UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
Departamento de Matemática

Monografia de Especialização

O Teorema do Eixo Principal para Corpos Arbitrários

Rildo Nascimento de Oliveira

Orientador: Csaba Schneider

2016

Rildo Nascimento de Oliveira

O Teorema do Eixo Principal para Corpos Arbitrários

Monografia de especialização apresentada ao curso Especialização em Matemática para Professores, do Instituto de Ciências Exatas da UFMG, Departamento de Matemática, como requisito para obtenção do título de Especialista.

Orientador: Csaba Schneider

Belo Horizonte, 2016

Rildo Nascimento de Oliveira

O Teorema do Eixo Principal para Corpos Arbitrários

Prof. Csaba Schneider (orientador) (UFMG).

Prof.(a) Jussara de Matos Moreira (UFMG).

Prof. Remy de Paiva Sanchis (UFMG).

Belo Horizonte, 06 de julho 2016

Dedicado a Daniel *(in memoriam)*.

AGRADECIMENTOS

- A Deus.
- Ao Professor Csaba. Pela paciência. Por ter acreditado que eu conseguiria.
- A minha família.

Veja bem, a verdadeira matemática não tem nada a ver com aplicações, nem com procedimentos de cálculo que se aprendem na escola. Ela estuda constructos intelectuais abstratos que, pelo menos enquanto o matemático está ocupado com eles, não entram de forma alguma em contato com o mundo físico, sensível.(Tio Petros - livro: Tio Petros e a Conjectura de Goldbach - p. 27-28).

RESUMO

Nosso objetivo nesse trabalho é verificar para quais corpos, diferentes de $\mathbb{R}$, o Teorema do Eixo Principal é válido. Ou seja, classificar os corpos que preservam a Propriedade do Eixo Principal. Para isso serão definidos os conceitos de corpos e corpos ordenados. Vamos provar o Axioma da Escolha. Definiremos um corpo formalmente real. Vamos definir pré-ordenação. Mostraremos, através do Lema da Extenção, que uma pré-ordenação pode ser extendida até obter uma ordenação. Mostraremos, ainda, que um corpo pode ser munido de várias ordenações. Vamos provar o Teorema de Artin-Schreier. Vamos definir um corpo pitagórico. Vamos definir, também, um corpo real fechado. Finalmente apresentamos uma caracterização dos corpos que preservam a Propriedade do Eixo Principal.

Palavras chaves: Conjuntos, corpo: ordenado, formalmente real, pitagórico, real fechado. Eixo principal, matrizes, diagonalização, ortogonalização, ortonormalização, autovalores, autovetores.

ABSTRACT

Sumário

Introdução

Como está bem conhecido, uma matriz simétrica com entradas reais é diagonalizável por uma matriz ortogonal. Esse teorema é conhecido como o Teorema do Eixo Principal. Nosso objetivo, nesse trabalho, é verificar para quais corpos o Teorema do Eixo Principal é válido. No Capítulo 1 introduzimos o conceito de matriz diagonal e definimos uma matriz ortogonal. Enuciamos o Teorema do Eixo Principal. Estabelecemos um processo para diagonalizar ortogonalmente uma matriz simétrica sobre $\mathbb{R}$. Através de alguns exemplos, mostramos que o Teorema do Eixo Principal não é válido para vários corpos diferentes de $\mathbb{R}$. Com os exemplos apresentados é possível detectar os principais problemas que impedem um corpo arbitrário, $\mathbb{K}$, de preservar a Propriedade do Eixo Principal. Finalizamos o Capitulo 1 com o problema levantado por Friedberg em [6] que pede para classificar, exatamente, os corpos para os quais o Teorema do Eixo Principal é válido. No Capitulo 2 definimos uma estrutura de corpo e provamos suas principais propriedades, como consequência direta da definição. Definimos, ainda, o que é uma relação de ordem e suas principais propriedades. Assim podemos definir uma estrutura de corpo ordenado. No Capitulo 3 enuciamos o polêmico Axioma da Escolha. Provamos a equivalência entre o Axioma da Escolha, o Lema de Zorn e o Teorema de Zermelo. No Capitulo 4, definimos corpo formalmente real. Mostramos através de Proposição 4.3 que um corpo ordenado está definido por seus elementos positivos. Mostramos que um corpo pode ter mais de uma ordenação. Definimos pré-ordenação e mostramos suas principais propriedades. Através do Lema da Extenção, mostramos que uma pré-ordenação pode ser estendida até obtermos uma ordenação. Enuciamos e provamos o Teorema de Artin-Schreier que nos leva a concluir que as afirmações seguintes são equivalentes:

(i) $\mathbb{K}$ é um corpo formalmente real;

(ii) $\mathbb{K}$ possui uma pré-ordenação;

(iii) $\mathbb{K}$ possui pelo menos uma ordenação.

Finalmente no Capitulo 5 definimos corpo pitagórico. Definimos, também, um produto interno sobre um corpo ordenado. Definimos corpo real fechado. Com as ferramentas desenvolvidas estamos, então prontos para responder a questão levantada em Capitulo 1.

Capítulo 1

Diagonalização de Matrizes Simétricas

Dizemos que uma matriz $M_{n\times n}$ é uma *matriz diagonal* se todas as entradas, fora da diagonal principal, de M são nulas. Assim a matriz

$$M = \begin{pmatrix} m_1 & 0 & \cdots & 0 \\ 0 & m_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & m_n \end{pmatrix}$$

é uma matriz diagonal.

Definição 1.1 (Matriz Ortogonal)**.** Seja M uma matriz quadrada. Se $M^{-1} = M^t$, então, neste caso, diremos que a matriz M é uma *matriz ortogonal*.

Se M é uma matriz quadrada e existem matrizes, P ortogonal e D diagonal, tais que $D = P^tMP$, diremos que P *diagonaliza ortogonalmente* M. Neste caso M é dita diagonalizável ortogonalmente. Normalmente uma matriz M é dita diagonalizável se existe uma matriz P invertivel, tal que $P^{-1}MP$ é diagonal. No entanto matrizes diagonalizáveis, neste sentido, não aparecem neste texto. Portanto nos usaremos a palavra *diagonalizável* como sinónimo da palavra *ortogonalmente diagonalizável*. Portanto a matriz M é semelhante ortogonalmente a uma matriz diagonal. Chamamos o processo de encontrar as matrizes P e D de *diagonalização de matrizes*. O Teorema do Eixo Principal incluído em vários textos de algebra linear escritos para graduação, afirma que toda matriz simétrica sobre o corpo dos números reais é ortogonalmente semelhante a uma matriz diagonal.

Teorema 1.2 (Teorema do Eixo Principal)**.** *Seja M uma matriz quadrada simétrica sobre o corpo dos números reais. Então existe uma matriz P ortogonal, tal que $D = P^tMP$ é diagonal.*
□

Um procedimento para diagonalizar ortogonalmente uma matriz simétrica M consiste em:

(1º): Determine os autovalores, $\lambda_1, \ldots, \lambda_n$, de M;

(2º): Encontre os autovetores $v_1, \ldots, v_n$ associados aos autovalores $\lambda_1, \ldots, \lambda_n$. É conhecido que se $\lambda_i \neq \lambda_j$, então v_i e v_j são ortogonais. Se $\lambda_i = \lambda_j$, então usando o processo de ortogonalização de Gran-Schmidt podemos escolher v_i e v_j, tal que eles sejam ortogonais. Logo podemos assumir sem perder generalidade que $v_1, \ldots, v_n$ é um sistema ortogonal. Normalizando os vetores $v_1, \ldots, v_n$, podemos assumir, sem perca de geneneralidade, que $u_1, \ldots, u_n$ é um sistema de vetores *ortonormais*;

(3º): Forme a matriz P com os vetores coluna $u_1, \ldots, u_n$;

(4º): A matriz $D = P^t M P$ será diagonal com entradas $\lambda_1, \ldots, \lambda_n$ na diagonal principal, onde λ_i é o autovalor associado ao autovetor u_i, para $i = 1, \ldots, n$.

Exemplo 1.3. Diagonalizar ortogonalmente a matriz $M = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 2 \\ 2 & 2 & 4 \end{pmatrix}$ sobre $\mathbb{R}$.

Solução. Primeiro passo (determinar os autovalores de M): os autovalores de M são as raízes do polinômio

$$\begin{aligned}
p(t) &= \det(M - tI_3) \\
&= \det\left(\begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 2 \\ 2 & 2 & 4 \end{pmatrix} - t\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \\
&= \det\begin{pmatrix} 4-t & 2 & 2 \\ 2 & 4-t & 2 \\ 2 & 2 & 4-t \end{pmatrix} \\
&= (4-t)\det\begin{pmatrix} 4-t & 2 \\ 2 & 4-t \end{pmatrix} - 2\det\begin{pmatrix} 2 & 2 \\ 2 & 4-t \end{pmatrix} + 2\det\begin{pmatrix} 2 & 4-t \\ 2 & 2 \end{pmatrix} \\
&= (4-t)((4-t)^2 - 4) - 2(2(4-t) - 4) + 2(4 - 2(4-t)) \\
&= (4-t)(16 - 8t + t^2 - 4) - 2(8 - 2t - 4) + 2(4 - 8 + 2t) \\
&= (4-t)(t^2 - 8t + 12) - 16 + 4t + 8 + 8 - 16 + 4t \\
&= (4-t)(t^2 - 8t + 12) + 8t - 16 \\
&= 4t^2 - 32t + 48 - t^3 + 8t^2 - 12t - 16 + 8t \\
&= -t^3 + 12t^2 - 36t + 32 \\
&= -t^3 + 10t^2 - 16t + 2t^2 - 20t + 32 \\
&= t(-t^2 + 10t - 16) - 2(-t^2 + 10t - 16) \\
&= (t-2)(-t^2 + 10t - 16).
\end{aligned}$$

Logo temos que resolver a equação $(t-2)(-t^2 + 10t - 16) = 0$ e, portanto uma das raízes será $t_1 = 2$. As outras raízes são dadas pela equação $-t^2 + 10t - 16 = 0$ que pode ser resolvida através da formula quadrática, assim:

$$t = \frac{-10 \pm \sqrt{10^2 - 4 \cdot (-1) \cdot (-16)}}{2 \cdot (-1)} = \frac{-10 \pm \sqrt{36}}{-2} = \frac{-10 \pm 6}{-2}$$

e, portanto, $t_2 = 2$ e $t_3 = 8$. Portanto os autovalores de M são $\lambda_1 = \lambda_2 = 2$ e $\lambda_3 = 8$.
Segundo passo (determinar os autovetores associados a $\lambda_1, \lambda_2, \lambda_3$): precisaremos resolver os sitemas $(M - \lambda_1 I_3)X = \bar{0}$ e $(M - \lambda_3 I_3)X = \bar{0}$. Assim $(M - \lambda_1 I_3)X = \bar{0}$ é equivalente à equação matricial

$$\left(\begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 2 \\ 2 & 2 & 4 \end{pmatrix} - \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}\right) \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

que pode ser escrita como

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Assim precisaremos resolver a seguinte equação linear homogênio:

$$2x_1 + 2x_2 + 2x_3 = 0 \tag{1.1}$$

cuja solução geral é $x_1 = \alpha$ e $x_2 = \beta$ com α e β reais e, portanto, $x_3 = -\alpha - \beta$. Logo, $\mathbb{V}_1 = \{(\alpha, \beta, -\alpha - \beta) \mid \alpha, \beta \in \mathbb{R}\}$ é o conjunto de todos os autovetores associados aos autovalores $\lambda_1 = \lambda_2 = 2$. Analogamente obtemos $\mathbb{V}_2 = \{(\alpha, \alpha, \alpha) \mid \alpha \in \mathbb{R}\}$ que é o conjunto de todos os autovetores associados ao autovalor $\lambda_3 = 8$. Seja $(\alpha, \beta, -\alpha - \beta) = \alpha(1, 0, -1) + \beta(0, 1, -1)$, assim os vetores $v_1 = (1, 0, -1)$ e $v_2 = (0, 1, -1)$ geram $\mathbb{V}_1$ e são $L.I.$ (ou seja um não é múltiplo escalar do outro). Agora vamos aplicar o processo de Gram-Schmidt aos vetores v_1 e v_2 para encontrarmos vetores ortonormais associados ao autovalor $\lambda_1 = 2$. Uma descrição detalhada do processo de Gram-Schmidt pode ser encontrada em Capítulo 5. Seja $w_1 = v_1 = (1, 0, -1)$, então

$$\begin{aligned} w_2 &= v_2 - \frac{\langle v_2, w_1 \rangle}{\langle w_1, w_1 \rangle} w_1 \\ &= (0, 1, -1) - \frac{(0, 1, -1)(1, 0, -1)}{(1, 0, -1)(1, 0, -1)}(1, 0, -1) \\ &= (0, 1, -1) - \frac{(0 \cdot 1 + 1 \cdot 0 + (-1)(-1))}{1^2 + 0^2 + (-1^2)}(1, 0, -1) \\ &= (0, 1, -1) - \left(\frac{1}{2}, 0, \frac{-1}{2}\right) \\ &= \left(-\frac{1}{2}, 1, -\frac{1}{2}\right). \end{aligned}$$

Os vetores w_1 e w_2 são ortogonais. Agora vamos normalizar w_1 e w_2. Seja

$$u_1 = \frac{w_1}{\|w_1\|} = \frac{(1, 0, -1)}{\sqrt{1^2 + 0^2 + (-1)^2}} = \frac{1}{\sqrt{2}}(1, 0, -1) = \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right)$$

e $u_2 = \frac{w_2}{\|w_2\|} = \left(-\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}}\right)$. Os vetores u_1 e u_2 são ortonormais. Seja $(\alpha, \alpha, \alpha) = \alpha(1, 1, 1)$, assim o vetor $v_3 = (1, 1, 1)$ gera $\mathbb{V}_2$. Sabe-se que dois autovetores de uma matriz simétrica real com autovalores distintos são ortogonais. Logo v_3 é ortogonal a u_1 e a u_2.

