_0(K)$.

Demonstração. É imediata.

■

Lema 2.4. $S_0(K)$ é fechado em relação à subtração e, portanto, também é fechado em relação à adição.

Demonstração. Se (a_n) e (b_n) são dois elementos quaisquer de $S_0(K)$. Então para todo $\varepsilon \in P^*$ existem números naturais p e q tais que

$$|a_n - 0| < \frac{1}{2}\,\varepsilon \text{ , } \forall\, n > p \text{ e}$$

$$|b_n - 0| < \frac{1}{2}\,\varepsilon\,,\ \forall\, n > q.$$

Pondo-se $n_0 = \max\{p, q\}$, teremos para todo $n > n_0$

$$|a_n - b_n| \leq |a_n| + |b_n| < \frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon$$

Logo, $(a_n - b_n) \in S_0(K)$.

Note que $(a_n - b_n) = (a_n + (-b_n)) \in S_0(K)$, portanto $S_0(K)$ também é fechado em relação à adição.

■

Lema 2.5. Se $(a_n) \in S_l(K)$ e se $(b_n) \in S_0(K)$, então $(a_n b_n) \in S_0(K)$. Daqui resulta, em particular, que $S_0(K)$ é fechado em relação à multiplicação.

Demonstração.
• $(a_n) \in S_l(K)$ então existe $M \in P^*$ tal que $|a_n| \leq M$ para todo $n \in \mathbb{N}$.

• $(b_n) \in S_0(K)$ então para todo $\varepsilon \in P^*$, existe $n_0 \in \mathbb{N}$ tal que

$$|b_n| < \frac{1}{M} \cdot \varepsilon,\ \forall n > n_0.$$

Portanto, pela Proposição 1.4, teremos para todo $n > n_0$,

$$|a_n b_n| = |a_n||b_n| < M\frac{1}{M}\varepsilon = \varepsilon.$$

Logo, $(a_n b_n) \in S_0(K)$.

■

Teorema 2.7. *$S_c(K)$ é um sub-anel unitário do anel $S_l(K)$.*

Demonstração. Já vimos no Lema 2.2 que $S_c(K) \subseteq S_l(K)$. Devemos provar que $S_c(K)$ é subanel de $S_l(K)$ e que $1 \in S_c(K)$. Tome a seqüência constante $(1) = 1$. Note que (1) converge para 1.

$|1 - 1| = 0 < \varepsilon$, pois $\varepsilon \in P^*$

Logo, $1 = (1) \in S_c(K)$.

Para provar que $S_c(K)$ é subanel de $S_l(K)$ devemos provar que $S_c(K)$ é fechado em relação à diferença e à multiplicação conforme a Proposição 1.10.

Se (a_n) e (b_n) são dois elementos quaisquer de $S_c(K)$ e se $\lim a_n = a$ e $\lim b_n = b$, então $(a_n - a) \in S_0(K)$ e $(b_n - b) \in S_0(K)$, pelo Lema 2.3.

$([a_n - b_n] - [a - b]) = (a_n - a) + (b_n - b)$ e

$(a_n b_n - ab) = (a_n - a)(b_n - b) + b(a_n - a) + a(b_n - b)$,

logo, conforme o Lema 2.4 e o Lema 2.5, teremos $([a_n - b_n] - [a - b]) \in S_0(K)$ e $(a_n b_n - ab) \in S_0(K)$.

Portanto $(a_n - b_n) \in S_c(K)$ e $(a_n b_n) \in S_c(K)$.

■

Corolário 2.3. *Se (a_n) e (b_n) são dois elementos quaisquer de $S_c(K)$, tem-se:*

(i) $\lim(a_n + b_n) = \lim(a_n) + \lim(b_n)$.

(ii) $\lim(-a_n) = -\lim(a_n)$.

(iii) $\lim(a_n b_n) = \lim(a_n) \cdot \lim(b_n)$.

Demonstração.

(i) Se (a_n) e (b_n) são dois elementos quaisquer de $S_c(K)$ e se (a_n) converge para a e (b_n) converge para b, então por definição, para todo $\varepsilon \in P^*$ existem $p, q \in \mathbb{N}$ tal que

$|a_n - a| < \frac{1}{2}\varepsilon$, $\forall\, n > p$ e

$|b_n - b| < \frac{1}{2}\varepsilon$, $\forall\, n > q$.

Tome $n_0 = \max\{p, q\}$. Assim, para todo $n > n_0$, teremos:

$$|(a_n+b_n)-(a+b)| = |(a_n-a)+(b_n-b)| \leq |a_n-a|+|b_n-b| < \frac{1}{2}\varepsilon+\frac{1}{2}\varepsilon = \varepsilon$$

Logo $(a_n + b_n)$ converge para $(a + b)$, ou seja,

$\lim(a_n + b_n) = a + b = \lim(a_n) + \lim(b_n)$.

(ii) Temos que (a_n) converge para a. Como no item anterior, $|a_n - a| < \varepsilon$, $\forall n > p$.

$$\begin{aligned} |a_n - a| < \varepsilon &\Longrightarrow -\varepsilon < a_n - a < \varepsilon \\ &\Longrightarrow -(-\varepsilon) > -(a_n - a) > -\varepsilon \\ &\Longrightarrow -\varepsilon < -a_n + a < \varepsilon, \end{aligned}$$

ou seja, $(-a_n)$ converge para $-a = -\lim(a_n)$.

Logo, $\lim(-a_n) = -\lim(a_n)$.

(iii) Se (a_n) e (b_n) são dois elementos quaisquer de $S_c(K)$ e se (a_n) converge para a e (b_n) converge para b, então:

$$|a_nb_n - ab| = |(a_n - a)(b_n - b) + a(b_n - b) + b(a_n - a)|$$
$$\leq |(a_n - a)(b_n - b)| + |a(b_n - b)| + |b(a_n - a)| < \varepsilon,$$

pelo Lema 2.3 e pelo Lema 2.5.

Assim, (a_nb_n) converge para (ab), ou seja,

$\lim(a_nb_n) = ab = \lim(a_n) \cdot \lim(b_n)$.

■

Lema 2.6. Se $(a_n) \in S_c(K)$, então $(|a_n|) \in S_c(K)$ e $\lim |a_n| = |\lim a_n|$.

Demonstração. $(a_n) \in S_c(K)$ então, por definição, (a_n) converge para um elemento a de K.

Pelo Corolário 2.3 temos que $\lim(-a_n) = -\lim a_n = -a$, ou seja, $(-a_n)$ converge para $-a$, de onde vem que, $(-a_n) \in S_c(K)$. Logo, $(|a_n|) \in S_c(K)$.

Falta verificar que $\lim |a_n| = |\lim a_n|$.

• Se $(a_n) \geq 0$ temos $a = \lim(a_n) > 0$, ou seja, $\lim |a_n| = \lim a_n = |\lim a_n|$.

• Se $(a_n) < 0$ temos $-a = \lim(a_n) < 0$, ou seja, $\lim |a_n| = -\lim a_n = |\lim a_n|$.

■

Lema 2.7. Se $(a_n) \in S_c(K)$ e se $\lim a_n = a \neq 0$, então existe $M \in P^*$ e existe $n_0 \in \mathbb{N}$ tal que $M < |a_n|$, para todo $n > n_0$.

Demonstração. De acordo com o Lema anterior temos que $\lim |a_n| = |\lim a_n|$. Seja $\lim a_n = a \in K$. Dado $M = \frac{1}{2}|a| \in P^*$, existe $n_0 \in \mathbb{N}$ tal que

$||a_n| - |a|| < M$, para todo $n > n_0$.

$$||a_n| - |a|| < M \Longrightarrow -M < |a_n| - |a| < M$$
$$\Longrightarrow |a| - M < |a_n| < |a| + M$$
$$\Longrightarrow M < |a_n|.$$

■

Teorema 2.8. *Uma seqüência $(a_n) \in S_c(K)$ é inversível no anel $S_c(K)$ se, e somente se, $a_n \neq 0$ para todo $n \in \mathbb{N}$ e $\lim a_n = a \neq 0$; neste caso, tem-se*

$$(a_n)^{-1} = (a_n^{-1}) \text{ e } \lim a_n^{-1} = a^{-1}.$$

Demonstração.
($\Longrightarrow$) Se (a_n) é inversível em $S_c(K)$, então existe $(b_n) \in S_c(K)$ tal que

$$\begin{aligned}(a_n)(b_n) = (1) &\Longrightarrow a_n b_n = 1 \\ &\Longrightarrow b_n = a_n^{-1}\ \forall n \in \mathbb{N}, \text{ pois } a_n \neq 0.\end{aligned}$$

Portanto, $(a_n)^{-1} = (a_n^{-1})$. Além disso, de acordo com o Corolário 2.3, temos:

$$\begin{aligned}1 &= \lim(1) \\ &= \lim(a_n b_n) \\ &= \lim(a_n) \cdot \lim(b_n) \\ &= a \cdot b,\end{aligned}$$

logo como $a \neq 0$, $b = a^{-1}$, ou seja, $\lim a_n^{-1} = a^{-1}$.

($\Longleftarrow$) Suponhamos que $(a_n) \neq 0$, para todo $n \in \mathbb{N}$ e que $\lim a_n = a \neq 0$. Neste caso, a seqüência (a_n) é inversível em $S(K)$ e sua inversa é (a_n^{-1}). Basta demonstrar que $(a_n^{-1}) \in S_c(K)$.

De acordo com o Lema 2.7 e como $\lim a_n = a$, temos

• $\exists\, M \in P^*$ e $\exists\, p \in \mathbb{N}$ tais que $M < |a_n|$, para todo $n > p$;

• $\forall\, \varepsilon \in P^*$, $\exists\, q \in \mathbb{N}$ tal que $|a_n - a| < M|a|\varepsilon$, qualquer que seja $n > q$.

Pondo-se $n_0 = \max\{p, q\}$, teremos $\forall\, n > n_0$:

$$\begin{aligned}|a_n^{-1} - a^{-1}| &= |a_n^{-1} a^{-1}(a - a_n)| \\ &= |a_n|^{-1} \cdot |a|^{-1} \cdot |a - a_n| < M^{-1} \cdot |a|^{-1} \cdot M \cdot |a| \cdot \varepsilon = \varepsilon.\end{aligned}$$

Portanto, (a_n^{-1}) é convergente para a^{-1}.

■

Terminaremos esta secção estabelecendo uma caracterização de um corpo ordenado arquimediano pelas seqüências de elementos de seu corpo primo.

