

CORPOS FORMALMENTE REAIS, VALORIZAÇÕES
E GRUPO DE GALOIS

OSVALDO GERMANO DO ROCIO

Orientador

Prof. Dr. TENKASI M. WISVANATHIAN

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do título de Mestre em Matemática Pura.

- 1982 -

UNICAMP
BIBLIOTECA CENTRAL

À memória de meu pai
José Germano Neto.

ÍNDICE

INTRODUÇÃO	i
CAPÍTULO I - VALORIZAÇÕES E ORDENS	1
I.1 - Ordens Compatíveis com Valorizações	1
I.2 - Corpos Henselianos Formalmente Reais	19
I.3 - Exemplos e Aplicações	24
CAPÍTULO II - QUESTÕES DE DENSIDADE EM CORPOS VALORIZADOS .	42
II.1 - Topologia de um Corpo Valorizado e Subcorpos Densos .	42
II.2 - Subcorpos Densos de Corpos Reais Fechados	47
II.3 - Exemplos.	52
CAPÍTULO III - CORPOS HEREDITARIAMENTE PITAGÓRICOS E GRUPOS	
DE GALOIS	57
III.1 - Generalização do Teorema de Artim-Schreier	57
III.2 - Corpos Hereditariamente Pitagóricos e Estritamente	
Pitagóricos	62
III.3 - Caracterização de Corpos Hereditariamente Pitagó-	
ricos	69
III.4 - Caracterização de Corpos Hereditariamente Eucli-	
deanos	81
III.5 - Exemplos	83
CAPÍTULO IV - CORPOS COM A PROPRIEDADE DE MUDANÇA DE SINAL.	88
IV.1 - Grupos de Valores e Polinômios Definidos	89
IV.2 - Corpos Residuais e Polinômios Definidos	97
CAPÍTULO V - UM TEOREMA DE KAPLANSKY SOBRE CORPOS REAIS FE-	
CHADOS	105
BIBLIOGRAFIA	115

INTRODUÇÃO

Este trabalho nasceu de uma tentativa de estudar sistematicamente aspectos da teoria de corpos formalmente reais, relacionadas com a teoria das valorizações. A primeira prova de tal relacionamento, encontra-se num trabalho de S. Lang [9] e um grande passo no assunto deu-se com um trabalho marcante de A. Prestel [17] onde, em certos casos, é dada a descrição completa de todas as ordens de um corpo formalmente real.

No capítulo I, desenvolveremos aspectos gerais da relação existente entre corpos formalmente reais e valorizações reais, isto é, corpos valorizados com corpos residuais, formalmente reais. Motivados por tal relação, no parágrafo três de tal capítulo, mostraremos que o corpo $\mathbb{R}(X)$ possui, a menos de um $\mathbb{R}$ -automorfismo de ordem sobre $\mathbb{R}(X)$, uma única ordem (I.3.5a). Prosseguindo, mostraremos, também, que todas as ordens não-arquimedianas do corpo $\mathbb{Q}(X)$ são restrições de ordens de $\mathbb{R}(X)$, (I.3.7).

Seja $(K, \leq)$ um corpo ordenado. Se $f(X) \in K[X]$ é um polinômio tal que $f(a)f(b) < 0$ para certos elementos $a, b \in K$, então, f tem uma raiz no fecho real $\tilde{K}$ de $(K, \leq)$. Este é um resultado fundamental da teoria dos corpos formalmente reais. Por outro lado, conforme (IV.1.2), a recíproca deste resultado não é verdadeira.

Se para todo elemento $\alpha \in \tilde{K}$, o polinômio minimal f de α sobre K for tal que $f(a)f(b) < 0$, para certos elementos $a, b \in K$, então, dizemos que $(K, \leq)$ tem a *propriedade de mudança de sinal*.

Se $(K, \leq)$ não admitir extensão ordenada de grau par ou, se $(K, \leq)$ for denso em $\tilde{K}$, no sentido de que entre dois elementos distintos de $\tilde{K}$ existe um elemento de K , então, $(K, \leq)$ tem tal propriedade ; isto não é difícil de se vêr. Os corpos ordenados com a propriedade de não possuírem extensão ordenadas de grau par, são caracterizados como corpos hereditariamente euclidianos, [18]. Interessamo-nos, pela recíproca deste fato; a saber, dado um corpo formalmente real K com a propriedade de mudança de sinal, será que K é denso em seu fecho real, ou é hereditariamente euclidiano? O Teorema (IV.2.4), devido a Viswanathan, responde afirmativamente a essa pergunta e trata de uma bela aplicação da técnica de valorizações reais, devido a Lang e Prestel.

Para o estudo de questões de densidade, dedicamos o Capítulo II. Aí, tal assunto, é visto sobre dois pontos de vista diferentes: No primeiro, usamos a topologia de Hahn definida por uma valorização e, no segundo, usamos a topologia intervalo aberto, definida por uma ordem $\leq$. No segundo caso, a técnica do Capítulo I é bastante usada. Ressaltamos que os resultados principais do Capítulo II são os teoremas (II.1.3) devido a Engler e (II.2.5) devido a Viswanathan.

O principal resultado do Capítulo III, é o Teorema (III.4.1), devido a Geyer e Prestel-Ziegler, que será imprescindível para o Capítulo V. Tal Capítulo trata de uma família de corpos mais amplo que a de corpos hereditariamente euclidianos, a saber, a classe de corpos hereditariamente pitagóricos. Procedemos assim, porque a melhor maneira de estudar a primeira família de corpos é

o estudo da segunda. O Capítulo III é baseado em trabalhos de Becker [3] e é desenvolvido com o conceito de extensões quadraticamente fechadas, ao invés de extensões algebricamente fechadas, como é usual.

Finalmente, no Capítulo V, motivados pelos estudos realizados nos Capítulos I e II, encerramos nosso trabalho, com um estudo sobre a estrutura de completamento de um corpo valorizado real fechado. O principal resultado deste capítulo é o Teorema (V.4), devido a Kaplansky. Tal teorema tem uma demonstração bastante simplificada usando os resultados dos Capítulos I e II.

Assim, esta tese une alguns resultados de Lang, Prestel, Viswanathan, Engler, Geyer, Prestel-Ziegler e Becker.

CAPÍTULO I

VALORIZAÇÃO E ORDENS

Neste capítulo introduziremos uma técnica importante, devido a Lang [15] e Prestel [17], da teoria de valorizações em estudos de corpos formalmente reais. A noção de compatibilidade de ordens, com certas valorizações de um corpo formalmente real K , leva a uma dependência, do conjunto de ordens de K , com grupos de valores e corpos de restos associados a estas valorizações. Estes resultados, (1.8) e (1.17). As ordens de K , obtidas desta maneira, são todas não-arquimedianas (Corolário (1.2a)). Reciprocamente, toda ordem não-arquimediana de um corpo formalmente real provém de uma valorização compatível (Teorema (1.13a)).

Há dois casos importantes neste estudo: o caso em que K é um corpo real-fechado com uma ordem não-arquimediana e o caso em que K é um corpo valorizado Henseliano. Estes casos são tratados no Parágrafo 2. Finalmente no Parágrafo 3, abordaremos exemplos sugeridos pelas técnicas deste capítulo.

1. ORDENS COMPATÍVEIS COM VALORIZAÇÕES

1.1. DEFINIÇÃO. Seja $(K, \leq)$ um corpo ordenado e v uma valorização de K . Dizemos que v é compatível com $\leq$ (ou que $\leq$ é compatível com v) se quaisquer que forem os elementos $a, b \in K$, com $0 < a < b$, ocorrer $v(b) \leq v(a)$.

Iniciamos com algumas observações simples sobre grupos ordenados abelianos. Estes fatos podem ser encontrados em Ribemboim [20], Bigard [4] ou em Engler [17].

Sejam $(G, \leq)$ um grupo abeliano ordenado e $H \subseteq G$. Dizemos que H é convexo em G com relação a $\leq$ se H satisfaz a seguinte condição:

$$0 < x \leq y \text{ com } y \in H \implies x \in H.$$

Se H for um subgrupo do grupo abeliano $(G, \leq)$, e queremos munir o grupo quociente G/H com uma estrutura de grupo ordenado, é natural proceder da seguinte maneira, em G/H , $g+H \geq 0$ se existe $a \geq 0$ em G tal que $g+H = a+H$. Para que esta relação defina uma estrutura de grupo ordenado, é necessário e suficiente que H seja um subgrupo convexo de G . Note que, se $g+H > 0$, nesta ordem, então $g > 0$ e daí $g > h$ para todo $h \in H$. A ordem é chamada de ordem quociente de G por H e o grupo quociente G/H munido desta ordem é chamado de grupo quociente ordenado $(G, \leq)$ por H .

1.2. PROPOSIÇÃO. Sejam $(K, \leq)$ um corpo ordenado e v uma valorização de K . Então são equivalentes.

- (1) A ordem $\leq$ é compatível com a valorização v .
- (2) O anel de valorização A_v é convexo em $(K, \leq)$
- (3) O ideal de valorização M_v é convexo em $(A_v, \leq)$
- (4) O corpo residual K_v é um corpo ordenado com a ordem quociente de A_v por M_v .

DEMONSTRAÇÃO. (1) $\Rightarrow$ (2). Sejam $a, b \in K$ tais que $b \in A_V$ e $0 < a \leq b$. Então pela compatibilidade segue que $v(b) \leq v(a)$, e como $0 \leq v(b)$ temos então que $a \in A_V$.

(2) $\Rightarrow$ (3). Sejam $a \in A_V$ e $m \in M_V$ tais que $0 < a < m$. Se $a \notin M_V \Rightarrow a^{-1} \in A_V$. Mas $0 < m^{-1} < a^{-1}$, e como A_V é convexo em K , temos, então, que $m^{-1} \in A_V$, um absurdo.

(3) $\Rightarrow$ (4). Segue das observações feitas anteriores a proposição.

(3) $\Rightarrow$ (1). Sejam $a, b \in K$ tais que $v(a) < v(b)$ e $a > 0$. Então $v(ba^{-1}) > 0$ e daí $ba^{-1} \in M_V$. Como M_V é convexo segue que $ba^{-1} < 1$, isto é, $b < a$. Assim v é compatível com $\leq$.

1.2a. COROLÁRIO. Se $\leq$ é compatível com v , e v é não trivial, então a ordem $\leq$ é não-arquimédiana.

DEMONSTRAÇÃO. Basta observar que, $\forall x \in M_V \quad \forall n \in \mathbb{N}, nx < 1$ e que $M_V \neq 0$.

A proposição (1.2) afirma que se $\leq$ é uma ordem compatível com uma valorização não trivial de K , então o corpo residual K_V é ordenado com cone positivo $\bar{P}_V = \{a + M_V \mid a \geq 0\}$ em A_V .

Então, surge logo a seguinte pergunta: Como construir a ordem P de K partindo da ordem $\bar{P}_V$ de K_V ? É natural esperar que nesta construção, o grupo de valores G , de v desempenhe um papel relevante.

Assim a volta de $\bar{P}_v$ para P é feita via G , e para isto precisamos do conceito de q -seção de v .

Observemos que se v é compatível com $\leq$, então Q , o corpo primo de K , está contido em A_v .

1.3. DEFINIÇÃO. Uma q -seção de uma valorização $v: \dot{K} \longrightarrow G$ é uma aplicação $s: G \longrightarrow \dot{K}$ satisfazendo:

$$q1) \quad s(0) = 1$$

$$q2) \quad v(s(g)) = g, \text{ para todo } g \in G$$

$$q3) \quad s(g+h) \equiv s(g) \cdot s(h) \pmod{\dot{K}^2}, \text{ para todo } g, h \in G.$$

Como consequência imediata da definição temos:

1.4. PROPOSIÇÃO. Se s é uma q -seção da valorização $v: \dot{K} \longrightarrow G$, então

$$a) \quad s(2g) \in \dot{K}^2$$

$$b) \quad \text{Se } g \equiv h \pmod{2G}, \text{ então, } s(g) \equiv s(h) \pmod{\dot{K}^2}.$$

DEMONSTRAÇÃO. (a) $s(2g) \equiv s(g)^2 \pmod{\dot{K}^2}$, então $s(2g)s(g)^{-1} \in \dot{K}^2$, como $s(g)^2 \in \dot{K}^2$, que é grupo multiplicativo, concluímos que $s(2g) \in \dot{K}^2$.

(b) Notemos que se $g \in G$, então por q_3 $s(-g) \equiv s(g)^{-1} \pmod{\dot{K}^2}$. Suponhamos que $g \equiv h \pmod{2G}$, então $g-h \in 2G$ logo, por (a), $s(g-h) \in \dot{K}^2$. Por q_3 $s(g-h) \equiv s(g)s(-h) \pmod{\dot{K}^2}$, então $s(g-h) \equiv s(g)s(h)^{-1} \pmod{\dot{K}^2}$ e assim $s(g) \equiv s(h) \pmod{\dot{K}^2}$.

1.5. PROPOSIÇÃO. Para toda valorização $v: K^* \longrightarrow G$ existe uma q -seção de v .

DEMONSTRAÇÃO. Se $g \in G$, definimos $s(2g) = a^2$, onde a é escolhido em $X_g = \{a \in K^*; v(a) = g\}$; em particular definimos $s(0) = 1$. Consideremos agora o grupo quociente $G/2G$ como um espaço vetorial sobre o corpo $\mathbb{Z}/2\mathbb{Z}$. Seja B um subconjunto de G tal que $\{g + 2G; g \in B\}$ seja uma base do espaço vetorial $G/2G$. Se $g \in G$, definimos $s(g) = a$, onde a é escolhido em X_g . Vamos agora definir s globalmente. Para todo $g \in G$ existem elementos $g_1, g_2, \dots, g_n$, em B , tais que $g = g_1 + \dots + g_n + 2g'$ para algum $g' \in G$. Daí definimos $s(g) = s(g_1)s(g_2)\dots s(g_n)s(2g')$. s é bem definida, pois todo $\bar{g} \in G/2G$ se escreve de maneira única como combinação linear dos elementos da base.

$$(q_1) \quad s(0) = 1 \quad \text{por definição}$$

$$(q_2) \quad v(s(g)) = v(s(g_1)) + \dots + v(s(g_n)) + v(s(2g')) = \\ = g_1 + \dots + g_n + 2g' = g, \quad \text{para todo } g \in G.$$

$$(q_3) \quad \text{Sejam } g, h \in G. \quad g = g_1 + g_2 + \dots + g_n + 2g' \quad \text{e} \\ h = h_1 + \dots + h_r + 2h' \quad \text{para certos } g_i, h_j \in B \quad \text{e } g', h' \in G. \text{ Suponhamos que } g_i = h_i, \quad 0 \leq i \leq \ell, \text{ onde } \ell \leq \min\{n, r\} \text{ e } g_0 = h_0 = 0. \\ \text{Então, } g+h = g_{\ell+1} + \dots + g_n + h_{\ell+1} + \dots + h_r + 2(g' + h' + g_1 + \dots + g_\ell), \text{ donde } \\ s(g+h) = s(g_{\ell+1}) \dots s(g_n) s(h_{\ell+1}) \dots s(h_r) \cdot s(2(g'+h' + g_1 + \dots + g_\ell)). \text{ Portanto, } s(g+h) \cdot (s(g) s(h))^{-1} = \\ = [s(g_{\ell+1}) \dots s(g_n) s(h_{\ell+1}) \dots s(h_r) s(2(g'+h'+g_1 + \dots + g_\ell))] / \\ / [(s(g_1) \dots s(g_\ell))^2 \cdot s(g_{\ell+1}) \dots s(g_n) s(h_{\ell+1}) \dots s(h_r) s(2g') \cdot s(2h')] \\ = [s(2(g'+h'+g_1 + \dots + g_\ell))] / [(s(g_1) \dots s(g_\ell))^2 s(2g') \cdot s(2h')] \in K^{*2}.$$

daí, $s(g+h) \equiv s(g)s(h) \pmod{\dot{K}^2}$ e assim q é uma q -seção de v .

Na próxima proposição relacionaremos uma ordem P , compatível com uma valorização v de K , com o grupo de valores e o corpo de restos de v .

1.6. PROPOSIÇÃO. *Sejam $v : \dot{K} \rightarrow G$ uma valorização de K , $s : G \rightarrow \dot{K}$ uma q -seção de v e P uma ordem de K compatível com v . Então P induz:*

i) Um homomorfismo $\sigma_P : G/2G \rightarrow \{-1, 1\}$ de $G/2G$ no grupo multiplicativo $\{1, -1\}$ dado por $\sigma_P(\bar{g}) := 1$ se, e somente se $s(g) \in P$.

ii) Uma ordem $\bar{P}_v$ do corpo residual K_v dada da seguinte maneira: $b + M_v \in \bar{P}_v$ se, e somente se existe $p \in P$ tal que $b + M_v = p + M_v$.

DEMONSTRAÇÃO. Vamos mostrar inicialmente que σ_P é bem definida. Se $\bar{g} = \bar{h}$, isto é, $g \equiv h \pmod{2G}$, então, por (1.4b), $s(g) \equiv s(h) \pmod{\dot{K}^2}$; daí, $s(g)s(h)^{-1} \in \dot{K}^2 \subset P$. Logo $s(g)$ e $s(h)$ possuem o mesmo sinal, portanto $\sigma_P(\bar{g}) = \sigma_P(\bar{h})$.

σ_P é um homomorfismo de grupos: Sejam $g, h \in G$, então,

$$\sigma_P(\bar{g} + \bar{h}) = 1 \Leftrightarrow s(g+h) \in P$$

$$\Leftrightarrow s(g) \cdot s(h) \in P$$

$$\Leftrightarrow s(g), s(h) \in P \text{ ou } s(g), s(h) \notin P$$

$$\Leftrightarrow \sigma_P(\bar{g}) \cdot \sigma_P(\bar{h}) = 1.$$

$$\begin{aligned}
\sigma_P(\bar{g} + \bar{h}) = -1 &\Leftrightarrow s(g) \cdot s(h) \notin P \\
&\Leftrightarrow s(g) \in P \text{ e } s(h) \notin P \text{ ou } s(g) \notin P \text{ e } s(h) \in P \\
&\Leftrightarrow \sigma_P(\bar{g}) \cdot \sigma_P(\bar{h}) = -1
\end{aligned}$$

Logo $\sigma_P(\bar{g} + \bar{h}) = \sigma_P(\bar{g}) \cdot \sigma_P(\bar{h}) \quad \forall g, h \in G$, e assim σ_P é de fato um homomorfismo de grupos.

Mostremos agora que $\bar{P}_V$ é uma ordem de K_V .

a) Sejam $a + M_V, b + M_V \in \bar{P}_V$ e suponhamos que $a, b \in U_V \cap P$. Então, pela compatibilidade de v , $v(a+b) = 0$, donde $a+b \in U_V \cap P$. Assim $(a+M_V) + (b+M_V) \in \bar{P}_V$, portanto $\bar{P}_V + \bar{P}_V \subseteq \bar{P}_V$.

b) $\bar{P}_V \cdot \bar{P}_V \subseteq \bar{P}_V$ pois $a, b \in U_V \cap P \Rightarrow a \cdot b \in U_V \cap P$.

c) $P_V \cap -P_V = 0$ pois, se $a, b \in P \cap A_V$ e $a+M_V = -b+M_V \Rightarrow a+b \in M_V$. Como $0 \leq a \leq a+b$, $0 \leq b \leq a+b$ e M_V é convexo, temos então que $a, b \in M_V$.

d) $\bar{P}_V \cup -P_V = K_V$ (claramente).

Dizemos que $\bar{P}_V$ é a ordem canônica sobre K_V induzida por P .

Queremos traçar o caminho de volta para P , partindo de $\bar{P}_V$ e σ_P .

1.7. PROPOSIÇÃO. Sejam $v: \dot{K} \rightarrow G$ uma valorização de K , $s: G \rightarrow K$ uma q -seção de v , $\bar{Q}$ uma ordem de K_V e $\sigma: G/2G \rightarrow \{-1, 1\}$ um homomorfismo de grupos. Então $(\bar{Q})_{\sigma}^{\bullet} = \{a \in \dot{K} \mid \frac{a}{s(v(a))} \cdot \sigma(va) + M_V \in \bar{Q}^{\bullet}\}$ é uma ordem de K , compatível com v .