Normalizando v_3 obtemos $u_3 = \frac{v_3}{\|v_3\|} = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right)$.
Terceiro passo (formar a matriz a P): as colunas da matriz P são os vetores u_1, u_2, u_3. Portanto:

$$P = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{pmatrix}$$

Quarto passo: A matriz $P^tMP = D$ é uma matriz diagonal, como queríamos.

Em geral o processo de encontrar a matriz P que diagonaliza ortogonalmente uma matriz simétrica M com entradas reais é feito como no Exemplo 1.3. Stephen H. Friedberg em [6], concentrando a atenção em corpos diferentes de $\mathbb{R}$, mostra que existem matrizes simétricas sobre tais corpos que não são ortogonalmente semelhantes a uma matriz diagonal.

Exemplo 1.4. Diagonalizar ortogonalmente a matriz simétrica $Z = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$ sobre $\mathbb{C}$.

Solução. Determinamos primeiro os autovalores da matriz Z. Os autovalores da matriz Z são as raízes do polinômio

$$\begin{aligned} p(t) &= \det(Z - tI_2) \\ &= \det\left(\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix} - \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}\right) \\ &= \det\begin{pmatrix} 1-t & i \\ i & -(1+t) \end{pmatrix} \\ &= -(1-t)(1+t) - i^2 = -(1-t^2) - (-1) = t^2 - 1 + 1 = t^2. \end{aligned}$$

Logo para encontrar os autovalores da matriz Z temos que encontrar as raízes da equação $t^2 = 0$ e, portanto, $t = 0$. Logo os autovalores da matriz Z são $\lambda_1 = \lambda_2 = 0$. Se Z fosse ortogonalmente diagonalizável ela seria semelhante a uma matriz diagonal cujas entradas na diagonal principal são os autovalores de Z. No entanto, os autovalores de Z são ambos iguais a zero. Então, neste caso, Z seria semelhante à matriz nula, que é um absurdo. Essa contradição nos leva a concluir que o Teorema do Eixo Principal não é válido em $\mathbb{C}$.

Exemplo 1.5. Diagonalizar ortogonalmente a matriz simétrica $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ sobre $\mathbb{Q}$.

Solução. Determinamos os autovalores da matriz Q. Os autovalores da matriz Q são as raízes do polinômio:

$$\begin{aligned} p(t) &= \det(Q - tI_2) \\ &= \det\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}\right) \\ &= \det\begin{pmatrix} 1-t & 1 \\ 1 & -t \end{pmatrix} \\ &= -t(1-t) - 1 = t^2 - t - 1. \end{aligned}$$

Logo para encontrar os autovalores da matriz Q temos que encontrar as raízes da equação $t^2 - t - 1 = 0$. Aplicando a formula quadrática obtemos:

$$t = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}. \tag{1.2}$$

Logo as soluções de (1.2) não pertencem ao conjunto $\mathbb{Q}$ e, portanto, os autovalores da matriz Q não pertencem ao conjunto $\mathbb{Q}$. Assim a matriz simétrica Q não é diagonalizável sobre $\mathbb{Q}$. Assim o Teorema do Eixo Principal não é válido em $\mathbb{Q}$.

Exemplo 1.6. Diagonalizar ortogonalmente a matriz simétrica $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ sobre $\mathbb{Z}_2$.

Solução. Determinamos os autovalores da matriz B. Os autovalores de B são as raízes do polinômio:

$$\begin{aligned} p(t) &= \det(B - tI_2) \\ &= \det(\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}\right) \\ &= \det \begin{pmatrix} 1-t & 1 \\ 1 & -t \end{pmatrix} \\ &= -t(1-t) - 1 = t^2 - t - 1. \end{aligned}$$

Logo para encontrar os autovalores da matriz B temos que encontrar as raízes do polinômio $p(t) = t^2 - t - 1$ sobre $\mathbb{Z}_2$. No entanto, $p(0) = -1$ e $p(1) = -1$. Logo $p(t)$ não tem raízes em $\mathbb{Z}_2$ e, portanto, a matriz B não tem autovalores. Assim a matriz B não pode ser diagonalizada ortogonalmente sobre $\mathbb{Z}_2$. Portanto, o Teorema do Eixo Principal não é válido em $\mathbb{Z}_2$.

Exemplo 1.7.

Observação 1.8. Existe em $\mathbb{Z}_p$ (p é primo e ímpar) um elemento que não é quadrado. Definimos a aplicação:

$$\begin{aligned} \psi : \mathbb{Z}_p &\to \mathbb{Z}_p; \\ x &\mapsto x^2. \end{aligned}$$

A aplicação ψ, assim definida, não é injetiva. De fato: se $a \in \mathbb{Z}_p$, então $\psi(a) = \psi(-a)$. Logo ψ não é sobrejetiva. Assim existe um elemento, $b \in \mathbb{Z}_p$, tal que $b \neq 0, 1$ e b não é um quadrado em $\mathbb{Z}_p$. Seja $b \in \mathbb{Z}_p$ um tal elemento, tal que $b - 1$ é um quadrado em $\mathbb{Z}_p$ logo $a^2 = b - 1$.

Diagonalizar ortogonalmente a matriz $T = \begin{pmatrix} 1 & \frac{a}{2} \\ \frac{a}{2} & 0 \end{pmatrix}$ sobre $\mathbb{Z}_p$ com p primo ímpar.

Solução. Determinamos os autovalores da matriz T. Os autovalores da matriz T são as

raízes do polinômio:

$$\begin{aligned} p(t) &= \det(T - tI_2) \\ &= \det\left(\begin{pmatrix} 1 & \frac{a}{2} \\ \frac{a}{2} & 0 \end{pmatrix} - \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}\right) \\ &= \det\begin{pmatrix} 1-t & \frac{a}{2} \\ \frac{a}{2} & -t \end{pmatrix} \\ &= (1-t)(-t) - \left(\frac{a}{2}\right)^2 = t^2 - t - \frac{a^2}{4}. \end{aligned}$$

Logo para encontrar os autovalores da matriz T temos que encontrar as raízes do polinômio

$$p(t) = t^2 - t - \frac{a^2}{4} \tag{1.3}$$

sobre $\mathbb{Z}_p$. Assim as raízes de (1.3) são dadas por:

$$t = \frac{1 \pm \sqrt{1+a^2}}{2} = \frac{1 \pm \sqrt{b}}{2}.$$

Como, por Observação 1.8, b foi escolhido, tal que não existe $\sqrt{b}$, a matriz T, embora seja simétrica, não tem autovalores. Portanto T não é diagonalizável sobre $\mathbb{Z}_p$.

Nos exemplos 1.4, 1.5, 1.6 e 1.7, os problemas que impediram a diagonalização das matrizes dadas surgiram devido a dois motivos principais:

(1): Em Exemplo 1.4, o problema foi causado pela existência de $\sqrt{-1}$;

(2): Em Exemplo 1.5, o problema foi causado pelo fato de que a soma de dois quadrados $(1^2 + 2^2)$ não é um quadrado em $\mathbb{Q}$;

(3): Em Exemplos 1.6 e 1.7, as matrizes dadas não puderam ser diagonalizadas devido à uma combinação dos dois problemas detectados em Exemplos 1.4 e 1.5.

Friedberg conclui seu trabalho com o seguinte problema: *Classificar, exatamente, para quais tipos de corpos o Teorema do Eixo Principal é válido.* Já vimos nos exemplos acima que o Teorema do Eixo Principal não é válido, por exemplo, em $\mathbb{Q}$. Nosso objetivo, nesse trabalho, é fazer a classificação desses corpos (o conceito de corpo será introduzido em Capitulo 2) para os quais o Teorema do Eixo Principal é válido. Provaremos em Teorema 5.4 que, evitando os problemas detectados em Exemplos 1.4, 1.5, 1.6 e 1.7, então um corpo $\mathbb{K}$ preserva a Propriedade do Eixo Principal. Dizemos que um corpo $\mathbb{K}$ tem a Propriedade do Eixo Principal se toda matriz simétrica sobre $\mathbb{K}$ é ortogonalmente semelhante a uma matriz diagonal em $\mathbb{K}$.

Capítulo 2

Corpos e corpos ordenados

Nosso objetivo, nesse trabalho, será classificar quais corpos preservam a Propriedade do Eixo Principal. Por isso o nosso primeiro passo será definir, e exemplificar, o que são corpos e corpos ordenados. Adotaremos, sem definição, os seguintes termos primitivos: *conjunto* e a *relação de pertinência* $\in$. Usaremos, ainda, o símbolo $A \subseteq B$ para dizer que: $a \in A \Rightarrow a \in B$. Denotaremos por $\mathcal{P}(X)$ o conjunto formado por todos os subconjuntos de X. Assim $\mathcal{P}(X) = \{A \mid A \subseteq X\}$.

2.1 Corpos

Definição 2.1 (Corpo)**.** Seja $\mathbb{K}$ um conjunto munido de duas operações binárias chamadas adição $(+)$ e multiplicação $(\cdot)$, com as seguintes propriedades, para todo $a, b, c \in \mathbb{K}$:

(A1): Se $a, b \in \mathbb{K}$, então $a + b \in \mathbb{K}$ (Fechado para adição);

(A2): $(a + b) + c = a + (b + c)$ (Associatividade);

(A3): $a + b = b + a$ (Comutatividade);

(A4): Existe um elemento $e \in \mathbb{K}$, tal que $a + e = a$, para todo $a \in \mathbb{K}$. O elemento e será chamado "zero" e denotado por 0 (Elemento Neutro);

(A5:) Para todo $a \in \mathbb{K}$ existe um elemento, denotado por $-a$, tal que $a + (-a) = 0$ (Simétrico Aditivo);

(M1): Se $a, b \in \mathbb{K}$, então $a \cdot b \in \mathbb{K}$ (Fechado para multiplicação);

(M2): $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associatividade);

(M3): $a \cdot b = b \cdot a$ (Comutatividade);

(M4): Existe um elemento $u \in \mathbb{K}$, tal que $a \cdot u = a$, para todo $a \in \mathbb{K}$. O elemento u será chamado "um" e denotado por 1 (Elemento Identidade);

(M5): Para todo $a \neq 0$, existe um elemento denotado por a^{-1}, tal que $a \cdot a^{-1} = 1$ (Inverso Multiplicativo);

(D1): $a \cdot (b + c) = a \cdot b + a \cdot c$, (Distributividade).

Diremos que o terno $(\mathbb{K}, +, \cdot)$, é um *corpo* munido das operações de adição $(+)$ e multiplicação $(\cdot)$ com as propriedades listadas acima. É comum denotarmos (não havendo possibilidade de confusão) o produto $a \cdot b$ por ab.

Definição 2.2 (Característica de um corpo)**.** Seja $\mathbb{K}$ um corpo. Se existe n inteiro positivo, tal que $n \cdot 1 = 0$, então o menor tal n é chamado de *característica* de $\mathbb{K}$. Se não existe tal n, então a característica de $\mathbb{K}$ é zero. A característica de $\mathbb{K}$ será denotada por $\text{car}(\mathbb{K})$.

Assim, por exemplo, os corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm característica zero. Os corpos $\mathbb{Z}_p$ das classes residuais módulo p, têm característica p. A seguir um lema que lista algumas propriedades que são consequência direta de Definição 2.1:

Lema 2.3. *Seja $\mathbb{K}$ um corpo, então:*

(1) O zero é único;

(2) O simétrico de todo elemento é único;

(3) Se $a + b = a + c$, então $b = c$;

(4) A identidade é única;

(5) O inverso de todo elemento diferente de zero é único;

(6) Se $a \neq 0$ e $ab = ac$, então $b = c$;

(7) $a0 = 0$, para todo $a \in \mathbb{K}$;

(8) Se $ab = 0$, então $a = 0$ ou $b = 0$.

Demonstração.

(1): Assumimos que 0 e $0'$ sejam neutros, temos que mostrar que $0 = 0'$:
De fato: $0 + a = a$. Em particular, para $a = 0'$, temos $0 + 0' = 0'$. Da mesma forma obtemos que $0' + 0 = 0$ e, portanto, $0' = 0 + 0' = 0' + 0 = 0$.

(2): Assumimos que a_1 e a_2 são simétricos de a e, portanto, $a + a_1 = 0$ e $a + a_2 = 0$. Então $a_2 = 0 + a_2 = (a_1 + a) + a_2 = a_1 + (a + a_2) = a_1 + 0 = a_1$.

(3): Adicionando $-a$ em ambos os lados da igualdade obtemos: $a + (-a) + b = a + (-a) + c$, então $0 + b = 0 + c$ e, portanto, $b = c$.
As provas de (4) e (5) são analogas à (1) e (2).

(6): Se $ab = ac$ com $a \neq 0$, então $a^{-1}ab = a^{-1}ac$ logo $1b = 1c$ e, portanto, $b = c$.