Teorema 2.9. *Um corpo ordenado K é arquimediano se, e somente se, todo elemento de K é o limite de uma seqüência de elementos do corpo primo K_0 de K.*

Demonstração.
($\Longrightarrow$) Suponhamos que o corpo ordenado K seja arquimediano e seja b um elemento qualquer de K. Podemos, evidentemente, supor que b seja estritamente positivo. Para cada número natural n consideremos o conjunto

$$B_n = \{j \in \mathbb{N} \text{ tal que } 2^{-n} j \geq b\}.$$

Como K é arquimediano resulta que B_n é não vazio. Assim definimos j_n como sendo o elemento mínimo de B_n, $n \in \mathbb{N}$. Note que $j_n - 1 \notin B_n$, portanto

$$\begin{aligned} 2^{-n}(j_n - 1) < b \leq 2^{-n} j_n &\Longrightarrow 2^{-n} j_n - 2^{-n} < b \leq 2^{-n} j_n. \\ &\Longrightarrow -2^{-n} < b - 2^{-n} j_n \leq 0 \\ &\Longrightarrow 0 \leq 2^{-n} j_n - b < 2^{-n}. \ (*) \end{aligned}$$

Ora, a seqüência (2^{-n}) é convergente a zero (Exemplo 2.18). Portanto, de $(*)$ resulta que a seqüência $(2^{-n} j_n)$ é convergente para b.

Falta provar que a seqüência $(2^{-n} j_n) \in K_0$.

Por definição, K_0 é a intersecção de todos os subcorpos de K. Assim basta provar que $(2^{-n} j_n) \subseteq L$, para todo subcorpo L de K.

Seja então L um subcorpo de K. Como $1 \in L$ temos que $2 = 1 + 1 \in L$. Segue que $2^{-1} \in L$ e então $2^{-n} = (2^{-1})^n \in L$.

Desde que $j_n \in \mathbb{N}$ e $2^{-n} \in L$, temos $2^{-n} j_n \in L$.

Portanto, $(2^{-n} j_n) \subseteq L$.

$(\Longleftarrow)$ Suponhamos que todo elemento de K seja o limite de uma seqüência de elementos de K_0 e seja b um elemento estritamente positivo de K.

Por hipótese, existe uma seqüência convergente $(b_n) \in S(K_0)$ tal que $\lim(b_n) = b$. Portanto, dado $1 \in P^*$ existe $n_0 \in \mathbb{N}$ tal que

$$\begin{aligned} |b_n - b| < 1 &\Longrightarrow -1 < b_n - b < 1 \\ &\Longrightarrow -1 - b_n < -b < 1 - b_n \\ &\Longrightarrow b_n - 1 < b < b_n + 1, \forall\, n > n_0. \end{aligned}$$

Como o corpo ordenado K_0 é arquimediano resulta que existe um múltiplo inteiro $q \cdot 1$ de seu elemento unidade que é estritamente maior do que $b_n + 1$ (Teorema 1.13). Portanto, em virtude deste mesmo teorema, o corpo ordenado K também é arquimediano.

■

2.3 Seqüências Fundamentais

Definição 2.20. Diz-se que uma **seqüência** $(a_n) \in S(K)$ é **fundamental** (ou de Cauchy) se, e somente se, para todo $\varepsilon \in P^*$ existe $n_0 \in \mathbb{N}$ tal que

$$|a_m - a_n| < \varepsilon,$$

quaisquer que sejam os números naturais m e n , com $m > n_0$ e $n > n_0$.

Sendo assim, uma seqüência $(a_n) \in S(K)$ será chamada seqüência fundamental ou seqüência de Cauchy em K se o valor absoluto da diferença entre dois termos da seqüência tender a zero à medida que os seus índices aumentem.

Notação: Indicaremos por $S_f(K)$ o conjunto de todas as seqüências fundamentais de elementos do corpo ordenado K.

O próximo resultado nos fornecerá a relação entre seqüências convergentes e fundamentais.

Lema 2.8. $S_c(K) \subset S_f(K)$, isto é, toda seqüência convergente é fundamental.

Demonstração. Seja $(a_n) \in S_c(K)$ e suponha que $\lim(a_n) = a$. Temos que para todo $\varepsilon \in P^*$, existe $n_0 \in \mathbb{N}$ tal que

$$|a_n - a| < \frac{\varepsilon}{2} \text{ e } |a_m - a| < \frac{\varepsilon}{2},$$

para quaisquer m, n naturais com $m, n > n_0$.

Segue então

$$|a_n - a_m| = |(a_n - a) - (a_m - a)| \leq |a_n - a| + |a_m - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

logo, (a_n) é fundamental em K.

■

O lema acima nos fornece uma condição necessária, em termos de propriedades intrínsecas, para que uma seqüência $(a_n) \in S(K)$ seja convergente em K.

Exemplo 2.20. A seqüência $(a_n) \in S(\mathbb{Q})$ definida por $(a_n) = (-1)^n$, é não fundamental, logo não converge em $\mathbb{Q}$.

O próximo exemplo mostra que não vale a recíproca do Lema 2.8.

Exemplo 2.21. Seja (a_n) definido por $a_0 = 0$ e $a_{n+1} = \dfrac{1}{2 + a_n}$ e suponhamos que $\lim(a_n) = a$. Então

$$\lim(a_{n+1}) = \lim(a_n) = \lim \frac{1}{2 + a_n} = \frac{1}{2 + \lim(a_n)}.$$

Logo,

$$\begin{aligned} a = \frac{1}{2+a} &\Longrightarrow a - \frac{1}{2+a} = 0 \\ &\Longrightarrow 2a + a^2 - 1 = 0 \\ &\Longrightarrow (a+1)^2 - 2 = 0 \\ &\Longrightarrow (a+1)^2 = 2, \end{aligned}$$

o que não é possível com $a \in \mathbb{Q}$. Isso mostra que (a_n) não é convergente.

Por outro lado,

$$\begin{aligned}|a_{n+1} - a_n| &= \left|\frac{1}{2+a_n} - \frac{1}{2+a_{n-1}}\right| \\ &= \left|\frac{(2+a_{n-1}) - (2+a_n)}{(2+a_n).(2+a_{n-1})}\right| \\ &= \left|\frac{a_{n-1} - a_n}{(2+a_n).(2+a_{n-1})}\right| \leq \frac{1}{4}|a_n - a_{n-1}|,\end{aligned}$$

e então

$$|a_3 - a_2| \leq \frac{1}{4}|a_2 - a_1|,$$

$$|a_4 - a_3| \leq \frac{1}{4}|a_3 - a_2| \leq \left(\frac{1}{4}\right)^2 |a_2 - a_1|,$$

...

$$|a_{n+1} - a_n| \leq \left(\frac{1}{4}\right)^{n-1} |a_2 - a_1|.$$

Daí,

$$\begin{aligned}|a_{n+p} - a_n| &\leq |a_{n+p} - a_{n+p-1}| + ... + |a_{n+1} - a_n| \\ &\leq \left(\left(\frac{1}{4}\right)^{n+p-2} + ... + \left(\frac{1}{4}\right)^{n-1}\right)|a_2 - a_1| = \frac{\left(\frac{1}{4}\right)^{n-1}}{1 - \frac{1}{4}}|a_2 - a_1|,\end{aligned}$$

o que mostra que a seqüência (a_n) é de Cauchy, pois é fácil ver que

$$\begin{aligned}\lim \frac{\left(\frac{1}{4}\right)^{n-1}}{1 - \frac{1}{4}}|a_2 - a_1| &= \lim \frac{4}{3.4^{n-1}}|a_2 - a_1| \\ &= \frac{1}{3.4^{n-2}}|a_2 - a_1| = 0.\end{aligned}$$

Lema 2.9. $S_f(K) \subset S_l(K)$, isto é, toda seqüência fundamental é limitada.

Demonstração. Se $(a_n) \in S_f(K)$, então dado $1 \in P^*$ existe $p \in \mathbb{N}$ tal que

$|a_m - a_n| < 1$; quaisquer que sejam m e n naturais , com $m > p$ e $n > p$.

Fixando-se $n = p + 1$ teremos, para todo $m > p$:

$|a_m| = |a_m - a_{p+1} + a_{p+1}| \leq |a_m - a_{p+1}| + |a_{p+1}| < 1 + |a_{p+1}|$.

Pondo-se $M = \max\{|a_0|, |a_1|, ..., |a_p|, 1 + |a_{p+1}|\}$ teremos $|a_m| \leq M$, para todo $m \in \mathbb{N}$. Portanto (a_n) é limitada.

■

Teorema 2.10. *$S_f(K)$ é um subanel unitário de $S_l(K)$.*

Demonstração. É imediato que $1 \in S_f(K)$. Tome a seqüência constante (1), temos que

$1 = a_m = a_n, \forall m, n \in \mathbb{N}$.

Então $|a_m - a_n| = |1 - 1| = 0 < \varepsilon$, pois $\varepsilon \in P^*$.

Basta então provar que $S_f(K)$ é fechado em relação à adição e à multiplicação. Vimos no Lema 2.4 que se um conjunto é fechado em relação à subtração é também fechado em relação à adição.

• $S_f(K)$ é fechado em relação à subtração.

Sejam (a_n) e (b_n) dois elementos quaisquer de $S_f(K)$ então, para todo $\varepsilon \in P^*$ existem números naturais p e q tais que

$|a_m - a_n| < \frac{1}{2}\varepsilon$, para $m > p$ e $n > p$ e

$|b_m - b_n| < \frac{1}{2}\varepsilon$, para $m > q$ e $n > q$.

Tome $n_0 = \max\{p, q\}$. Assim, teremos para todo $m > n_0$ e para todo $n > n_0$:

$|(a_m + b_m) - (a_n + b_n)| = |(a_m - a_n) + (b_m - b_n)|$

$|(a_m - a_n) + (b_m - b_n)| \leq |a_m - a_n| + |b_m - b_n| < \frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon$.

Portanto, a seqüência $(a_m + b_m)$ é fundamental.

• $S_f(K)$ é fechado em relação à multiplicação.

Sejam (a_n) e (b_n) dois elementos quaisquer de $S_f(K)$. Conforme o Lema 2.9 estas seqüências são limitadas, logo, existem M_1 e M_2, em P^*, tais que

$|a_n| \leq M_1$ e $|b_n| \leq M_2, \forall n \in \mathbb{N}$.

Por outro lado, $\forall \varepsilon \in P^*$ existem números naturais p e q tais que

$|a_m - a_n| < \frac{1}{2M_2}\varepsilon$, para $m > p$ e $n > p$ e

$|b_m - b_n| < \frac{1}{2M_1}\varepsilon$, para $m > q$ e $n > q$.

Tome $n_0 = \max\{p, q\}$, assim teremos para todo $m > n_0$ e para todo $n > n_0$:

$$|(a_m b_m - a_n b_n| = |a_m(b_m - b_n) + b_n(a_m - a_n)|$$
$$|a_m(b_m - b_n) + b_n(a_m - a_n)| \leq |a_m||b_m - b_n| + |b_n||a_m - a_n|$$
$$< M_1 \frac{1}{2M_1}\varepsilon + M_2 \frac{1}{2M_2}\varepsilon = \varepsilon.$$

Portanto, a seqüência $(a_m b_m)$ é fundamental.