DEMONSTRAÇÃO. (a) $(\bar{Q})_{\sigma}^{\cdot} + (\bar{Q})_{\sigma}^{\cdot} \subseteq (\bar{Q})_{\sigma}^{\cdot}$: Sejam $a, b \in (\bar{Q})_{\sigma}^{\cdot}$ elementos quaisquer. Então $\frac{a\sigma(\bar{v}a)}{s(v(a))} + M_V \in \bar{Q}^{\cdot}$ e $\frac{b\sigma(\bar{v}b)}{s(v(b))} + M_V \in \bar{Q}^{\cdot}$, daí $(\frac{a\sigma(\bar{v}a)}{s(v(a))} + M_V) + (\frac{b\sigma(\bar{v}b)}{s(v(b))} + M_V) \in \bar{Q}^{\cdot}$. Temos dois casos:

CASO 1: Se $v(a) = v(b)$, então $\frac{\sigma(\bar{v}a)(a+b)}{s(va)} + M_V \in \bar{Q}^{\cdot}$, donde $v(a+b) = v(a)$. Assim $\frac{(a+b)\sigma(\bar{v}a)}{s(va)} + M_V = \frac{(a+b)\sigma(\bar{v}(a+b))}{s(v(a+b))} + M_V \in \bar{Q}^{\cdot}$, donde $a+b \in (\bar{Q})_{\sigma}^{\cdot}$.

CASO 2. Se $v(a) \neq v(b)$, podemos supor que $v(a) < v(b)$, neste caso $v(a \pm b) = v(a)$ e $v(\frac{\pm b\sigma(\bar{v}a)}{s(va)}) = v(\pm b - va) > 0$. Então

$$\frac{a\sigma(\bar{v}a)}{s(v(a))} + M_V = \frac{(a \pm b)\sigma(\bar{v}a)}{s(va)} + M_V = \frac{(a \pm b)\sigma(\bar{v}(a \pm b))}{s(v(a \pm b))} + M_V \in \bar{Q}^{\cdot}.$$

Portanto $a \pm b \in (\bar{Q})_{\sigma}^{\cdot}$.

b) $(\bar{Q})_{\sigma}^{\cdot}(\bar{Q})_{\sigma}^{\cdot} \subseteq (\bar{Q})_{\sigma}^{\cdot}$: Sejam $a, b \in (\bar{Q})_{\sigma}^{\cdot}$ elementos quaisquer.

Temos que $s(v(a) + v(b)) = s(va).s(vb) = \alpha^2$ para algum $\alpha \in \dot{K}$;

assim obrigatoriamente $\alpha \in U_V$. Como σ é homomorfismo de grupos,

$$\text{tem-se: } \frac{a.b\sigma(\bar{v}(a.b))}{s(v(a.b))} + M_V = \frac{a.b(\sigma(\bar{v}a) \cdot (\bar{v}b))}{s(va)s(vb)\alpha^2} + M_V = (\frac{a\sigma(\bar{v}a)}{s(va)} + M_V) \cdot (\frac{b\sigma(\bar{v}b)}{s(vb)} + M_V).$$

$(\frac{b\sigma(\bar{v}b)}{s(vb)} + M_V) \cdot ((\frac{1}{\alpha})^2 + M_V)$. Como $\bar{Q}^{\cdot}$ é ordem de K_V e $a, b \in (\bar{Q})_{\sigma}^{\cdot}$ concluímos que $a.b \in (\bar{Q})_{\sigma}^{\cdot}$.

c) $(\bar{Q})_{\sigma}^{\bullet} \cup -(\bar{Q})_{\sigma}^{\bullet} = \dot{K}$: Decorre do fato de $\bar{Q}$ ser ordem e $v(a) = v(-b)$ $\forall a \in K$.

d) $(\bar{Q})_{\sigma}^{\bullet}$ é compatível com v : Decorre de a), 2º caso, ao notar que $v(a) < v(b)$, $a, b \in (\bar{Q})_{\sigma}^{\bullet} \Rightarrow a-b \in (\bar{Q})_{\sigma}^{\bullet}$.

O seguinte resultado é importante, uma vez que ele descreve o conjunto de ordens de um corpo K , compatível com uma valorização dada.

1.8. TEOREMA (Prestel). Seja $v: \dot{K} \rightarrow G$ uma valorização de K tal que K_v seja formalmente real e s uma q -seção de v . Então as construções de (1.6) e (1.7) produzem uma correspondência inversível entre $\{P; P \text{ é ordem de } K \text{ compatível com } v\}$ e $\{\bar{Q}; \bar{Q} \text{ é ordem de } K_v\} \times \{\sigma; \sigma \text{ é homomorfismo de } G/2G \text{ em } \{-1, 1\}\}$.

DEMONSTRAÇÃO. Seja $\dot{P}$ uma ordem de K compatível com v e σ_P , $\bar{P}_v$ definidos em (1.6). Então $a \in (\bar{P}_v)_{\sigma_P}^{\bullet} \Rightarrow \frac{a}{s(v(a))} \sigma_P(\bar{v}(a)) + M_v \in \dot{P}_v \Rightarrow \frac{a}{s(v(a))} \sigma_P(\bar{v}(a)) \in U_v \cap P \Rightarrow a \in P$, pois, pela definição de σ_P , $\sigma_P(\bar{v}(a)) \cdot \frac{1}{s(v(a))} \in P$. Logo $(\bar{P}_v)_{\sigma_P}^{\bullet} \subseteq P$ donde $(\bar{P}_v)_{\sigma_P}^{\bullet} = \dot{P}$, pois ambos são cones positivos.

Seja agora σ um homomorfismo de $G/2G$ em $\{-1, 1\}$, $\bar{Q}$ uma ordem de K_v , e consideremos $(\bar{Q})_{\sigma}^{\bullet}$ como foi construído em (1.7). Mostremos inicialmente que $\sigma(\bar{Q})_{\sigma}^{\bullet} = \dot{\sigma}$. Seja $g \in G$. Pela definição de $\sigma(\bar{Q})_{\sigma}^{\bullet}$, temos que $\sigma(\bar{Q})_{\sigma}^{\bullet}(g) \cdot s(g) \in (\bar{Q})_{\sigma}^{\bullet}$ e isto acontece, se, e somente

$$\text{se } \frac{\sigma_{(\bar{Q})_\sigma} \cdot (\bar{g}) s(g) \cdot \overline{\sigma(v(\sigma_{(\bar{Q})_\sigma} \cdot (\bar{g}) s(g)))}}{s(v(\sigma_{(\bar{Q})_\sigma} \cdot (\bar{g}) s(g)))} + M_V = \sigma_{(\bar{Q})_\sigma} \cdot (\bar{g}) \sigma(\bar{g}) + M_V \in \bar{Q}.$$

Como σ e $\sigma_{(\bar{Q})_\sigma}$ assumem seus valores em $\{-1,1\}$, temos então que

$$\sigma_{(\bar{Q})_\sigma}(\bar{g}) = \sigma(\bar{g}), \text{ donde } \sigma_{(\bar{Q})_\sigma} = \sigma.$$

Resta mostrar que $(\bar{Q}, \sigma) = \overline{((\bar{Q})_\sigma)_V}$, $\sigma_{(\bar{Q})_\sigma}$. Seja $a \in \dot{K}$, se $a + M_V \in \overline{((\bar{Q})_\sigma)_V} \Rightarrow a \in U_V \cap (\bar{Q})_\sigma \Rightarrow a \in (\bar{Q})_\sigma \Rightarrow \frac{a}{s(va)} \sigma(va) + M_V \in \bar{Q}$. Como $a \in U_V$, temos $v(a) = 0$, $s(va) = 1$ e $\sigma(va) = 1$, donde $a + M_V \in \bar{Q}$. Logo, $\overline{((\bar{Q})_\sigma)_V} \subseteq \bar{Q}$; donde $\bar{Q} = \overline{((\bar{Q})_\sigma)_V}$.

O resultado que segue, fornece um critério para que um corpo formalmente real, possua uma ordem compatível com uma valorização v .

1.9. COROLÁRIO. Seja $v: \dot{K} \rightarrow G$ uma valorização de K . Então as seguintes afirmações são equivalentes:

- 1) Existe uma ordem P de K , compatível com v .
- 2) O corpo residual K_V é formalmente real.

DEMONSTRAÇÃO. (1) $\Rightarrow$ (2): Segundo (1.6), P fornece uma ordem $\bar{P}_V$ de K_V . (2) $\Rightarrow$ (1): Seja σ o homomorfismo constante de $G/2G$ em $\{-1,1\}$ cujo valor é 1. Se $\bar{Q}$ é uma ordem de K_V , a Proposição (1.7) proporciona uma ordem $(\bar{Q})_\sigma$ de K , compatível com v .

Observemos que, se o número de ordens do corpo K , compatíveis

com uma valorização v de K for um inteiro finito r , então fixada uma q -seção de v , teremos $r = m.n$, onde m = o número de ordens de K_v e n = o número de homomorfismo de $G/2G$ no grupo multiplicativo $\{-1,1\}$.

1.10. DEFINIÇÃO. Uma valorização v , não trivial, de K satisfazendo as condições equivalentes do Corolário (1.9), será denominada de valorização real de K .

Reparamos que na literatura sobre valorizações, às vezes uma valorização é dita real, se ela for de posto 1 e a função valorização assume valores reais, usando-se uma notação multiplicativa. Achamos melhor, no caso, usar a frase "valorização real exponencial". De qualquer modo, no progresso desta tese, não há possibilidade de confusão.

Vamos agora verificar a forma dos anéis de valorização, associados a valorizações reais de um corpo K .

1.11. DEFINIÇÃO. Sejam $(K, \leq)$ um corpo ordenado e $A \subset B$ subconjunto de K ; então A é dito *ser cofinal* em B , com respeito a ordem $\leq$, se para todo $b \in B$, existir $a \in A$ tal que $|b| \leq a$. Se F for um subconjunto de K , denotaremos o subconjunto $\{\alpha \in K ; |\alpha| \leq a \text{ para algum } a \in F\}$ de K , por $A_F^{\leq}$ ou A_F quando não houver chance de interpretações difusas. Lembremo-nos, de que $|\alpha|$ denota α se $0 \leq \alpha$ e $-\alpha$ se $\alpha < 0$.

1.12. LEMA. Seja $(K, \leq)$ um corpo ordenado e F um subcorpo de K . Então $A_F^{\leq}$ é um anel de valorização de K , convexo com respeito à ordem dada $\leq$.

DEMONSTRAÇÃO. Sejam $\alpha, \beta \in A_F$ e $a, b \in F$ tais que $|\alpha| \leq a$, $|\beta| \leq b$; então $|\alpha + \beta| \leq |\alpha| + |\beta| \leq a + b \in F$ e $|\alpha \cdot \beta| \leq a \cdot b \in F$. Assim A_F é fechado por adição e multiplicação.

Se $\alpha \in K$ e $\alpha \notin A_F$, então $a < |\alpha|$ para todo $a \in F$ donde $|\alpha^{-1}| < |a|$ para todo $a \in F$. Portanto $\alpha^{-1} \in A_F$. As outras propriedades são óbvias. Assim A_F é um anel de valorização de K , convexo em $(K, \leq)$.

Observemos que o ideal maximal M_F de A_F é o conjunto $\{0\} \cup \{\alpha \in A_F \mid \alpha^{-1} \notin A_F\} = \{0\} \cup \{\alpha \in A_F \mid |\alpha| < |a| \forall a \in F\}$. Segundo Lang, [15] os elementos não nulos de M_F são ditos *infinitamente pequenos* sobre F , e esta propriedade é representada por $\alpha \ll F$.

Se $\alpha \in K$ e $\alpha \notin A_F$ então α é dito ser *infinitamente grande* sobre F , e escreve-se $\alpha \gg F$.

Assim $A_F = \{\alpha \in K \mid \alpha \gg F\}$ e seu ideal maximal é $M_F = \{\alpha \in K \mid \alpha \ll F\} \cup \{0\}$.

Por (1.12) e (1.2), se F não for cofinal em $(K, \leq)$, $A_F^{\leq}$ será um anel de valorização não trivial, e teremos uma valorização v compatível com a ordem de K . A valorização v é real. Neste caso diremos apenas que $A_F^{\leq}$ é um anel de valorização real.

Mostraremos que todo anel de valorização real de um corpo K é do tipo $A_F^{\leq}$ para algum subcorpo F de K , e alguma ordem $\leq$ de K .

1.13. PROPOSIÇÃO. Seja $(K, \leq)$ um corpo ordenado, então:

(a) o conjunto dos anéis de valorização convexos com respeito a $\leq$ é totalmente ordenado e $A_Q^{\leq}$ é elemento mínimo de tal conjunto.

(b) se v_1, v_2 são valorizações de K tais que v_1 é compatível com $\leq$ e $A_{v_1} \subset A_{v_2}$, então v_2 é compatível com $\leq$.

DEMONSTRAÇÃO. (a) Sejam A_1, A_2 anéis de valorização de K , convexos com relação a $\leq$. Se $A_1 \not\subseteq A_2$, então $\exists y \in A_1$ tal que $y \notin A_2$. Assim, da convexidade de A_2 , $|x| < |y| \quad \forall x \in A_2$; daí $A_2 \subseteq A_1$.

Seja agora A um anel de valorização convexo com relação a $\leq$. $Q \subseteq A$; consideremos $A_Q^{\leq}$ como foi definido em (1.11); então para todo $\alpha \in A_Q^{\leq}$ existe $r \in Q \subset A$ tal que $\alpha \leq r$; como A é convexo concluímos que $A_Q^{\leq} \subseteq A$.

(b) Sejam $a, b \in K$ com $0 < a$ e $v_2(a) < v_2(b)$, então $v_2(ab^{-1}) < 0 \Rightarrow ab^{-1} \notin A_{v_2} \Rightarrow ab^{-1} \notin A_{v_1} \Rightarrow v_1(ab^{-1}) < 0 \Rightarrow v_1(a) < v_1(b)$, daí $b < a$ pois v_1 é compatível com $\leq$. Portanto v_2 é de fato compatível com $\leq$.

O seguinte resultado, fornece uma recíproca do corolário (1.2a).

1.13a. TEOREMA. Seja $(K, \leq)$ um corpo ordenado. Então $\leq$ é uma ordem não arquimediana $\iff$ existe uma valorização não trivial v de K compatível com $\leq$.

DEMONSTRAÇÃO. $\Leftarrow$) Corolário (1.2a). $\Rightarrow$) Suponhamos que $\leq$ é não-arquimediana. Então o anel de valorização $A_Q^<$ é convexo em $(K, \leq)$ e é não-trivial. Logo a valorização de $A_Q^<$ é compatível com $\leq$, isto por (1.2).

1.13b. OBSERVAÇÃO. No exemplo (3.1) consta a construção explícita da valorização dada por $A_Q^<$.

1.14. PROPOSIÇÃO. Sejam $v: K \rightarrow G$ uma valorização de K , $F \subset A_v$ um subcorpo de K e $\pi: A_v \rightarrow K_v$ o place canônico de K associado a v . Então $\pi|_F: F \rightarrow K_v$ é injetor; mais ainda, se F for um subcorpo maximal de A_v , então $K_v|_{\pi F}$ será uma extensão algébrica de corpos.

DEMONSTRAÇÃO. Temos que $F \cap M_v = \{0\}$, já que F é um corpo, donde segue que $\pi|_F$ é injetor e assim πF é um subcorpo de K_v .

Suponhamos agora, que F seja um subcorpo maximal de A_v . Seja $\alpha \in A_v$ e suponhamos que $\alpha \notin F$. Então $F(\alpha) \not\subset A_v$ e assim $F(\alpha) \cap M_v \neq \{0\}$. Sejam $f(x) = x^n + a_1 x^{n-1} + \dots + a_n \in F[x] \subset A_v[x]$ e $g(x) = x^m + b_1 x^{m-1} + \dots + b_m \in F[x] \subset A_v[x]$ tais que

$f(\alpha) g(\alpha)^{-1} \neq 0$ e $f(\alpha) g(\alpha)^{-1} \in M_V$, então $0 < v(f(\alpha)g(\alpha)^{-1}) =$
 $= v(f(\alpha)) - v(g(\alpha))$, donde $v(f(\alpha)) > v(g(\alpha)) \geq 0$; assim
 $f(\alpha) \in M_V$, isto é, $\bar{f}(x) = x^n + \pi a_2 x^{n-2} + \dots + \pi a_n \in \pi F[x]$,
 é tal que $\bar{f}(\bar{\alpha}) = \bar{0}$ ($\bar{\alpha} = \alpha + M_V$). Portanto, de fato, $K_V | \pi F$ é
 extensão algébrica.

1.15. LEMA. Seja $(K, \leq)$ um corpo ordenado e $K|F$ uma extensão algébrica de corpos. Então F é cofinal em K com respeito a F .

DEMONSTRAÇÃO. Seja $\alpha \in K$, $\alpha > 0$, e $f(x) = x^n + a_1 x^{n-1} + \dots + a_n \in F[x]$
 tal que $f(\alpha) = 0$. Se $u = \max\{1, |a_1| + |a_1| + \dots + |a_n|\}$, en-
 tão $u \in F$, e mais ainda, todas as raízes de f , num fecho real
 R , de $(K, \leq)$, estão no intervalo $(-u, u)$ de R . Assim, $|\alpha| < u \in F$.

1.16. OBSERVAÇÃO. Lembremo-nos da teoria de valorizações, que se $K|F$ é uma extensão algébrica de corpos e se A_1, A_2 são anéis de valorização de K tais que $A_1 \subset A_2$ e $A_1 \cap F = A_2 \cap F$, então $A_1 = A_2$.

Os próximos dois teoremas tratam de uma versão mais forte que Prestel deu, a dois resultados devido a Lang.

1.17. TEOREMA. Sejam $(K, \leq)$ um corpo ordenado e A um anel de valorização de K , convexo com relação a $\leq$. Indicamos por M, v, π e K_V o ideal maximal de A , a valorização de K , o place de K associados

a A e o corpo residual K_v de v , respectivamente. Então existe um subcorpo F de K tal que $A = A_F^{\leq}$; mais ainda, pode se escolher F de maneira que F seja algebricamente fechado em K e $K_v|_{\pi F}$ seja uma extensão algébrica de corpos.

DEMONSTRAÇÃO. Seja P o cone positivo de K associado a $\leq$. Como A é convexo com respeito a P , temos que $\bar{P}_v = \{a + M_A; a \in U_A \cap P\} \cup \{0\}$ é um cone positivo de K_v , e que $Q \subseteq A$, sendo Q o corpo primo de K . Então, pelo lema de Zorn, concluímos que existem subcorpos maximais contidos em A . Seja F um deles. Por (1.14), $K_v|_{\pi F}$ é uma extensão algébrica, então, por (1.15), πF é cofinal em K_v com respeito a $\bar{P}_v$. Daí, F é cofinal em A , pois, se $\alpha \in A$, então $\bar{\alpha} = \alpha + M \in K_v$ donde existiria um elemento $a \in F$ tal que $(a + M) - (\alpha + M) = (a - \alpha) + M \in \bar{P}_v$. Daí $a - \alpha \in U_A \cap P$ e $a - \alpha \in P$, ou seja $\alpha < a$. Portanto, $A \subseteq A_F^{\leq}$. Agora, se $\alpha \in A_F^{\leq}$, então existe $a \in F \subset A$ tal que $|\alpha| \leq a$ donde $A_F^{\leq} \subset A$, pois A é convexo. Portanto, $A = A_F^{\leq}$.

Seja F um subcorpo maximal de A , vamos mostrar que F é algebricamente fechado em K . Para isto, seja $\alpha \in K$ um elemento qualquer algébrico sobre F . Então F é cofinal em $F(\alpha) = F[\alpha]$, na ordem induzida de K . Assim, $F(\alpha) \subset A_F^{\leq} = A$, mas como F é um subcorpo maximal contido em A , temos $\alpha \in F$.