(7): Se $a0 + 0 = a0 = a(0 + 0) = a0 + a0$, então $a0 = 0$ (devido à (3)).

(8): Se $a = 0$, não temos nada a ser provado. Assumimos que $a \neq 0$, então $ab = 0$ implica que $= a^{-1}ab = 0$, logo $1b = 0$ e, portanto, $b = 0$. □

Os conjuntos $\mathbb{R}$, $\mathbb{Q}$ e $\mathbb{C}$, dos números reais, racionais e complexos respectivamente, munidos das operações de adição e multiplicação são exemplos de corpos. Se p é primo o conjunto $\mathbb{Z}_p := \{0, 1, \cdots, p-1\}$, munido das operações de adição e multiplicação módulo p é um corpo.
Um número, real ou complexo, é *algébrico* se é solução de uma equação algébrica com coeficientes inteiros, ou seja, se um número satisfaz alguma equação da forma $c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0 = 0$ com coeficientes inteiros, $1 \leq n$ e $c_n \neq 0$, dizemos que ele é um *número algébrico*. O conjunto dos números algébricos munido das operações de adição e multiplicação é um corpo.
O conjunto $\mathbb{Q}(t)$, das funções racionais $r(t) = \frac{p(t)}{q(t)}$, onde p e q são polinômios com coeficientes racionais, sendo q não identicamente nulo é um corpo. Pode-se verificar, facilmente, que os exemplos acima são corpos, porém vamos fazer a verificação, apenas, para o próximo exemplo.

Proposição 2.4. *Seja p um primo e $\mathbb{A} := \{\alpha + \beta\sqrt{p} : \alpha, \beta \in \mathbb{Q}\}$, munido das operações de soma e multiplicação. O terno $(\mathbb{A}, +, \cdot)$ é um corpo.*

Demonstração. Observamos que $\mathbb{A} \subseteq \mathbb{R}$ e que $\mathbb{A}$ é fechado para a soma e multiplicação. Logo as propriedades A_1 e M_1 são válidas. As propriedades A2, A3, M2, M3 e D1 decorrem do fato de que $(\mathbb{R}, +, \cdot)$ é um corpo.

((A4) (M4): O conjunto $\mathbb{A}$ tem elemento neutro e identidade. De fato, $0 = 0 + 0\sqrt{p} \in \mathbb{A}$; $1 = 1 + 0\sqrt{p} \in \mathbb{A} \setminus \{0\}$.

(A5): Todo elemento de $\mathbb{A}$ tem simétrico. De fato, se $\alpha + \beta\sqrt{p} \in \mathbb{A}$, então

$$-(\alpha + \beta\sqrt{p}) = -\alpha + (-\beta)\sqrt{p} \in \mathbb{A}.$$

(M5): Seja $c = (\alpha + \beta\sqrt{p}) \in \mathbb{A} \setminus \{0\}$, então $c^{-1} \in \mathbb{A}$; de fato,

$$c^{-1} = \frac{1}{\alpha + \beta\sqrt{p}} \left(\frac{\alpha - \beta\sqrt{p}}{\alpha - \beta\sqrt{p}} \right) = \frac{\alpha}{\alpha^2 - \beta^2 p} + \frac{-\beta}{\alpha^2 - \beta^2 p}\sqrt{p} \quad .$$

□

2.2 Corpos Ordenados

Uma relação em um conjunto X é um subconjunto de $X \times X$. Dada uma relação $\mathcal{R}$ em X, escrevemos $x\mathcal{R}y$ para dizer que (x, y) pertence à relação.

Definição 2.5 (Relação de Ordem)**.** Seja X um conjunto qualquer. Uma *ordem parcial* em X é uma relação $\leq$ com as seguintes propriedades:

(a) $x \leq x$, para todo, $x \in X$ (reflexiva);

(b) Se $x \leq y \quad e \quad y \leq z$, então $x \leq z$, para todo, $x, y, z \in X$ (transitiva);

(c) Se $x \leq y \quad e \quad y \leq x$, então $x = y$, para todo, $x, y \in X$ (antissimétrica).

Se X está munido com uma ordem parcial, então X é um conjunto *parcialmente ordenado*. Se além das propriedades (a), (b), (c) a relação $\leq$ verificar a propriedade:

(d) $x \leq y$ ou $y \leq x$, para todo, $x, y \in X$.

diremos que $\leq$ é uma relação de *ordem total* e, neste caso X é dito *totalmente ordenado*.

A relação de inclusão entre conjuntos, por exemplo, é uma ordem parcial em $\mathcal{P}(X)$. Um exemplo de ordem total é a relação "$\leq$" em $\mathbb{R}$.

Definição 2.6. Seja X um conjunto parcialmente ordenado, e seja $A \subseteq X$.

(a) Se existir $a_0 \in A$, tal que $a_0 \leq a \ \forall \ a \in A$, então a_0 é um *elemento mínimo* de A.

(b) Se existir $a_n \in A$, tal que $a \leq a_n \ \forall \ a \in A$, então a_n é um *elemento máximo* de A.

(c) Se existir $a_0 \in A$, tal que $a = a_0$ sempre que $a \in A$ e $a \leq a_0$, então a_0 é um *elemento minimal* de A.

(d) Se existir $a_n \in A$, tal que $a = a_n$ sempre que $a \in A$ e $a \leq a_n$, então a_n é um *elemento maximal* de A.

(e) Se existir $b_0 \in X$, tal que $b_0 \leq a, \forall a \in A$, diremos que A é limitado inferiormente e que b_0 é uma *cota inferior* de A.

(f) Se existir $b_n \in X$, tal que $a \leq b_n, \forall a \in A$, diremos que A é limitado superiormente e que b_n é uma *cota superior*.

(g) Diremos que A é uma *cadeia* se, na ordem induzida, for totalmente ordenado.

(h) Diremos que A é *bem ordenado* se cada subconjunto não-vazio de A possui um elemento mínimo.

Nota: O elemento mínimo de um conjunto bem ordenado é único. Se um dado conjunto A possuir elemento mínimo usaremos a notação $\min(A)$ para denotar o elemento mínimo do conjunto A.

Proposição 2.7. *O par* $(\mathbb{N}, \leq)$ *é bem ordenado.*

Demonstração. Precisaremos mostrar que todo subconjunto não vazio $A \subseteq \mathbb{N}$ possui elemento mínimo. Se $1 \in A$, então 1 é o elemento mínimo de A, portanto, assumimos que $1 \notin A$. Seja $X = \{n \in \mathbb{N} \mid \{1, \ldots, n\} \subseteq \mathbb{N} \setminus A\}$, assim dizer que $n \in X$ significa afirmar que $n \notin A$ e que todos os numeros naturais menores do que n também não pertencem a A. Como $1 \notin A$, então $1 \in X$. Como A é não vazio e $X \subseteq \mathbb{N} \setminus A$, temos $X \neq \mathbb{N}$. Logo, pelo princípio de indução, existe $n_0 \in X$, tal que $n_0 + 1 \notin X$, ou seja, $1, \ldots, n_0 \notin A$ e $n_0 + 1 \in A$. Assim, $n_0 + 1$, é o elemento mínimo de A. □

O par $(\mathbb{R}, \leq)$ é totalmente ordenado, mas não é bem ordenado, o intervalo $(a, b) \subseteq \mathbb{R}$ com $a < b$, por exemplo, não possui elemento mínimo.

Definição 2.8 (Corpo Ordenado)**.** Seja $\mathbb{K}$ um corpo. Diremos que $\mathbb{K}$ é um *corpo ordenado* se está dada uma *ordem total* $\leq$ em $\mathbb{K}$ que satisfaz, para todo $a, b, c \in \mathbb{K}$,

(e) Se $a \leq b$, então $a + c \leq b + c$ (Compatibilidade com adição);

(f) Se $a \leq b$, então $ac \leq bc$ sempre que $0 \leq c$ e $bc \leq ac$ sempre que $c \leq 0$ (Compatibilidade com produto).

Os corpos $(\mathbb{R}, +, \cdot)$ e $(\mathbb{Q}, +, \cdot)$ são ordenados pela relação "$\leq$" (menor ou igual).

Lema 2.9. *Se* $\mathbb{K}$ *é um corpo ordenado, então* $1 > 0$ *e* $-1 < 0$.

Demonstração. Seja $a, b \in \mathbb{K}$, tal que $a < b$. Assim, por de Definição 2.8(f), $1a < 1b$ e, portanto, $1 > 0$.
Assumimos por absurdo que $-1 > 0$. Segue, de Definição 2.8(e), que $1 - 1 > 1$, logo $0 > 1$. Obtemos assim uma contradição e, portanto, $-1 < 0$. □

Capítulo 3

O Axioma da Escolha, O Lema de Zorn e o Teorema de Zermelo

A história do Axioma da Escolha e sua relação com outros axiomas famosos estão apresentadas em [1] por I. Bicudo. Aqui nós resumimos a parte relevante para este capítulo.

Em 1870, G. Cantor começou a produzir uma sequência de artigos, nos quais elaborou, a hoje conhecida, *teoria dos conjuntos*. Até então a teoria dos conjuntos não era tida como uma disciplina matemática. Cantor, através de seus trabalhos, obteve resultados que tornaram possível a caracterização de números cardinais e ordinais finitos. Cantor associou o conceito de número ordinal à *ordem* de um *conjunto bem ordenado* elevando, assim, o conceito de número ordinal, a um nível de extrema importância (lembramos que tais conceitos foram definidos em Seção 2.2). Semelhantemente o conceito de conjunto bem ordenado, também, foi elevado ao nível máximo de importância. Cantor provou ainda, em seus trabalhos, que um conjunto infinito pode ser munido de várias ordens. Foi, então em 1883, que G. Cantor fez o polêmico enunciado (sem demonstrá-lo): *Todo conjunto pode ser bem ordenado.* Porém os matemáticos da época não quiseram aceitar o enuciado, hoje conhecido como *Princípio da Boa Ordenação.* Portanto, Cantor passou a dedicar seus esforços em demonstrar seu princípio como verdadeiro.

Em 1904, não se sabia se o princípio de Cantor era verdadeiro ou falso, pois o mesmo, ainda não havia sido demonstrado. Então Ernst Zermelo, na tentativa de demonstrar o Princípio da Boa Ordenação, formulou pela primeiro vez o polêmico *Axioma da Escolha.* A afirmação de Zermelo foi basicamente a seguinte: *Dada uma coleção de conjuntos não vazios e, dois a dois disjuntos, em qualquer quantidade, podemos escolher um membro em cada um desses conjuntos. Logo, pelo Axioma da Escolha, podemos fazer de uma só vez "uma infinidade de escolhas".* Por se tratar de um princípio extremamente existencial e não construtivo o Axioma da Escolha, assim como o Princípio da Boa Ordenação, foi alvo de muitas críticas. O Axioma da Escolha garante a existência de uma função escolha sem, no entanto, fornecer meios para construí-la.

David Hilbert, em 1926, escreveu que o Axioma da Escolha de Zermelo foi o axioma "mais atacado até o presente na literatura matemática...". As palavras de Abraham Fraenkel, em 1958, foram "o axioma da escolha é, provavelmente, o mais interessante e, apesar de

seu aparecimento tardio, o mais discutido axioma da matemática, secundado apenas pelo axioma das paralelas de Euclides, que foi introduzido há mais de dois mil anos."
Gregory H. Moore, em 1982, disse "Raramente os praticantes da matemática, uma disciplina conhecida pela certeza de suas conclusões, difereriam tão veementemente sobre uma das premissas centrais, como o fizeram sobre o Axioma da Escolha. No entanto, sem o Axioma, a matemática hoje seria muito diferente. A própria natureza da matemática moderna seria alterada e, se prevalecessem as mais severas críticas construtivistas ao Axioma, a matemática estaria reduzida a uma coleção de algoritmos. De fato, o Axioma resume as mudanças fundamentais - matemáticas, filosóficas e psicológicas - ocorridas, quando os matemáticos começaram, seriamente, a estudar coleções infinitas de conjuntos." Moore observa ainda que: "É uma ironia histórica que muitos matemáticos, que posteriormente se opuseram ao Axioma da Escolha, tenham-no usado implicitamente em suas próprias pesquisas. Isso ocorreu, principalmente, com aqueles que estavam seguindo a teoria dos conjuntos de Cantor ou procurando aplicá-la à análise real. Na virada do seculo XX, tais analistas incluiam René Baire, Émile Borel e Henri Lebesgue, na França, (...). Mas a demonstração de Zermelo, em 1904, do Teorema da Boa Ordem levou-os a desenvolver sua filosofia construtivista da matemática e a tornarem-se, crescentemente, intolerantes para com métodos não contrutivos, como o Axioma da Escolha". A verdade é que as várias tentativa de "livrar" a matemática do Axioma da Escolha só contribuiram para o surgimento de um grande número de resultados, todos equivalentes ao Axioma da Escolha, em vários ramos da matemática. Um outro fato importante é que, uma boa parte dos teoremas já demonstrados hoje, não poderiam ser demonstrados sem o Axioma da Escolha. Assim o Axioma da Escolha torna-se fundamental para a matemática atual. O objetivo desta seção será provar a equivalência entre: Axioma da Escolha, Lema de Zorn e Teorema de Zermelo. O nosso primeiro passo será enunciar estas três afirmações; em seguida vamos enunciar e demonstrar o teorema que prova a equivalência entre as três. As demonstrações aqui apresentadas seguem [8].