■

Lema 2.10. Se $(a_n) \in S_f(K)$ e se $(a_n) \notin S_0(K)$ então existe $M \in P^*$ e existe $n_0 \in \mathbb{N}$ tais que $M < |a_n|$, para todo $n > n_0$.

Demonstração. Suponha que a propriedade acima não fosse verdadeira, então, para todo $M \in P^*$ e para todo $n_0 \in \mathbb{N}$ existiria $m \in \mathbb{N}$, $m < n_0$ tal que $|a_m| \leq M$. Por outro lado, a seqüência (a_n) é fundamental logo, dado $M \in P^*$, existe $n_0 \in \mathbb{N}$ tal que

$|a_m - a_n| < M$; $\forall m, n \in \mathbb{N}$, $m > n_0$ e $n > n_0$.

Portanto, teríamos

$$|a_n| = |a_n - a_m + a_m| \leq |a_n - a_m| + |a_m| < M + M = 2M,$$

ou seja, a seqüência $(a_n) \in S_0(K)$, contra a hipótese.

■

A próxima propriedade será utilizada no Capítulo 3 para definir uma número real positivo.

Lema 2.11. Se $(a_n) \in S_f(K)$ e se $(a_n) \in S_0(K)$, então existe $M \in P^*$ e existe $n_0 \in \mathbb{N}$ tais que

$$M < a_n, \forall n > n_0$$

ou

$$a_n < -M, \forall n > n_0.$$

Demonstração. Pelo lema anterior, existe $M \in P^*$ e existe $p \in \mathbb{N}$ tal que

$2M < |a_n|$, $\forall n > p$.

Por outro lado, a seqüência (a_n) é fundamental, logo, dado $M \in P^*$ existe $q \in \mathbb{N}$ tal que $|a_n - a_m| < M$, quaisquer que sejam $m, n \in \mathbb{N}$, com $m > q$ e $n > q$.

$$|a_n - a_m| < M \Longrightarrow -M < a_n - a_m < M$$
$$\Longrightarrow a_m - M < a_n < a_m + M$$

Seja $n_0 = \max\{p, q\}$.

• Se existir $m > n_0$ tal que $2M < a_m$ teremos

$M < a_m - M < a_n \Longrightarrow M < a_n, \forall n > n_0.$

• Se existir $m > n_0$ tal que $a_m < -2M$ teremos

$a_n < a_m + M < -M \Longrightarrow a_n < -M, \forall n > n_0.$

■

Teorema 2.11. *Uma seqüência $(a_n) \in S_f(K)$ é inversível em $S_f(K)$ se, e somente se, $(a_n) \notin S_0(K)$ e $a_n \neq 0$ para todo $n \in \mathbb{N}$.*

Demonstração.
($\Longrightarrow$) Se $(a_n) \in S_f(K)$ é inversível em $S_f(K)$ então, existe $(b_n) \in S_f(K)$ tal que

$(a_n) \cdot (b_n) = (1) \Longrightarrow a_n \cdot b_n = 1,$

logo $(a_n) \neq 0$ para todo $n \in \mathbb{N}$.

Se $(a_n) \in S_0(K)$ teríamos, conforme o Lema 2.5, $(a_n \cdot b_n) \in S_0(K)$ o que seria absurdo, pois $a_n \cdot b_n = 1$.

($\Longleftarrow$) Suponhamos que $(a_n) \notin S_0(K)$ e que $(a_n) \neq 0$, $\forall n \in \mathbb{N}$. Neste caso, (a_n) é inversível em $S(K)$ e sua inversa é (a_n^{-1}), portanto, basta demonstrar que $(a_n^{-1}) \in S_f(K)$.

Como $(a_n) \notin S_0(K)$ temos que (a_n) não é convergente a zero logo, em virtude do Lema 2.10, existe $M \in P^*$ e $p \in \mathbb{N}$ tal que

$M < |a_n|, \forall n > p.$

Ora, (a_n) é fundamental então $\forall \varepsilon \in P^*$, $\exists q \in \mathbb{N}$ tal que

$|a_m - a_n| < \varepsilon \cdot M^2, \forall\, m, n$ com $m > q$ e $n > q$.

Pondo-se $n_0 = \max\{p,q\}$, teremos para todo $m > n_0$ e para todo $n > n_0$:

$$\begin{aligned} |a_m^{-1} - a_n^{-1}| &= |a_m^{-1} a_n^{-1}(a_n - a_m)| \\ &= |a_m|^{-1} \cdot |a_n|^{-1} \cdot |a_n - a_m| < M^{-1} \cdot M^{-1} \cdot \varepsilon \cdot M^2 = \varepsilon. \end{aligned}$$

Portanto, (a_n^{-1}) é fundamental.

■

Terminaremos este Capítulo estabelecendo diversas caracterizações de um corpo ordenado completo.

Veremos, inicialmente, algumas propriedades das seqüências crescentes e decrescentes de um corpo ordenado K.

2.4 Caracterizações de um Corpo Ordenado Completo

Definição 2.21. Diz-se que uma seqüência $(a_n) \in S(K)$ é **crescente** se, e somente se, $a_n \leq a_{n+1}$ para todo número natural n.

Definição 2.22. Diz-se que uma seqüência $(a_n) \in S(K)$ é **decrescente** se, e somente se, $a_{n+1} \leq a_n$ para todo número natural n.

Exemplo 2.22. $a_n = 1 - \dfrac{1}{n}$, $\forall n \in \mathbb{N}$.

Seja $n \in \mathbb{N}$.

$$\begin{aligned} n+1 > n &\Longrightarrow \frac{1}{n+1} < \frac{1}{n} \\ &\Longrightarrow -\frac{1}{n+1} > -\frac{1}{n} \\ &\Longrightarrow 1 - \frac{1}{n+1} > 1 - \frac{1}{n} \\ &\Longrightarrow a_{n+1} > a_n, \end{aligned}$$

ou seja, (a_n) é crescente.

Exemplo 2.23. $a_n = a + (n-1)r$, com $a \in \mathbb{R}$ e $r \in \mathbb{R}^*$.

Seja $n \in \mathbb{N}$, temos:

$a_n = a + (n-1)r = a + nr - r$ e

$a_{n+1} = a + [(n+1) - 1]r = a + nr$.

- Se $r > 0$ temos $a_n < a_{n+1}$, ou seja, (a_n) é crescente;
- Se $r < 0$ temos $a_n > a_{n+1}$, ou seja, (a_n) é decrescente.

Se (a_n) é crescente e convergente, então o Lema 2.2 nos garante que (a_n) é majorada. Os exemplos abaixo nos mostram que, em geral, nem toda seqüência crescente e majorada ou decrescente e minorada é convergente.

Exemplo 2.24. A seqüência $(n) \in S_c(K)$, onde K é um corpo ordenado não arquimediano, é crescente e majorada e, é imediato que esta seqüência não é convergente.

Exemplo 2.25. Consideremos a seqüência $(a_n) \in S_c(K)$ definida por $a_0 = 1$ e $a_{n+1} = \dfrac{4a_n}{2 + a_n^2}$ para todo número natural n.

Conforme vimos no Exemplo 2.8, temos $0 < a_n$ e $a_n^2 < 2$, para todo n natural, logo, a seqüência (a_n) é limitada.

Por outro lado,

$$\begin{aligned} a_{n+1} - a_n &= \frac{4a_n}{2 + a_n^2} - a_n \\ &= \frac{4a_n - 2a_n - a_n^3}{2 + a_n^2} \\ &= \frac{2a_n - a_n^3}{2 + a_n^2} \\ &= \frac{a_n(2 - a_n^2)}{2 + a_n^2} > 0. \end{aligned}$$

Portanto, (a_n) é crescente.

Se esta seqüência fosse convergente para $a \in \mathbb{Q}$ teríamos, por passagem ao limite:

$$\begin{aligned} a = \frac{4a}{2 + a^2} &\Longrightarrow 2a + a^3 = 4a \\ &\Longrightarrow a^3 - 2a = 0 \\ &\Longrightarrow a(a^2 - 2) = 0 \\ &\Longrightarrow a^2 = 2, \end{aligned}$$

o que seria absurdo, pois a é um número racional não nulo.

Exemplo 2.26. Consideremos a seqüência $(b_n) \in S(\mathbb{Q})$ definida por $b_0 = 2$ e $b_{n+1} = \dfrac{2 + b_n^2}{2b_n}$, para todo n natural.

Conforme vimos no Exemplo 2.8, temos $0 < b_n$ e $b_n^2 > 2$, para todo n natural, logo, a seqüência (b_n) é limitada.

Por outro lado,

$$\begin{aligned} b_n - n_{n+1} &= b_n - \frac{2 + b_n^2}{2b_n} \\ &= \frac{2b_n^2 - 2 - b_n^2}{2b_n} \\ &= \frac{b_n^2 - 2}{2b_n} > 0. \end{aligned}$$

Portanto, (b_n) é decrescente.

Se esta seqüência fosse convergente para $b \in \mathbb{Q}$ teríamos, por passagem ao limite:

$$b = \frac{2+b^2}{2b} \Longrightarrow 2b^2 = 2 + b^2$$
$$\Longrightarrow b^2 = 2,$$

o que seria absurdo, pois b é um número racional.

Temos o seguinte critério para determinar em que condições uma seqüência crescente e majorada é convergente.

Teorema 2.12. *Uma seqüência crescente $(a_n) \in S(K)$ é convergente se, e somente se, esta seqüência admite supremo $a \in K$. Neste caso, tem-se* $\lim a_n = a$.

Demonstração.
($\Longrightarrow$) (a_n) é crescente então $\forall\, p, q \in \mathbb{N}$, $p < q$ implica $a_p < a_q$.

Além disso, como (a_n) converge para a temos:

dado $\varepsilon \in P^*$, existe $n_0 \in \mathbb{N}$ tal que $|a_n - a| < \varepsilon$, para todo $n > n_0$.

Considere o conjunto $\{a_n, n \in \mathbb{N}\} = A$. Gostaria de provar que a é cota superior de A e que a é a menor das cotas superiores, ou seja, $a = \sup\, a$ (Definição 2.7).

(a) Afirmação: a é cota superior de A, ou seja, $a_n \leq a$, $\forall n \in \mathbb{N}$.

Suponha, por absurdo, que existe $p \in \mathbb{N}$ tal que $a < a_p$, ou seja, $0 < a_p - a$. Tome $\varepsilon = a_p - a \in P^*$.

$$|a_n - a| < \varepsilon \Longrightarrow -\varepsilon < a_n - a < \varepsilon$$
$$\Longrightarrow a - \varepsilon < a_n < a + \varepsilon = a + a_p - a = a_p.$$

Tomando-se $n > \max\{n_0, p\}$, teremos $a_n < a_p$. Contradição, pois (a_n) é crescente.