1.18. COROLÁRIO. Seja $v: \dot{K} \longrightarrow G$ uma valorização real de K . Então existe uma ordem $\leq$ de K e um subcorpo F de K tal que $A_v = A_F^{\leq}$.

DEMONSTRAÇÃO. Seja $\leq$ ordem de K compatível com v . Por (1.2) A_v é convexo com respeito a $\leq$. Então, por (1.17), existe um subcorpo F de K tal que $A_v^{\leq} = A_F^{\leq}$.

O próximo teorema responde a uma pergunta importante: Se v é uma valorização real de um corpo K e $L|K$ é uma extensão de corpos, como estender v a uma valorização real de L ?

1.19. TEOREMA. Seja $v: \dot{K} \longrightarrow G$ uma valorização real de K e $\leq$ uma ordem de K . Seja $\tilde{K}$ um fecho real de $(K, \leq)$. Então v se estende a uma valorização real $\tilde{v}$ de $\tilde{K}$ se, e somente se a ordem $\leq$ é compatível com v .

Caso v se estenda a $\tilde{K}$, esta extensão é única, a menos de equivalência e $\tilde{K}_{\tilde{v}}$ é o fecho real de $(K_v, \bar{P}_v)$, sendo $\bar{P}_v$ a ordem canônica induzida sobre K_v por P , a ordem de K .

DEMONSTRAÇÃO. $\Rightarrow$) Suponhamos que v se estenda a uma valorização real $\tilde{v}$ de $\tilde{K}$. Então, por (1.18), $A_{\tilde{v}} = A_{\tilde{F}}^{\bar{P}}$, onde $\tilde{F}$ é um subcorpo de $\tilde{K}$ e $\bar{P}$ é uma ordem de $\tilde{K}$. Agora $\tilde{K}$ tem uma única ordem, logo $\bar{P} \cap K = P$. Repare que $A_{\tilde{v}} \cap K = A_v$. Daí A_v é convexo com respeito a P e $\leq$ é compatível com v .

Para mostrar a unicidade de $\tilde{v}$, quando existe; suponhamos que v_1 seja uma outra extensão de v a uma valorização real de $\tilde{K}$. Então v_1 é compatível com $\tilde{P}$, a única ordem de $\tilde{K}$. Daí, por (1.13) $A_{V_1} \subset A_{\tilde{V}}$ ou $A_V \subset A_{V_1}$, como $A_{\tilde{V}} \cap K = A_{V_1} \cap K$ e $\tilde{K}|K$ é extensão algébrica, por (1.16), $A_{\tilde{V}} = A_{V_1}$. Portanto $\tilde{v}$ é equivalente a v_1 .

$\Leftarrow$) Suponhamos que P seja compatível com v . Por (1.17) $A_V = A_F^P$ para algum subcorpo F de K , onde podemos supor que F é subcorpo maximal contido em A_V e que $K_V|\pi F$ é uma extensão algébrica. Seja $\tilde{K}$ o fecho real de (K, P) e $\tilde{P}$ sua única ordem. Então $A_F^{\tilde{P}}$ é anel de valorização de $\tilde{K}$ estendendo $A_V = A_F^P$ e assim, se $\tilde{v}$ é uma valorização de $\tilde{K}$, associada a $A_F^{\tilde{P}}$, teremos que $\tilde{v}$ é valorização de $\tilde{K}$ estendendo v e compatível com $\tilde{P}$; isto é, $\tilde{v}$ é uma valorização real de $\tilde{K}$ estendendo v .

Para concluir a demonstração, resta mostrar que $\tilde{K}_{\tilde{V}}$ é o fecho real de $(K_V, \tilde{P}_V)$. Para isto, seja F_1 o fecho real de $(F, P \cap F)$ contido em $\tilde{K}$. Então F_1 é real fechado e desde que F é cofinal em F_1 ($F_1|F$ é extensão algébrica) concluímos que $F_1 \subset A_F^{\tilde{P}} = A_{\tilde{V}}$. Se $\tilde{\pi}$ é o place canônico de $\tilde{K}$, associado a $\tilde{v}$, então, por (1.14), $\tilde{\pi}F_1 \subset F_1$ é um subcorpo real fechado do corpo ordenado $(\tilde{K}_{\tilde{V}}, \tilde{P}_{\tilde{V}})$, onde $\tilde{P}_{\tilde{V}} = \{\alpha + M_V \mid \alpha \in U_{\tilde{V}} \cap \tilde{P}\}$.

Agora, $\tilde{K}_{\tilde{V}}|\pi F$ é extensão algébrica, pois $\tilde{K}_{\tilde{V}}|K_V$ e $K_V|\pi F$ são extensões algébricas. Como $F \subset F_1$ e $\tilde{\pi}$ estende π , concluímos que $\tilde{K}_{\tilde{V}}|\tilde{\pi}F_1$ é extensão algébrica. Daí, $(\tilde{K}_{\tilde{V}}, \tilde{P}_{\tilde{V}})$ é real fechado e

portanto é o fecho real de $(K_v, \bar{P}_v)$.

1.20. COROLÁRIO. Se (K, v) é um corpo real fechado e v é compatível com a única ordem de K , então o corpo residual K_v é real fechado.

Podemos reunir os resultados (1.2), (1.9), (1.12) e (1.18) da seguinte maneira. Repare que ele já sugere uma maneira de descrever todas as ordens de um corpo formalmente real como veremos no parágrafo seguinte.

1.21. TEOREMA. Seja (K, v) um corpo valorizado. Então as seguintes afirmações são equivalentes.

- 1) Existe uma ordem P de K compatível com v .
- 2) v é uma valorização real.
- 3) Existe uma ordem P de K na qual A_v é convexo.
- 4) Existe uma ordem P de K na qual M_v é convexo.

2. CORPOS HENSELIANOS FORMALMENTE REAIS.

Como mencionamos no fim do parágrafo anterior, os métodos desenvolvidos no mesmo, são suficientes para dar uma descrição completa de todas as ordens, em alguns casos. Um caso importante é o caso de corpos henselianos.

Vamos primeiramente, fazer um breve resumo dos fatos que serão mais usados neste parágrafo, a respeito de corpos valorizados henselianos.

Assumiremos como definição de corpo henseliano, a propriedade que geralmente é conhecida como Lema de Hensel.

2.1. DEFINIÇÃO. Um corpo valorizado (K, v) é dito *henseliano*, se para qualquer polinômio mônico $f(x) \in A_v[x]$ e para todo $a \in A_v$, tal que $f(a) \in M_v$ e $f'(a) \notin M_v$, existe $b \in A_v$ tal que $f(b) = 0$ e $b - a \in M_v$.

Se, além de ser henseliano, o corpo valorizado (K, v) for formalmente real, diremos que (K, v) é um corpo henseliano formalmente real.

Lembre-mos de que uma extensão de corpos valorizados (K_1, v_1) de (K, v) é *imediate* se os monomorfismos naturais de G_v em G_{v_1} e de K_v em K_{v_1} forem sobrejetores. Aqui, K_v e G_v indicam o corpo residual de v e o grupo de valores de v , respectivamente.

A seguinte proposição contém os fatos sobre corpos henselianos, que usaremos neste parágrafo. Sua demonstração pode ser encontrada em Endler [9] ou Ribemboim [19].

2.2. PROPOSIÇÃO. Seja (K, v) um corpo valorizado. Então são válidas as seguintes afirmações:

1) (K, v) é henseliano se, e somente se a valorização v de K se estende, de maneira única, para qualquer extensão algébrica de K .

2) Se a característica do corpo residual K_v é zero, então (K, v) é henseliano se, e somente se não existe extensão algébrica imediata própria de (K, v) .

3) Para todo corpo valorizado (K, v) existe, a menos de um isomorfismo sobre (K, v) , uma única extensão algébrica imediata de (K, v) que é henseliano.

Se $K^H | K$ for a única extensão da Alínea 3), da Proposição (2.2), então K^H é chamado de Henselização ou fecho Henseliano de (K, v) .

O próximo resultado mostra a simplicidade de um corpo henseliano formalmente real.

2.3. PROPOSIÇÃO. Seja (K, v) um corpo valorizado henseliano. Então K é formalmente real se, e somente se K_v é formalmente real. Mais ainda, toda ordem de K é compatível com v .

DEMONSTRAÇÃO. $\Leftarrow$) Se K_v é formalmente real, então, por (1.9), K é formalmente real.

$\Rightarrow$) Seja $\leq$ uma ordem de K . Usando (1.9), basta mostrar que $\leq$ é compatível com v . Façamos isto: Sejam $a, b \in K$ elementos tais que $0 < a$ e $v(a) < v(b)$. Então $ba^{-1} \in M_v$. Ora; $f(x) = x^2 + x + ba^{-1} \in A_v[x]$ é um polinômio e $f(x) \equiv x^2 + x \pmod{M_v}$. $f(0) = 0 \in M_v$, $f'(0) = 1 \notin M_v$. Neste caso, do fato de (K, v) ser henseliano, existem elementos $c, d \in K$ tais que $f(x) = (x+c)(x+d) = x^2 + (c+d)x + dc$. Daí $c+d=1$ e $ba^{-1} = cd$, assim $(c-c^2)a = c(1-c)\frac{b}{cd} = (1-c)\frac{b}{d} = \frac{(1-c)}{(1-c)}b = b$. ($c \neq 1$, pois $d \neq 0$ e $b \neq 0$). Assim $0 \leq a(\frac{1}{2} - c)^2 = a(\frac{1}{4} - c - c^2) = \frac{1}{4}a - a(c - c^2) = \frac{1}{4}a - b$, donde $b \leq \frac{1}{4}a \leq a$. Portanto $\leq$ é compatível com v .

O significado do resultado anterior é que, se (K, v) é henseliano e v é uma valorização real de K , então o conjunto das ordens de K , compatíveis com v , coincide com o conjunto de todas as ordens de K .

Este resultado juntamente com (1.8), (1.9), (1.18), (1.19) e (1.21) são os que proporcionam à teoria de valorizações um papel significativo em estudos de corpos formalmente reais.

2.4. COROLÁRIO. Se (K, v) é um corpo henseliano formalmente real e v é uma valorização não trivial, então toda ordem de K é não arquimediana.

DEMONSTRAÇÃO. Se $\leq$ é uma ordem de K , então, por (2.3), $\leq$ é compatível com v . Daí, por (2.3), $\leq$ é não arquimediana.

2.5. PROPOSIÇÃO. Seja (K, v) um corpo valorizado e (K_1, v_1) sua henselização. Se v é uma valorização real, então, a menos de equivalência, v_1 é a única valorização real de K_1 , estendendo v .

DEMONSTRAÇÃO. (K_1, v_1) é extensão imediata de (K, v) , então $(K_1)_{v_1}$ é isomorfo a K_v . Assim v_1 é valorização real de K_1 . Para mostrar a unicidade de v_1 , seja v_2 uma outra valorização real de K_1 , estendendo v . Se fixarmos uma ordem P_1 de K_1 , concluímos, por (2.3), que P_1 é compatível com v_1 e v_2 . Daí, por (1.13), $A_{v_1} \subset A_{v_2}$ ou $A_{v_2} \subset A_{v_1}$. Como $K \cap A_{v_1} = K \cap A_{v_2}$ e $K_1 | K$ é uma extensão algébrica, concluímos, por (1.16), que v_2 é equivalente a v_1 . Portanto, a menos de equivalência, v_1 é a única valorização real de K_1 estendendo v .

2.6. TEOREMA (Prestel). Seja $v: K \rightarrow G$ uma valorização real de K com corpo residual K_v . Então, K é realmente fechado se, e somente se:

- 1) O grupo G é divisível
- 2) O corpo K_v é real fechado
- 3) (K, v) é henseliano.

DEMONSTRAÇÃO. $\Rightarrow$) Suponhamos que K é real fechado e denotemos por P sua única ordem. Como v é valorização real, temos então que P é compatível com v . Vamos demonstrar 1), 2) e 3).

1) Dado $g \in G$, seja $a \in P$ tal que $v(a) = (g)$. Como K é real fechado, dado $n \in \mathbb{Z}_+$, existe $b \in K$ tal que $a = b^n$. Daí, $g = v(a) = nv(b)$.

2) K_v é real fechado pelo Corolário (1.20).

3) Vamos usar ((2.2), (2)): K_v é formalmente real, em particular, a característica de K_v é zero. Como K é real fechado, a única extensão algébrica de K é $K(i)$ ($i = \sqrt{-1}$). Se $(K(i), v_1)$, for extensão imediata de (K, v) , para alguma valorização v_1 , então v_1 é valorização real de $K(i)$, o que não pode acontecer, pois $K(i)$ não é formalmente real. Então a única extensão algébrica imediata que (K, v) admite, é a trivial. Como a característica de K_v é zero, temos então que (K, v) é de fato henseliano.

$\Leftarrow$) Suponhamos agora 1), 2) e 3). Seja P uma ordem de K compatível com v . Então, por (1.19), v estende-se a uma única valorização real $\tilde{v}$ de $\tilde{K}$, onde $\tilde{K}$ é um fecho real de (K, P) e, mais ainda, o corpo residual $\tilde{K}_v$ é isomorfo ao fecho real do corpo ordenado

$(K_v, \bar{P}_v)$, sendo $\bar{P}_v$ a ordem canônica de K_v , induzida por P . Agora, por (2), K_v é real fechado; então $\tilde{K}_v \simeq K_v$. Se $\tilde{G}$ é o grupo de valores de $\tilde{v}$, podemos supor $G \subseteq \tilde{G}$. Assim, do fato de $\tilde{K}|K$ ser uma extensão algébrica, o grupo quociente $\tilde{G}/G$ é de torção. Logo, dado $a \in \tilde{G}$, existe $m \in \mathbb{Z}_+$ tal que $ma \in G$; isto é, $ma = g$ para algum $g \in G$; por (1) existe $g' \in G$ tal que $g = mg'$, então $ma = g = mg' \Rightarrow m(a - g') = 0$. Como $a - g' \in \tilde{G}$, que é um grupo totalmente ordenado, (portanto sem torção), concluímos que $a = g' \in G$. Assim $\tilde{G} = G$. Portanto $(\tilde{K}, \tilde{v})$ é uma extensão imediata de (K, v) . Agora, $\tilde{K}|K$ é uma extensão algébrica; (K, v) é henseliano e a característica de K_v é zero. Então, por (2.2, (2)), concluímos que $K \simeq \tilde{K}$; isto é, K é de fato real fechado.

3. EXEMPLOS E APLICAÇÕES

Usando a técnica dos Parágrafos 1 e 2 vamos dar explicitamente todas as ordens do corpo de frações racionais $\mathbb{R}(X)$ e descrever as ordens de $\mathbb{Q}(X)$. Vamos, também, dar explicitamente, todas as ordens dos corpos de séries formais $\mathbb{R}[[X]]$ e $\mathbb{Q}[[X]]$.

No primeiro exemplo (ver Wiswanathan [22]) descreveremos a valorização associada ao anel de valorização A_Q^P , de um corpo ordenado não-arquimediano (K, P) , definido em (1.12).

3.1. EXEMPLO.

Sejam $(K, <)$ um corpo ordenado, $\mathbb{Q}$ o corpo primo de K e $\mathbb{Z}$ o conjunto dos inteiros de K . Denotemos por S o conjunto das classes

arquimedianas de K' ; isto é, S é o conjunto quociente de K' pela relação de equivalência $\sim$, definida da seguinte forma: $x \sim y$ se se existem inteiros $m, n \in \mathbb{Z}$, tais que $|x| \leq |my|$ e $|y| \leq |nx|$ (ver [22], pag. 90). Note que $x \sim 0 \iff x = 0$ e assim $\bar{0} \notin S$. Definindo em S a operação $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$ = a classe arquimediana contendo xy , S torna-se um grupo abeliano, onde temos: o elemento identidade de S é a classe arquimediana $\bar{1}$, onde 1 é o elemento identidade de K ; o inverso $(\bar{x})^{-1}$ de $\bar{x} \in S$ é a classe arquimediana $\overline{x^{-1}}$ $\in S$.

Sejam $\bar{x}, \bar{y} \in S$, dizemos que $\bar{x} \leq \bar{y}$ se existe $n \in \mathbb{Z}$ tal que $|y| \leq |nx|$. Essa relação define uma estrutura de grupo totalmente ordenado em S ; pois:

a) Se $\bar{x} \leq \bar{y}$ e $\bar{y} \leq \bar{x}$, então existem inteiros $m, n \in \mathbb{Z}$ tais que $|y| \leq |nx|$ e $|x| \leq |my|$ e assim $\bar{x} = \bar{y}$

b) Se $\bar{x} \leq \bar{y}$ e $\bar{y} \leq \bar{z}$, então existem inteiros não nulos $m, n \in \mathbb{Z}$ tais que $|y| \leq |nx|$ e $|z| \leq |my|$. Daí $|z| \leq |my| = |m| |y| \leq |m| |nx| = |m \cdot n x|$ e como $m \cdot n \in \mathbb{Z}$ segue que $\bar{x} \leq \bar{z}$.

c) Se $\bar{x} \leq \bar{y}$ e $\bar{z} \in S$, então existe $n \in \mathbb{Z}$ tal que $|y| \leq |nx|$ donde $|z| |y| \leq |z| |nx|$, ou seja $|zy| \leq |nxz|$. Logo $\bar{z} \cdot \bar{x} \leq \bar{z} \cdot \bar{y}$.

d) Se $\bar{x}, \bar{y} \in S$ e $\bar{x} \not\leq \bar{y}$, então $|nx| \leq |y|$ qualquer que seja $n \in \mathbb{Z}$. Logo $|x| \leq |y|$ e assim $\bar{y} \leq \bar{x}$.

Desse modo, S é de fato um grupo abeliano totalmente ordenado. Daqui pra frente, trataremos S como grupo aditivo em vez de grupo multiplicativo.

Definimos agora uma aplicação v de K^* em S , por $v(x) = \bar{x} =$ a classe arquimediana de x ; v assim definido é uma valorização de K^* ; pois:

$$a) \quad v(x \cdot y) = \overline{xy} = \bar{x} + \bar{y} = v(x) + v(y)$$

b) Sejam $x, y \in K^*$ e suponhamos que $\min\{\bar{x}, \bar{y}\} = \bar{x}$, isto é, que $\bar{x} \leq \bar{y}$. Então existe $n \in \mathbb{Z}$ tal que $|y| \leq |nx|$. Logo $|x + y| \leq |x| + |y| \leq |x| + |nx| = |(n+1)x|$, donde $\bar{x} \leq \overline{x+y}$ e, assim, $v(x+y) = \overline{x+y} \geq \bar{x} = \min\{v(x), v(y)\}$.

Portanto, v é uma valorização de K e tem como anel de valorização $A_v = \{x \in K^* \mid v(x) \geq \bar{0}\} \cup \{0\} = \{x \in K^* \mid |x| \leq |n| \text{ para algum } n \in \mathbb{Z}\} \cup \{0\} = A_Q^{\leq} =$ o anel de valorização de K definido em (1.12).

Vamos agora, mencionar certos fatos, bem conhecidos da teoria das valorizações, que nos permitirão descrever todas as valorizações reais dos corpos $\mathbb{Q}(X)$ e $\mathbb{R}(X)$.

3.2. Sejam, K um corpo, X uma indeterminada sobre K e v uma valorização do corpo $K(X)$ das frações racionais sobre K . Se v é trivial sobre K , então v é uma valorização $p(X)$ -ádica, onde $p(X) \in K[X]$ é um polinômio irreduzível, ou v é a valorização ∞ -ádica dada pelo grau.

Se v é uma valorização $p(X)$ -ádica, então seu corpo residual é isomorfo ao corpo $K[X]/p(X)$, onde $p(X)$ é o ideal maximal de $K[X]$, gerado por $p(X)$. Se v é a valorização ∞ -ádica, então, seu corpo residual é isomorfo ao corpo K .