Axioma da Escolha. *Suponha que* $\{C_\alpha\}_{\alpha\in J}$ *é uma família de conjuntos disjuntos e não-vazios. Então existe uma função* $\varphi : \{C_\alpha\}_{\alpha\in J} \longrightarrow \bigcup_{\alpha\in J} C_\alpha$, *tal que* $\varphi(C_\alpha) \in C_\alpha$.

Lema de Zorn. *Seja* X *um conjunto parcialmente ordenado, tal que toda cadeia tenha, pelo menos, uma cota superior. Então* X *tem um elemento maximal.*

Sabemos, por definição, que um conjunto X é bem ordenado se, todo subconjunto $A \subseteq X$ tem um elemento mínimo. Em particular, se um conjunto for bem ordenado, então será totalmente ordenado pois $\{x, y\}$ tem menor elemento quaisquer que sejam x, y.

Teorema de Zermelo. *Dado qualquer conjunto* X. *Existe uma relação de ordem* $\leq$, *tal que* $(X, \leq)$ *é bem ordenado.*

Teorema 3.1. *As seguintes afirmações são equivalentes:*

(i) O Axioma da Escolha;

(ii) O Lema de Zorn;

(iii) O Teorema de Zermelo.

Demonstração.

((iii) $\Rightarrow$ (i)): Dada uma coleção de conjuntos $\{C_\alpha\}_{\alpha\in J} \neq \emptyset$, existe, por hipótese do Teorema de Zermelo, uma boa ordenação em $\bigcup_\alpha C_\alpha$. Tomamos, então, $\varphi(C_\alpha)$ como o elemento mínimo de C_α que pode ser tomada como uma função de escolha.

((ii) $\Rightarrow$ (iii)): Seja X um conjunto não vazio. Consideramos os subconjuntos $A \subseteq X$, tal que exista uma ordem em A, digamos $\leq_A$, de forma que A seja bem ordenado. Seja $\mathcal{B}$ o conjunto de todos os pares $(A, \leq_A)$ onde $A \subseteq X$ e $\leq_A$ torna A bem ordenado. Podemos perceber que $\mathcal{B}$ é não-vazio pois, em particular, $\emptyset \in \mathcal{B}$. Temos que mostrar, então, que $X \in \mathcal{B}$: Definimos uma ordem parcial em $\mathcal{B}$ da seguinte forma: Dados $(A, \leq_A), (B, \leq_B) \in \mathcal{B}$, diremos que $(A, \leq_A) \prec (B, \leq_B)$ se:

(a) $A \subseteq B$;

(b) A ordem $\leq_A$ é induzida por $\leq_B$;

(c) Se $x \in B \setminus A$ e $y \in A$, então $y \leq_B x$, onde $B \setminus A = \{x \in X; x \in B \, e \, x \notin A\}$.

Note que, por (a) e (b), a relação $\prec$ é reflexiva, transitiva e antissimétrica e, portanto, $\mathcal{B}$ é parcialmente ordenado. Temos que mostrar que $\mathcal{B}$ satisfaz as hipóteses do Lema de Zorn. Seja $(A_\alpha, \leq_\alpha)$ uma cadeia em $\mathcal{B}$. Consideramos o conjunto $U = \bigcup_\alpha A_\alpha$ e $a, b \in U$. Existe, então, α_0, tal que $a, b \in A_{\alpha_0}$. Definimos $a \leq_U b$ se, e somente se, $a \leq_{\alpha_0} b$ por (b), a relação assim definida é coerente e define uma ordem parcial, e mais, essa relação deverá ser uma boa ordenação. De fato, se $a \in A_\alpha$ e $b \leq_U a$, então $b \in A_\alpha$. Então, se $L \subseteq \bigcup_\alpha A_\alpha$ é não vazio existe α_0, tal que $L \cap A_{\alpha_0} \neq \emptyset$, então o menor elemento de $L \cap A_{\alpha_0}$ será também o menor elemento de L. Como, para todo α, $(A_\alpha, \leq_\alpha) \prec (\bigcup_\alpha A_\alpha, \leq_U)$ obtemos a cota superior desejada. Usando o Lema de Zorn, obtemos um elemento maximal digamos A_M. Se $A_M \neq X$ existiria $a \in X \setminus A_M$ e poderíamos obter um novo conjunto bem ordenado $A_M \cup \{a\}$ em que $\{a\}$ seria declarado o maior elemento contradizendo, assim, a maximalidade de A_M. Consequentemente, $X \in \mathcal{B}$ e $(X, \leq_X)$ é bem ordenado.

((i) $\Rightarrow$ (ii)): Para provarmos que o Axioma da Escolha implica o Lema de Zorn precisaremos de dois lemas e da próxima definição.

Definição 3.2. Dado um conjunto X parcialmente ordenado e $A \subseteq X$, o conjunto $\Im(A) := \{x \in X \mid a \leq x \ \forall \ a \in A\}$ é chamado de *conjunto das cotas superiores* de A.

Lema 3.3. *Assumindo o Axioma da Escolha e seja X parcialmente ordenado, dado $a \in X$, existe $S \subseteq X$, que é bem ordenado com a ordem induzida, tal que $a \in S$ e $\Im(S) \subseteq S$.*

Lema 3.4. *Se todo subconjunto bem ordenado de X tem alguma cota superior, então X tem um elemento maximal.*

Observe que o Lema de Zorn decorre do Lema 3.4. De fato, assumimos que X é parcialmente ordenado, tal que toda cadeia tem uma cota superior. Como um subconjunto bem ordenado de X é uma cadeia, obtemos por Lema 3.4 que X tem um elemento máximo. Vejamos, primeiramente, como o Lema 3.3 implica o Lema 3.4. Primeiro demonstraremos Lema 3.4 assumindo Lema 3.3. A demonstração de Lema 3.3 será apresentada em seguida.

Demonstração de Lema 3.4. Tome $a \in X$ e $S \subseteq X$, como em Lema 3.3. Seja $x \in \Im(S)$ (que não é vazio por hipótese de Lema 3.4). Afirmamos que x é maximal em X, pois, se $x \leq y \in X$, então teremos que $y \in \Im(S)$, logo, $y \in S$, então $y \leq x$ e, portanto, $x = y$. □

Demonstração de Lema 3.3. Assumimos, por absurdo, que existe $a \in X$ para o qual as conclusões de Lema 3.3 não são satisfeitas (assim dizer que $a \in X$ significa afirmar que para todo $S \subseteq X$, tal que $a \in S$ e S é bem ordenado, temos que $\Im(S)$ não está contido em S). Seja:

$$\mathcal{A} := \{S \subseteq X \mid S \quad \text{é bem ordenado e} \quad a = \min(S)\}.$$

Notamos que $\{a\} \in \mathcal{A}$ e, portanto, o conjunto $\mathcal{A}$ é não vazio. Definimos, usando o Axioma da Escolha, a função:

$$\begin{aligned} \varphi : \mathcal{A} &\to X; \\ S &\mapsto \varphi(S) \in \Im(S) \setminus S. \end{aligned}$$

Se $S \in \mathcal{A}$ e $x \in X$, definimos as seções $S_x := \{y \in S \mid y < x\}$. Note que cada seção está bem definida mesmo que $x \notin S$.

Afirmação 3.5. *Se $S \in \mathcal{A}$ e $x \in S \setminus \{a\}$, então $S_x \in \mathcal{A}$.*

Demonstração. Como $S_x \subseteq S$, então S_x é bem ordenado, pois S é bem ordenado. Como $a \leq y$, para todo $y \in S$ concluímos que $a \leq y$, para todo $y \in S_x$ logo $a = \min(S_x)$ e, portanto, $S_x \in \mathcal{A}$. □

Definimos o conjunto

$$\mathcal{A}_0 = \{S \in \mathcal{A} \mid \forall x \in S \setminus \{a\}, \quad \varphi(S_x) = x\}.$$

Note que $\{a\} \in \mathcal{A}_0$ e, portanto, o conjunto $\mathcal{A}_0$, assim definido, é não vazio.

Afirmação 3.6. *Se $S \in \mathcal{A}_0$, então $S \cup \{\varphi(S)\} \in \mathcal{A}_0$.*

Demonstração. Seja $\bar{S} = S \cup \{\varphi(S)\}$. Como $a < \varphi(S)$ e $a \in \bar{S}$ obtemos que $a = \min(\bar{S})$. Além disso $\bar{S}$ é bem ordenado e, portanto, $\bar{S} \in \mathcal{A}$. Seja $x \in \bar{S}$: se $x = \varphi(S)$, então $\bar{S}_x = S$, logo $\varphi(\bar{S}_x) = x$. Se, porém, $x \neq \varphi(S)$, então $\bar{S}_x = \{y \in \bar{S} \mid y < x\} = \{y \in \bar{S} \mid y < x \text{ e } y < \varphi(S)\} = \{y \in S \mid y < x\} = S_x$, logo $\varphi(\bar{S}_x) = \varphi(S_x) = x$. □

Afirmação 3.7. *Se S, $S' \in \mathcal{A}_0$, então um dos seguintes três casos tem que ser verdade:*

(i) $S = S'$;

(ii) $S' = S_s$, *com* $s \in S$;

(iii) $S = S'_{s'}$, *com* $s' \in S'$.

Demonstração. Seja:

$$C = \{x \in S \cap S' \mid S_x = S'_x\}.$$

O conjunto C assim definido é não vazio pois, em particular, $\{a\} \in C$. Seja $x \in C$. Então $S_x = S'_x$. Seja $y \in S_x$, então $y < x$ e, portanto, $S_y = (S_x)_y = (S'_x)_y = S'_y$. Logo, $y \in C$. Portanto, podemos concluir que, se $x \in C$ e $y \in S \setminus C$, então $x < y$. Assumimos que $C \neq S$ e seja $s = \min(S \setminus C)$ (o elemento s de fato existe, pois, o conjunto S é bem ordenado). Então $C = S_s$. De fato, $C \subseteq S_s$ se $c \in C$, então $c \in S$. Como $s \in S \setminus C$ concluímos, pela Afirmação 3.6, que $c < s$ logo $c \in S_s$. Reciprocamente, se $c \in S$, então $c < s$. Logo, como $s = \min(S \setminus C)$, não podemos ter $c \in S \setminus C$ e, portanto, $c \in C$. E, assim, concluímos que, ou $C = S$ ou $C = S_s$, tal que $s \in S \setminus \{a\}$. Analogamente obtemos que, ou $C = S'$ ou $C = S'_{s'}$, tal que $s' \in S' \setminus \{a\}$. Resta mostrar que não podemos ter $C = S_s = S'_{s'}$. De fato, nesse caso teríamos que $s = \varphi(S_s) = \varphi(S'_{s'}) = s'$ logo, $s = s' \in S \cap S'$ e $s = s' \in C$, o que nos levaria a uma contradição. Portanto, $C = S_s = S'_{s'}$ não é uma possibilidade possível. □

Seja $\tilde{S} = \bigcup_{S \in \mathcal{A}_0} S$.

Afirmação 3.8. *Se $x \in S \in \mathcal{A}_0$, então $\tilde{S}_x = S_x$.*

Demonstração. Seja $y \in \tilde{S}_x$. Existe $S' \in \mathcal{A}_0$, tal que $y \in S'$ e assim temos três casos a considerar:

(i) $S = S'$;

(ii) $S' = S_s$, tal que $s \in S \setminus \{a\}$;

(iii) $S = S'_{s'}$, tal que $s' \in S' \setminus \{a\}$.

Vamos analisar esses três casos. Em (i) temos: $y \in S$ e $y < x$ logo, $y \in S_x$. Em (ii) temos: $y \in S_s$ logo, $y \in S_x$. Finalmente, em (iii) temos: $y \in S'$ e $y < x$, além disso, como $x \in S$ temos que $x < s'$ e, portanto, $y < s'$ e $y \in S'_{s'} = S$. Portanto, $y \in S$ e $y \in S_x$. Observe que nos três casos obtemos que $y \in S_x$ e $\tilde{S}_x \subseteq S_x$. Por outro lado se $y \in S_x$, então $y \in \tilde{S}$ e $y < x$ logo, $y \in \tilde{S}_x$, então $S_x \subseteq \tilde{S}_x$ e, portanto, $S_x = \tilde{S}_x$. □

Afirmação 3.9. *O conjunto $\tilde{S}$ é bem ordenado.*

Demonstração. Para mostrar que a Afirmação 3.9 é de fato verdade consideramos um conjunto $D \subseteq \tilde{S} \neq \emptyset$. Se $x \in D$, existe $S \in \mathcal{A}_0$, tal que $x \in S$. Definimos $m = \min(D \cap (S_x \cup \{x\}))$. (Note que m existe, pois S é bem ordenado). Pela Afirmação 3.8, $S_x = \tilde{S}_x$. Seja $y \in D$ vamos mostrar que ou $y < m$ ou $m \leq y$. De fato, como $y \in D$, então $y \in \tilde{S}$ logo, existe $S' \in \mathcal{A}_0$, tal que$y \in S'$. Por Afirmação 3.8, temos três casos a considerar para S e S'. Se $S = S'$, então $m, y \in S$. Se $S' = S_s$, então $S' \subseteq S$ e, portanto $m, y \in S$. Se $S = S'_{s'}$, então $S \subseteq S'$ e, portanto, $m, y \in S'$. Portanto m, y são elementos de um conjunto bem ordenado. Então, $y < m$ ou $m \leq y$. Logo, se $y \in D$ e $y < m$, então $y < x$ e $y \in \tilde{S}_x$. Como $S_x = \tilde{S}_x$, então $y \in S_x$ e $y \in S_x \cap D$, então $m \leq y$ e, portanto, $m = \min(D)$. Logo, D tem elemento minimal. □

Se $x \in \tilde{S}$, então $x \in S$ com $S \in \mathcal{A}_0$ e $\tilde{S}_x = S_x$. Logo, $\varphi(\tilde{S}_x) = \varphi(S_x) = x$, então $\tilde{S} \in \mathcal{A}_0$. Portanto, por uma afirmação anterior, $\bar{S} = S \cup \{\varphi(\tilde{S})\} \in \mathcal{A}_0$. Logo, como $\tilde{S} = \bigcup_{S \in \mathcal{A}_0} S$, obtemos que $\bar{S} \subseteq \tilde{S}$. Logo $\bar{S} = \tilde{S}$ e $\varphi(\tilde{S}) \in \tilde{S}$ (o que contradiz a construção da função φ). □

□

Observação: Na demonstração acima, foi provado que dado um elemento qualquer a de um conjunto parcialmente ordenado, então existe uma cadeia maximal que o contém.