(b) Afirmação: a é a menor das cotas superiores de A.

Suponha que $a' \in K$ seja a menor das cotas superiores, ou seja, $a' < a$ o que implica que, $0 < a - a'$. Tome $\varepsilon = a - a' \in P^*$.

Por (a_n) ser convergente temos que $\exists n_0 \in \mathbb{N}$ tal que $\forall n > n_0$, $|a_n - a| < \varepsilon$.

$$|a_n - a| < \varepsilon \Longrightarrow -\varepsilon < a_n - a < \varepsilon$$
$$\Longrightarrow a - \varepsilon < a_n < a + \varepsilon$$
$$\Longrightarrow a - (a - a') < a_n$$
$$\Longrightarrow a' < a_n.$$

Contradição, pois a' é supremo do conjunto A.

($\Longleftarrow$) Suponha que (a_n) admita supremo $a \in K$. Logo, $a_n \leq a$ para todo $n \in \mathbb{N}$.

Seja $\varepsilon \in P^*$. Por a ser a menor das cotas superiores existe $p \in \mathbb{N}$ tal que $a - \varepsilon < a_p \leq a$.

Como (a_n) é crescente temos

$a - \varepsilon < a_p \leq a_n \leq a \Longrightarrow |a_n - a| < \varepsilon, \forall n > p.$

Portanto, (a_n) converge para a e $\lim(a_n) = a$.

■

Corolário 2.4. *Uma seqüência decrescente $(a_n) \in S(K)$ é convergente se, e somente se, esta seqüência admite ínfimo $a \in K$. Neste caso tem-se $\lim a_n = a$.*

Demonstração. (a_n) é decrescente então $\forall\, p, q \in \mathbb{N}$, $p < q$ temos $a_p \geq a_q$.

$a_p \geq a_q \Longrightarrow -a_p \leq -a_q$,

ou seja, $(-a_n)$ é crescente. Basta então usar o teorema anterior.

■

Teorema 2.13. *Um corpo K é arquimediano se, e somente se, toda seqüência de elementos de K, crescente e majorada, é fundamental.*

Demonstração.
($\Longrightarrow$) Suponhamos que o corpo K seja arquimediano e que $(a_n) \in S(K)$ é uma seqüência crescente e majorada. Seja ε um elemento qualquer de P^* e consideremos o conjunto S de todos os números naturais s tais que

$a_n \leq b - s\varepsilon$; $\forall n \in \mathbb{N}$, onde b é um majorante de (a_n).

Note que $S \neq \{\,\}$ pois para $s = 0$ temos $a_n \leq b - 0\varepsilon = b$, o que se verifica já que b é majorante de (a_n).

Como K é arquimediano existe $q \in \mathbb{N}$ tal que $a_n > b - q\varepsilon$. Portanto, S é majorado. Seja $p = \max S$, tal que $a_n \leq b - p\varepsilon$, $\forall n \in \mathbb{N}$. Ora, $p + 1 \notin S$ já que $p = \max S$. Logo, existe $n_0 \in \mathbb{N}$ tal que $b - (p+1)\varepsilon < a_{n_0}$. Logo, se m e n são dois números naturais quaisquer com $m \geq n > n_0$, temos:

$b - (p+1)\varepsilon < a_{n_0} \leq a_n \leq a_m \leq b - p\varepsilon \Longrightarrow |a_m - a_n| < \varepsilon$,

isto é, a seqüência (a_n) é fundamental.

($\Longleftarrow$) Se o corpo ordenado K não é arquimediano, então a seqüência $(n) \in S(K)$ é crescente e majorada e é imediato que esta seqüência não é fundamental.

■

Veremos adiante que uma condição necessária e suficiente para que um corpo ordenado seja completo, é que este corpo seja arquimediano e satisfaça o axioma dos intervalos encaixantes. Portanto, vamos apresentar aqui este axioma.

Se a e b, com $a < b$ são dois elementos quaisquer de um conjunto E, totalmente ordenado pela ordem $\leq$, então o conjunto

$$[a, b] = \{x \in E; a \leq x \leq b\}$$

é chamado intervalo fechado (de E) de extremidades a e b ou ainda de origem a e extremo b.

Definição 2.23. Diz-se que um corpo ordenado K satisfaz o **axioma dos intervalos encaixantes** se, e somente se, é válida a seguinte condição:

se $(I_n)_{n\in\mathbb{N}}$ é uma seqüência qualquer de intervalos fechados de K e se $I_{n+1} \subset I_n$ para todo $n \in \mathbb{N}$, então o conjunto $\bigcap\limits_{n\in\mathbb{N}} (I_n)$ não é vazio.

Exemplo 2.27. Mostraremos que o corpo ordenado $\mathbb{Q}$ dos números racionais não satisfaz o axioma dos intervalos encaixantes.

Com efeito, consideremos as seqüências (a_n) e (b_n) definidas, respectivamente, no Exemplo 2.25 e no Exemplo 2.26.

Afirmação: $a_n.b_n = 2$.

Vamos provar esta afirmação por indução sobre n.

• Para $n = 0$ temos $a_n.b_n = a_0.b_0 = 1.2 = 2$.

• Para $n = k > 0$, k fixo temos $a_k.b_k = 2$ (hipótese de indução).

• Para $n = k + 1$ temos

$$\begin{aligned}
a_{k+1}.b_{k+1} &= \frac{4a_k}{2 + a_k^2} . \frac{2 + b_k^2}{2b_k} \\
&= \frac{4a_k.(2 + b_k^2)}{(2 + a_k^2).2b_k} \\
&= \frac{8a_k + 4a_k.b_k^2}{4b_k + 2b_k.a_k^2} \\
&= \frac{8a_k + 4a_k.b_k.b_k}{4b_k + 2b_k.a_k.a_k} \\
&= \frac{8a_k + 4.2b_k}{4b_k + 2.2a_k} \\
&= \frac{8a_k + 8b_k}{4b_k + 4a_k} \\
&= \frac{8(a_k + b_k)}{4(b_k + a_k)}
\end{aligned}$$

$= 2.$

Daqui resulta que

$$\begin{aligned} b_{n+1} - a_{n+1} &= \frac{2 + b_n^2}{2b_n} - \frac{4a_n}{2 + a_n^2} \\ &= \frac{(2 + b_n^2).(2 + a_n^2) - 2.4.b_n.a_n}{2b_n(2 + a_n^2)} \\ &= \frac{4 + 2a_n^2 + 2b_n^2 + b_n^2.a_n^2 - 8b_n.a_n}{2b_n(2 + a_n^2)} \\ &= \frac{4 + 2(a_n^2 + b_n^2) + 4 - 8b_n.a_n}{2b_n(2 + a_n^2)} \\ &= \frac{2 + (a_n^2 + b_n^2) + 2 - 4b_n.a_n}{b_n(2 + a_n^2)} \\ &= \frac{4 + (a_n^2 + b_n^2) - 8}{b_n(2 + a_n^2)} \\ &= \frac{-4 + (a_n^2 + b_n^2)}{b_n(2 + a_n^2)} \\ &= \frac{(a_n - b_n)^2}{b_n(2 + a_n^2)} > 0, \, (*) \end{aligned}$$

logo, $a_n < b_n$ para todo número natural n.

Se $I_n = [a_n, b_n]$, então é imediato que $I_{n+1} \subset I_n$, pois (a_n) é crescente e (b_n) é decrescente.

Suponhamos, por absurdo, que $\bigcap\limits_{n \in \mathbb{N}} I_n \neq \{\}$, logo, existe um número racional c tal que

$a_n < c < b_n$, $(**)$

para todo $n \in \mathbb{N}$.

Ora, de $(*)$ resulta

$$b_{n+1} - a_{n+1} \leq \frac{1}{6}(b_n - a_n)^2 \Longrightarrow b_n - a_n \leq \left(\frac{1}{6}\right)^{2^n - 1}. \, (***)$$

De $(**)$ e $(***)$ concluímos que (a_n) e (b_n) são convergentes para o número racional c, contra os resultados estabelecidos no Exemplo 2.25 e no Exemplo 2.26.

Demonstraremos, a seguir, o principal Teorema desta secção que nos dará algumas caracterizações de um corpo ordenado completo.

Teorema 2.14. *As seguintes condições, sobre um mesmo corpo ordenado K, são equivalentes:*

(i) *K é completo;*

(ii) *K é arquimediano e $S_c(K) = S_f(K)$;*

(iii) *toda seqüência crescente e majorada, de elementos de K, é convergente;*

(iv) *K é arquimediano e K satisfaz o axioma dos intervalos encaixantes.*

Demonstração.
$(i) \Longrightarrow (ii)$ Já vimos que todo corpo ordenado completo é arquimediano (Corolário 2.1) e que $S_c(K) \subseteq S_f(K)$ (Lema 2.8). Basta então provar que $S_f(K) \subseteq S_c(K)$.

Seja $(a_n) \in S_f(K)$.

Já vimos que toda seqüência fundamental é limitada (Lema 2.9). Então como (a_n) é limitada e K é completo temos que para todo subconjunto de $\{a_n\}$ existe supremo, ou seja, para cada $n \in \mathbb{N}$ existe $b_n = \sup (a_i)_{i \geq n}$.

É imediato que (b_n) é decrescente e minorada.

Note que (b_n) é o conjunto de todas as seqüências (a_i) e (a_i) é limitada. Dessa forma (b_n) é limitada e, como é decrescente, é também minorada. Além disso, como K é completo existe $a = \inf(b_n)$.

De acordo com o Corolario 2.4, a seqüência (b_n) é convergente para a. Se $\varepsilon \in P^*$ então $\exists p \in \mathbb{N}$ tal que

$$|b_p - a| < \frac{\varepsilon}{3}.$$

Como $a = \inf(b_n)$ temos que $a \leq b_n$, $\forall n \in \mathbb{N}$. Em particular,

$$\begin{aligned} a \leq b_p &\Longrightarrow 0 \leq b_p - a \\ &\Longrightarrow |b_p - a| = b_p - a, \end{aligned}$$

por definição de módulo. Ficamos com:

$$\begin{aligned} |b_p - a| = b_p - a < \frac{\varepsilon}{3} &\Longrightarrow b_p - a + a < a + \frac{\varepsilon}{3} \\ &\Longrightarrow b_p < a + \frac{\varepsilon}{3} \\ &\Longrightarrow a \leq b_p < a + \frac{\varepsilon}{3}. \end{aligned}$$

Logo, para todo $n > p$, temos

$$a \leq b_n < a + \frac{\varepsilon}{3}.$$

Por outro lado, de $b_n = \sup(a_i)_{i \geq n}$ resulta que existe $i_n \geq n$ tal que

$$a - \frac{\varepsilon}{3} < a_{i_n} \leq b_n.$$

Como (a_n) é fundamental, existe $q \in \mathbb{N}$ tal que $|a_m - a_n| < \frac{\varepsilon}{3}$, quaisquer que sejam m e n, com $m > q$ e $n > q$. Pondo-se $n_0 = \max\{p, q\}$ teremos, para todo $n > n_0$:

$$|a_n - a| = |(a_n - a_{i_n}) + (a_{i_n} - b) + (b_n - a)| \leq |(a_n - a_{i_n})| + |(a_{i_n} - b)| + |(b_n - a)|$$

$$|(a_n - a_{i_n})| + |(a_{i_n} - b)| + |(b_n - a)| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.$$

Portanto, $\lim(a_n) = a$ e $(a_n) \in S_c(K)$, de onde vem que, $S_f(K) = S_c(K)$.