Se v é uma valorização real do corpo $\mathbb{R}(X)$, onde $\mathbb{R}$ é o corpo dos números reais, então, por (1.18), $v|_{\mathbb{R}}$ é a valorização trivial de $\mathbb{R}$. Assim, v deve ser uma das valorizações $p(X)$ -ádicas de $\mathbb{R}(X)$, ou a valorização ∞ -ádica denotada por v_{∞} . Agora, se $p(X) \in \mathbb{R}[X]$ é um polinômio irredutível, então $p(X) = X - \alpha$, onde $\alpha \in \mathbb{R}$ ou $p(X) = (X - \alpha)^2 + \beta$, onde $\alpha, \beta \in \mathbb{R}$ com $\beta \neq 0$. Por (3.2), o corpo residual da valorização $((X - \alpha)^2 + \beta)$ -ádica é isomorfa a $\mathbb{C}$, o corpo dos números complexos, e o corpo da valorização $(X - \alpha)$ -ádica, denotada por v_{α} , é isomorfo a $\mathbb{R}$.

Notemos que, se $\alpha \neq \beta$ são números reais, então $v_{\alpha}(X - \alpha) = 1$, $v_{\alpha}(X - \beta) = 0$, $v_{\beta}(X - \alpha) = 0$ e $v_{\beta}(X - \beta) = 1$ e assim as valorizações v_{α} e v_{β} de $\mathbb{R}(X)$ não são comparáveis. Note também que as valorizações v_{∞} e v_{β} , onde $\alpha \in \mathbb{R}$ não são comparáveis.

Resumidamente temos.

3.3. PROPOSIÇÃO. *As únicas valorizações reais de $\mathbb{R}(X)$, são as valorizações $(X - \alpha)$ -ádicas, onde $\alpha \in \mathbb{R}$, denotadas por v_{α} , e a valorização ∞ -ádica, v_{∞} , dada pelo grau. Mais ainda, se $\alpha, \beta \in \mathbb{R} \cup \{\infty\}$ e $\alpha \neq \beta$, então os anéis de valorização A_{α} e A_{β} correspondentes às valorizações v_{α} e v_{β} , respectivamente, não são comparáveis.*

Vamos agora descrever as valorizações reais do corpo $Q(X)$.

Seja v uma valorização real de $Q(X)$, então, como em $\mathbb{R}(X)$, v é uma das valorizações $p(X)$ -ádicas de $Q(X)$ ou a valorização ∞ -ádica denotada por v_∞ dada pelo grau. Por (3.2) v_∞ é valorização real de $Q(X)$ e o corpo residual da valorização $p(X)$ -ádica, denotada por $v_{p(X)}$, é isomorfo ao corpo $Q[X]/(p(X))$. Logo $v_{p(X)}$ é uma valorização real de $Q(X)$ se, e somente se $Q[X]/(p(X))$ é um corpo formalmente real, ou seja, se, e somente se $p(X)$ tem raízes em $\mathbb{R}$. No caso em que isto aconteça, o número de ordens de $Q[X]/(p(X))$ é exatamente igual ao número raízes reais do polinômio $p(X) \in Q[X]$.

Resumidamente temos:

3.4. PROPOSIÇÃO. As únicas valorizações reais de $Q(X)$ são as valorizações $p(X)$ -ádicas, denotadas por $v_{p(X)}$, onde $p(X) \in Q[X]$ é um polinômio irredutível tendo raízes reais, e a valorização v_∞ dada pelo grau. Estas valorizações são duas a duas incomparáveis e o número de ordens do corpo residual $Q[X]/(p(X))$ associado a valorização $v_{p(X)}$ é o número de raízes reais de $p(X)$.

3.5. ORDENS DE $\mathbb{R}(X)$.

Em (3.3) temos dado todas as valorizações reais de $\mathbb{R}(X)$. Tais valorizações tem $\mathbb{R}$ como corpo residual e $\mathbb{Z}$ como grupo de valores. Então, fixada uma valorização real v de $\mathbb{R}(X)$, por (1.8), existem exatamente duas ordens de $\mathbb{R}(X)$ compatíveis com v .

Para analisar a natureza destas ordens, vamos estudar três casos:

CASO I. $\alpha = 0$ ou seja valorização x -ádica de $\mathbb{R}(X)$.

Neste caso cabe a $\mathbb{R}(X)$ duas ordens; provenientes da seguinte maneira:

i) *Ordem anti-lexicográfica*: Um polinômio $f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_n x^n \in \mathbb{R}[X]$ com $a_m \neq 0$ e $m \leq n$ é positivo, se o coeficiente do termo de menor grau a_n é positivo, isto é, se $a_n \in \mathbb{R}^2$. Um quociente $f(x)/g(x) \in \mathbb{R}(X)$ é positivo se o polinômio $f(x).g(x)$ é positivo.

Se indicarmos por P_1 , esta ordem, então $(\mathbb{R}(X), P_1)$ é um corpo ordenado e P_1 é denominado de ordem *anti-lexicográfica* de $\mathbb{R}(X)$.

ii) *Ordem anti-lexicográfica via o automorfismo $X \rightarrow -X$* . Como a função $X \rightarrow -X$ define um $\mathbb{R}$ -automorfismo τ do corpo $\mathbb{R}(X)$; τ define uma ordem P_2 de $\mathbb{R}(X)$ da seguinte maneira: $f(x)/g(x) \in P_2$, onde $f(x)/g(x) \in \mathbb{R}(X)$ se, e somente se $\tau(f(x)/g(x)) \in P_1$.

Assim, $(\mathbb{R}(X), P_2)$ é um corpo ordenado e P_2 é denominado a *ordem anti-lexicográfica* de $\mathbb{R}(X)$ via o automorfismo $X \rightarrow -X$. Repare que um polinômio $f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_n x^n \in \mathbb{R}[X]$, com $n \leq m$, pertence a P_2 se, e somente se $(-1)^n a_n \in \mathbb{R}^2$. Repare também, que $P_1 \neq P_2$ e que estas duas ordens são compatíveis com a valorização x -ádica de $\mathbb{R}(X)$.

As ordens P_1 e P_2 são, então, as duas ordens de $\mathbb{R}(X)$ compatíveis com a valorização X -ádica, dadas pelo teorema (1.8). P_1

corresponde ao homomorfismo constante σ_1 de $\mathbb{Z}/\partial\mathbb{Z}$ em $\{-1,1\}$ e P_2 corresponde ao homomorfismo σ_2 de $\mathbb{Z}/\partial\mathbb{Z} \rightarrow \{-1,1\}$ tal que $\sigma_2(\bar{1}) = -1$.

O Teorema (1.8) descreve P_1 e P_2 da seguinte maneira: $f(X) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_n X^n \in \mathbb{R}[X]$ com $m \geq n$ está em P_1 se, e somente se $\frac{f(X)}{s_0(v_0(f(X)))} \sigma_1(\overline{vf(X)}) + M_0 \in (A_0/M_0)_+$, ou seja, se, e somente se $a_n \in \mathbb{R}^2$, e $f(x) \in P_2$ se, e somente se $\frac{f(X)}{s_0(v_0(f(X)))} \sigma_2(\overline{vf(X)}) + M_0 \in (A_0/M_0)$, ou seja, se, e somente se $(-1)^n a_n \in \mathbb{R}^2$. Aqui s_0 é uma q -seção da valorização dada por $s_0(n) = X^n$.

CASO II. Valorização $(X-\alpha)$ -ádica de $\mathbb{R}(X)$ ($\alpha \in \mathbb{R}$).

Neste caso, o $\mathbb{R}$ -automorfismo τ_α de $\mathbb{R}(X)$, que leva X em $X-\alpha$ dá origem a duas ordens $P_1(\alpha)$ e $P_2(\alpha)$ de $\mathbb{R}(X)$, provenientes de P_1 e P_2 , respectivamente, da seguinte maneira:

$$P_1(\alpha) = \tau_\alpha(P_1) = \{f(X)/g(X) \in \mathbb{R}(X) \mid \tau_\alpha^{-1}(f(X)/g(X)) \in P_1\}$$

e

$$P_2(\alpha) = \tau_\alpha(P_2) = \{f(X)/g(X) \in \mathbb{R}(X) \mid \tau_\alpha^{-1}(f(X)/g(X)) \in P_2\}.$$

Observemos que $P_1(\alpha)$ corresponde a ordem anti-lexicográfica P_1 de $\mathbb{R}(X)$, no seguinte sentido: $f(X) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_n X^n \in \mathbb{R}[X]^*$ ($n \leq m$) pertence a $P_1(\alpha)$ se, e somente se $f(X+\alpha) = a_m (X+\alpha) + a_{m-1} (X+\alpha)^{m-1} + \dots + a_n (X+\alpha)^n \in P_1$. Uma outra

maneira de escrever $P_i(\alpha)$, $i = 1, 2$ é a seguinte: Escrevemos $f(X)$ como; $f(X) = (X-\alpha)^t f_1(X)$, onde $f_1(\alpha) \neq 0$. Então, $f(X) \in P_1(\alpha)$ se $f_1(\alpha) > 0$ em $\mathbb{R}$ e $f(X) \in P_2(\alpha)$ se $(-1)^t f_1(\alpha) > 0$ em $\mathbb{R}$.

Desde que $X-\alpha \in P_1(\alpha) \setminus P_2(\alpha)$, a ordem $P_1(\alpha)$ é diferente da ordem $P_2(\alpha)$. Geralmente, se $\alpha \neq \beta$, então $\{P_1(\alpha), P_2(\alpha)\} \cap \{P_1(\beta), P_2(\beta)\} = \emptyset$. Para a confirmação da última afirmação, se supormos $\beta < \alpha$ (em $\mathbb{R}$), note que $X-\alpha = (X-\beta) + (\beta-\alpha) \in P_1(\alpha) \setminus P_1(\beta)$ ($i = 1, 2$), e que $2(X-\alpha) + (\alpha-\beta) = 2(X-\beta) + (\beta-\alpha) \in P_2(\alpha) \setminus P_1(\beta)$ ($i = 1, 2$).

Observemos que as ordens $P_1(\alpha)$ e $P_2(\alpha)$ são compatíveis com a valorização $(X-\alpha)$ -ádica de $\mathbb{R}(X)$. Assim, $A_\alpha = A_{\mathbb{Q}}^{P_1(\alpha)} = A_{\mathbb{Q}}^{P_2(\alpha)}$. Como os anéis de valorização A_α e A_β não são comparáveis, se $\alpha \neq \beta$, então, da última igualdade, também vemos que $\{P_1(\alpha), P_2(\alpha)\} \cap \{P_1(\beta), P_2(\beta)\} = \emptyset$.

CASO III. Valorização ∞ -ádica de $\mathbb{R}(X)$.

Considerando o $\mathbb{R}$ -automorfismo τ_∞ de $\mathbb{R}(X)$, que leva X em $\frac{1}{X}$, então $P_1(\infty) = \tau_\infty(P_1) = \{\frac{f(X)}{g(X)} \in \mathbb{R}(X) \mid \tau_\infty^{-1}(f(X)/g(X) \in P_1\}$ e $P_2(\infty) = \tau_\infty(P_2)$ são ordens de $\mathbb{R}(X)$. Claramente um polinômio $f(X) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_n X^n \in \mathbb{R}[X]$, com $n \leq m$, pertence a $P_1(\infty)$ se, e somente se $a_m \in \mathbb{R}^2$ e da mesma maneira, $f(X) \in P_2(\infty)$ se, e somente se $(-1)^m a_m \in \mathbb{R}^2$. $P_1(\infty)$ é geralmente citada como a ordem lexicográfica de $\mathbb{R}(X)$.

Notemos que $P_1(\infty)$ e $P_2(\infty)$ são ordens de $\mathbb{R}(X)$, compatíveis com a valorização ∞ -ádica de $\mathbb{R}(X)$ e também, usando um argumento

de valorização ou algum outro raciocínio, podemos mostrar que $\{P_1(\infty), P_2(\infty)\} \cap \{P_1(\alpha), P_2(\beta)\} = \emptyset \quad \forall \alpha \in \mathbb{R}$.

Como conseguimos descrever toda valorização real de $\mathbb{R}(X)$ e as duas ordens compatíveis com cada uma delas, já descrevemos todas as ordens não arquimedianas de $\mathbb{R}(X)$. Por outro lado, $\mathbb{R}(X)$ não tem ordem arquimediana; portanto $\{P_1(\alpha)\} \cup \{P_2(\alpha)\}_{\alpha \in \mathbb{R} \cup \{\infty\}}$ é o conjunto de ordens de $\mathbb{R}(X)$ e $P_i(\alpha) = P_j(\beta)$ se, e somente se $i = j$ e $\alpha = \beta$.

Nossa análise mostra que todas as ordens de $\mathbb{R}(X)$ provêm da ordem anti-lexicográfica via $\mathbb{R}$ -automorfismos de $\mathbb{R}(X)$. Assim, podemos melhorar um resultado devido a Banaschewski [1].

3.5.a. TEOREMA. Definida em $\mathbb{R}(X)$ uma estrutura de corpo ordenado $(\mathbb{R}(X), \leq)$, então $(\mathbb{R}(X), \leq)$ é $\mathbb{R}$ -isomorfo como corpo ordenado a $(\mathbb{R}(X), P)$, onde P é a ordem anti-lexicográfica de $\mathbb{R}(X)$.

Portanto, quaisquer duas estruturas de corpos ordenados de $\mathbb{R}(X)$ são isomorfas.

3.5.b. OBSERVAÇÃO. Cabe observar que todo $\mathbb{R}$ -automorfismo de $\mathbb{R}(X)$ provém de uma aplicação $X \longrightarrow \frac{aX+b}{cX+d}$ com $ad - bc \neq 0$ e $a, b, c, d \in \mathbb{R}$. No entanto, nem todo $\mathbb{R}$ -automorfismo de $\mathbb{R}(X)$ conduz a novas ordens. Como então descrever a relação entre os automorfismos e as ordens de $\mathbb{R}(X)$?

Vamos analisar a situação. Sejam σ um automorfismo do corpo $\mathbb{R}(X)$ dado por $X \longrightarrow \frac{aX+b}{cX+d}$, com $\Delta_\sigma = ad - bc \neq 0$, e P_0 a

ordem $\sigma(P)$ onde P é a ordem anti-lexicográfica de $\mathbb{R}(X)$. Então, $P_\sigma = P_i(\alpha)$ para algum $\sigma \in \mathbb{R} \cup \{\infty\}$ e para algum $i = 1, 2$. Quere-mos identificar α e i . Há dois casos a considerar:

1º CASO. $a \neq 0$. Seja $f(X) \in \mathbb{R}[X]$ um polinômio qualquer. $f(X) \in P_\sigma$ se, e somente se $\sigma^{-1}(f(X)) \in P$. Seja f_1 o único polinômio em $\mathbb{R}[X]$ tal que $f(X) = (X + \frac{b}{a})^t f_1(X)$ e $f_1(-\frac{b}{a}) \neq 0$. Se $f_1(X) = c_n X^n + c_{n-1} X^{n-1} + \dots + c_0$, observando que $\sigma^{-1}(X) = \frac{b-dX}{cX-a}$ temos, então que $\sigma^{-1}(f(X)) = [\frac{(bc-ad)}{(cX-a)a}]^t \cdot \frac{[c_n (b-dX)^n + c_{n-1} (b-dX)^{n-1} (cX-a) + \dots + c_0 (cX-a)^n]}{(cX-a)^n}$.

Assim, $\sigma^{-1}(f(X)) \in P$ se, e somente se $|\frac{ad-bc}{a^2}|^t f_1(-b/a) \in \mathbb{R}_+$, ou seja, $f(X) \in P_\sigma$ se, e somente se $(ad-bc)^t f_1(-b/a) > 0$ em $\mathbb{R}$. Portanto, $P_\sigma = P_1(-b/a)$ se $\Delta_\sigma = ad-bc > 0$ e $P_\sigma = P_2(-b/a)$ se $\Delta_\sigma = ad-bc < 0$.

2º CASO. $a = 0$. Seja $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{R}[X]$. Então, $\sigma^{-1}(f(X)) = \frac{a_n (b-dX)^n + a_{n-1} (b-dX)^{n-1} cX + \dots + a_0 (cX)^n}{(cX)^n}$.

Logo, $f(X) \in P_\sigma$ se, e somente se $a_n (bc)^n \in \mathbb{R}_+$ e assim, $P_\sigma = P_2(\infty)$ se $\Delta_\sigma = -bc > 0$ e $P_\sigma = P_1(\infty)$ se $\Delta_\sigma = -bc < 0$.

Analisando, mais ainda, a relação entre os automorfismos de $\mathbb{R}(X)$ e as ordens de $\mathbb{R}(X)$, apresentamos uma relação interessante a qual não encontramos na literatura.

Seja G o grupo de $\mathbb{R}$ -automorfismos de $\mathbb{R}(X)$. Então G pode ser identificado com o grupo de matrizes $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}$. Seja $H = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid ad > 0 \right\}$. Podemos mostrar que H é um grupo de G , embora não seja um subgrupo normal de G .

3.6. PROPOSIÇÃO. Existe uma correspondência bijetora entre o conjunto Y das ordens de $\mathbb{R}(X)$ e o conjunto das classes laterais à direita Hg de H em G .

DEMONSTRAÇÃO. Definimos uma aplicação θ de G em Y por: $\theta(\sigma) = P_\sigma$ onde P_σ é a ordem de $\mathbb{R}(X)$, definida anteriormente. θ é uma aplicação bem definida. Vamos mostrar, que a imagem inversa, por θ , de um elemento de Y é uma classe lateral à direita de H em G .

$$\begin{aligned} \theta^{-1}(P_1(0)) &= \{ \sigma \in G \mid \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ com } a \neq 0, -\frac{b}{a} = 0 \text{ e } ad - bc > 0 \} = \\ &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid ad > 0 \right\} = H. \end{aligned}$$

$$\text{Se } \alpha \neq 0, \quad \theta^{-1}(P_1(\alpha)) = \left\{ \sigma \in G \mid \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ com } a \neq 0, \right.$$

$$\left. -\frac{b}{a} = \alpha \text{ e } ad - bc > 0 \right\}, \text{ por exemplo, } T = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} \in$$

$$\in \theta^{-1}(P_1(\alpha)).$$

$$\text{Afirmamos que } \theta^{-1}(P_1(\alpha)) = HT.$$

De fato: Se $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in H$, então $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \cdot T = \begin{pmatrix} a & -a\alpha \\ c & -c\alpha + d \end{pmatrix}$ possui determinante $-a\alpha + ad + a\alpha = ad > 0$. Logo $HT \subseteq \theta^{-1}(P_1(\alpha))$.

Por outro lado, se $\sigma \in \theta^{-1}(P_1(\alpha))$, então $\sigma = \begin{pmatrix} a & -a\alpha \\ c & d \end{pmatrix}$ com $ad + a\alpha > 0$ e $a \neq 0$. Ora, $\sigma T^{-1} = \begin{pmatrix} a & -a\alpha \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & c\alpha + d \end{pmatrix}$ possui determinante $a(c\alpha + d) > 0$. Logo, $\sigma T^{-1} \in H$, ou seja $\sigma \in HT$. Portanto $\theta^{-1}(P_1(\alpha)) \subseteq HT$, donde $HT = \theta^{-1}(P_1(\alpha))$.

Do mesmo modo, mostramos que $\theta^{-1}(P_2(\alpha)) = HT_2$, onde $T_2 = \begin{pmatrix} 1 & -\alpha \\ 0 & -1 \end{pmatrix}$.

Resta analisar os elementos $P_1(\infty)$ e $P_2(\infty)$ de Y . Temos, $\theta^{-1}(P_1(\infty)) = \{\sigma \in G \mid \sigma = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \text{ com } -bc < 0\}$ e assim ,

$\lambda = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \theta^{-1}(P_1(\infty))$. Afiramos neste caso que $\theta^{-1}(P_1(\infty)) =$

$H\lambda$. De fato: Se $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in H$, então $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =$

$= \begin{pmatrix} 0 & a \\ d & c \end{pmatrix}$ possui determinante $-ad < 0$. Logo $H\lambda \subseteq \theta^{-1}(P_1(\infty))$.