Conclusão 3.10. Os três axiomas são equivalentes.

Capítulo 4

Ordenações em Um Corpo

O objetivo desta seção é definir o que vem a ser um corpo *formalmente real*, apresentar, e demonstrar, as propriedades de corpos formalmente reais.
Seja $\mathbb{K}$ um corpo arbitrário. Denotaremos por $\mathbb{K}^*$ o grupo multiplicativo dos elementos não nulos de $\mathbb{K}$. Um quadrado do corpo $\mathbb{K}$ é um elemento $y = x^2$, tal que $x \in \mathbb{K}$.
Denotaremos por $\mathbb{K}^2 := \{x^2 \mid x \in \mathbb{K}\}$ o subconjunto dos quadrados de $\mathbb{K}$ e $\mathbb{K}^{*2} := \{x^2 \mid x \in \mathbb{K}^*\}$. Serão usadas, ainda, as notações:

$$\sigma(\mathbb{K}) = \{x_1^2 + \cdots + x_n^2 \mid x_i \in \mathbb{K}, n \in \mathbb{N}, 0 < n\} \quad e \quad \sigma(\mathbb{K})^* = \sigma(\mathbb{K}) \setminus \{0\}.$$

Assim, por exemplo, $\sigma(\mathbb{R}) = \{x \in \mathbb{R} \mid 0 \leq x\}$. Seja $\mathbb{Z}_7$ o corpo das classes residuais módulo 7, então $\sigma(\mathbb{Z}_7) = \mathbb{Z}_7$. Cada elemento de $\mathbb{Z}_7$ é um quadrado ou soma de dois quadrados:

$$\overline{0} = \overline{0}^2;\ \overline{1} = \overline{1}^2;\ \overline{2} = \overline{3}^2;\ \overline{3} = \overline{3}^2 + \overline{1}^2;\ \overline{4} = \overline{2}^2;\ \overline{5} = \overline{2}^2 + \overline{1}^2;\ \overline{6} = \overline{3}^2 + \overline{2}^2.$$

Proposição 4.1. *Seja $\mathbb{K}$ um corpo, então $\sigma(\mathbb{K})^*$ é um subgrupo multiplicativo de $\mathbb{K}^*$.*

Demonstração. Observamos que $\sigma(\mathbb{K})^* \subseteq \mathbb{K}$ e, portanto, a operação "$\cdot$" é associativa e existe o elemento neutro. Temos que mostrar que $\sigma(\mathbb{K})^*$ é fechado para produto; se $x = \sum_i x_i^2$ e $y = \sum_j y_j^2 \in \sigma(\mathbb{K})^*$, então $xy = \sum_{i,j}(x_i y_j)^2 \in \sigma(\mathbb{K})^*$. Resta mostrar que todo elemento $x \in \sigma(\mathbb{K})^*$ possui um inverso $x^{-1} \in \sigma(\mathbb{K})^*$. De fato $x^{-1} = \frac{1}{x} = \frac{x}{x^2} = \sum_i \left(\frac{x_i}{x}\right)^2 \in \sigma(\mathbb{K})^*$. □

Definição 4.2. Um corpo $\mathbb{K}$ é *formalmente real* se $-1 \notin \sigma(\mathbb{K})$.

Um corpo formalmente real tem característica zero. De fato, se $\mathbb{K}$ não tem característica zero, então $\mathbb{K}$ tem característica p, tal que $p \in \mathbb{Z}$, $0 < p$ e p é primo. Logo; $\mathbb{Z}_p \subseteq \mathbb{K}$ e, portanto, $0 = p \cdot 1_{\mathbb{K}}$. Segue-se que: $-1_{\mathbb{K}} = (p-1) \cdot 1_{\mathbb{K}} \in \sigma(\mathbb{K})$, obtemos, assim, uma contradição.
Sabemos pela Definição 2.8 que uma ordem sobre um corpo $\mathbb{K}$ é uma relação binária $\leq$ que é reflexiva, antissimétrica, transitiva, total e compatível com as operações do corpo. Essa definição motiva a proposição a seguir:

Proposição 4.3. *Um corpo $\mathbb{K}$ é ordenado se, e somente se, existe um subconjunto $P \subseteq \mathbb{K}$, tal que:*

(a) $P + P \subseteq P$;

(b) $P \cdot P \subseteq P$;

(c) $\mathbb{K} = P \cup (-P)$, *onde* $-P := \{-x \mid x \in P\}$;

(d) $P \cap (-P) = \{0\}$.

O conjunto P da Proposição 4.3 é chamado de *conjunto dos elementos positivos da ordem.*

Demonstração.

($\Rightarrow$) Se $\leq$ é uma relação de ordem sobre $\mathbb{K}$, definimos $P := \{x \in \mathbb{K} \mid 0 \leq x\}$. Vamos mostrar que o conjunto P, assim definido, satisfaz as quatro propriedades acima. De fato, P é fechado para soma: sejam $a, b \in P$, logo $0 \leq a$ e $0 \leq b$, então pela Definição 2.8(e), $b \leq a + b$ logo, por transitividade, $0 \leq a + b$ e, portanto, $a + b \in P$. O conjunto P é fechado para produto: sejam $a, b \in P$, logo $0 \leq a$ e $0 \leq b$, então pela Definição 2.8(f), $0 \leq ab$ e, portanto, $ab \in P$. Resta mostrar que o conjunto P satisfaz os itens (c) e (d) desta proposição. De fato, seja $a \in \mathbb{K} \setminus P$, logo por Lema 2.9 $(-1)a > 0$ ou $0 < -a$ e, portanto, $-a \in P$, ou seja, $a \in -P$. Isso mostra que $\mathbb{K} = P \cup (-P)$. Temos que mostrar, ainda, que $P \cap (-P) = \{0\}$, de fato: seja $a \in P \cap (-P)$, então $0 \leq a$ e $0 \leq -a$, então pela Definição 2.8(f), $a \leq 0$ e, portanto, pela Definição 2.5(c), $a = 0$.

($\Leftarrow$) Se existe $P \subseteq \mathbb{K}$ satisfazendo as propriedades de Proposição 4.3, então podemos definir a seguinte relação sobre $\mathbb{K}$: $a\mathcal{R}b$ se $b - a \in P$. A relação $\mathcal{R}$, assim definida, é uma relação de ordem total e compatível com as operações de $\mathbb{K}$. De fato a relação $\mathcal{R}$ satisfaz as propriedades seguintes:

($\mathcal{R}1$). Transitiva: Sejam $a, b, c \in \mathbb{K}$, tais que $a\mathcal{R}b$ e $b\mathcal{R}c$, então $b - a \in P$ e $c - b \in P$. Como P é fechado para soma podemos escrever, $(b - a) + (c - b) = c - a \in P$ e, portanto, $a\mathcal{R}c$.

($\mathcal{R}2$). Antissimétrica: Sejam $a, b \in \mathbb{K}$, tais que $a\mathcal{R}b$ e $b\mathcal{R}a$. Logo $b - a \in P$ e $a - b \in P$, então $-(a - b) = b - a \in -P$. Logo $b - a \in P \cap (-P)$ assim, pelo item (d) de Proposição 4.3, $b - a = 0$ e, portanto, $a = b$.

($\mathcal{R}3$). Reflexiva: Seja $a \in \mathbb{K}$, pelo item (A5) de Definição 2.1, $a - a = 0$ logo, pelo item (d) de Proposição 4.3, $0 = a - a \in P$ e, portanto, $a\mathcal{R}a$.

($\mathcal{R}4$). Total: Sejam $a, b \in \mathbb{K}$ logo $a - b \in P$ ou $a - b \in -P$. Note que, se $a - b \in -P$, então $b - a \in P$ e, portanto, $b\mathcal{R}a$ ou $a\mathcal{R}b$.

($\mathcal{R}5$). Compatibilidade com a soma: Sejam $a, b, c \in \mathbb{K}$, tais que $a\mathcal{R}b$ logo $b - a \in P$, então $b + c - c - a \in P$, assim $(b + c) - (c + a) \in P$ e, portanto, $(a + c)\mathcal{R}(b + c)$.

($\mathcal{R}6$). Compatibilidade com o produto: Sejam $a, b, c \in \mathbb{K}$, tal que $a\mathcal{R}b$ e assim $b - a \in P$. Assumimos $0\mathcal{R}c$, ou seja, $c-0 = c \in P$. Pelo item (vi) da Definição 2.8, $(b-a)c \in P$, então $bc - ac \in P$ e, portanto, $ac\mathcal{R}bc$. Seja $c\mathcal{R}0$ com $c \neq 0$, ou seja, $-c \in P$. Logo, $(b-a)(-c) \in P$, então $ac - bc \in P$ e, portanto, $bc\mathcal{R}ac$.

O conjunto dos elementos positivos desta ordenação é, exatamente, P pois $0\mathcal{R}a$ se, e somente se, $a - 0 \in P$. □

Corolário 4.4. *Se $P \subseteq \mathbb{K}$ satisfaz as propriedades de Proposição 4.3, então $\sigma(\mathbb{K}) \subseteq P$.*

Demonstração. De fato, de acordo com a Proposição 4.3, P é fechado para a adição, temos que mostrar que $\mathbb{K}^2 \subseteq P$. Se $x \in P$, então $x^2 \in P$ pois, pela Proposição 4.3, P é fechado para multiplicação. Caso $-x \in P$, então $x^2 = (-x)^2 \in P$. Portanto, em qualquer caso, $x \in P$ ou $-x \in P$, temos $x^2 \in P$. Pela parte (iii) da Proposição 4.3, $\mathbb{K} = P \cup (-P)$ e, portanto, $\mathbb{K}^2 \subseteq P$. □

Corolário 4.5. *Se $P \subseteq \mathbb{K}$ satisfaz as propriedades de Proposição 4.3, então $-1 \notin P$.*

Demonstração. Seja $\leq$ a ordem induzida por P em $\mathbb{K}$. Então $\mathbb{K}$ é um corpo ordenado. Assim por Lema 2.9 $-1 < 0$ e, portanto, $-1 \notin P$. □

Conclusão 4.6. As propriedades de Proposição 4.3 nos dá uma bijeção entre ordens sobre um corpo $\mathbb{K}$ e os subconjuntos $P \subseteq \mathbb{K}$ que satisfazem essas propriedades. Assim podemos dizer que P é uma ordenação sobre $\mathbb{K}$ ao nos referirmos a ordem $\leq$ sobre $\mathbb{K}$, tal que $P = \{x \in \mathbb{K} \mid 0 \leq x\}$.

Sabemos pela Definição 4.2 que $-1 \in \sigma(\mathbb{K})$, se a característica de $\mathbb{K}$ é $p > 0$ logo, pelos Corolários 4.4 e 4.5, corpos com característica $p > 0$ não são ordenados. Segue, ainda, que o corpo $\mathbb{C}$ não pode ser ordenado pois, $-1 = i^2$.

Definição 4.7. Uma *pré-ordenação* sobre um corpo $\mathbb{K}$ é um subconjunto $T \subseteq \mathbb{K}$ que satisfaz as seguintes propriedades:

(i) $T + T \subseteq T$;

(ii) $T \cdot T \subseteq T$;

(iii) $\mathbb{K}^2 \subseteq T$;

(iv) $-1 \notin T$.

Nota: Por definição e pelas consequências e conclusões da Proposição 4.3, toda ordenação é uma pré-ordenação.

Proposição 4.8. *Seja T uma pré-ordenação de um corpo $\mathbb{K}$. Então*

(i) $\sigma(\mathbb{K}) \subseteq T$;

(ii) $T \cap (-T) = \{0\}$;

(iii) $T^* := T \setminus \{0\}$, *é um subgrupo de* $\mathbb{K}^*$.

Demonstração.

(i): Para mostrar que $\sigma(\mathbb{K}) \subseteq T$, observamos que T é fechado para adição devido ao item (i) da Definição 4.7 e $\mathbb{K}^2 \subseteq T$. Portanto, usando indução em n obtemos $x = \sum_{j=1}^{n} x_j^2 \in \sigma(\mathbb{K})$.