$(ii) \Longrightarrow (iii)$ Como o corpo K é arquimediano resulta, conforme o Teorema 2.13, que toda seqüência crescente e majorada é fundamental e, como $S_c(k) = S_f(K)$, concluímos que toda seqüência crescente e majorada é convergente.

$(iii) \Longrightarrow (iv)$ Admitindo-se (iii) resulta que toda seqüência crescente e majorada é fundamental, isso porque toda seqüência convergente é fundamental. Agora, em virtude do Teorema 2.13, K é arquimediano.

Consideremos então uma seqüência $(I_n)_{n\in\mathbb{N}}$ de intervalos fechados de K tal que $I_{n+1} \subset I_n$ e ponha $I_n = [a_n, b_n]$ para todo número natural n. Nestecaso, temos $a_n < b_n$ e em virtude do Teorema 2.12 $a = \lim(a_n) = \sup(a_n)$.

Afirmo: $a \in I_n$, ou seja, $a_n \leq a \leq b_n$, para todo $n \in \mathbb{N}$.

Com efeito temos $a_n \leq a$, pois $a = \sup(a_n)$.

Falta provar que $a \leq b_n$, para todo $n \in \mathbb{N}$. Suponha, por absurdo, que exista $p \in \mathbb{N}$ tal que $b_p < a = \sup(a_n)$ então existe $q \in \mathbb{N}$ tal que $b_p < a_q \leq a$. Pondo-se $r = \max\{p, q\}$ teríamos

$$b_r \leq b_p < a_q \leq a_r \Longrightarrow b_r < a_r,$$

contradição. Portanto o elemento a pertence à interseção de todos os intervalos fechados I_n.

$(iv) \Longrightarrow (i)$ Seja S um subconjunto não vazio e majorado de K. Para K ser completo devemos ter que S admite supremo.

Para cada número natural n consideremos o conjunto

$$B_n = \{j \in \mathbb{N} \,;\, 2^{-n}j \text{ é majorante de} S\};$$

como K é arquimediano resulta que B_n é não vazio, logo, existe $j_n = \min B_n$.

Para cada números n, coloquemos $I_n = [a_n, b_n]$. É imediato que $I_{n+1} \subset I_n$. Portanto, por hipótese, existe um elemento $a \in K$ tal que $a_n \leq a \leq b_n$, $\forall n \in \mathbb{N}$.

Afirmo: $a = \sup S$. Para isso vamos verificar as condições da Definição de supremo.

• Se, por absurdo, existe $s \in S$ com $a < s$ então existe $n \in \mathbb{N}$ tal que

$a_n \leq b_n < s$, pois $a = \inf(b_n)$

e obtemos assim uma contradição, pois (b_n) é majorante de S.

• Se $a' < a$, com $a' \in S$, existe $n \in \mathbb{N}$ tal que $a' < a_n \leq a$, pois $\sup(a_n) = a$ e, neste caso, existe $s \in S$ tal que

$a_n \leq s \leq a \leq b_n$ e temos $a' < s \leq a$;

contradição.

■

Capítulo 3

Corpo dos Números Reais

Realizaremos neste capítulo a construção dos números reais, por intermédio das seqüências fundamentais de números racionais. Este processo se deve a Cantor, criador da Teoria dos Conjuntos.

3.1 Construção do Corpo dos Números Reais

Consideremos o corpo ordenado $\mathbb{Q}$ e seja $S_f(\mathbb{Q})$ o anel das seqüências fundamentais de elementos de $\mathbb{Q}$. Definiremos uma relação $\sim$ sobre $S_f(\mathbb{Q})$ do seguinte modo:

Definição 3.1. Se (a_n) e (b_n) são dois elementos quaisquer de $S_f(\mathbb{Q})$, então $(a_n) \sim (b_n)$ se, e somente se, $(a_n - b_n) \in S_0(\mathbb{Q})$.

Definição 3.2. Lembramos que uma relação R sobre um conjunto E é uma **relação de equivalência** se, e somente se, são válidas as seguintes condições

(E_1): para todo a em E, tem-se aRa (propriedade reflexiva).

(E_2): quaisquer que sejam a e b em E, se aRb, então bRa (propriedade simétrica).

(E_3): quaisquer que sejam a, b e c em E, se aRb e bRc, então aRc (propriedade transitiva).

Teorema 3.1. *A relação $\sim$, introduzida pela Definição 3.1, é uma relação de equivalência sobre o conjunto $S_f(\mathbb{Q})$, que é compatível com a adição e a multiplicação do anel $S_f(\mathbb{Q})$.*

Demonstração.
(E_1): $(a_n) \sim (a_n)$

Como $(a_n - a_n)$ é a seqüência nula temos:

$(a_n - a_n) \in S_0(\mathbb{Q}) \Longrightarrow (a_n) \sim (a_n)$.

(E_2): se $(a_n) \sim (b_n)$ então $(b_n) \sim (a_n)$

$$\begin{aligned}(a_n) \sim (b_n) &\Longrightarrow (a_n - b_n) \in S_0(\mathbb{Q}) \\ &\Longrightarrow -(b_n - a_n) \in S_0(\mathbb{Q}) \\ &\Longrightarrow (b_n) \sim (a_n).\end{aligned}$$

(E_3): Se $(a_n) \sim (b_n)$ e $(b_n) \sim (c_n)$ então $(a_n) \sim (c_n)$.

$(a_n) \sim (b_n) \Longrightarrow (a_n - b_n) \in S_0(\mathbb{Q})$.
$(b_n) \sim (c_n) \Longrightarrow (b_n - c_n) \in S_0(\mathbb{Q})$.

Como $S_0(\mathbb{Q})$ é fechado em relação à soma temos,

$$\begin{aligned}(a_n - b_n) + (b_n - c_n) \in S_0(\mathbb{Q}) &\Longrightarrow (a_n - c_n) \in S_0(\mathbb{Q}) \\ &\Longrightarrow (a_n) \sim (c_n).\end{aligned}$$

Falta verificar que a relação de equivalência sobre o conjunto $S_f(\mathbb{Q})$ é compatível com a adição e a multiplicação do anel $S_f(\mathbb{Q})$.

Se (a_n), (b_n) e (c_n) são elementos quaisquer de $S_f(\mathbb{Q})$ e se $(a_n) \sim (b_n)$ gostaria de provar que

$(a_n + c_n) \sim (b_n + c_n)$ e $(a_n c_n) \sim (b_n c_n)$.

• $(a_n - b_n) = (a_n + c_n) - (b_n + c_n)$.

Como $(a_n) \sim (b_n)$ temos que $(a_n - b_n) \in S_0(\mathbb{Q})$, ou seja,

$(a_n + c_n) - (b_n + c_n) \in S_0(\mathbb{Q}) \Longrightarrow (a_n + c_n) \sim (b_n + c_n)$.

• $(a_n c_n) - (b_n c_n) = (a_n - b_n)c_n$.

Como $(a_n - b_n) \in S_0(\mathbb{Q})$ e $(c_n) \in S_l(\mathbb{Q})$ (Lema 2.9) então pelo Lema 2.5

$(a_n - b_n)c_n \in S_0(\mathbb{Q})$.

■

Corolário 3.1. *Se (a_n), (b_n), (c_n) e (d_n) são elementos quaisquer de $S_f(\mathbb{Q})$ e se $(a_n) \sim (b_n)$ e $(c_n) \sim (d_n)$, então $(a_n + c_n) \sim (b_n + d_n)$ e $(a_n c_n) \sim (b_n d_n)$.*

Demonstração. Pelo teorema anterior temos que:

$(a_n + c_n) \sim (b_n + c_n)$ e $(b_n + c_n) \sim (b_n + d_n)$.

Por $\sim$ ser uma relação de equivalência temos que $(a_n + c_n) \sim (b_n + d_n)$. Da mesma forma, $(a_n c_n) \sim (b_n d_n)$.

■

Se (a_n) é um elemento qualquer de $S_f(\mathbb{Q})$, indicaremos por $\overline{(a_n)}$ a classe de equivalência módulo $\sim$ determinada por (a_n), isto é,

$$\overline{(a_n)} = \{(x_n) \in S_f(\mathbb{Q})\,;\,(x_n) \sim (a_n)\}.$$

Teorema 3.2. *Seja R uma relação de equivalência sobre um conjunto não vazio E e sejam a e b dois elementos quaisquer de E. As seguintes condições são equivalentes entre si:*

(i) $a \equiv b (mod\, R)$*;*

(ii) $a \in \overline{b}$*;*

(iii) $b \in \overline{a}$*;*

(iv) $\overline{a} = \overline{b}$*.*

Demonstração.
• $(i) \Longrightarrow (ii)$ Note que, por definição, $\overline{b} = \{x \in E \,/\, x \equiv b(\text{mod}\, R)\}$ então, por (i), temos que $a \equiv b(\text{mod}\, R)$ o que implica que $a \in \overline{b}$.

• $(ii) \Longrightarrow (iii)$ De (ii) resulta que $a \equiv b(\text{mod}\, R)$, logo pela propriedade simétrica $b \equiv a(\text{mod}\, R)$ e portanto $b \in \overline{a}$.

• $(iii) \Longrightarrow (iv)$ De (iii) resulta que $b \equiv a(\text{mod}\, R)$, então pelas propriedades simétrica e transitiva temos que $x \equiv a(\text{mod}\, R)$ se, e somente se, $x \equiv b(\text{mod}\, R)$, o que implica que $\overline{a} = \overline{b}$.

• $(iv) \Longrightarrow (i)$ Suponha verdadeira $\overline{a} = \overline{b}$, então se $a \in \overline{a}$ teremos $a \in \overline{b}$. Portanto, $a \equiv b(\text{mod}\, R)$.