Por outro lado, se $\sigma \in \theta^{-1}(P_1(\infty))$, então $\sigma = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$ com

$-bc < 0$. Daí, $\sigma\lambda^{-1} = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & c \end{pmatrix}$ possui

um determinante $bc > 0$. Logo $\theta^{-1}(P_1(\infty)) \subseteq H\lambda$ e, portanto ,

$\theta^{-1}(P_1(\infty)) = H\lambda$. Analogamente, $\theta^{-1}(P_2(\infty)) = H\lambda_2$, onde

$\lambda_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Definimos agora a aplicação $\bar{\theta}$ de Y em $\bar{G} = \{H\sigma \mid \sigma \in G\}$ por $\bar{\theta}(P) = \theta^{-1}(P)$. $\bar{\theta}$ é uma bijeção pois: Se $g \in G$, então, $\theta(g) \in Y$ e $\bar{\theta}(\theta(g)) = \theta^{-1}(\theta(g)) = Hg$. Agora, se $\sigma, \varphi \in G$ e $H\varphi = \theta^{-1}(\theta(\varphi)) = \theta^{-1}(\theta(\sigma)) = H\sigma$, então $\varphi = h\sigma$ para algum $h \in H$. Logo $\varphi(P_1(0)) = h\sigma(P_1(0)) = \sigma(P_1(0))$. Isto mostra que $\bar{\theta}$ é uma bijeção.

Do mesmo modo que demos todas as ordens de $\mathbb{R}(X)$, vamos agora, dar todas as ordens não arquimedianas de $Q(X)$. Veremos que tais ordens são restrições de ordens de $\mathbb{R}(X)$.

Para o que segue, se $\alpha \in \mathbb{R} \cup \{\infty\}$ e $\ell = 1, 2$, vamos denotar a ordem $P_\ell(\alpha) \cap Q(X)$ de $Q(X)$, por $P'_\ell(\alpha)$. Aqui, $P_\ell(\alpha)$ é a ordem de $\mathbb{R}(X)$, dada pelo $\mathbb{R}$ -automorfismo τ_α de $\mathbb{R}(X)$ definido por $\tau_\alpha(X) = X - \alpha$ se $\alpha \in \mathbb{R}$ e $\tau_\infty(X) = \frac{1}{X}$.

Em (3.4) temos dado todas as valorizações reais de $Q(X)$. Vamos primeiro dar as ordens de $Q(X)$ compatíveis com a valorização ∞ -ádica e posteriormente às valorizações $p(X)$ -ádicas, onde $p(X)$ tem raiz real.

É óbvio que a valorização ∞ -ádica ω_∞ de $\mathbb{R}(X)$ estende a valorização real ∞ -ádica v_∞ de $Q(X)$. Como $P_i(\infty)$ ($i=1, 2$) são ordens de $\mathbb{R}(X)$, compatíveis com ω_∞ temos, então, que $P'_i(\infty)$ ($i=1, 2$) são ordens de $Q(X)$ compatíveis com a valorização v_∞ . Agora, $P'_1(\infty) \neq P'_2(\infty)$ pois $\frac{1}{X} \in P'_1(\infty) \setminus P'_2(\infty)$, portanto estas são exatamente as duas ordens de $Q(X)$ compatíveis com v_∞ .

Seja agora, α um número algébrico real e $p(X) \in Q[X]$ seu polinômio minimal. Sobre $\mathbb{R}[X]$, o polinômio $p(X)$ se fatora como, $p(X) = (X-a_1)(X-a_2)\dots(X-a_t)g_1(X)\dots g_k(X)$ onde $g_i(X)$ ($1 \leq i \leq k$) são polinômios mônicos irredutíveis de grau 2, se $k > 1$, e $g_1(X) = 1$, se $k = 1$. Se considerarmos a valorização $p(X)$ -ádica $v_{p(X)}$ de $Q(X)$ e a valorização $(X-a_i)$ -ádica v_{a_i} ($1 \leq i \leq t$) de $\mathbb{R}(X)$, então, claramente, v_{r_i} é uma extensão de $v_{p(X)}$. Daí as ordens $P'_\ell(a_i)$ ($\ell = 1, 2; 1 \leq i \leq t$) de $Q(X)$ são todas

compatíveis com a valorização $v_{p(X)}$. Vamos mostrar agora, que estas são as únicas ordens compatíveis com $v_{p(X)}$. Para isto, usando (1.8), basta mostrar, que elas são duas a duas distintas.

Vamos primeiro mostrar, que para i fixo entre 1 e t , $P'_1(a_i) \neq P'_2(a_i)$. Se considerarmos o polinômio $p(X+a_i)$, então seu termo de menor grau é X , isto porque $p(X+a_i) = X h_i(X+a_i)$ onde $h_i(X) = (X-a_1) \dots (X-a_{i-1})(X-a_{i+1}) \dots (X-a_t) g_1(X) \dots g_k(X)$. (Note que $h_i(a_i) \neq 0$). Daí, $p(X+r_i) \in P_1$ se, e somente se $h_i(a_i) > 0$ em $\mathbb{R}$ e $p(X+a_i) \in P_2$ se, e somente se $h_i(a_i) < 0$ em $\mathbb{R}$. Isto mostra que $p(X) \notin P'_1(a_i) \cap P'_2(a_i)$, mas que $p(X) \in P'_\ell(a_i)$ para $\ell = 1$ ou $\ell = 2$. Assim, $P'_1(a_i) \neq P'_2(a_i)$.

Sejam agora a e b números reais distintos. Suponhamos que $a < b$. Então, do fato de $\mathbb{Q}$ ser denso em $\mathbb{R}$, existe $r \in \mathbb{Q}$ tal que $a < r < b$, isto é, $b-r > 0$ e $a-r < 0$. Logo o polinômio $X+(a-r) \notin P_\ell$ ($\ell = 1, 2$) e o polinômio $X+(b-r) \in P_\ell$ ($\ell = 1, 2$). Portanto, o polinômio $X-r$ pertence a $P_\ell(b)$ ($\ell = 1, 2$) e não pertence a $P_\ell(a)$ ($\ell = 1, 2$). Logo, $P'_\ell(a) \neq P'_\ell(b)$ ($\ell = 1, 2$; $k = 1, 2$). Como já mostramos que $P_1(a_i) \neq P_2(a_i)$ ($1 \leq i \leq t$), segue-se, que $P'_\ell(a_i) = P'_k(a_j)$ se, e somente se $\ell = k$ e $a_i = a_j$ ($\ell, k = 1, 2$; $1 \leq i, j \leq t$). Portanto, estas são as $2 \cdot t$ ordens distintas de $\mathbb{Q}(X)$ compatíveis com a valorização $v_{p(X)}$, (ver (1.8)).

Conforme, já mencionamos, nossa intenção é mostrar que, toda ordem não-arquimediana de $\mathbb{Q}(X)$ é uma restrição de uma ordem de $\mathbb{R}(X)$. Ora; por (1.12) uma tal ordem de $\mathbb{Q}(X)$ é compatível com alguma valorização real de $\mathbb{Q}(X)$. Como já temos dado toda ordem de $\mathbb{Q}(X)$ compatível com essas valorizações, já conseguimos nosso

objetivo.

Observemos, ainda, que: se $a \in \mathbb{R}$ e $s \in \mathbb{Q}$ é tal que $s - a^2 > 0$ em $\mathbb{R}$, então $x^2 - s \in P_\ell(\infty)$ ($\ell = 1, 2$) e $x^2 - s \notin P_\ell(a)$ ($\ell = 1, 2$). Portanto, também ocorre $P_\ell(\infty) \neq P_k(a)$ ($\ell = 1, 2; k = 1, 2$). Resumidamente temos:

3.7. PROPOSIÇÃO. As ordens não arquimedianas de $Q(X)$ são as ordens $P'_\ell(a) = P_\ell(a) \cap Q(X)$ ($\ell = 1, 2$) onde a é um número real algébrico sobre $\mathbb{Q}$ ou $a = \infty$ e $P_\ell(a)$ ($\ell = 1, 2$) é a ordem de $\mathbb{R}(X)$ dada em (3.5). Mais ainda, $P'_\ell(a) = P'_k(b)$ se, e somente se $\ell = k$ e $a = b$, e essas ordens são todas isomorfas.

Passamos agora a descrever as ordens arquimedianas de $Q(X)$.

É conhecido, que um corpo K com uma ordem arquimediana isomorfa a um subcorpo de $\mathbb{R}$ com ordem induzida. Daí, se P é uma ordem arquimediana, de $Q(X)$, existe um $\mathbb{Q}$ -monomorfismo de corpos $\sigma : Q(X) \rightarrow \mathbb{R}$ tal que $P = \sigma^{-1}(\mathbb{R}_+)$.

Assim, existe um número não enumerável de ordens arquimedianas de $Q(X)$. De fato:

Como existe um número não enumerável de números reais, transcendentes sobre $\mathbb{Q}$, basta mostrar que, se σ e σ' são dois $\mathbb{Q}$ -monomorfismos de $Q(X)$ em $\mathbb{R}$, então as ordens induzidas $P_\sigma = \sigma^{-1}(\mathbb{R}_+)$ e $P_{\sigma'} = \sigma'^{-1}(\mathbb{R}_+)$ são distintas.

Sejam $\sigma(X) = \alpha$ e $\sigma'(X) = \alpha'$ e suponhamos que $\alpha < \alpha'$. Então, existe $r \in \mathbb{Q}$ tal que $\alpha < r < \alpha'$. Daí, $X - r \notin P$ enquanto que $X - r \in P_{\sigma'}$; assim, $P_\sigma \neq P_{\sigma'}$.

Prosseguindo com os exemplos, vamos agora dar as valorizações reais e as ordens dos corpos das séries formais $\mathbb{Q}((X))$ e $\mathbb{R}((X))$.

Seja K um corpo e X uma indeterminada sobre K . O conjunto $K((X))$ dos elementos a da forma $a = \sum_{i \in \mathbb{Z}} a_i X^i$, onde $a_i \in K$ e $a_i = 0$ para quase todo $i < 0$, munido da adição $(\sum_{i \in \mathbb{Z}} a_i X^i) + (\sum_{i \in \mathbb{Z}} b_i X^i) = \sum_{i \in \mathbb{Z}} (a_i + b_i) X^i$ e da multiplicação $(\sum_{i \in \mathbb{Z}} a_i X^i) \cdot (\sum_{i \in \mathbb{Z}} b_i X^i) = \sum_{i \in \mathbb{Z}} c_i X^i$ onde $c_k = \sum_{i+j=k} a_i b_j$, é um corpo, (note que $c_k = 0$ para quase todo $k < 0$), $K((X))$ com esta estrutura é usualmente denominado de *corpo das séries formais sobre K* . Para simplificar a notação, um elemento $a \in K((X))$ sempre será considerado como $a = \sum_{i=-\infty}^{\infty} a_i X^i$.

A aplicação $v: K((X)) \rightarrow \mathbb{Z} \cup \{\infty\}$ definida de maneira natural, isto é, $v(a) = \min\{i \in \mathbb{Z} \mid a_i \neq 0\}$ se $a \neq 0$ e $v(0) = \infty$ é uma valorização de $K((X))$. Por [9] (5.8) e (16.7)) o corpo valorizado $(K((X)), v)$ é henseliano.

Vamos agora supor, que K é um corpo formalmente real com uma única ordem, denotada por K_+ (por exemplo; K pode ser o corpo $\mathbb{Q}$, o corpo $\mathbb{R}$ ou qualquer corpo real fechado). Com esta suposição e do fato do corpo residual $K((X))_v$ ser isomorfo a K , segue que v é uma valorização real do corpo $K((X))$. Daí, por (2.3), se P é uma ordem de $K((X))$, P é compatível com v , isto porque, conforme mencionamos, o corpo valorizado $(K((X)), v)$ é henseliano. Agora, estamos supondo K com única ordem, e o grupo de valores

da valorização v é $\mathbb{Z}$, então, por (1.8), existem exatamente duas ordens de $K((X))$ compatíveis com v . Portanto, $K((X))$ tem exatamente duas ordens, estas ordens são não arquimedianas e mostraremos logo abaixo, que elas são isomorfas. Observemos também, que a valorização v , em questão, é a única valorização real de $K((X))$.

Podemos munir $K((X))$ de uma estrutura de corpo ordenado de maneira natural, isto é, o subconjunto P_1 de $K((X))$ consistindo dos elementos $a \in K((X))$ tais que $a_{v(a)} \in K_+$, se $a \neq 0$ e de 0 é uma ordem de $K((X))$. (Observe que pela definição da valorização v , $a_i = 0$, $\forall i < v(a)$). P_1 é denominada de *ordem anti-lexicográfica* de $K((X))$. Se considerarmos o K -automorfismo τ de $K((X))$ dado por $\tau: X \rightarrow -X$ então $P_2 = \tau(P_1) = \{a \in K((X)) \mid \tau^{-1}(a) \in P_1\}$ é também uma ordem de $K((X))$. Claramente $P_2 \neq P_1$ ($X \in P_1 \setminus P_2$) e assim P_1 e P_2 são as únicas ordens de $K((X))$. Observe que $a \in P_2 \iff (-1)^{|v(a)|} a_{v(a)} \in K_+$.

Resumidamente temos:

3.8. PROPOSIÇÃO. Sejam K um corpo formalmente com uma única ordem K_+ e $K((X))$ o corpo das séries formais sobre K . Então, $K((X))$ possui uma única valorização real. A saber, a valorização ω dada

por $\omega(\sum_{i=-\infty}^{+\infty} a_i X^i) = \min\{i \mid a_i \neq 0\}$ se $a \neq 0$ e $\omega(0) = \infty$. $K((X))$,

possui também, exatamente duas ordens que são K -isomorfas; a saber, P_1 e P_2 onde $P_1 = \{a \in K((X)) \mid a_{v(a)} \in K_+\}$ e

$$P_2 = \{a \in K((X)) \mid (-1)^{|v(a)|} a_{v(a)} \in K_+\}.$$

As ordens P_1 e P_2 são compatíveis com a valorização w e são ambas não arquimedianas.

CAPÍTULO III

QUESTÕES DE DENSIDADE EM CORPOS VALORIZADOS

Se (K, v) é um corpo valorizado, então v define em K uma topologia compatível com sua estrutura de corpo. Por outro lado, se K é um corpo formalmente real com uma ordem K_+ , então K_+ também define uma topologia em K compatível com a sua estrutura de corpo. A topologia definida por K_+ é chamada de Topologia intervalo aberto.

Se supormos que a ordem K_+ é compatível com a valorização v , então a topologia definida por v coincide com a topologia intervalo aberto definida por K_+ .

Nossa meta é dar uma aplicação, bem bonita, devido a Viswanathan de conceitos desenvolvidos no Capítulo . Para isto precisamos de caracterizar corpos valorizados K e L tais que K seja denso em L , na topologia definida por valorizações (Teorema (2.5)). Este teorema, por sua vez, depende de resultados devidos a Engler (Teorema (1.3)). Finalmente, no parágrafo 3, daremos 2 exemplos usando anéis de grupo. Um deles é a construção explícita de um corpo ordenado não arquimediano, denso em seu fecho real.

1. TOPOLOGIA DE UM CORPO VALORIZADO E SUBCORPOS DENSOS

Se (K, A) é um corpo valorizado, então A define uma topo

logia em K , compatível com a estrutura de corpo, de tal maneira que os conjuntos $V_A(x, \gamma) = \{y \in K \mid v_A(x-y) > \gamma\}$ ($\gamma \in G_A$) formam um sistema fundamental de vizinhanças de $x \in K$. Denotaremos esta topologia por T_A ou por T_{V_A} , onde v_A é a valorização associada ao anel A .

1.1. PROPOSIÇÃO. Sejam K um corpo e duas valorizações v e w de K . Se v e w são tais que $A_v \subset A_w$, então v e w definem uma mesma topologia em K ; isto é, $T_{A_v} = T_{A_w}$.

DEMONSTRAÇÃO. Como $A_v \subset A_w$, existe um homomorfismo de ordem $\theta: G_v \longrightarrow G_w$ tal que $w = \theta \circ v$.

Sejam $a \in K$ e $\gamma \in G_v$ elementos quaisquer e consideremos $\delta = \theta(\gamma) \in G_w$. Então, se $x \in V_w(a, \delta) \Rightarrow w(a-x) = \theta(v(a-x)) > \delta \Rightarrow v(a-x) > \gamma \Rightarrow x \in V_v(a, \gamma)$. Assim $V_w(a, \delta) \subseteq V_v(a, \gamma)$ e isto mostra que $T_v \subseteq T_w$.

Resta mostrar agora que $T_w \subseteq T_v$. Para isto consideremos $a \in K$ e $\gamma \in G_w$ elementos quaisquer. Escolhamos agora $\delta \in \theta^{-1}(\gamma)$ e $\gamma_1 \in G_w$ tal que $\gamma_1 < \gamma$. Então, se $x \in V_v(a, \delta) \Rightarrow v(a-x) > \delta \Rightarrow \theta(v(a-x)) = w(a-x) \geq \theta(\delta) = \gamma > \gamma_1$. Logo $V_v(a, \delta) \subseteq V_w(a, \gamma)$ e assim $T_w \subseteq T_v$.

1.2. LEMA. Sejam (L, C) um corpo valorizado próprio e $B = \{B \mid B \text{ é subanel próprio de } L \text{ contendo } C\}$. Suponhamos ainda, que para todo $B \in B$, posto $B \neq 1$. Então valem as seguintes afirmações:

$$1) \bigcap_{B \in \mathcal{B}} M_B = \{0\}$$

$$2) \bigcup_{B \in \mathcal{B}} U_B = L \setminus \{0\}$$

3) Dados $x \in L$ e $\gamma \in G_C$, existem subanéis $B, B' \in \mathcal{B}$ tais que $x \in U_B$ e $x + M_{B'} \subseteq V_C(x, \gamma)$.

DEMONSTRAÇÃO (1). $\mathcal{B}$ é uma família totalmente ordenada por inclusão, então $D = \bigcup_{B \in \mathcal{B}} B$ é um anel de valorização de L , contendo

C . Agora, $D \notin \mathcal{B}$, pois D é um elemento maximal de $\mathcal{B}$, portanto $D = L$. Seja agora $x \in \bigcup_{B \in \mathcal{B}} M_B$; se $x \neq 0$, então $x^{-1} \notin B$, $\forall B \in \mathcal{B}$, ou seja, $x^{-1} \notin D = L$. Isto não acontece, pois L é um corpo, então $x = 0$ e $\bigcap_{B \in \mathcal{B}} M_B = \{0\}$.

(2) Se $x \in L \setminus \{0\}$, por (1), $x \notin M_{B'}$ para algum $B' \in \mathcal{B}$. Por outro lado, $x \in B''$ para algum $B'' \in \mathcal{B}$ e temos 2 casos:

1º) $B' \subset B''$. Neste caso $M_{B'} \supset M_{B''}$ o que acarreta $x \in U_{B''}$.

2º) $B'' \subset B'$. Neste caso $x \in B' \setminus M_{B'} = U_{B'}$.

(3) Para cada $B \in \mathcal{B}$, seja λ_B o homomorfismo de ordem, de G_C sobre G_B , tal que $v_B = \lambda_B \circ v_C$. Sejam $x \in L \setminus \{0\}$ e $\gamma \in G_C$ elementos quaisquer e consideremos $y \in v_C^{-1}(\gamma)$. Escolhamos agora $B' \in \mathcal{B}$ tal que $y \notin M_{B'}$. Então, $v_{B'}(y) \leq 0$, donde $v_{B'}(m) > v_{B'}(y) \quad \forall m \in M_{B'}$, isto é, $\lambda_{B'}(v_C(m)) > \lambda_{B'}(v_C(y)) \quad \forall m \in M_{B'}$. Como $\lambda_{B'}$ conserva ordem, segue então, que $v_C(m) > v_C(y) = \gamma \quad \forall m \in M_{B'}$, ou seja, $x + M_{B'} \subseteq v_C(x, \gamma)$.