(ii): Seja $y \in T \cap (-T)$, então $y = -x$ com $x, y \in T$. Assumimos que $x \neq 0$. Como $\mathbb{K}^2 \subseteq T$, $-1 = \left(\frac{y}{x}\right) = xy\left(\frac{1}{x^2}\right) \in T$. Obtemos, assim, uma contradição e, portanto, $x = y = 0$.

(iii): Sejam $x, y \in T^*$. Sabemos, pela Definição 4.7, que T é fechado para multiplicação e $\mathbb{K}^2 \subseteq T$ e, portanto, xy e $\left(\frac{1}{y}\right)^2 \in T^*$. Novamente,usando o fato de que T é fechado para multiplicação, temos: $xy^{-1} = xy\left(\frac{1}{y}\right)^2 \in T^*$. □

O próximo lema garante que uma pré-ordenação pode ser extendida até obter uma ordenação.

Lema 4.9 (Lema da Extensão)**.** *Sejam T uma pré-ordenação sobre um corpo $\mathbb{K}$ e $a \in \mathbb{K} \setminus T$. Então, $T' := T - aT$, onde $T - aT = \{t_1 - at_2 \mid \quad t_1, t_2 \in T\}$ é uma pré ordenação sobre $\mathbb{K}$ que contém T e o elemento $-a$.*

Demonstração. Uma vez que $0, 1 \in T$, T' contém T e $-a$. Sejam $x = t_1 - at_2$, $y = t_3 - at_4 \in T'$, (onde $t_i \in T$), então $x + y = t_1 + t_3 - a(t_2 + t_4) \in T'$. T' é fechado para produto. De fato: $xy = t_1t_3 + a^2t_2t_4 - a(t_2t_3 + t_1t_4) \in T'$. Também $\mathbb{K}^2 \subseteq T \subseteq T'$. Temos que mostrar que $-1 \notin T'$; de fato se $-1 \in T'$, então $-1 = t_1 - at_2, \quad t_i \in T'$. Se $t_2 \neq 0$, então $a = \frac{1+t_1}{t_2} = \frac{(1+t_1)t_2}{t_2^2} \in T$. Isso contraria a hipótese que $a \notin T$. Então $t_2 = 0$, assim obtemos, $-1 = t_1 \in T$ (outra contradição) e, portanto, $-1 \notin T'$. □

Corolário 4.10. *Seja T uma pré-ordenação sobre $\mathbb{K}$. Então:*

(1) T é uma ordenação sobre $\mathbb{K}$ se, e somente se, T é uma pré-ordenação maximal (no sentido de inclusão de conjuntos);

(2) $T \subseteq P$ para alguma ordenação P de $\mathbb{K}$.

Demonstração. (1): (⇒): Suponha que T é uma ordem sobre $\mathbb{K}$. Então T é uma pré-ordenação maximal. Logo: $T = \{x \in \mathbb{K} \mid 0 \leq x\}$. Precisaremos mostrar que: se T' é uma pré-ordenação, tal que $T \subsetneq T'$, então isso nos levaria a uma contradição.

Assumimos que T' é uma pré-ordenação, tal que $T \subsetneq T'$. Logo: existe $a \in T'$, tal que $a \notin T$. Se $a < 0$, então $-a \in T$, logo $-a \in T'$, então $-1 = \frac{-a}{a} = \frac{-(a)a}{a^2} \in T'$. Portanto, $-1 \in T'$ o que nos leva a uma contradição. Como ordenações são pré ordenações segue que T é uma pré-ordenação maximal.

($\Leftarrow$): Se T é uma pré-ordenação maximal, então por definição os itens (i) e (ii) da Proposição 4.3 são satisfeitos. Pela Proposição 4.8 (b), o item (iv) da Proposição 4.3, também é satisfeito. Temos que provar o item (iii) da Proposição 4.3, ou seja, provar que $\mathbb{K} = T \cup (-T)$. Para cada $a \in \mathbb{K}$, se $a \notin T$, pelo Lema da Extenção $T' = T - aT$ é uma pré ordenação. Como, pela Definição 4.7 (viii), $T' \neq \mathbb{K}$, temos por hipótese que $T' = T$. Logo $-a \in T$ e, portanto, $\mathbb{K} = T \cup (-T)$.

(2): Como T é uma pré-ordenação de $\mathbb{K}$ o conjunto $S := \{T \subseteq \mathbb{K} \mid T \quad \text{é pré-ordenação}\}$ é não vazio. Ordenemos S pela inclusão de conjuntos. Se U é uma cadeia em S, então $\bigcup_{T \in U} T \in S$. De fato todos os elementos de U são comparáveis, ou seja, se $T_1, T_2 \in U$, então $T_1 \subseteq T_2$ ou $T_2 \subseteq T_1$. Assim $\bigcup_{T \in U} T$ é uma cota superior para U.
Pelo Lema de Zorn, S tem um elemento maximal, digamos T_0. Então T_0 satisfaz a Definição 4.7. Para mostrar que T_0 é uma ordenação, considerando a Proposição 4.8 (b), temos que mostrar que $\mathbb{K} = T_0 \cup (-T_0)$:
Seja $a \in \mathbb{K} \setminus T_0$. Pelo Lema da Extensão, $T' = T_0 - aT_0$ é uma pré-ordenação que contém T_0. Com $T' \neq \mathbb{K}$ (pela Definição 4.7) e, T_0 maximal, vem que $T_0 = T'$, então $-a \in T_0$ e, portanto, $\mathbb{K} = T_0 \cup (-T_0)$ e, assim T_0 é uma ordenação que contém T.

□

4.1 O Teorema de Artin-Schreier

Nesta seção vamos apresentar a demonstração do Teorema de Artin-Schreier, que diz que um corpo $\mathbb{K}$ admite uma ordenação se, e somente se, $\mathbb{K}$ é formalmente real. Este resultado, que completa a ligação entre corpos ordenados e formalmente reais, foi provado, pela primeira vez, por E. Artin em 1920 como parte da solução do 17º problema de Hilbert. A construção de uma ordenação sobre um corpo formalmente real invoca o Axioma da Escolha. Este resultado pode ser encontrado em [11].

Teorema 4.11 (Artin-Schreier)**.** *Seja $\mathbb{K}$ um corpo. As seguintes afirmações são equivalentes:*

(1) $\mathbb{K}$ é formalmente real;

(2) $\sigma(\mathbb{K})$ é uma pré-ordenação sobre $\mathbb{K}$;

(3) $\mathbb{K}$ possui pelo menos uma ordenação.

Demonstração.

((1)⇒(2)): $\sigma(\mathbb{K})$ contém $\mathbb{K}^2$ e é fechado para adição e multiplicação. Se $\mathbb{K}$ é formalmente real, então $-1 \notin \sigma(\mathbb{K})$ e, portanto, $\sigma(\mathbb{K})$ é uma pré-ordenação.

((2)⇒(3)): Pela parte 2 do Corolário 4.10 $\sigma(\mathbb{K})$ está contido em uma ordenação P. Portanto $\mathbb{K}$ possui uma ordenação.

((3)⇒(1)): Se $\mathbb{K}$ possui pelo menos uma ordenação, então $\mathbb{K}$ é formalmente real. De fato: Se $\mathbb{K}$ possui uma ordenação P, então $-1 \notin P$ (senão $P \cap (-P) \neq \{0\}$). Como $\sigma(\mathbb{K}) \subseteq P$, então $-1 \notin \sigma(\mathbb{K})$ e, portanto, $\mathbb{K}$ é formalmente real. □

Capítulo 5

Corpos com a Propriedade do Eixo Principal

Neste capítulo definimos e exemplificamos o que é um *corpo pitagórico*. Definiremos, também, o que é um *corpo real fechado*. Assim, vamos usar os conceitos vistos até aqui para caracterizar corpos que satisfazem a Propriedade do Eixo Principal.

Definição 5.1 (Corpo Pitagórico)**.** Um corpo $\mathbb{K}$ é pitagórico se toda soma de quadrados em $\mathbb{K}$ é um quadrado em $\mathbb{K}$.

Assim, por exemplo, os corpos $\mathbb{R}$ e $\mathbb{C}$ dos números reais e complexos respectivamente, são pitagóricos. O corpo $\mathbb{Q}$ não é pitagórico pois a soma $4+9$, por exemplo, não é um quadrado em $\mathbb{Q}$. Usando a terminologia introduzida até esta parte do trabalho temos a seguinte proposição:

Proposição 5.2. *Se $\mathbb{K}$ é um corpo com a Propriedade do Eixo Principal, então $\mathbb{K}$ é pitagórico e formalmente real. Além disso,* $\operatorname{car}(\mathbb{K}) = 0$.

Demonstração. Assumimos que $\mathbb{K}$ tem a Propriedade do Eixo Principal. Temos que mostrar que $\mathbb{K}$ é pitagórico. De fato, se $\operatorname{car}(\mathbb{K}) = 2$, então $a^2 + b^2 = (a+b)^2$ para todo $a, b \in \mathbb{K}$ e, portanto, um corpo de característica 2 é pitagórico. Assumimos agora que $\operatorname{car}(\mathbb{K}) \neq 2$. Sejam $a', b', c' \in \mathbb{K}$, tal que $c' = a'^2 + b'^2$ não é um quadrado. Neste caso $a'^2 \neq 0$, logo $1 + \left(\frac{b'}{a'}\right)^2 = \frac{c'}{a'^2}$ não é um quadrado. Seja $a = \frac{b'}{a'}$ e $b = \frac{c'}{a'^2}$, assim temos $b - 1 = a^2$ (como em Exemplo 1.7). Considere a matriz

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

Usando o argumento do Exemplo 1.7 pode-se verificar que a matriz T não tem autovalores em $\mathbb{K}$. Logo a matriz T não é diagonalizável. Portanto se $\mathbb{K}$ tem a Propriedade do Eixo Principal, então $\mathbb{K}$ é pitagórico.
Assumimos agora que $\mathbb{K}$ é pitagórico e vamos mostrar que $\mathbb{K}$ e formalmente real. De

fato, se $\mathbb{K}$ não é formalmente real, então $-1 = x_1^2 + \cdots + x_n^2$. Logo existe $i \in \mathbb{K}$, tal que $i = \sqrt{-1}$. Assim podemos considerar a matriz

$$Z = \begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix}$$

como em Exemplo 1.4. Como foi mostrado neste exemplo, o único autovalor da matriz Z é $\lambda = 0$ e, portanto, a matriz Z não é diagonalizável. Portanto, se $\mathbb{K}$ é pitagórico e $\mathbb{K}$ tem a Propriedade do Eixo Principal, então $\mathbb{K}$ é formalmente real. Assumimos, agora, que $\text{car}(\mathbb{K}) = p$ onde p é um primo. Se $p = 2$, então $\sqrt{-1} = 1$, logo $\mathbb{K}$ não é formalmente real. Se p é ímpar, então foi mostrado em Observação 1.8, de Exemplo 1.7, que existe um elemento $b \in \mathbb{K}$, tal que b é um quadrado mas $1 + b$ não é. Logo $\mathbb{K}$ não é pitagórico. Portanto $\text{car}(\mathbb{K}) = 0$. □

Portanto, para encontrar corpos que satisfazem a Propriedade do Eixo Principal devemos procurar entre corpos pitagóricos formalmente reais. Nestes corpos podemos introduzir um produto interno que tem as mesmas propriedades do produto interno sobre $\mathbb{R}$. Lembramos que $\sigma(\mathbb{K})$ significa o conjunto dos elementos de $\mathbb{K}$ na forma $x_1^2 + \cdots + x_n^2$.

Lema 5.3. *Seja $\mathbb{K}$ um corpo pitagórico formalmente real e seja $\geq$ uma relação de ordem sobre $\mathbb{K}$. Se $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n) \in \mathbb{K}^n$, definimos*

$$\langle u, v \rangle = u_1 v_1 + \cdots + u_n v_n.$$

Assim a aplicação

$$\langle \cdot, \cdot \rangle : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K} \tag{5.1}$$

satisfaz as seguintes propriedades.

(i): $\langle u, v \rangle = \langle v, u \rangle$ *(Simetria);*

(ii): $\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$ *(Bilinearidade);*

(iii): $\langle u, u \rangle \geq 0$, $\langle u, u \rangle \in \sigma(\mathbb{K})$, $\langle u, u \rangle = 0$ *se, e somente se,* $u = \bar{0}$ *(Positividade).*

(iv): Para cada $u \in \mathbb{K}^n$ existe um único elemento $\|u\| \in \mathbb{K}$ com $\|u\| \geq 0$ e $\|u\|^2 = \langle u, u \rangle$.

A aplicação $\langle \cdot, \cdot \rangle$ é chamada de *produto interno* em $\mathbb{K}^n$.

Demonstração. Seja $u, v, w \in \mathbb{K}^n$ e $\alpha, \beta \in \mathbb{K}$ temos que mostrar que:

(i) $\langle u, v \rangle = \langle v, u \rangle \in \mathbb{K}$. De fato, $\mathbb{K}$ é um corpo e, portanto $u_1 v_1 + \cdots + u_n v_n = v_1 u_1 + \cdots + v_n u_n \in \mathbb{K}$.