■

Chamaremos de **conjunto quociente de $S_f(\mathbb{Q})$ pela relação** $\sim$ ao conjunto:

$$\mathbb{R} = \frac{S_f(\mathbb{Q})}{\sim} = \{\overline{(x_n)}; (x_n) \in S_f(\mathbb{Q})\}.$$

Definiremos a soma e o produto de dois elementos quaisquer $\alpha = \overline{(a_n)}$ e $\beta = \overline{(b_n)}$, de $\mathbb{R}$, por meio de

$$\alpha + \beta = \overline{(a_n + b_n)}$$
$$\alpha \cdot \beta = \overline{(a_n b_n)}.$$

De acordo com o Corolário 3.1 é imediato que estas definições não dependem dos representantes (a_n) e (b_n) das classes de equivalência α e β. Ficam assim definidas operações de adição e de multiplicação

$$(\overline{(a_n)}, \overline{(b_n)}) \longmapsto \overline{(a_n + b_n)}$$
$$(\overline{(a_n)}, \overline{(b_n)}) \longmapsto \overline{(a_n b_n)},$$

sobre o conjunto quociente $\mathbb{R} = \dfrac{S_f(\mathbb{Q})}{\sim}$.

Teorema 3.3. *As operações acima definem uma estrutura de corpo sobre o conjunto* $\mathbb{R}$.

Demonstração. Precisamos verificar as condições das Definições 1.10, 1.11, 1.12 e 1.27.

Sejam $\overline{a_n}$, $\overline{b_n}$ e $\overline{c_n} \in \mathbb{R}$.

• (A_1): $(\overline{(a_n)} + \overline{(b_n)}) + \overline{(c_n)} = \overline{(a_n + b_n)} + \overline{(c_n)}$
$= \overline{((a_n + b_n) + c_n)}$
$= \overline{(a_n + (b_n + c_n))}$
$= \overline{(a_n)} + (\overline{(b_n) + (c_n)})$
$= \overline{(a_n)} + (\overline{(b_n)} + \overline{(c_n)})$.

• (A_2): $\overline{(a_n)} + \overline{(b_n)} = \overline{(a_n + b_n)}$
$= \overline{(b_n + a_n)}$
$= \overline{(b_n)} + \overline{(a_n)}$.

• (A_3): Considerando-se a classe de equivalência $\overline{(0)}$, determinada pela seqüência constante (0), temos para todo $\overline{(a_n)} \in \mathbb{R}$,

$\overline{(a_n)} + \overline{(0)} = \overline{(a_n + 0)} = \overline{(a_n)}$.

• (A_4): Considere a classe de equivalência $\overline{(-a_n)}$, então temos

$\overline{(a_n)} + \overline{(-a_n)} = \overline{(a_n - a_n)} = \overline{(0)}$.

Portanto, $\overline{(-a_n)}$ é o oposto de $\overline{(a_n)}$.

• (M_1): $(\overline{(a_n)} \cdot \overline{(b_n)}) \cdot \overline{(c_n)} = \overline{(a_n \cdot b_n)} \cdot \overline{(c_n)}$
$= \overline{((a_n \cdot b_n) \cdot c_n)}$
$= \overline{(a_n \cdot (b_n \cdot c_n))}$
$= \overline{(a_n)} \cdot \overline{(b_n \cdot c_n)}$
$= \overline{(a_n)} \cdot (\overline{(b_n)} \cdot \overline{(c_n)})$.

• (M_2): $\overline{(a_n)} \cdot (\overline{(b_n)} + \overline{(c_n)}) = \overline{(a_n)} \cdot \overline{(b_n + c_n)}$
$= \overline{(a_n \cdot (b_n + c_n))}$

$$= \overline{(a_n \cdot b_n + a_n \cdot c_n)}$$
$$= \overline{(a_n \cdot b_n)} + \overline{(a_n \cdot c_n)}$$
$$= \overline{(a_n)} \cdot \overline{(b_n)} + \overline{(a_n)} \cdot \overline{(c_n)}.$$

• (M_3): $(\overline{(b_n)} + \overline{(c_n)}) \cdot \overline{(a_n)} = \overline{(b_n + c_n)} \cdot \overline{(a_n)}$
$$= \overline{((b_n + c_n) \cdot a_n)}$$
$$= \overline{(b_n \cdot a_n + c_n \cdot a_n)}$$
$$= \overline{(b_n \cdot a_n)} + \overline{(c_n \cdot a_n)}$$
$$= \overline{(b_n)} \cdot \overline{(a_n)} + \overline{(c_n)} \cdot \overline{(a_n)}.$$

• (M_4): $\overline{(a_n)} \cdot \overline{(b_n)} = \overline{(a_n \cdot b_n)}$
$$= \overline{(b_n \cdot a_n)}$$
$$= \overline{(b_n)} \cdot \overline{(a_n)}.$$

• (M_5): Considerando-se a classe de equivalência $\overline{(1)}$, determinada pela seqüência constante (1), temos $\forall\, \overline{(a_n)} \in \mathbb{R}$:

$\overline{(a_n)} \cdot \overline{(1)} = \overline{a_n \cdot 1} = \overline{(a_n)}$

• (M_7): Seja $\overline{(a_n)} \neq \overline{(0)}$, logo, $(a_n) \notin S_0(\mathbb{Q})$ e daqui resulta, em virtude do Lema 2.10, que existe um número natural p tal que $a_n \neq 0$ para todo $n > p$.

Consideremos, então a seqüência $(b_n) \in S(\mathbb{Q})$ definida por

$b_i = 1$ para $i = 0, 1, ..., p$ e $b_n = a_n$ para todo $n > p$.

Note que $(b_n) \in S_f(\mathbb{Q})$ e que $(b_n) \sim (a_n)$, logo $\overline{(a_n)} = \overline{(b_n)}$. De acordo com o Teorema 2.8 a seqüência (b_n) é inversível em $S_f(\mathbb{Q})$ e sua inversa é a seqüência (b_n^{-1}). Como $\overline{(a_n)} = \overline{(b_n)}$, concluimos que $\overline{(a_n)}$ é inversível.

■

Os elementos do corpo $\mathbb{R}$, construído acima, passam a ser denominados números reais e $(\mathbb{R}, +, \cdot)$ é chamado **corpo dos números reais**.

Teorema 3.4. *O subconjunto $\mathbb{Q}'$, de $\mathbb{R}$, formado por todas as classes de equivalência $\overline{(a)}$ onde $a \in \mathbb{Q}$, é um subcorpo de $\mathbb{R}$ e a função $f : \mathbb{Q} \longrightarrow \mathbb{Q}'$ definida por $f(a) = \overline{a}$ é um isomorfismo do corpo $\mathbb{Q}$ dos números racionais no corpo $\mathbb{Q}'$.*

Demonstração. Precisamos verificar as condições da Definição 1.31, para isso vamos utilizar a Proposição 1.10.

• $1 \in \mathbb{Q}$ então $f(1) = \overline{1} \in \mathbb{Q}'$.

• Sejam $a, b \in \mathbb{Q}$ então $a - b \in \mathbb{Q}$ e $a \cdot b \in \mathbb{Q}$ (pois $\mathbb{Q}$ é corpo). Então

$f(a-b) = \overline{a-b} \in \mathbb{Q}'$ e $f(a \cdot b) = \overline{a \cdot b} \in \mathbb{Q}'$.

• Como $\mathbb{Q}$ é corpo temos que para todo $b \in \mathbb{Q}$, $b \neq 0$, existe $b^{-1} \in \mathbb{Q}$ tal que $b \cdot b^{-1} = 1$.

Seja $b \in \mathbb{Q}$, $b \neq 0$. Já vimos que $\overline{1} \in \mathbb{Q}'$ então,

$\overline{1} = f(1) = f(b \cdot b^{-1}) = \overline{b \cdot b^{-1}} = \overline{b} \cdot \overline{b^{-1}}$.

Logo, $(\overline{b})^{-1} = \overline{b^{-1}}$.

Falta provar que $f : \mathbb{Q} \longrightarrow \mathbb{Q}'$ definida por $f(a) = \overline{a}$ é um isomorfismo. Vamos provar primeiro que f é um homomorfismo pela Definição 1.15. Sejam $a, b \in \mathbb{Q}$.

• $f(a+b) = \overline{a+b} = \overline{a} + \overline{b} = f(a) + f(b)$;

• $f(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = f(a) \cdot f(b)$.

Por fim, devemos provar que f é bijetora, para isso vamos utilizar a Proposição 1.8 e a Definição 1.18.

• $N(f) = \{x \in \mathbb{Q}; f(x) = 0\} = \{x \in \mathbb{Q}; \overline{x} = \overline{0}\} = \{0\}$, logo f é injetora.

• $Im(f) = \{f(x); x \in \mathbb{Q}\} = \{\overline{x}; x \in \mathbb{Q}\} = \mathbb{Q}'$, logo f é sobrejetora.

Portanto, f é um isomorfismo do corpo $\mathbb{Q}$ no corpo $\mathbb{Q}'$.

■

A partir de agora, o corpo $\mathbb{Q}$ dos números racionais passa a ser considerado como o corpo primo do corpo $\mathbb{R}$ dos números reais. Em particular, todo número racional é um número real, um número real que não seja racional é denominado número irracional.

Notação: Indiquemos por P_0 (respectivamente, P_0^*) o conjunto de todos os números racionais positivos (respectivamente, estritamente positivos).

Definição 3.3. Diz-se que uma seqüência $(a_n) \in S_f(\mathbb{Q})$ é **estritamente positiva** se, e somente se, existe $M \in P_0^*$ e existe $n_0 \in \mathbb{N}$ tais que $M < a_n$, para todo $n > n_0$.

Lema 3.1. Uma seqüência $(a_n) \in S_f(\mathbb{Q})$ é estritamente positiva se, e somente se, $(a_n) \notin S_0(\mathbb{Q})$ e existe $n_0 \in \mathbb{N}$ tais que $M < a_n$, para todo $n > n_0$.

Demonstração.
($\Longrightarrow$) $(a_n) \in S_f(\mathbb{Q})$ então, existe $M \in P_0^*$ e existe $n_0 \in \mathbb{N}$ tal que

$M < a_n, \forall n > n_0$.

Como $M \in P_0^*$ temos que $0 < M$, logo, por transitividade

$0 < a_n, \forall n > n_0$.

Dessa forma $(a_n) \notin S_0(\mathbb{Q})$.

$(\Longleftarrow)$ É imediato do Lema 2.10.

■

A relação $\sim$ conserva as seqüências estritamente positivas em virtude do seguinte lema.

Lema 3.2. Sejam (a_n) e (b_n) dois elementos quaisquer de $S_f(\mathbb{Q})$. Se $(b_n) \sim (a_n)$ e se (a_n) é estritamente positiva, então (b_n) também é estritamente positiva.

Demonstração. De acordo com a Definição 3.3 existem $M \in P_0^*$ e $p \in \mathbb{N}$ tais que

$M < a_n, \forall n > p$.

Por outro lado de $(b_n) \sim (a_n)$ temos que $(b_n - a_n)$ é convergente a zero, logo, dado $\dfrac{M}{2} \in P_0^*$ existe $q \in \mathbb{N}$ tal que

$$|b_n - a_n| < \frac{M}{2} \Longrightarrow a_n - \frac{M}{2} < b_n < a_n + \frac{M}{2}, \forall n > q.$$

Pondo-se $n_0 = \max\{p, q\}$, teremos para todo $n > n_0$

$$b_n > a_n - \frac{M}{2} > M - \frac{M}{2} = \frac{M}{2}.$$

Portanto, (b_n) é estritamente positiva.