1.3. TEOREMA (Engler). *Sejam, (L, C) um corpo valorizado próprio, $B = \{B \mid B \text{ é subanel próprio de } L \text{ contendo } C\}$ e K um subcorpo de L . Suponhamos que K seja denso no espaço topológico (L, T_C) . Então, $\forall B \in \mathcal{B}$ o corpo valorizado (L, B) é extensão imediata de $(K, B \cap K)$.*

Se supormos, mais ainda, que posto $B \neq 1$, $\forall B \in \mathcal{B}$, então vale a recíproca.

DEMONSTRAÇÃO. $\Rightarrow$) Suponhamos que K seja denso em (L, T_C) . Seja $B \in \mathcal{B}$ e coloquemos $D = B \cap K$. Queremos mostrar que os monomorfismos canônicos de D / M_D (resp G_D) em B / M_B (resp G_B) são sobrejetores.

Seja $x \in B \setminus M_B$. O conjunto $x + M_B$ é aberto de T_B ($x + M_B = v_B(x, 0)$), pela Proposição (1.1), $T_B = T_C$; daí, pela densidade de K em (L, T_C) , $(x + M_B) \cap K \neq \emptyset$. Seja $y \in (x + M_B) \cap K$; então $y - x \in M_B$, donde $y \in D$ e $y + M_B = x + M_B$. Isto mostra que os corpos residuais de B e $B \cap K$ são canonicamente isomorfos.

Seja agora $x \in L \setminus \{0\}$. Desde que U_B é aberto em T_B ($u \in U_B \Rightarrow v(u, 0) \subset U_B$) e $T_B = T_C$, pela densidade de K em (L, T_C) , $x U_B \cap K \neq \emptyset$. Seja $y \in x U_B \cap K$. Então $y = x \cdot u$ para algum $u \in U_B$ e $y \in K$; e daí $v_B(y) = v_B(x \cdot u) = v_B(x)$. Logo os grupos de valores G_B e G_D são também canonicamente isomorfos.

Reciprocamente, suponhamos que não exista anel de valoriza-

ção de posto 1 em B e que $\forall B \in \mathcal{B}$. $(L, B) \mid (K, B \cap K)$ seja extensão imediata. Vamos mostrar que K é denso em (L, T_C) .

Sejam $x \in L$, $\gamma \in G_C$ elementos quaisquer e consideremos a vizinhança básica $v_C(x, \gamma)$ de x . Como, $\forall B \in \mathcal{B}$, posto $B \neq 1$, pelo Lema (1.2), existem $B, B' \in \mathcal{B}$ tais que $x \in U_B$ e $x + M_{B'} \subset v_C(x, \gamma)$. Desde que $\mathcal{B}$ é totalmente ordenado por inclusão temos dois casos: 1º) $B \subset B'$ ou 2º) $B' \subset B$.

1º Caso) Se $B \subset B'$, então $x \in U_{B'}$. Por hipótese $(L, B') \mid (K, K \cap B')$ é extensão imediata. Assim existe $y \in B' \cap K$ tal que $y + M_{B'} = x + M_{B'}$, donde $y \in K \cap v_C(x, \gamma)$.

2º Caso) Se $B' \subset B$. Neste caso $M_{B'} \supset M_B$ e daí $x + M_B \subset x + M_{B'}$; assim $x \in U_B$ e $x + M_B \subset v_C(x, \gamma)$. Novamente pela hipótese de $(L, B) \mid (K, K \cap B)$ ser extensão imediata, existe $y \in K \cap B$, tal que $y + M_B = x + M_B$. Então $y - x \in M_B$, donde $y \in x + M_B \subset v_C(x, \gamma)$.

Portanto, em ambos os casos, provamos que K é denso em (L, T_C) .

O próximo resultado é útil nos estudos de corpos valorizados densos.

1.4. PROPOSIÇÃO. *Sejam, (L, B) um corpo valorizado e $K \subset L$ um subcorpo. Então, K é denso no espaço topológico (L, T_B) se, e somente se $(K, A = K \cap B)$ e (L, B) possuem o mesmo completamento.*

DEMONSTRAÇÃO. $\Leftarrow$) Suponhamos que o completamento $(\hat{L}, \hat{B})$ de (L, B) coincida com o completamento $(\hat{K}, \hat{A})$ de (K, A) . Como K é den-

so em seu completamento, temos que K é denso no espaço topológico $(\hat{L}, T_{\hat{B}})$. Como (L, T_B) é um subespaço topológico de $(\hat{L}, T_{\hat{B}})$, concluímos, então, que K é denso em (L, T_B) .

$\Rightarrow$). Suponhamos agora que K seja denso no espaço topológico (L, T_B) . Seja $(\hat{L}, \hat{B})$ o completamento de (L, B) . Como (L, T_B) é um subespaço topológico denso de $(\hat{L}, T_{\hat{B}})$, segue que L é denso em $(\hat{L}, T_{\hat{B}})$. Agora, $(K, A) \subset (\hat{L}, \hat{B})$ e $(\hat{L}, \hat{B})$ é um corpo valorizado completo, então, o fecho topológico $\bar{K}$ de K , com respeito à topologia $T_{\hat{B}}$, é o único subcorpo de $\hat{L}$, tal que $(\bar{K}, \hat{B} \cap \bar{K})$ é um completamento de (K, A) . Mas $\bar{K} = \hat{L}$, então $\hat{B} \cap \bar{K} = \hat{B}$ e daí, $(\bar{K}, \hat{B} \cap \bar{K}) = (\hat{L}, \hat{B})$. Assim (L, B) e (K, A) possuem o mesmo completamento.

2. SUBCORPOS DENSOS DE CORPOS REAIS FECHADOS

Neste parágrafo, faremos um estudo sobre corpos ordenados densos em seus respectivos fechos reais, isto é, estudaremos os corpos ordenados $(K, \leq)$, onde para cada dois elementos $\alpha, \beta \in \tilde{K}$ com $\beta < \alpha$ existir um elemento $a \in K$, tal que $\beta < a < \alpha$. Aqui, $\tilde{K}$ denota o fecho real de $(K, \leq)$.

Inicialmente mostraremos que, para nosso propósito, somente é necessário considerar ordens não arquimedianas.

2.1. PROPOSIÇÃO. Se $(K, \leq)$ é um corpo ordenado arquimadiano, então $\mathbb{Q}$ é denso em K .

DEMONSTRAÇÃO. Sejam $a, b \in K$ com $a < b$. Então $0 < (b-a)^{-1}$. Seja $n \in \mathbb{Z}$ um inteiro tal que $(b-a)^{-1} < n$. Daí conseguimos $0 < \frac{1}{n} < b-a$. Seja $m \in \mathbb{Z}$ o primeiro inteiro positivo tal que $m > na$. Então $m < mb$, pois, caso contrário $n(b-a) = nb-na \leq m-na \leq 1$ e assim $(b-a) \leq \frac{1}{n}$. Logo $na < m < nb$ e portanto $a < \frac{m}{n} < b$.

Se (K, K_+) é um corpo ordenado não arquimediano, então K admite uma valorização não trivial compatível com K_+ . Por outro lado $A_0^{K_+} = \{a \in K \mid \exists r \in \mathbb{Q} \text{ com } r-a \in K_+\}$ é o menor anel de valorização de K , convexo em relação a K_+ ; isto é, se A é anel de valorização de K , convexo em relação a K_+ , então $A \subset D_0^{K_+}$. Neste caso, por (1.1), as topologias T_A e $T_{A_0^{K_+}}$ de K coincidem. A topologia $T_{A_0^{K_+}}$ de K , é usualmente denominada de *topologia de Hahn* (ver [22]). Desse modo, todas as valorizações de K compatíveis com K_+ definem em K , a topologia de Hahn.

Se (K, K_+) é um corpo ordenado, podemos considerar em K , a *topologia intervalo aberto*, na qual, uma base de vizinhanças abertas da origem, é dada pela família de intervalos abertos $(-a, a)$, onde $a \in K_+$.

O próximo resultado mostra, que não existe diferença entre trabalhar com essas duas topologias comentadas.

2.2. PROPOSIÇÃO. Para um corpo ordenado não arquimediano (K, K_+) , as topologias Hahn e intervalo aberto são as mesmas.

DEMONSTRAÇÃO. Seja w uma valorização não trivial de K , compatível com K_+ e com grupo de valores G_w . Seja $V(0,h) = \{y \in K \mid w(y) > h\}$ um aberto básico qualquer, do sistema fundamental de vizinhanças da origem, na topologia Hahn. Se $y \in V(0,h) \cap K_+$, então $(-y,y) \subset V(0,h)$. De fato: Se $x \in (-y,y) \cap K_+$, então pela compatibilidade de w , $h < w(y) \leq w(x)$, donde $x \in V(0,h)$. Como $w(x) = w(-x)$, $\forall x \in K$, o fato está concluído. Por outro lado, dado um aberto básico qualquer, $(-a,a)$ do sistema fundamental de vizinhanças da origem, na topologia intervalo aberto, seja $h = w(a)$. Então $V(0,h) \subset (-a,a)$, pois, se $y \in V(0,h) \cap K_+$ segue que $w(y) > h = w(a)$ donde, pela compatibilidade $y < a$. Como $(-a,a)$ é simétrico e $y \notin K_+$ implica em $-y \in K_+$ concluímos que $V(0,h) \subseteq (-a,a)$.

Observemos que dizer; o corpo ordenado não arquimediano (K, K_+) é denso em seu fecho real $\tilde{K}$, no sentido de que entre dois elementos de $\tilde{K}$ existe um elemento de K , é equivalente a dizer; K é denso em $\tilde{K}$ com a topologia intervalo aberto. Assim, em virtude da proposição acima, isto é, equivalente a dizer; K é denso em $\tilde{K}$, com a topologia Hahn.

A seguir mencionaremos dois resultados sobre corpos densos em seu fecho real.

2.3. PROPOSIÇÃO. Sejam (K, K_+) um corpo ordenado não-arquimediano e w uma valorização não trivial de K . Se w é compatível com K_+ e K é denso em seu fecho real $\tilde{K}$, então o grupo de valores G_w é divisível e o corpo residual K_w é real fechado.

DEMONSTRAÇÃO. Seja $\tilde{w}$ a única extensão de w a uma valorização real de $\tilde{K}$, (1.19). Por (2.6), $\tilde{K}_{\tilde{w}}$ é real fechado e $G_{\tilde{w}}$ é divisível. Agora, das observações feitas acima, do Teorema (1.3) e da hipótese de K ser denso em $\tilde{K}$, concluímos, que $(\tilde{K}, \tilde{w})$ é extensão imediata de (K, w) . Assim a demonstração está concluída.

A recíproca da Proposição (2.3) ocorre em um importante caso. Em (3.2) daremos um exemplo para mostrar que tal recíproca não é válida no caso geral.

2.4. PROPOSIÇÃO. Sejam (K, K_+) um corpo ordenado e w uma valorização não trivial de K . Suponhamos que w seja, de posto 1 e compatível com K_+ . Se G_w for divisível e K_w for real fechado, então K é denso em seu fecho real.

Observe que nestas condições, K_+ é obrigatoriamente uma ordem não arquimediana.

DEMONSTRAÇÃO. Seja $(\tilde{K}, \tilde{w})$ a henselização de (K, w) . Como henselização é extensão imediata, concluímos, que $\tilde{K}_{\tilde{w}}$ é real fechado e que $G_{\tilde{w}}$ é divisível. Nestas condições, por (2.6), $\tilde{K}$ é real fechado. Daí podemos supor que $(\tilde{K}, \tilde{w})$ é $(\tilde{K}, \tilde{w})$, onde $\tilde{K}$ é o fecho real de K e $\tilde{w}$ é a única extensão de w a uma valorização real de $\tilde{K}$.

O completamento $(\hat{K}, \hat{v})$ de (K, v) é henseliano, pois posto de v é 1. Desse modo, podemos supor que $(\hat{K}, \hat{v})$ é extensão de $(\tilde{K}, \tilde{v})$. Como K é denso em $\hat{K}$, concluímos, então, que K é

denso em $\tilde{K}$.

2.5. TEOREMA. Seja (K, K_+) um corpo ordenado não arquimediano. Então são equivalentes as seguintes afirmações:

- 1) K é denso em seu fecho real.
- 2) Para toda valorização não trivial w de K , compatível com K_+ , o grupo de valores G_w é divisível e o corpo residual K_w é real fechado.
- 3) Existe uma valorização w de K , compatível com K_+ satisfazendo a seguinte propriedade: para toda valorização v de K tal que v seja não trivial e seu anel de valorização A_v contenha o anel A_w , o grupo de valores G_v é divisível e o corpo residual K_v é real fechado.

DEMONSTRAÇÃO. 1) $\Rightarrow$ 2) Proposição (2.3). 2) $\Rightarrow$ 3) Considere o anel de valorização $A_Q^{K+} = \{\alpha \in K \mid \exists r \in \mathbb{Q} \text{ com } r\alpha \in K_+\}$ e w a valorização Hahn de K associada ao anel A_Q^{K+} . Se v é valorização de K tal que $A_v \supseteq A_w$, por (1.13), v é também compatível com K_+ . Daí, por (2), G_v é divisível e K_v é real fechado.

3) $\Rightarrow$ 1) Seja $\tilde{K}$ o fecho real de K e $\tilde{w}$ a única extensão de w a uma valorização real de $\tilde{K}$. Seja $\mathcal{B}$ a família de todos os anéis de valorização não triviais de $\tilde{K}$ que contêm $A_{\tilde{w}}$. $\mathcal{B}$ é uma família totalmente ordenada por inclusão e $\tilde{K}|K$ é extensão algébrica. Então, se $\tilde{B}_1, \tilde{B}_2$ são anéis de valorização de $\tilde{K}$, tais que $K \cap \tilde{B}_1 = K \cap \tilde{B}_2 \supset A_w$, teremos que $\tilde{B}_1 = \tilde{B}_2$. Assim; se $\tilde{B} \in \mathcal{B}$, $\tilde{B}$ é o único anel de valorização de $\tilde{K}$ estendendo

$B = \tilde{B} \cap K \supset A_w$ tal que $\tilde{B}$ é anel de valorização real. Como, por (3), B/M_B é real fechado e G_B é divisível, concluímos que $(\tilde{K}, \tilde{B})$ é extensão imediata de $(K, \tilde{B} \cap K)$.

Se todo $\tilde{B} \in \mathcal{B}$ tiver posto $\neq 1$, o Teorema (1.3) garante que K é denso em $\tilde{K}$. Se, por outro lado, existir $D \in \mathcal{B}$ com posto 1, então $A = D \cap K \supset A_w$ é anel de valorização de K de posto 1, compatível com K_+ , com grupo de valor G_A divisível e corpo residual K_A real fechado. Então, pela Proposição (2.4), K é denso em $\tilde{K}$.

3. EXEMPLOS

Daremos agora dois exemplos: No primeiro será construído explicitamente um corpo ordenado não arquimediano denso em seu fecho real e propriamente contido nele. No segundo será construído um corpo F com uma ordem não arquimediana F_+ tal que o grupo de valores e o corpo residual associados ao anel de valorização real A_0^{F+} de F são respectivamente divisível e real fechado mas (F, F_+) não é denso em seu fecho real. O segundo exemplo servirá para mostrar que a recíproca da Proposição (2.3) não é válida.

Vamos primeiramente, introduzir uma notação a ser usada em tais exemplos.

Sejam k um corpo qualquer e G um grupo abeliano totalmente ordenado com ordem G_+ . O conjunto $k[G]$ consistindo dos elementos a da forma $a = \sum_{g \in G_+} a_g X^g$, onde $a_g \in k$ e $a_g = 0$ qua

se sempre; isto é, $a_g \neq 0$ a menos de um número finito de índices $g \in G$, munido da adição $(\sum_{g \in G_+} b_g X^g) + (\sum_{g \in G_+} b'_g X^g) = \sum_{g \in G_+} (a_g + b'_g) X^g$ e da multiplicação $(\sum_{g \in G_+} a_g X^g) \cdot (\sum_{g \in G_+} b_g X^g) = \sum_{g \in G_+} c_g X^g$, onde $c_g = \sum_{h+l=g} a_h b_l$ é um anel (Repare que, se $a_g = 0$ e $b_g = 0$ quase sempre, então $c_g = 0$ quase sempre). Tal anel é denominado de *Anel do grupo G sobre o corpo K* e é um domínio de integridade.

A aplicação v de $k[G]$ em G que associa a cada elemento $a = \sum a_g X^g \neq 0$ o $\min \text{ supp } (a) = \min \{g \mid a_g \neq 0\}$ e $v(0) = \infty$ é bem definida; além do mais v é uma valorização do domínio de integridade $k[G]$. Logo podemos da maneira natural estender v a uma valorização v do corpo quociente $k(G)$ do domínio de integridade $k[G]$ (esta valorização é denominada de *valorização de ordem de $k(G)$*). É lógico que o grupo de valores de v é G . Também podemos, sem muito trabalho, verificar que o corpo residual $(k(G))_v$ é isomorfo a k .

3.1. EXEMPLO.

Seja $k = \mathbb{R} = \bar{\mathbb{Q}} \cap \mathbb{R}$ o fecho real do corpo dos números racionais e $G = \mathbb{Q}$ o grupo aditivo dos números racionais. Então a valorização v do corpo $K = \mathbb{R}(G)$, definida como acima, é uma valorização real. Logo existe uma ordem K_+ de K tal que K_+ é compatível com v .

Como $\mathbb{R}$ é real fechado e $\mathbb{Q}$ é um grupo divisível de posto 1, por (2.4), K é denso em seu fecho real. Vamos mostrar agora que K não é real fechado.

Desde que $1 \in K_+^*$ e $0 = v(1) < 1 = v(x)$, segue da compatibilidade de K_+ com v que $1-x \in K_+^*$. Agora $1-x \notin K^2$ pois, segundo a ordem lexicográfica de K , $1-x$ é negativo; então K não é real fechado.

3.2. EXEMPLO.

Continuando com a mesma notação de (3.1) seja $F = K(G)$ e w a valorização de ordem do corpo F . Temos $F_w \cong K$ e assim w é valorização real de F . Logo, como em (3.1), existe uma ordem F_+ de F compatível com w . Além do mais, se colocarmos em F_w a ordem $(F_w)_+$, proveniente do isomorfismo de F_w com K , então F_+ pode ser escolhida de maneira tal, que $(F_w)_+ = \{\alpha + M_w \mid \alpha \in U_w \cap F_+\} \cup \{0\}$. Com tal escolha a aplicação residual $\theta_w : A_w \longrightarrow F_w \cong K$ é um homomorfismo de ordem e também a valorização v de K dá origem a aplicação residual $\theta_v : A_v \longrightarrow K_v \cong R$.

Se π_w e π_v são os places associados a θ_w e θ_v , respectivamente, então $\pi = \pi_v \circ \pi_w$ é um place de F , com anel de valorização $\theta_w^{-1}(A_v) \subseteq A_w$, (8.3; [9]).

Seja φ é uma valorização de F tal que $A_\varphi = A_\pi$; φ satisfaz:

- a) F_φ é real fechado.
- b) φ é compatível com F_+ .
- c) G_φ , o grupo de valores de φ , é divisível.

De fato:

a) Do fato de π_v, π_w e portanto π serem places sobrejetores implica $F_\varphi \simeq R$, (8.1; [9]).

b) Segue do fato de A_w (resp A_v) ser convexo com relação a F_+ (resp K_+) e de θ_w conservar ordem.

c) A fim de facilitar a notação vamos supor que $A_w/M_w = K$. Neste caso $\theta_w: A_w \rightarrow K$ é um homomorfismo sobrejetor tal que seu núcleo é M_w .