(ii) Seja $\alpha \in \mathbb{K}$. Então: $\langle \alpha u, v\rangle = \alpha\langle u, v\rangle$. De fato:

$$\begin{aligned}\langle \alpha u, v\rangle &= \langle \alpha(u_1, \ldots, u_n), (v_1, \ldots, v_n)\rangle \\ &= \langle (\alpha u_1, \ldots, \alpha u_n), (v_1, \ldots, v_n)\rangle \\ &= \alpha u_1 v_1 + \cdots + \alpha u_n v_n \\ &= \alpha(u_1 v_1 + \cdots + u_n v_n) \\ &= \alpha\langle u, v\rangle.\end{aligned}$$

(ii') $\langle u + w, v\rangle = \langle u, v\rangle + \langle w, v\rangle$. De fato:

$$\begin{aligned}\langle u + w, v\rangle &= \langle (u_1, \ldots, u_n) + (w_1, \ldots, w_n), (v_1, \ldots, v_n)\rangle \\ &= \langle (u_1 + w_1, \ldots, u_n + w_n), (v_1, \ldots, v_n)\rangle \\ &= (u_1 + w_1)v_1 + \cdots + (u_n + w_n)v_n \\ &= u_1 v_1 + w_1 v_1 + \cdots + u_n v_n + w_n v_n \\ &= \langle u, v\rangle + \langle w, v\rangle.\end{aligned}$$

Disto segue que $\langle \cdot, \cdot \rangle$ é uma forma bilinear simétrica.

(iii) $\langle u, u\rangle \geq 0$. De fato, por Corolário 4.4, $\mathbb{K}$ é formalmente real e, portanto, $\langle u, u\rangle = u_1 u_1 + \cdots + u_n u_n = u_1^2 + \cdots + u_n^2 \geq 0 \in \sigma(\mathbb{K})$. E, ainda: Se $u \neq \bar{0} \in \mathbb{K}^n$, então $u = (u_1, \ldots, u_i, \ldots, u_n)$, $u_i \neq 0$ e, portanto, $\langle u, u\rangle \neq 0$.

(iv) Resta mostrar que para todo $u \in \mathbb{K}^n$ existe, um único elemento $\|u\| \in \mathbb{K}$, tal que $\|u\| \geq 0$ e $\|u\|^2 = \langle u, u\rangle$. De fato: $\langle u, u\rangle = u_1 u_1 + \cdots + u_n u_n = u_1^2 + \cdots + u_n^2 \in \sigma(\mathbb{K})$. Como $\mathbb{K}$ é pitagórico, $\langle u, u\rangle \in \mathbb{K}^2$. Logo existe z, tal que $z^2 = \langle u, u\rangle$. De fato a equação $x^2 = \langle u, u\rangle$ tem duas soluções z e $-z$. Precisamente uma dessas soluções será maior ou igual a zero. □

As propriedades do produto interno em $\mathbb{K}^n$ são similares ao produto interno em $\mathbb{R}^n$. O valor $\|u\|$ em Lema 5.3 é chamado de norma de u.
Seja V um espaço vetorial munido de um produto interno. Um conjunto de vetores $\{v_1, \ldots, v_n\}$ em V é chamado um *conjunto ortogonal* se, quaisquer dois vetores distintos do conjunto são ortogonais, ou seja, $\langle v_i, v_j\rangle = 0$ para todo $i \neq j$. Um conjunto ortogonal de vetores, onde cada vetor tem norma 1, é chamado de *conjunto ortonormal*. O processo de multiplicar um vetor não-nulo, v, pelo inverso de sua norma para obter um vetor de norma 1, é chamado de *normalização* de v. O processo de ortonormalização de Gram-Schmidt, é um algoritmo que nos ensina a transformar um conjunto linearmente independente de vetores em um conjunto de vetores ortonormais. A seguir apresentamos o processo de Gram-Schmidt.
Seja V um espaço vetorial munido de um produto interno. Suponha que $\{v_1, \ldots, v_n\}$ é um conjunto de vetores linearmente independentes de V. Vamos produzir um conjunto de vetores ortogonais, $\{w_1, \ldots, w_n\}$. Em seguida produzimos um conjunto $\{u_1, \ldots, u_n\}$ de vetores ortonormais:

1º passo: Seja $w_1 = v_1$;

2º passo: Obter w_2 que é ortogonal a w_1 da seguinte forma: $w_2 = v_2 - \frac{\langle v_2, w_1\rangle}{\langle w_1, w_1\rangle} w_1$;

3º passo: Obter w_3 que é ortogonal a w_1 e w_2: $w_3 = v_3 - \frac{\langle v_3, w_1\rangle}{\langle w_1, w_1\rangle} w_1 - \frac{\langle v_3, w_2\rangle}{\langle w_2, w_2\rangle} w_2$;

4º passo: Obter w_4 que é ortogonal a w_1, w_2, w_3: $w_4 = v_4 - \frac{\langle v_4, w_1\rangle}{\langle w_1, w_1\rangle} w_1 - \frac{\langle v_4, w_2\rangle}{\langle w_2, w_2\rangle} w_2 - \frac{\langle v_4, w_3\rangle}{\langle w_3, w_3\rangle} w_3$.

Continuando dessa maneira obtemos no n-ésimo passo o vetor:

$$w_n = v_n - \frac{\langle v_n, w_1\rangle}{\langle w_1, w_1\rangle} w_1 - \frac{\langle v_n, w_2\rangle}{\langle w_2, w_2\rangle} w_2 - \frac{\langle v_n, w_3\rangle}{\langle w_3, w_3\rangle} w_3 - \frac{\langle v_n, w_4\rangle}{\langle w_4, w_4\rangle} w_4 - \cdots - \frac{\langle v_n, w_{n-1}\rangle}{\langle w_{n-1}, w_{n-1}\rangle} w_{n-1}.$$

E assim obtemos o conjunto $\{w_1, \ldots, w_n\}$ de vetores ortogonais.

5º passo: Normalizar os vetores obtidos: $u_1 = \frac{w_1}{\|w_1\|}, \ldots, u_n = \frac{w_n}{\|w_n\|}$.

Assim obtemos o conjunto $\{u_1, \ldots, u_n\}$, de vetores ortonormais, como queríamos.
Agora já podemos apresentar a questão levantada por E. A. Bender em [2].

Teorema 5.4. *Seja $\mathbb{K}$ um corpo pitagórico formalmente real. Então as seguintes afirmações são equivalentes:*

(i) $\mathbb{K}$ tem a Propriedade do Eixo Principal;

(ii) Toda matriz simétrica sobre $\mathbb{K}$ é diagonalizável, não necessariamente ortogonalmente, sobre $\mathbb{K}$;

(iii) Se M é uma matriz simétrica $n \times n$ sobre $\mathbb{K}$, então $\mathbb{K}$ contém n autovalores de M contando com multiplicidade;

(iv) Toda matriz simétrica $n \times n$ sobre $\mathbb{K}$ tem um autovalor em $\mathbb{K}$.

Demonstração. Primeiro notamos que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)$. Então temos que mostrar que:

$(iv) \Rightarrow (i)$: Seja $M \in \mathbb{K}$ uma matriz simétrica $n \times n$. Seja λ um autovalor de M. Vamos provar que M é ortogonalmente diagonalizável usando indução sobre n. De fato, para $n = 1$ o resultado é verdadeiro. Seja $\{e_1, \ldots, e_n\}$ a base canônica ortonormal para $\mathbb{K}^n$. Existe um autovetor $v \in \mathbb{K}^n$, associado ao autovalor λ, da matriz M. Seja $\{v_1 \ldots, v_n\}$ uma base de $\mathbb{K}^n$, tal que $v_1 = v$. Agora, usando o processo de ortogonalização de Gram-Schmidt, construímos uma base ortonormal, $\{u_1, \ldots, u_n\}$, para $\mathbb{K}^n$. Observamos que $u_1 = \frac{v}{\|v\|}$ é um autovetor de M associado ao autovalor λ. Seja P a matriz em que suas colunas são os vetores u_i. Então P é uma matriz ortogonal, ou seja, $P^tP = I$, logo $P^{-1} = P^t$. Seja $S = P^tMP$. Como

$$S^t = (P^tMP)^t = P^tM^tP = P^tMP,$$

então S é uma matriz simétrica. Logo a primeira coluna de S será:

$$Se_1 = P^tMPe_1 = P^tMu_1 = P^t\lambda u_1 = \lambda P^t u_1 = \lambda e_1 = \begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Como S é simétrica ela tem a seguinte forma:

$$S = \begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ \vdots & & & S_0 & & \\ 0 & & & & & \\ 0 & & & & & \end{pmatrix}$$

em que S_0 é uma matriz simétrica do tipo $(n-1)\times(n-1)$. Assim, por indução, existe uma matriz R_0 ortogonal do tipo $(n-1)\times(n-1)$, tal que $R_0^{-1} = R_0^t$ e $R_0^{-1}S_0R_0 = D$ em que D é uma matriz diagonal. Definimos a matriz:

$$R = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ \vdots & & & R_0 & & \\ 0 & & & & & \\ 0 & & & & & \end{pmatrix}$$

e consideramos a matriz PR. Podemos ver que $(PR)^{-1} = (PR)^t$, e

$$(PR)^{-1}M(PR) = \begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 0 & & & & & \\ 0 & & & & & \\ \vdots & & & D & & \\ 0 & & & & & \\ 0 & & & & & \end{pmatrix}$$

□

Seja $\mathbb{K}$ um corpo formalmente real. A extensão $\mathbb{K}\left(\sqrt{-1}\right)$ pode ser construída da seguinte forma. Seja $i = \sqrt{-1}$ e seja $\widetilde{\mathbb{K}}$ o conjunto de combinações lineares formais $\alpha + \beta i$, tal que $\alpha, \beta \in \mathbb{K}$. Definimos $(\alpha_1 + \beta_1 i) + (\alpha_2 + \beta_2 i) := (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)i$ e $(\alpha_1 + \beta_1 i)(\alpha_2 + \beta_2 i) := \alpha_1\alpha_2 - \beta_1\beta_2 + (\alpha_1\beta_2 + \alpha_2\beta_1)i$.

Afirmação 5.5. $\widetilde{\mathbb{K}}$ *é um corpo.*

Como $\mathbb{K}$ é formalmente real, podemos assumir por Teorema 4.11 que $\mathbb{K}$ é ordenado. Logo se $\alpha \in \mathbb{K} \setminus \{0\}$, então $\alpha < 0$ ou $0 < \alpha$, nos dois casos obtemos, por Definição 2.8(f), que $0 < \alpha^2$. Similarmente se $\beta \in \mathbb{K} \setminus \{0\}$, então $0 < \beta^2$. Logo, por Definição 2.8(e) $0 < \alpha^2 + \beta^2$.

Demonstração. Os axiomas de corpo em Definição 2.1 são claramente satisfeitos com a exceção de (M_5). Portanto verificaremos somente (M_5). Seja $\alpha + \beta i \in \widetilde{\mathbb{K}}$. Assim temos $(\alpha + \beta i)(\alpha - \beta i) = \alpha^2 + \beta^2 \neq 0 \in \mathbb{K}$. Logo $(\alpha + \beta i)\frac{\alpha-\beta i}{\alpha^2+\beta^2} = 1$. Ou seja, $(\alpha + \beta i)^{-1} = \frac{\alpha-\beta i}{\alpha^2+\beta^2} \in \widetilde{\mathbb{K}}$, todo elemento não nulo de $\widetilde{\mathbb{K}}$ possui inverso. Logo $\widetilde{\mathbb{K}}$ é a extensão de $\mathbb{K}$ por $\sqrt{-1}$. □

Definição 5.6 (Corpo Real Fechado)**.** Seja $\mathbb{K}$ um corpo. Dizemos que $\mathbb{K}$ é um corpo *real fechado* se $\mathbb{K}$ é pitagórico, formalmente real e $\mathbb{K}(\sqrt{-1})$ (a extensão de $\mathbb{K}$ por $\sqrt{-1}$) é algebricamente fechado.

Assim, em particular, o corpo dos números reais é um exemplo de corpo real fechado. Seja $\mathbb{K}$ um corpo real fechado. Denotaremos $\mathbb{K}(\sqrt{-1})$ por $\widetilde{\mathbb{K}}$. Se $c = \alpha + \beta i \in \widetilde{\mathbb{K}}$, então definimos $\bar{c} := \alpha - \beta i$. O elemento $\bar{c}$ é chamado o conjugado de c. As propriedades do conjugado são similares ao conjugado complexo. Nomeadamente $\bar{\bar{c}}_1 = c_1$, $\overline{c_1 + c_2} = \bar{c}_1 + \bar{c}_2$ e $\overline{c_1 c_2} = \bar{c}_1 \bar{c}_2$, para todo $c_1, c_2 \in \widetilde{\mathbb{K}}$. Além disso se $c = \alpha + \beta i \in \widetilde{\mathbb{K}}$, então $c\bar{c} = \alpha^2 + \beta^2 \in \sigma(\mathbb{K})$ e $c\bar{c} = 0$ se, e somente se, $c = 0$.

Proposição 5.7. *Seja $\mathbb{K}$ um corpo real fechado. A aplicação*

$$\begin{aligned} \langle \cdot, \cdot \rangle : \widetilde{\mathbb{K}}^n \times \widetilde{\mathbb{K}}^n &\to \mathbb{K} \\ (u, v) &\mapsto \langle u, v \rangle = u_1 \bar{v}_1 + \cdots + u_n \bar{v}_n \end{aligned}$$

satisfaz as seguintes propriedades. Seja $u, v, w \in \widetilde{\mathbb{K}}^n$ e $\alpha, \beta \in \mathbb{K}$.