■

Definição 3.4. Diz-se que um **número real** $\alpha = \overline{(a_n)}$, onde $(a_n) \in S_f(\mathbb{Q})$, **é estritamente positivo** se, e somente se, a seqüência (a_n) é estritamente positiva.

O Lema 3.2 nos mostra que esta definição não depende do representante (a_n) da classe de equivalência $\alpha = \overline{(a_n)}$ e o Lema 3.1 nos mostra que α é estritamente positivo, então $\alpha \neq 0$.

Indicaremos por P^* o conjunto de todos os números reais que são estritamente positivos e colocaremos $P = P^* \bigcup \{0\}$. Definiremos uma relação $\leq$, sobre $\mathbb{R}$, do seguinte modo: se α e β são dois números reais quaisquer, então $\alpha \leq \beta$ se, e somente se, $\beta - \alpha \in P$. Portanto, se $\alpha = \overline{(a_n)}$ e se $\beta = \overline{(b_n)}$, temos que $\alpha < \beta$ se, e somente se, $(a_n - b_n)$ não é convergente a zero e existe $n_0 \in \mathbb{N}$ tal que $a_n \leq b_n$ para todo $n > n_0$.

Teorema 3.5. *A relação $\leq$, definida acima, é uma ordem total sobre $\mathbb{R}$ que é compatível com a adição e com a multiplicação.*

Demonstração. Precisamos verificar as condições (I), (II), (III) e (IV) do Teorema 1.7.

(I) $P + P \subset P$.

Sejam $\alpha = \overline{(a_n)}$ e $\beta = \overline{(b_n)}$ dois elementos quaisquer de P.

Se $\alpha = 0$ ou $\beta = 0$, é imediato que $\alpha + \beta \in P$, logo, podemos supor que $\alpha \neq 0$ e $\beta \neq 0$. Neste caso, conforme a Definição 3.3, existem números naturais p e q e existem números racionais $M_1 \in P_0^*$ e $M_2 \in P_0^*$ tais que

$M_1 < a_n$ para todo $n > p$ e

$M_2 < b_n$ para todo $n > q$.

Pondo-se $n_0 = \max\{p, q\}$, teremos para todo $n > n_0$:

$0 < M_1 + M_2 < a_n + b_n$;

portanto, $(a_n + b_n)$ é estritamente positiva e então $\alpha + \beta \in P^*$.

(II) $P \bigcap (-P) = \{0\}$.

Seja $\alpha = \overline{(a_n)}$ um elemento de $P \bigcap (-P)$ e suponhamos que $\alpha \neq 0$.

Como $P = P^* \bigcup \{0\}$ temos que $\alpha \in P^*$ o que resulta, em virtude do Lema 3.1, que existe $p \in \mathbb{N}$ tal que $0 < a_n$ para todo $n > p$.

De $\alpha \in -P$ vem que $-\alpha = (\overline{-a_n}) \in P^*$, logo, existe $q \in \mathbb{N}$ tal que $0 < -a_n$ ou $a_n < 0$, para todo $n > q$.

Tomando-se $n > \max\{p, q\}$ teremos $0 < a_n$ e $a_n < 0$ e chegamos assim a uma contradição.

(III) $P \bigcup (-P) = \mathbb{R}$.

Seja $\alpha = \overline{(a_n)}$ um números real qualquer e suponhamos que $\alpha \notin P$, logo, (a_n) não é convergente a zero. Portanto, de acordo com o Lema 2.11, existe $M \in P_0^*$ e existe $n_0 \in \mathbb{N}$ tais que $a_n < -M$, para todo $n > n_0$, ou seja, $-\alpha \in P^*$ e então $-\alpha \in P$.

(IV) $P \cdot P \subset P$.

Sejam $\alpha = \overline{(a_n)}$ e $\beta = \overline{(b_n)}$ dois elementos quaisquer de P.

Se $\alpha = 0$ ou $\beta = 0$, é imediato que $\alpha \cdot \beta \in P$, logo, podemos supor que $\alpha \neq 0$ e $\beta \neq 0$. Neste caso, temos $\alpha \cdot \beta = \overline{(a_n \cdot b_n)} \neq 0$, ou seja, $(a_n \cdot b_n)$ não é convergente a zero.

Por outro lado, em virtude do Lema 3.1, existem números naturais p e q tais que

$a_n > 0$ para todo $n > p$ e

$b_n > 0$ para todo $n > q$.

Logo, para todo $n > \max\{p, q\}$ teremos $(a_n \cdot b_n) > 0$, ou seja, $(a_n b_n)$ é estritamente positiva.

■

Lema 3.3. O corpo ordenado $\mathbb{R}$ é arquimediano.

Demonstração. De acordo com o Teorema 1.14 basta demonstrar que

se $\alpha = \overline{(a_n)} \in P^*$, então existe um número natural a tal que $\alpha < a$.

Ora, (a_n) é fundamental, logo, é majorada em $\mathbb{Q}$, isto é, existe $M \in P_0^*$ tal que $a_n < M$, para todo $n \in \mathbb{N}$.

Como $\mathbb{Q}$ é arquimediano existe $a \in \mathbb{N}$ tal que $M < a$, portanto, o número natural $a = \overline{(a)}$ é estritamente maior do que $\alpha = \overline{(a_n)}$.

■

Sendo $\mathbb{R}$ um corpo arquimediano, para todo $\varepsilon_1 \in P^*$ existe, em virtude do Corolário 1.9, um número racional $\varepsilon \in P_0^*$ tal que $\varepsilon < \varepsilon_1$. Portanto, para mostrar que uma seqüência $(a_n) \in S(\mathbb{R})$ é fundamental, basta mostrar que, para todo número racional estritamente positivo ε, existe $n_0 \in \mathbb{N}$ tal que $|\alpha_m - \alpha_n| < \varepsilon$, quaisquer que sejam m e n, com $m > n_0$ e $n > n_0$. Vale uma observação análoga para seqüências convergentes de números reais.

Lema 3.4. Se $(a_n) \in S_f(\mathbb{Q})$, então $(a_n) \in S_c(\mathbb{R})$, isto é, toda seqüência fundamental, de números racionais, é convergente para um número real; além disso temos $\lim a_n = \overline{(a_n)}$.

Demonstração. Para todo número racional $\varepsilon \in P_0^*$ existe $n_0 \in \mathbb{N}$ tal que

$|a_m - a_n| < \varepsilon \Longrightarrow a_n - \varepsilon < a_m < a_n + \varepsilon$,

quaisquer que sejam m e n, com $m > n_0$ e $n > n_0$.

Fixemos $p > n_0$ e indiquemos a_p por a. Conforme a identificação de $\mathbb{Q}$ com (Q') (Teorema 3.4), temos

$a + \varepsilon = \overline{(a + \varepsilon)}$ e $a - \varepsilon = \overline{(a - \varepsilon)}$.

Pondo-se $\alpha = \overline{(a_n)}$ e observando-se que $a - \varepsilon < a_m < a + \varepsilon$, para todo $m > n_0$, teremos

$$\overline{(a-\varepsilon)} < \alpha < \overline{(a+\varepsilon)} \Longrightarrow \overline{(-\varepsilon)} < \alpha - \overline{(a)} < \overline{(\varepsilon)}$$
$$\Longrightarrow |\alpha - a_p| = |\alpha - a| = |\alpha - \overline{(a)}| < \overline{(\varepsilon)} = \varepsilon.$$

Em resumo, dado $\varepsilon \in P_0^*$ existe $n_0 \in \mathbb{N}$ tal que $|\alpha - a_p| < \varepsilon$, para todo $p > n_0$. Portanto, $\lim a_n = \alpha$.

■

Teorema 3.6. *O corpo ordenado $\mathbb{R}$ dos números reais é completo.*

Demonstração. O Lema 3.3 nos mostra que $\mathbb{R}$ é arquimediano. Portanto, em virtude do Teorema 2.14, precisamos demonstrar que $S_f(\mathbb{R}) = S_c(\mathbb{R})$.

Seja (α_n) uma seqüência fundamental de números reais. De acordo com o Teorema 2.9, existe, para cada $n \in \mathbb{N}$, uma seqüência crescente $(a_{i,n})_{i\in\mathbb{N}}$ que é convergente para α_n, logo, para todo $\varepsilon \in P_0^*$ existe um menor número natural i tal que

$$|a_{i,n} - \alpha_n| < \frac{\varepsilon}{3}$$

e para este índice i colocaremos $b_n = a_{i,n}$. Obtemos, deste modo, uma seqüência (b_n) de números racionais tal que

$$|b_n - \alpha_n| < \frac{\varepsilon}{3},$$

para todo $n \in \mathbb{N}$. Mostraremos, inicialmente, que esta seqüência é fundamental. Com efeito, como (α_n) é fundamental, existe $n_0 \in \mathbb{N}$ tal que

$$|\alpha_m - \alpha_n| < \frac{\varepsilon}{3},$$

quaisquer que sejam m e n, com $m > n_0$ e $n > n_0$. Portanto, se m e n são dois números naturais quaisquer, com $m > n_0$ e $n > n_0$, teremos

$$|b_m - b_n| \leq |b_m - \alpha_m| + |\alpha_m - \alpha_n| + |\alpha_n - b_n| < 3.\frac{\varepsilon}{3} = \varepsilon,$$

ou seja, (b_n) é fundamental. Conforme o lema anterior, (b_n) é convergente para $\alpha = \overline{(b_n)}$, logo, existe $n_1 \in \mathbb{N}$ tal que

$$b_n - \alpha < 2.\frac{\varepsilon}{3},$$

para todo $n > n_1$. Por outro lado, tem-se

$$|\alpha_n - \alpha| \leq |\alpha_n - b_n| + |b_n - \alpha| < \frac{\varepsilon}{3} + |b_n - \alpha|.$$

para todo $n \in \mathbb{N}$. Portanto, qualquer que seja $n > n_1$, teremos

$$|\alpha_n - \alpha| < \frac{\varepsilon}{3} + 2.\frac{\varepsilon}{3} = \varepsilon,$$

isto é, (α_n) é convergente para α.

■

Para demonstrar que o corpo $\mathbb{R}$ dos números reais só pode ser ordenado de um único modo daremos, inicialmente, o seguinte lema.

Lema 3.5. Para todo número real positivo a existe um único número real positivo b tal que $b^2 = a$.