Seja $x \in F^*$ e n um inteiro positivo. $w(x) \in G$, então existe $y \in F^*$ tal que $w(x) = w(y^n)$, isto é, $xy^{-n} \in U_w$. Assim $\theta_w(xy^{-n}) \in K^*$. Do fato do θ_w ser sobrejetor e G ser divisível, existe $z \in A_w$ tal que $v(\theta_w(xy^{-n})) = nv(\theta_w(z)) = v(\theta_w(z^n))$ (observamos que $z \in U_w$), isto é,

$$\begin{aligned} \theta_w(xy^{-n})(\theta_w(z^n))^{-1} &= \theta_w(xy^{-n})\theta_w(z^{-n}) = \theta_w(xy^{-n}z^{-n}) = \\ &= \theta_w(x.(y.z)^{-n}) \in U_v = \pi_v^{-1}(R^*) \end{aligned}$$

Como $x(y.z)^{-n} \in U_w$ temos $\theta_w(x(yz)^{-n}) = \pi_w(x(yz)^{-n})$. Logo $\pi_v(\pi_w(x(yz)^{-n})) = \pi(x(yz)^{-n}) \in R^*$, donde $x(yz)^{-n} \in \pi^{-1}(R^*) = U_\varphi$, isto é, $\varphi(x) = n\varphi(yz)$, mostrando assim que G_φ é divisível.

Portanto, w e φ são valorizações de F compatíveis com F_+ e $F_w = K$ não é real fechado. Assim F não é denso em seu fecho real, pois, se fosse, pela Proposição (2.3), o corpo residual de qualquer valorização compatível com F_+ seria real fechado.

Observemos que no exemplo anterior a valorização w tem posto 1 enquanto que φ tem posto 2.

CAPÍTULO III

CORPOS HEREDITARIAMENTE PITAGÓRICOS E GRUPO DE GALOIS.

Neste capítulo abordamos um aspecto diferente da teoria dos corpos formalmente reais. Ao invés de trabalharmos com o conceito de fecho algébrico, como é comum, vamos trabalhar com uma extensão Galosiana $\Omega|k$, onde k é um corpo formalmente real e Ω é um corpo quadraticamente fechado, isto é, Ω não admite 2-extensão Galosiana finita. No primeiro parágrafo desenvolveremos certos aspectos da teoria de Artin-Schreier para tais extensões, onde destacamos o Teorema (1.4) que, generaliza o bem conhecido teorema de Artin-Schreier, para corpos ordenados maximais.

Se um corpo k e toda extensão formalmente real de K for pitagórico, k é dito ser um corpo hereditariamente pitagórico. No Parágrafo 3, daremos uma caracterização em diversas maneiras, dos corpos intermediários, de uma extensão de corpos $\Omega|k$ quadraticamente fechada, que são hereditariamente pitagóricos.

No parágrafo 4, abordaremos uma família, bem especial, de corpos h.p. que são corpos h.e. (hereditariamente Euclidianos) e finalmente no parágrafo 5, daremos exemplos de corpos h.e. e h.p.

1. GENERALIZAÇÃO DO TEOREMA DE ARTIM-SCHREIER.

Sejam K um corpo, p um número primo e $\bar{K}$ um fecho algébrico

fixo de K . Consideremos a família F dos corpos intermediários L de $\bar{K}|K$ tais que $L|K$ seja uma p -extensão Galoisiana finita e denotemos o corpo gerado pelos elementos de F por K_p . O grupo de Galois de $K_p|K$ é um pró- p -grupo, pois, sendo um subgrupo do grupo produto $\prod_{L \in F} G(L|K)$, sua ordem é uma potência de p (ordem no sentido de número super natural). Agora, se N for um corpo intermediário de $\bar{K}|K_p$, tal que $N|K$ é extensão Galoisiana de $G(N|K)$ é um pró- p -grupo, então, $N \subset K_p$; de fato: se $\alpha \in N$, seja $L|K$ uma extensão Galoisiana finita com $K(\alpha) \subset L \subset N$. Como $N|K$ é uma p -extensão, $L|K$ é uma p -extensão Galoisiana finita. Daí, $L \in F$ e $\alpha \in K(\alpha) \subset L \subset K_p$. Consequentemente, $K_p|K$ é a maior extensão Galoisiana de K , com um pró- p -grupo de Galois.

K_p é denominado de *p-extensão Galoisiana maximal de K* e, quando $K_p = K$, diz-se que K é *p-fechado*.

1.1. DEFINIÇÃO. Dado um número primo p , uma extensão Galoisiana $\Omega|K$ é dita ser *p-fechada* se $\Omega = \Omega_p$, isto é, se Ω for *p-fechado*.

Se 2 divide o grau $[\Omega : K]$ e Ω for p -fechado para todo p que divide $[\Omega : K]$, $\Omega|K$ é dita ser uma extensão *prima-fechada*.

Seja $\alpha \in K_p$ um elemento qualquer e $\Omega|K$ uma extensão p -fechada. Consideremos um corpo intermediário L da extensão $K_p|K$ tal que $\alpha \in L$ e $L|K$ seja Galoisiana finita. Então, $[L : K] = p^r$ para algum $r \in \mathbb{N}$, o corpo composto $L\Omega$ é extensão Galoisiana finita de Ω e o grupo de Galois $G(L\Omega|\Omega)$ é isomorfo ao grupo $G(L|\Omega \cap L)$, que, por sua vez, é um subgrupo do p -grupo finito $G(L|K)$. Então,

$G(\Omega L|\Omega)$ é também um p -grupo finito. Como estamos supondo $\Omega|K$ uma extensão p -fechada, concluímos que $\Omega L = \Omega$. Portanto, $\alpha \in \Omega$ e daí resulta a seguinte proposição.

1.2. PROPOSIÇÃO. *Seja $\Omega|K$ uma extensão p -fechada. Então, a p -extensão Galoisiana maximal K_p de K é um subcorpo de Ω .*

Mencionaremos agora, sem provar, um Teorema, devido a Becker, que generaliza o Teorema de Artin-Schreier para corpos ordenados maximais, da seguinte forma.

1.3. TEOREMA (Becker). *Se para algum primo p , a p -extensão Galoisiana maximal K_p de um corpo K , é tal que $[K_p : K] < \infty$, então segue: $K = K_p$ ou K é formalmente real, $p = 2$ e $K_p = K(i)$.*

Observemos que, no último caso, isto é, quando K é formalmente real e $K_2 = K(i)$, então K é um corpo Euclideano. Isto porque, se $\alpha \in K$ é positivo, em alguma ordem de K , então $K(\sqrt{\alpha})$ é formalmente real. Reciprocamente, se K for um corpo Euclideano, então, $K(i)$ não admite extensão quadrática e, assim, $K(i) = K_2$.

Afim de facilitar a linguagem a ser usada, assumiremos, salvo menção contrária, que $\Omega|k$ é uma extensão Galoisiana 2-fechada e que k é um corpo formalmente real. Observemos que, se K é um corpo intermediário de $\Omega|k$, então $\Omega|K$ é da mesma forma uma extensão 2-fechada.

Pelo Lema de Zorn, a família dos corpos intermediários formalmente reais de $\Omega|k$, possui elemento maximais. Um tal elemento

será chamado de Ω -fecho real de k . No próximo resultado que é quase um corolário de (1.3), veremos que um Ω -fecho real de k é um corpo Euclidiano.

1.4. TEOREMA. Seja k um corpo intermediário de $\Omega|k$. Então, as seguintes afirmações são equivalentes:

- 1) k é um Ω -fecho real de k
- 2) $k(i) = \Omega$ e $\Omega \neq k$ ($i = \sqrt{-1}$)
- 3) $[\Omega : k] = 2^t$ para algum $t \in \mathbb{N}^*$.

DEMONSTRAÇÃO. 1) $\Rightarrow$ 2). Seja F um 2-Sylow corpo de $\Omega|k$, isto é, F é o corpo fixo de um 2-Sylow subgrupos do grupo $G(\Omega|k)$. Então $F|k$ é uma extensão de grau ímpar e consequentemente F é formalmente real. Logo, $F = k$ e, portanto, $\Omega|k$ é uma 2-extensão. Se $\alpha \in k$ é tal que $k(\sqrt{\alpha})$ é formalmente real, então $k(\sqrt{\alpha}) \subset \Omega$, pois, $\Omega = \Omega_2$, e daí, $k(\sqrt{\alpha}) = k$, isto é, $\alpha \in k^2$. Então, k é Euclidiano e, consequentemente, $k(i)$ é 2-fechado. Daí, $\Omega = k(i)$, pois conforme já mostramos, $\Omega|k$ é uma 2-extensão.

2) $\Rightarrow$ 3). Óbvio.

3) $\Rightarrow$ 1). Desde que $\Omega|k$ é uma 2-extensão não trivial, e conforme estamos supondo $\Omega = \Omega_2$, temos que $\Omega = k_2$. Então, pelo Teorema (1.3), concluimos que, $k(i) = \Omega$ e k é um corpo formalmente real. Daí, k é um Ω -fecho real de k .

1.5. OBSERVAÇÃO. Se assumirmos que $\Omega|k$ é uma extensão prima fechada,

podemos, em (1.4), substituir a condição (3) pela condição (3')
 $1 < [\Omega : k] < \infty$.

De fato: A implicação $(2) \Rightarrow (3')$ continua óbvia. Para mostrar $(3') \Rightarrow (1)$, seja p um primo divisor de $[\Omega : k]$ e considere um p -Sylow corpo F da extensão $\Omega|k$. Então, do fato de $\Omega|k$ ser p -fechado, $\Omega = F_p$. Assim, $1 < [F_p : F] < \infty$ e daí, por (1.3) $p = 2$, F é Euclideano e $F_p = F(i)$. Portanto, o único primo divisor de $[\Omega : k]$ é $p = 2$, e assim, $F = k$. Logo k é um Ω -fecho real de k .

1.6. COROLÁRIO. Seja k um Ω -fecho real de k . Então, k é um corpo euclideano e, conseqüentemente, o grupo de k -automorfismo de k é o grupo trivial.

1.7. COROLÁRIO. Seja $\sigma \in G(\Omega|k)$ um elemento finito não trivial de ordem 2^t ($t \in \mathbb{N}$). Então, σ é uma involução e $\sigma(i) = -i$.

DEMONSTRAÇÃO. Seja Ω^σ o corpo fixo do grupo finito gerado por σ . Então, $[\Omega : \Omega^\sigma] = 2^t$ e daí, $\Omega = \Omega^\sigma(i)$ onde $i \notin \Omega^\sigma$. Portanto, $\sigma(i) = -i$ e σ é uma involução.

1.8. COROLÁRIO. Se $G(\Omega|k)$ é gerado por involuções, então K é um corpo pitagórico.

DEMONSTRAÇÃO. Seja $(\sigma_i)_{i \in I}$ uma família de involuções geradoras de $G(\Omega|k)$. Os corpos $k_i = \Omega^{\sigma_i}$ ($i \in I$) são Ω -fechos reais de k .

Sabemos da teoria de Galois que $G(\Omega | \bigcap_{i \in I} k_i)$ é o grupo gerado por $\bigcup_{i \in I} \sigma_i$ que, por hipótese, é $G(\Omega | k)$. Portanto, $k = \bigcap_{i \in I} k_i$ é uma intersecção de corpos euclidianos. Daí, k é de fato um corpo pitagórico.

2. CORPOS HEREDITARIAMENTE PITAGÓRICOS E ESTRITAMENTE PITAGÓRICOS

Neste parágrafo k será suposto como sendo um corpo formalmente real.

Se P é um cone positivo de k , então, $(K^* : P) = 2$ e $-1 \notin P$. Por outro lado, se V é um subgrupo de k^* tal que $P \subsetneq V$, então, $-1 \in V$ e, assim, P é um subgrupo maximal de k^* sem conter -1 .

Cabe observar que podem existir subgrupos maximais V de k^* sem conter -1 com $k^{\cdot 2} \subset V$ tais que $V \cup \{0\}$ não é um cone positivo de k : Para ver isso, considere k como sendo um corpo formalmente real tal que $|\frac{k^*}{k^{\cdot 2}}| = 4$ e escreva $k^* = k^{\cdot 2} \cup -k^{\cdot 2} \cup ak^{\cdot 2} \cup -ak^{\cdot 2}$. Então $H = k^{\cdot 2} \cup -ak^{\cdot 2}$ é um subgrupo de k^* sem conter -1 . Se a é a soma de quadrados, então, H não pode ser um cone positivo de k^* . Para um exemplo mais concreto, tomemos $k \subseteq \mathbb{R}$ como sendo maximal em relação à exclusão de $\sqrt{2}$, dentro de $\mathbb{R}$, isto é, $\sqrt{2} \notin k$ e qualquer subcorpo de $\mathbb{R}$ contendo k , contém $\sqrt{2}$. Não é difícil mostrar que $|\frac{k^*}{k^{\cdot 2}}| = 4$. No caso tomamos $a = 2$.

2.1. Por um subgrupo maximal de k^* , entendemos um subgrupo U de k^* tal que $-1 \notin U$, $k^{\cdot 2} \subset U$ e com a propriedade de ser maximal sem conter -1 .

Observemos que; se U é um subgrupo de k^* tal que $-1 \notin U$ e $(k^* : U) = 2$, então, U é um subgrupo maximal de k^* . Por outro lado, se U é um subgrupo maximal de k^* , então $(k^* : U) = 2$. De fato: seja $x \in k^*$, então $x^2 \in U$. Se $x \notin U$, então $U + xU$ é um subgrupo de k^* contendo propriamente U . Logo $U + xU = k^*$, donde $-1 = u + xv$ para certos u, v em U . Portanto, $x = -(1+u)v^{-1} \in -U$ e, assim, $k^* = U \cup -U$.

Lembre-mo-nos de que um subconjunto T de k é um *pré-cone positivo* de k , se: $k^2 \subset T$, $T+T \subset T$, $T \cdot T \subset T$ e $T \cap -T = \{0\}$.

2.2. DEFINIÇÃO. Um pré-cone positivo T de um corpo formalmente real k é dito ser um "*fam*" (leque), se para todo subgrupo maximal U de k^* contendo T^* , o conjunto $U \cup \{0\}$ for um cone positivo de k .

2.3. PROPOSIÇÃO. Seja k um corpo formalmente real e T um pré-cone positivo de k . Então as seguintes afirmações são equivalentes.

- 1) T é um *fam*
- 2) $T + aT \subset T \cup aT$ qualquer que seja $a \in k \setminus -T$.

DEMONSTRAÇÃO. 1) $\Rightarrow$ 2) Seja $V = T^* \cup aT^*$. Então, $-1 \notin V$, pois T^* é um subgrupo multiplicativo de k^* ($t \in T^* \Rightarrow t^{-1} = (t^{-1})^2$, $t \in T^*$). V é um subgrupo de k^* e, além do mais $k^2 \subset V$. Nestas condições, podemos demonstrar de maneira análoga à demonstração de que um pré-cone é a intersecção de todos os cones que o contém,

que V é a interseção de todos os subgrupos maximais de k^* que o contêm. Desde que T^* é um fam, $V \cup \{0\}$ torna-se um pré-cone de k e assim $T + aT \subset V \cup \{0\} = T \cup aT$.

2) $\Rightarrow$ 1). Seja U um subgrupo maximal de k^* contendo T^* e $a \in U$. Então, $a \notin -T^*$ pois, se $a = -t$ com $t \in T^* \Rightarrow -1 = a^{t-1} \in U$. Assim, por hipótese, $1+a \in T \cup aT$, donde $1+a \in U$. Logo, U é aditivamente fechado e baseando-se em comentários já feitos, a respeito de subgrupos maximais, podemos concluir que $U \cup \{0\}$ é um cone de k . Portanto, T é um fam.

Como exemplos simples de fam, temos os cones positivos de k . Para um exemplo menos trivial, tomemos P e Q dois cones positivos de k . Então, $T = P \cap Q$ é um fam. Para ver isso seja $\alpha \in k \setminus -T$. Então, $\alpha \in P$ ou $\alpha \in Q$. Suponhamos que $\alpha \in P$. Seja agora $a \in T$ um elemento qualquer. Temos de mostrar que $1+a\alpha \in T \cup \alpha T$. Se $1+a\alpha \notin Q$, então, $\alpha \notin Q$ e $\frac{1}{\alpha} \notin Q$, donde, $\frac{1}{\alpha}(1+a\alpha) = \frac{1}{\alpha} + a \in Q$. Assim, $1+a\alpha = \alpha(\frac{1}{\alpha} + a) \in \alpha T$.

Relembremos, que um corpo formalmente real k , é *pitagórico* se $k^2 + k^2 \subset k^2$, isto é, se a soma de quadrados de k é novamente um quadrado em k .

Um resultado simples, que nos será útil futuramente o o seguinte:

2.4. PROPOSIÇÃO. Um corpo formalmente real k é *pitagórico* se, e somente se $k(\sqrt{-1})$ é a única extensão quadrática não real de k .

DEMONSTRAÇÃO. $\Rightarrow$). Seja L uma extensão quadrática não real de k . Podemos supor $L = k(\sqrt{a})$, onde a não é positivo em toda ordem de k . Daí, a é um quadrado ou seja, $k(\sqrt{a}) = k(\sqrt{-1})$, como queríamos.

$\Leftarrow$) Suponhamos que k não seja pitagórico. Existe, então, $b \in k$ tal que $1+b^2 \notin k^2$. Por outro lado, $-(1+b^2) \in -\Sigma k^2$, donde $k(\sqrt{-(1+b^2)})$ é uma extensão quadrática não real de k . Assim, $k(\sqrt{-(1+b^2)}) = k(\sqrt{-1})$, donde, $\sqrt{-(1+b^2)} = a+ci$ com $a, b \in k$ e $i = \sqrt{-1}$. Daí, $-1-b^2 = a^2 + 2aci - c^2$, donde $-1-b^2 = a^2 - c^2$ e $2ac = 0$. Assim, $-(1+b^2) = a^2$ ou $-(1+b^2) = -c^2$ o que, em ambos os casos, é uma contradição.

Vamos agora fortalecer, ainda mais, o conceito de corpos pitagóricos.

2.5. DEFINIÇÃO. Seja $L|k$ uma extensão algébrica de corpos. Diz-se que k é *hereditariamente pitagórico* (notação h.p) relativamente a L , se k e todo corpo formalmente real entre k e L for pitagórico.

Se $L = \bar{k}$ for o fecho algébrico de k , é comum dizer que k é h.p, ao invés de h.p relativamente a $\bar{k}$.

Se em um corpo k , o conjunto k^2 é um fam, então, k é dito ser *estritamente pitagórico* ou *superpitagórico*.

Se k for estritamente pitagórico, então k é h.p relativamente a seu fecho quadrático k_2 . Este é o resultado (2.7) que demonstraremos usando o seguinte resultado, devido a Lam.

2.6. LEMA. Seja k um corpo formalmente real e $L = k(\sqrt{\alpha})$ uma extensão quadrática de k , então a seguinte sequência é exata:

$$1 \longrightarrow \{k^{\cdot 2}, \alpha k^{\cdot 2}\} \longrightarrow k^{\cdot}/k^{\cdot 2} \xrightarrow{\epsilon} L^{\cdot}/L^{\cdot 2} \xrightarrow{\bar{N}} k^{\cdot}/k^{\cdot 2}$$

onde ϵ é a aplicação induzida pela inclusão $k \longrightarrow L$ e $\bar{N}$ é o homomorfismo induzido pela função norma $N = N_{L|k}$.

DEMONSTRAÇÃO. A exatidão em $k^{\cdot}/k^{\cdot 2}$ é consequência de cálculos simples. Para mostrar a exatidão em $L^{\cdot}/L^{\cdot 2}$, seja $x = (a + b\sqrt{\alpha}) \in L^{\cdot}$, e suponhamos que $N(x) = a^2 - b^2\alpha \in k^{\cdot 2}$, isto é, $N(x) = c^2$ para algum $c \in k^{\cdot}$. Seja $y = c - \bar{x}$ onde $\bar{x} = a - b\sqrt{\alpha}$. Temos $x^2 = x(N(x) - 2c\bar{x} + \bar{x}\bar{x}) = xN(x) - 2cx\bar{x} + N(x)(x + \bar{x}) - 2cN(x) \in k$. Se $y = 0 \Rightarrow \bar{x} = c \in k^{\cdot} \Rightarrow x \in k^{\cdot}$. Se $y \neq 0$, então pelos cálculos já efetuados, $x = d(y^{-1})^2$ para $d \in k^2$, e assim, $xL^{\cdot 2} = dL^{\cdot 2} \in k^{\cdot}/L^{\cdot 2}$, donde segue a exatidão em $L^{\cdot}/L^{\cdot 2}$.