(i) $\langle u, v \rangle = \overline{\langle v, u \rangle}$;

(ii) $\langle \alpha u + \beta v, w \rangle = \alpha \langle u, w \rangle + \beta \langle v, w \rangle$;

(iii) $\langle u, u \rangle \in \sigma(\mathbb{K})^*$, $\langle u, u \rangle = 0$ *se, e somente se,* $u = \bar{0}$ *onde* $\bar{0}$ *denota o vetor nulo em* $\widetilde{\mathbb{K}}^n$.

Demonstração. Se $v = (v_1, \ldots, v_n) \in \widetilde{\mathbb{K}}^n$, então definimos $\bar{v} = (\bar{v}_1, \ldots, \bar{v}_n)$. Seja $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ e $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \widetilde{\mathbb{K}}^n$. Usando essa notação $\langle u, v \rangle$ pode ser calculado como $u^t \bar{v}$ para todo $u, v \in \widetilde{\mathbb{K}}^n$. Logo

(i) $\overline{\langle v, u \rangle} = \overline{v_1 \bar{u}_1 + \cdots + v_n \bar{u}_n} = \bar{v}_1 u_1 + \cdots + \bar{v}_n u_n = \langle u, v \rangle$.

(ii) $\langle \alpha u + \beta v, w \rangle = (\alpha u + \beta v)^t \bar{w} = \alpha u^t \bar{w} + \beta v^t \bar{w} = \alpha \langle u, w \rangle + \beta \langle v, w \rangle$.

(iii) Se $u \neq \bar{0}$, então $\langle u, u \rangle = u_1 \bar{u}_1 + \cdots + u_n \bar{u}_n \in \sigma(\mathbb{K})^*$.

□

Se $u \in \widetilde{\mathbb{K}}$, então $\langle u,u\rangle \in \sigma(\mathbb{K})$ e $\langle u,u\rangle = 0$ se, e somente se, $u = \bar{0}$. Logo podemos definir a norma $\|u\|$ como $\|u\| := \sqrt{\langle u,u\rangle}$ onde $\sqrt{\langle u,u\rangle}$ significa a raíz de $\langle u,u\rangle$ que satisfaz $0 \leq \sqrt{\langle u,u\rangle}$. Assim temos: $u_j = \alpha_j + i\beta_j$, então $u_j\bar{u}_j = \alpha_j^2 + \beta_j^2$. Logo $\|u\| = \sqrt{\langle u,u\rangle} \in \mathbb{K}$. Seja B uma matriz simétrica sobre $\widetilde{\mathbb{K}}$. A matriz $\bar{B}^t$, transposta conjugada, será denotada por B^*. Logo:

(iv) $\langle Bv, Bv\rangle = (Bv)^t\overline{(Bv)} = v^t(B^t\bar{B}\bar{v}) = \langle v, \bar{B}^t\bar{\bar{B}}\bar{\bar{v}}\rangle = \langle v, B^*Bv\rangle$.

Uma matriz quadrada B sobre $\widetilde{\mathbb{K}}$ é *normal* se $BB^* = B^*B$. Um resultado similar com o próximo corolário pode ser encontrado em [10].

Corolário 5.8. *Seja Ω um corpo real fechado. Então:*

(i) Todo corpo real fechado satisfaz a Propriedade do Eixo Principal.

(ii) Seja $\{\mathbb{K}_\alpha\}$ uma coleção de subcorpos contidos em um corpo Ω. Se cada $\mathbb{K}_\alpha$ satisfaz a Propriedade do Eixo Principal, então a interseção $\bigcap_\alpha \mathbb{K}_\alpha$, também, satisfaz a Propriedade do Eixo Principal.

Para provar Corolário 5.8 precisaremos do próximo lema.

Lema 5.9. *Seja B uma matriz $n \times n$ normal com entradas em $\widetilde{\mathbb{K}}$ e seja $v \in \widetilde{\mathbb{K}}^n$. Então*

(a) $\|Bv\| = \|B^*v\|$;

(b) Se $Bv = \lambda v$, então $B^*v = \bar{\lambda}v$.

Demonstração. (a) Seja $B_{n\times n}$ uma matriz normal sobre $\widetilde{\mathbb{K}}$ e $v \in \widetilde{\mathbb{K}}^n$. Assim:

$$\begin{aligned} \|Bv\|^2 &= \langle Bv, Bv\rangle \\ &= \langle v, B^*Bv\rangle \qquad \text{(por item (iv) de Proposição 5.7)} \\ &= \langle v, BB^*v\rangle \\ &= \langle B^*v, B^*v\rangle \\ &= \|B^*v\|^2. \end{aligned}$$

(b) De fato, B é normal, então $B^* - \bar{\lambda}I$ é normal. Observe que $(B-\lambda I)^* = B^* - \bar{\lambda}I$. Assim

$$\begin{aligned} (B-\lambda I)(B-\lambda I)^* &= (B-\lambda I)(B^* - \bar{\lambda}I) \\ &= BB^* - (\lambda+\bar{\lambda})B + \lambda\bar{\lambda}I. \end{aligned}$$

Logo se B é normal, então $B - \lambda I$ e $B^* - \bar{\lambda}I$ são normais. Então

$$\begin{aligned} \|B^*v - \bar{\lambda}v\| &= \|(B^* - \bar{\lambda}I)v\| \\ &= \|(B-\lambda I)v\| = 0. \end{aligned}$$

Portanto $B^*v = \bar{\lambda}v$.

□

Demonstração de Corolário 5.8. (i) Vamos mostrar que *se A é uma matriz simétrica sobre $\mathbb{K}$, então A tem um autovalor λ em $\mathbb{K}$.* De fato, se $\widetilde{\mathbb{K}}$ é algebricamente fechado, então A tem autovalor em $\widetilde{\mathbb{K}}$. Se A é simétrica sobre $\mathbb{K}$, então $A = A^*$. Seja $v \in \widetilde{\mathbb{K}}^n$, tal que $Av = \lambda v$, logo por Lema 5.9 $Av = A^*v = \bar{\lambda}v$, assim $\lambda = \bar{\lambda}$ e, portanto $\lambda \in \mathbb{K}$.

(ii) Seja $A_{n\times n} = (a_{ij})$ uma matriz simétrica sobre $\mathbb{K}$. Assim $a_{ij} \in \mathbb{K}_\alpha$, para todo α. Como, por hipótese, todo $\mathbb{K}_\alpha$ tem a Propriedade do Eixo Principal, segue de Teorema 5.4, que A tem todos os seus autovalores em $\mathbb{K}_\alpha$, para todo α. Assim A tem seus autovalores em $\bigcap\limits_\alpha \mathbb{K}_\alpha$ e, portanto, $\bigcap\limits_\alpha \mathbb{K}_\alpha$ preserva a Propriedade do Eixo Principal.

□

Conclusão 5.10. O resultado em Corolário 5.8 nos mostra que a interseção de qualquer coleção de corpos real fechado (onde os corpos em questão são subcorpos de um corpo comum) satisfaz a Propriedade do Eixo Principal. De fato todo corpo que satisfaz a Propriedade do Eixo Principal pode ser escrito como interseção de corpos real fechado. Para ver isso, precisamos de um segundo resultado técnico devido a F. Krakowski [7].

Assumimos, como anteriormente, que todos os corpos considerados estão contidos em algum corpo maior. Seja $\mathbb{K}$ um corpo e seja Ω uma extensão, algebricamente fechada fixa, de $\mathbb{K}$. Logo temos

$$\mathbf{E}(\mathbb{K}) = \bigcap\{\mathbb{F} | \mathbb{K} \subseteq \mathbb{F} \subseteq \Omega \quad \text{e} \quad \mathbb{F} \quad \text{é real fechado}\}.$$

Assim, por exemplo, definimos o conjunto dos numeros reais algébricos da seguinte forma $\mathbf{E}(\mathbb{Q}) := \bigcap\{\mathbb{R} | \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \quad \text{e} \quad \mathbb{R} \quad \text{é real fechado}\}$.
Logo, por Teorema 4.11, se $\mathbb{K}$ não é formalmente real, então $\mathbf{E}(\mathbb{K})$ é trivial. Por outro lado se $\mathbb{K}$ é formalmente real, então $\mathbf{E}(\mathbb{K})$ é uma extensão pitagórica formalmente real de $\mathbb{K}$. O próximo teorema não será, aqui demonstrado, porém um esboço de sua prova pode ser encontrado em [3].

Teorema 5.11. *Seja $\mathbb{K}$ um corpo pitagórico formalmente real. Se $\omega \in \mathbf{E}(\mathbb{K})$, então existe uma matriz, M, simétrica sobre $\mathbb{K}$, tal que ω é um autovalor da matriz M.* □

A prova de Teorema 5.11 nos mostra que, se $\omega \in \mathbf{E}(\mathbb{K})$ tem um grau n sobre $\mathbb{K}$, então ω é um autovalor de alguma matriz M simétrica. E. Bender mostra em [2], que todo número real algébrico de grau n é um autovalor de alguma matriz, $M_{(n+1)\times(n+1)}$ simétrica, sobre $\mathbb{Q}$. Logo para um corpo arbitrário $\mathbb{K}$ e $\omega \in \mathbf{E}(\mathbb{K})$, devemos nos perguntar qual deve ser, exatamente, a ordem da matriz M com entradas em $\mathbb{K}$, para ter ω como autovalor. Assim, com o resultado de Teorema 5.11, estamos prontos para dar uma caracterização completa, através do próximo teorema, dos corpos que preservam a Propriedade do Eixo Principal.

Teorema 5.12. *Um corpo $\mathbb{K}$ satisfaz a Propriedade do Eixo Principal se, e somente se, $\mathbb{K}$ é a interseção de corpos real fechado.*

Demonstração.

($\Leftarrow$): Seja $\mathbb{K} = \bigcap_{\alpha} \mathbb{K}_\alpha$ onde $\mathbb{K}_\alpha$ são corpos real fechado. Por Corolário 5.8(ii) $\mathbb{K}_\alpha$ satisfaz a Propriedade do Eixo Principal para todo α. Por Corolário 5.8(i) $\mathbb{K}$ satisfaz a Propriedade do Eixo Principal.

($\Rightarrow$): Assumimos que $\mathbb{K}$ satisfaz a Propriedade do Eixo Principal. Mostraremos que $\mathbb{K} = \mathbf{E}(\mathbb{K})$. Claramente $\mathbb{K} \subseteq \mathbf{E}(\mathbb{K})$. Seja $\omega \in \mathbf{E}(\mathbb{K})$. Existe uma matriz M sobre $\mathbb{K}$, tal que ω é um autovalor de de M. Mas todos os autovalores de M estão em $\mathbb{K}$. Logo $\omega \in \mathbb{K}$. Assim $\mathbf{E}(\mathbb{K}) \subseteq \mathbb{K}$ e, portanto, $\mathbb{K} = \mathbf{E}(\mathbb{K})$. □

Conclusão 5.13. O resultado em Teorema 5.12 completa a caracterização dos corpos que satisfazem a Propriedade do Eixo Principal.
□

Referências Bibliográficas

[1] I. Bicudo, Histórias Paralelas: O V Postulado de Euclides e o Axioma da Escolha. Revista Brasileira de História da Matemática-Vol 5 nº 9 (abril/2005-setembro/2005)- p. 5-17. Publicação Oficial da Sociedade Brasileira de História da Matemática. Disponível em: http://www.rbhm.org.br/issues/RBHM% 20-% 20vol.5,% 20no9,% 20abril% 20(2005)/Bicudo% 20-% 20RBHM,% 20Vol.% 205,% 20no% 209,% 20p.% 205-17,% 202005.pdf. Acesso em: 04/04/2016.

[2] E. A. Bender, The dimensions of symmetric matrices with a given minimum polynomial, Linear Alg. Appl. 3 (1970) p. 115-123.

[3] David Mornhinweg, Daniel B. Shapiro and K. G. Valente, The Principal Axis Theorem Over Arbitrary Fields, The America Mathematical Monthly, vol. 100, No. 8 (Oct. 1993), pp. 749-754. Disponível em: http://www.jstor.org/stable/2324781. Acesso em: 09/05/2016.

[4] E. Lages Lima, Curso de análise v.1, 12.ed. - RJ: Associação Instituto Nacional de Matemática Pura e Aplicada, 2010. p. 39-68.

[5] H. Eves, Introdução a História da Matemática; tradução: Hygino H. Domingues - Campinas, SP: Editora UNICAMP, 2004. p. 674-677.

[6] S. H. Friedberg. Extending the principal axis theorem to fields other than $\mathbb{R}$, Amer. Math. Monthly 97(1990) p. 147-149.

[7] F. Krakowski, Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern, Comment. Math. Helv. 32 (1958) p. 224-240.

[8] R. SANCHIS, O Axioma da Escolha, o Lema de Zorn e o Teorema de Zermelo. Disponível em: http://www.mat.ufmg.br/∼rsanchis/AxiomaEscolha.pdf. Acesso em: 04/04/2016.

[9] R. J. Santos, Um Curso de Geometria Analítica e Álgebra Linear. - BH: Imprensa Universitária da UFMG, 2009. p. 341-424.

[10] R. J. Santos, Álgebra Linear e Aplicações. - BH: Imprensa Universitária da UFMG, 2013. p. 165-185.

[11] W. Scharlau, Quadratic and Hermitian Forms, Springer Verlag, Berlin-Heidelberg-New York-Tokyo, 1985. p. 106-108.