Demonstração. O lema é imediato se $a = 0$, logo, podemos supor que $a \in P^*$. Se b e c são números reais positivos tais que

$$b^2 = a = c^2 \Longrightarrow b^2 - c^2 = (b-c)\cdot(b+c) = a - a = 0;$$

para isso devemos ter $(b-c) = 0$ ou $(b+c) = 0$, de onde vem, $b = c$ ou $b = -c$. Note que esta segunda igualdade não ocorre já que devemos ter $a,\ b \in P^*$. Logo, $b = c$.

Agora devemos provar que existe b tal que $b^2 = a$. Considere, então, o conjunto

$$S = \{x \in R \,/\, 0 \leq x \text{ e } x^2 \leq a\}.$$

É imediato que S é não vazio ($0 \in S$) e majorado (por $a+1$), logo, de acordo com o Teorema anterior , existe $b = \sup S$ e com isso temos que $0 < b$.

Afirmo: $b^2 = a$. Suponha, por absurdo, que $b^2 \neq a$. Temos dois casos a serem considerados:

• $b^2 < a$. Note que,

$$\begin{aligned}(a+b^2)\cdot b &= a\cdot b + b^3 \\ &= a\cdot b + b\cdot b^2 < a\cdot b + a\cdot b = 2\cdot ab.\end{aligned}$$

Seja $\dfrac{2\cdot ab}{a+b^2} = b_1$, então $b < b_1$. Por outro lado,

$$\begin{aligned}b_1^2 &= \frac{4a^2b^2}{(a+b^2)^2} \\ &= \frac{4a^2b^2}{a^2+2ab^2+b^4} \\ &= \frac{4a^2b^2}{(a-b^2)^2+4ab^2}.\end{aligned}$$

Afirmo: $\dfrac{4a^2b^2}{(a-b^2)^2+4ab^2} \leq a$.

Suponha, por absurdo, que $\dfrac{4a^2b^2}{(a-b^2)^2+4ab^2} > a$.

$$\begin{aligned}\frac{4a^2b^2}{(a-b^2)^2+4ab^2} > a &\Longrightarrow \frac{4a^2b^2}{(a-b^2)^2+4ab^2} - a > 0 \\ &\Longrightarrow \frac{4a^2b^2 - a(a-b^2)^2 - 4a^2b^2}{(a-b^2)^2+4ab^2} > 0\end{aligned}$$

$$\Longrightarrow \frac{-a(a-b^2)^2}{(a-b^2)^2+4ab^2} > 0$$

$$\Longrightarrow \frac{a(a-b^2)^2}{(a-b^2)^2+4ab^2} < 0$$

Mas, note que:

$0 < b \Longrightarrow 0 < b^2$.

Como $b^2 < a$ e $0 < b^2$, temos que $0 < a$. Além disso, temos que $0 < a - b^2$.

Então, pela Regra dos Sinais, temos que

$$\frac{a(a-b^2)^2}{(a-b^2)^2+4ab^2} > 0.$$

Contradição, ou seja, $b_1 = \dfrac{4a^2b^2}{(a-b^2)^2+4ab^2} \leq a$.

Logo, $b_1 \in S$, o que é absurdo pois $b_1 > b = \sup S$.

• $a < b^2$. Note que $a + b^2 < b^2 + b^2 = 2b^2$.

Seja $\dfrac{a+b^2}{2b} = b_2$, então $b_2 < b$. Por outro lado,

$$\begin{aligned} b_2^2 &= \frac{(a+b^2)^2}{4b^2} \\ &= \frac{a^2+2ab^2+b^4}{4b^2} \\ &= \frac{(a-b^2)^2+4ab^2}{4b^2}. \end{aligned}$$

Afirmo: $\dfrac{(a-b^2)^2+4ab^2}{4b^2} \geq a$.

A verificação deste fato é análoga a anterior.

Assim, $b_2^2 \geq a$ o que é absurdo pois $b_2 < b = \sup S$.

■

Se a é um número real positivo, então, o único número real positivo b tal que $b^2 = a$ é denominado raiz quadrada de a e será indicado pela notação $\sqrt{a}$. O lema acima nos mostra que todo número real positivo admite uma única raiz quadrada positiva.

Deste lema resulta, imediatamente, que o conjunto P dos elementos positivos, de $\mathbb{R}$, pela ordem $\leq$, coincide com o conjunto dos quadrados dos números reais. Portanto, a ordem $\leq$ é determinada de modo único e temos o seguinte teorema.

Teorema 3.7. *O corpo $\mathbb{R}$ dos números reais só pode ser ordenado de um único modo.*

A única ordem total, compatível com a estrutura de corpo definida sobre $\mathbb{R}$, passa a ser denominada ordem habitual dos números reais. Notemos que se a e b são dois números reais quaisquer, temos $a < b$ se, e somente se, existe um número real c tal que $b - a = c^2$.

Definição 3.5. Um **automorfismo** de um corpo K, é, por definição, um isomorfismo do corpo K nele próprio.

Teorema 3.8. *O único automorfismo do corpo $\mathbb{R}$ dos números reais é o automorfismo idêntico.*

Demonstração. Seja f um automorfismo de $\mathbb{R}$ e mostremos, inicialmente, que se a é um número real positivo, então $f(a)$ também é positivo. Isto é imediato, pois conforme o Lema 3.5, existe $b \in \mathbb{R}$ tal que $a = b^2$, de onde vem, $f(a) = (f(b))^2$ e então $f(a) > 0$. Consideremos agora o subconjunto

$$M = \{x \in \mathbb{R}; f(x) = x\}.$$

É fácil verificar que M é um subcorpo de R, logo $M \subset \mathbb{R}$.

Afirmamos que $M = \mathbb{R}$, ou seja, que f é um automorfismo idêntico de $\mathbb{R}$.

Com efeito, se $M \neq \mathbb{R}$ existe $a \in \mathbb{R}$ tal que $f(a) \neq a$ e suponhamos que $a < f(a)$ (se $f(a) < a$, a demonstração é análoga). De acordo com o Teorema 1.14, existe $r \in \mathbb{Q}$ tal que $a < r < f(a)$.

$a < r \Longrightarrow 0 < r - a \Longrightarrow 0 < f(r - a) = f(r) - f(a)$,

ou, $f(a) < f(r) = r$ o que está em contradição com $r < f(a)$.

■

3.2 Caracterizações do Corpo $\mathbb{R}$ dos Números Reais

Seja K um corpo ordenado pela ordem $\leq$. Indicaremos por 1_K o elemento unidade de K e por K_0 seu corpo primo.

Já sabemos que todo elemento de K_0 é da forma $\dfrac{m.1_K}{n.1_K}$, com m e n inteiros e $n \neq 0$.

Pondo-se $a = \dfrac{m}{n}$, escreveremos $a.1_K = \dfrac{m.1_K}{n.1_K}$, portanto, todo elemento de K_0 é da forma $a \cdot 1_K$, com $a \in \mathbb{Q}$.

Além disso, a função σ, de K_0 em $\mathbb{Q}$, definida por $\sigma(a) = a.1_K$, é um isomorfismo ordenado de K_0 em $\mathbb{Q}$. Se $(a_n.1_K) \in S(K_0)$, com $(a_n) \in S(\mathbb{Q})$, colocaremos, por definição,

$$\sigma((a_n.1_K)) = (a_n).$$

É fácil verificar que σ é um isomorfismo de $S(K_0)$ em $S(\mathbb{Q})$ e que $\sigma(S_f(K_0)) = S_f(\mathbb{Q})$, ou seja, σ transforma toda seqüência fundamental de elementos de K_0, numa seqüência fundamental de elementos de $\mathbb{Q}$.

Teorema 3.9. *Todo corpo arquimediano é ordenadamente isomorfo a um subcorpo do corpo dos números reais.*

Demonstração. Seja K um corpo arquimediano. De acordo com o Teorema 2.9, todo elemento α, de K, é limite de uma seqüência $(a_n 1_k) \in S_0(K)$, logo, esta seqüência é fundamental e então (a_n) também é fundamental. Conforme o Lema 3.4 esta seqüência (a_n) é convergente em $\mathbb{R}$ e $\lim a_n = \overline{(a)}$.

Consideremos, então, a aplicação g, de K em $\mathbb{R}$, que a todo $\alpha = \lim(a_n 1_k) \in K$ faz corresponder o número real $g(\alpha) = \lim a_n = \overline{(a_n)}$.

Se α e β são dois elementos quaisquer de K, tem-se

$\alpha = \lim(a_n 1_k)$ e $\beta = \lim(b_n 1_k)$,

com $(a_n) \in S_f(K)$ e $(b_n) \in S_f(K)$. Logo,

$\alpha + \beta = \lim((a_n + b_n)1_k)$ e

$\alpha\beta = \lim((a_n b_n)1_k)$,

de onde vem,

$g(\alpha + \beta) = \lim(a_n + b_n) = \lim a_n + \lim b_n = g(\alpha) + g(\beta)$ e

$g(\alpha\beta) = \lim(a_n b_n) = \lim a_n \cdot \lim b_n = g(\alpha) \cdot g(\beta)$.

Portanto, g é homomorfismo de K em $\mathbb{R}$ e como g não é a função nula resulta que g é um monomorfismo de K em $\mathbb{R}$. Além disso, é fácil ver que g é um monomorfismo ordenado.

■

Teorema 3.10. *Todo corpo ordenado completo é ordenadamente isomorfo ao corpo dos números reais.*

Demonstração. Suponhamos agora que o corpo K seja completo, logo, conforme o Corolário 2.1, K é arquimediano.

Consideremos, então, o monomorfismo ordenado g, de K em $\mathbb{R}$, definido anteriormente. Se $\alpha = (a_n)$ é um número real qualquer, onde $(a_n) \in S_f(K)$, então $(a_n 1_k) \in S_f(K_0)$ e como K é completo esta seqüência é convergente para $\alpha' \in K$ e é imediato que $g(\alpha) = \alpha'$.

■

Corolário 3.2. *Dois corpos ordenados completos são ordenadamente isomorfos.*

Demonstração. Sejam K_1 e K_2 dois corpos ordeandos completos então pelo teorema 3.10 temos que K_1 e K_2 são isomorfos ao corpo dos números reais; logo K_1 e K_2 são ordenadamente isomorfos.

■

Referências Bibliográficas

[1] ÁVILA, Geraldo - *Introdução à Análise Matemática*. Editora Edgard Blücher, São Paulo, 1993.

[2] ÁVILA, Geraldo - *Análise Matemática Para Licenciatura*. Editora Edgard Blücher, São Paulo, 2005.

[3] DOMINGUES, Hygino H.; IEZZI, Gelson - *Introdução à Álgebra*. Atual Editora, São Paulo, 1976.

[4] HEFEZ, Abramo - *Curso de Álgebra*. Volume 1, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1993.

[5] JR., Frank Ayres - *Álgebra Moderna*. Coleção Schaum, Ed. Mc. Graw-Hill do Brasil, 1974.

[6] MONTEIRO, L.H. Jacy - *Elementos de Álgebra*. 2ª edição, LTC, Rio de Janeiro, 1978.