2.7. COROLÁRIO. Com a mesma notação de (2.6), se k for estritamente pitagórico e L for uma extensão formalmente real de k , então, $L^{\cdot} = k^{\cdot}L^{\cdot 2} \cup \sqrt{\alpha}k^{\cdot}L^{\cdot 2}$ e a união é disjunta.

DEMONSTRAÇÃO. A inclusão $k^{\cdot}L^{\cdot 2} \cup \sqrt{\alpha}k^{\cdot}L^{\cdot 2} \subset L^{\cdot}$ é óbvia. Seja agora $y \in L^{\cdot}$. Do fato de $k^{\cdot 2}$ ser um fam e $\alpha \notin k^{\cdot 2} \cup -k^{\cdot 2}$, temos que $N(L^{\cdot}) \subset k^{\cdot 2} \cup -\alpha k^{\cdot 2}$. Então, $N(y) = x^2 \in k^{\cdot 2}$ ou $N(y) = -\alpha x^2 \in -\alpha k^{\cdot 2}$.

$$\text{Se } N(y) = x^2 = N(x) \Rightarrow N(yx^{-1}) = 1 \Rightarrow$$

$$(Yx^{-1})_{L \cdot 2} \in \text{Ker}(\bar{N}) = \text{Im} \varepsilon \Rightarrow (Yx^{-1})_{L \cdot 2} = zL \cdot 2 \text{ para algum } z \in k' \\ \Rightarrow Yx^{-1} = zt^2 \text{ (} t \in L' \text{)} \Rightarrow y = xzt^2 \in k' \cdot L \cdot 2.$$

Se $N(y) = -\alpha x^2$ com $x \in k'$. Como $N(\sqrt{\alpha}) = -\alpha$, então $N(y) = N(\sqrt{\alpha})x^2 \Rightarrow N(y\sqrt{\alpha}^{-1}) = x^2$, donde, pelo primeiro caso, $y\sqrt{\alpha}^{-1} \in k' \cdot L \cdot 2$ ou $y \in \sqrt{\alpha} k' \cdot L \cdot 2$.

Portanto, mostramos a inclusão $L' \subset k' \cdot L \cdot 2 \cup \sqrt{\alpha} k' \cdot L \cdot 2$ e, daí, $L' = k' \cdot L \cdot 2 \cup \sqrt{\alpha} k' \cdot L'$. A demonstração de que $k' \cdot L \cdot 2 \cap \sqrt{\alpha} k' \cdot L \cdot 2 = \emptyset$ é feita através de cálculos diretos.

2.8. TEOREMA. (Becker). Um corpo formalmente real k é h.p relativamente ao seu fecho quadrático k_2 se, e somente se k é estritamente pitagórico.

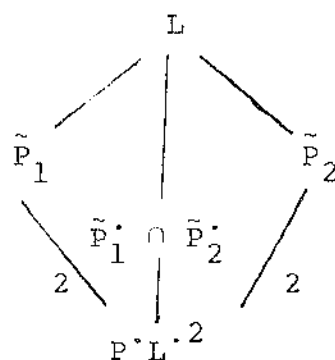
DEMONSTRAÇÃO. $\Rightarrow$) Suponhamos que k seja h.p relativamente a k_2 . Então, toda extensão quadrática formalmente real de k é pitagoreana. Devido a Proposição (2.3), devemos mostrar que $k^2 + \alpha k^2 \subset k^2 \cup \alpha k^2$ qualquer que seja $\alpha \in k \setminus -k^2$. E isto é equivalente a mostrar que $1 + \alpha a^2 \in k^2 \cup \alpha k^2$, onde $a \in k'$ e $\alpha \in k \setminus -k^2$.

Consideremos $a \in k'$ e $\alpha \in k \setminus -k^2$. Então, $\alpha \notin -k^2 = -\Sigma k^2$, e assim, existe uma ordem $<_1$ de k tal que $0 <_1 \alpha$, donde $0 <_1 1 + \alpha a^2$. Assim, $k(\sqrt{\alpha})$ e $k(\sqrt{1 + \alpha a^2})$ são extensões quadráticas formalmente reais de k , portanto, são corpos pitagóricos. Afirimo: $k(\sqrt{1 + \alpha a^2}) = k(\sqrt{\alpha})$. De fato: α é quadrado em $k(\sqrt{\alpha})$, então, $1 + a^2 \alpha \in k(\sqrt{\alpha})^2 \Rightarrow \sqrt{1 + a^2 \alpha} \in k(\sqrt{\alpha}) \Rightarrow k(\sqrt{1 + \alpha a^2}) \subset k(\sqrt{\alpha})$. A outra inclusão é óbvia.

Logo, existem elementos $x, y \in k$ tais que $\sqrt{1+a^2\alpha} = x+y\sqrt{\alpha}$
 $\Rightarrow 1+a^2\alpha = x^2 + 2xy\sqrt{\alpha} + y^2\alpha \Rightarrow x = 0$ ou $y = 0$. Assim, $1+a^2\alpha \in k^2 \cup \alpha k^2$ e, isto é suficiente para concluirmos que k^2 é um fam.

$\Leftarrow$) Seja $L = k(\sqrt{\alpha})$ uma extensão quadrática formalmente real do corpo k . Vamos mostrar que L é da mesma forma, estritamente pitagórico.

Seja U um subgrupo maximal de L^* e coloquemos $P^* = k^* \cap U$. Então, $-1 \notin P$, $k^{\cdot 2} \subset P$ e $(k^* : P) = 2$. Daí, P^* é um subgrupo maximal de k^* e, como k é estritamente pitagoreano, concluimos que $P^* \cup \{0\} = P$ é um cone positivo de k . $L^{\cdot 2} \subset U \Rightarrow \alpha \in P$, então existem dois cones, digamos $\tilde{P}_1$ e $\tilde{P}_2$, de L estendendo P . Por (2.7), $(L^* : k^* L^{\cdot 2}) = 2$, donde $(L^* : P^* L^{\cdot 2}) = 4$ e, como $P^* L^{\cdot 2} \subset \tilde{P}_i$ ($i=1,2$), obtemos $P^* L^{\cdot 2} = \tilde{P}_1 \cap \tilde{P}_2$. Desse modo, temos o seguinte diagrama:



Assim, $P^* L^{\cdot 2}$ é um fan de L^* e, como $U \supset P^* L^{\cdot 2}$ é maximal, concluímos que $U \cup \{0\}$ é um cone de L . Portanto, $L = k$ e $L = k(\sqrt{\alpha})$ é estritamente pitagórico.

Seja agora L um corpo intermediário formalmente real de $k_2 | k$.

Se $a, b \in L$ então, $k(a, b)|k$ é uma extensão finita e assim, podemos supor, sem perda de generalidade, que $L|k$ é uma extensão finita. Logo $[L:k] = 2^r$ para algum $r \in \mathbb{N}$ e daí, existe uma sequência de corpos $k = L_0 \subset L_1 \subset \dots \subset L_r = L$ com $[L_{i+1}:L_i] = 2$, $i = 0, 1, \dots, r-1$. Conforme mostramos L_1 é estritamente pitagoreano. Portanto L_2 e, assim, sucessivamente. Desde que corpos estritamente pitagóricos são claramente pitagóricos, a demonstração está concluída.

3. CARACTERIZAÇÃO DE CORPOS HEREDITARIAMENTE PITAGÓRICOS

Assim como no parágrafo anterior k será considerado, implicitamente, um corpo formalmente real. $\Omega|k$ será uma extensão Galoisiana 2-fechada e, entenderemos como sendo um Ω -fecho real de um corpo formalmente real $L \subset \Omega$, como sendo uma extensão ordenada maximal de L , contida no corpo Ω .

Vamos, neste parágrafo, dar uma caracterização, devida a Becker, dos corpos intermediários de $\Omega|k$ que são h.p relativamente a Ω . Tal caracterização é o Teorema (3.11).

Antes de dar esta caracterização, vamos demonstrar alguns resultados preliminares. O primeiro resultado é a respeito da teoria geral de grupos profinitos.

3.1. LEMA. Seja $L|K$ uma extensão Galoisiana arbitrária e V um subgrupo abeliano do grupo de Galois $G = G(L|K)$. Então, o fecho topológico de V em G é, também, um grupo abeliano.

DEMONSTRAÇÃO. Seja $a \in L$, um elemento qualquer, e M uma extensão de $K(a)$ em L tal que $M|K$ é Galoisiana e finita. Sejam σ_1 e σ_2 elementos arbitrários de $G(L|F)$ onde $F = \text{fix}(V)$ é o corpo fixo de V e consideremos as vizinhanças básicas $V_M(\sigma_i) = \{\tau \in G(L|K) \mid \tau|_M \equiv \sigma_i|_M\}$ ($i = 1, 2$) de σ_i na topologia de Krull de G . Do fato de V ser denso em $G(\Omega|M)$, existem elementos $\varphi_i \in V_M(\sigma_i)$ ($i=1, 2$), tais que $\varphi_1|_M \equiv \sigma_1|_M$, $\varphi_2|_M \equiv \sigma_2|_M$. Daí, $(\sigma_1\sigma_2)(a) = (\sigma_2\sigma_1)(a)$ e $G(L|F)$ é abeliano.

3.2. LEMA. Seja V um subgrupo abeliano do grupo de Galois $G(\Omega|K)$ e $F = \Omega^V$ seu corpo fixo. Então, V é finito com 2 elementos ou F não é formalmente real.

DEMONSTRAÇÃO. Suponhamos que F seja formalmente real. Neste caso, escolhamos k como sendo um Ω -fecho real de F . Sendo $G(\Omega|F)$ o fecho do grupo abeliano V , por (3.1), o mesmo é abeliano e, portanto, $k|F$ é uma extensão normal. Por k ser Euclídeano $\text{Aut}(k|F) = 1$, então, $F = k$ e assim, por (1.4), $\Omega = k(i) = F(i)$. Portanto, V tem dois elementos.

3.3. LEMA. Seja $U = G(\Omega|k(i))$ abeliano e σ uma involução em $G(\Omega|k)$. Então, $\sigma u \sigma = u^{-1}$, qualquer que seja $u \in U$.

DEMONSTRAÇÃO. Coloquemos $W = \{\sigma u \sigma \mid u \in U\}$. O Lema estará demonstrado se mostrarmos que $\#W = 1$.

Primeiramente, mostraremos que W é um subgrupo de U . Temos que $\sigma(i) = -i$ e que $u(i) = i$, $\forall u \in U$, então, $W \subset U$. Sejam agora u e v elementos quaisquer de U . Os elementos $\sigma u \sigma$ e $\sigma v \sigma$ também estão em U , então, do fato de U ser abeliano, $(\sigma u \sigma)(\sigma v \sigma) = (\sigma u \sigma)u(\sigma v \sigma)v = (\sigma u \sigma)(\sigma v \sigma)uv = \sigma uv \sigma$ está em W . Como $(\sigma u \sigma)(\sigma u^{-1} \sigma u^{-1}) = 1$, $\forall u \in U$, segue-se que W é um subgrupo de U .

Seja $F' = \Omega^W$ o corpo fixo de W e coloquemos $F = F' \cap \Omega^\sigma$. Então, $G(\Omega|F) = \langle \sigma \rangle \cdot \bar{W}$ é o grupo gerado por σ e $\bar{W}$, onde $\bar{W}$ é o fecho topológico de W em $G(\Omega|k)$, ($W = G(\Omega|F')$). Desde que W é abeliano e $\sigma(\sigma u \sigma) = \sigma(\sigma u \sigma)u = \sigma u(\sigma u \sigma) = (\sigma u \sigma)\sigma$, $\forall u \in U$, concluímos que $\langle \sigma \rangle \cdot W$ é abeliano. Daí, por (3.1), $G(\Omega|F)$ é também abeliano. Agora, F é formalmente real, isto porque, $[\Omega : \Omega^\sigma] = 2$ e $i \notin \Omega^\sigma$ ($\sigma(i) = -i$) é equivalente a afirmação de que Ω^σ é um Ω -fecho (1.4). Então, por (3.2), $\# \langle \sigma \rangle \cdot W = 2$ ou seja $\# W = 1$.

O seguinte resultado aponta a diferença existente, entre um corpo pitagórico e um corpo hereditariamente pitagórico.

3.4. LEMA. *Seja k_2 o fecho quadrático do corpo formalmente real k . Então, as seguintes afirmações são equivalentes.*

- 1) k é h.p relativamente a k_2 ;
- 2) Toda extensão não formalmente real de k em k_2 contém $i = \sqrt{-1}$.
- 3) O grupo de Galois, $G(k_2|k(i))$ é abeliano.

DEMONSTRAÇÃO. 1) $\Rightarrow$ 2). Seja L uma extensão não formalmente real de k em K_2 . Podemos assumir que $L|k$ é uma extensão finita e, dessa forma, $[L:k] = 2^r$ para algum inteiro positivo r . Portanto, existe uma sequência de corpos $K = L_0 \subset L_1 \subset \dots \subset L_r = L$ com $[L_j : L_{j-1}] = 2$ para $j = 1, 2, \dots, r$. Pela suposição sobre L , existe um inteiro n , tal que L_n é formalmente real, portanto, Pitagórico, mas L_{n+1} não é formalmente real. Como $L_{n+1}|L_n$ é uma extensão quadrática, por (2.4), $L_{n+1} = L_n(i)$ e, assim, $i \in L_{n+1} \subset L$.

2) $\rightarrow$ 3). Seja $U = G(k_2|k(i))$ e σ uma involução de $G(\Omega|k)$. Como $\sigma(i) = -i$, segue que $k_2^\sigma \cap k(i) = k$ e, portanto, $G(k_2|k) = \langle \sigma \rangle \cdot U$ é o fecho do grupo gerado pelos subgrupos $\langle \sigma \rangle$ e U .

Dado, $u \in U$, colocamos $F = k_2^{\sigma u}$. Desde que $u(i) = i$, temos que $(\sigma u)(i) = -i$. Assim, F é formalmente real e daí, por (3.2), com $v = \langle \sigma u \rangle$, concluímos que $\# \langle \sigma u \rangle = 2$, isto é, $\sigma u \sigma = u^{-1}$. Essa última relação é válida $\forall u \in U$. Logo, se u, v são elementos de U , segue que $u^{-1} v^{-1} = (\sigma u \sigma)(\sigma v \sigma) = \sigma u v \sigma = (uv)^{-1} = v^{-1} u^{-1}$ ou seja, $uv = vu$ e, U é um grupo abeliano.

3) $\rightarrow$ 1) Seja $G = G(k_2|k)$ e $U = G(k_2|k(i))$. Se σ é uma involução de G , então, $k_2^\sigma \cap k(i) = k$ (pois $\sigma(i) = -i$), donde $G = \langle \sigma \rangle \cdot U$. Como U é abeliano, pelo Lema (3.3), $(\sigma u)^2 = 1$, $\forall u \in U$ e assim G é gerado pelas involuções σu com $u \in U$. Daí, por (1.8) k é pitagoreano. Se L for um corpo formalmente real, intermediário de $k_2|k$, então $G(k_2|L(i))$ é também um grupo abeliano por ser subgrupo de $G(k_2|k(i))$. Dessa forma, o mesmo argumento já usado mostra que L é pitagórico. Portanto, 3) $\rightarrow$ 1) e o lema está demonstrado.

Para o Lema (3.6) necessitamos do seguinte resultado, sobre teoria dos grupos.

3.5. PROPOSIÇÃO. Seja G um grupo finito de ordem 2^t no qual todo elemento diferente da identidade tem ordem dois. Então, se $g \in G$ e $g \neq 1$, o número de subgrupos de índice dois de G não contendo g é exatamente 2^{t-1} .

DEMONSTRAÇÃO. Consideremos G como um espaço vetorial sobre o corpo $\mathbb{Z}_2$ e $\hat{G}$ como sendo o dual de G . Os subespaços de dimensão $t-1$ estão em correspondência bijetora com os núcleos dos elementos não triviais $\theta \in \hat{G}$. Então, o número de subgrupos de G possuindo ordem 2^{t-1} é 2^{t-1} . Agora, se $g \in G$ é diferente da identidade, existe uma correspondência bijetora entre o conjunto dos subgrupos de índice dois de G contendo g , e o conjunto dos subgrupos de índice 2 do grupo quociente $G/(g)$. A cardinalidade do último conjunto é $2^{t-1}-1$. Logo, o número de subgrupos de índice dois de G não contendo g é $2^t - 1 - (2^{t-1} - 1) = 2^{t-1}$.

3.6. LEMA. Seja $L|K$ uma extensão finita arbitrária com L sendo es
tritamente pitagórico. Então, existe $t \in \mathbb{N}$ satisfazendo as seguin
tes condições:

$$1) (L^* : K \cdot L^{\cdot 2}) = 2^t$$

2) Se P é um cone positivo de K que admite extensão a L , en
tão, o número de tais extensões é exatamente 2^t .

DEMONSTRAÇÃO. Seja P um cone positivo de k que admite extensão a L . Então PL^2 é um pré-cone positivo de L pois, se $\alpha, \beta \in L^*$ e $a \in P^*$, então $a \in L \setminus L^2$ e daí, do fato de L^2 ser um fam, segue que $\alpha^2 + a\beta^2 \in L \cdot L^2 \cup aL \cdot L^2 \subset P \cdot L^2$.

Os cones positivos de L contendo PL^2 são, precisamente, as extensões de P a L e são em número finito, pois $L|k$ é uma extensão finita. Daí e, do fato de L^2 ser um fam, os cones positivos de L que contêm $P \cdot L \cdot L^2$ são, precisamente os subgrupos maximais de L^* que contêm $P \cdot L \cdot L^2$. Como PL^2 é um pré-cone de L , concluímos que $P \cdot L \cdot L^2$ é a interseção de todos subgrupos maximais de L^* , contendo $P \cdot L \cdot L^2$. Agora, o número de tais subgrupos é finito e cada um contém $L \cdot L^2$. Então, o grupo $L^*/P \cdot L \cdot L^2$ é finito e possui todo elemento com ordem 1 ou 2. Daí, $(L^* : P \cdot L \cdot L^2) = 2^{t+1}$ para algum $t \in \mathbb{N}$ e, portanto, $(L^* : k \cdot L \cdot L^2) = 2^t$ o que prova a condição 1.

Para concluirmos a condição 2, usando (3.5), basta observarmos que o número de subgrupos maximais de L^* contendo $P \cdot L \cdot L^2$ exatamente o número de subgrupos de $L^*/P \cdot L \cdot L^2$ que não contêm $-P \cdot L \cdot L^2$.

3.7. COROLÁRIO. Seja $L|k$ uma extensão de grau ímpar, onde L é estritamente pitagórico. Então, um cone de k , que admite extensão a L tem exatamente uma extensão, a saber, $P \cdot L^2$.

DEMONSTRAÇÃO. Do fato de $L|k$ ser extensão de grau ímpar, P admite um número ímpar de extensão a L . Por (3.6), existe $t \in \mathbb{N}$ tal que o número de extensões de P a L é 2^t . Então, $t = 0$ e, sendo PL^2 um pré-cone de L , temos que PL^2 é o cone de L estendendo P .

Antes de enunciar o próximo resultado, observemos que: se $L|k$ for uma extensão Galoisiana finita e $\tilde{P}$ for um cone de L tal que $P = \tilde{P} \cap K$, então, a aplicação $\psi : G(L|k) \longrightarrow \{\text{cones de } L \text{ estendendo } P\}$ onde $\psi(\sigma) = \sigma(\tilde{P})$ é uma bijeção.

Para a confirmação deste fato, note que; se $\sigma(\tilde{P}) = \tilde{P}$, então, $\sigma = \text{identidade}$ e que a cardinalidade do contra domínio de ψ é menor ou igual que o grau da extensão $L|k$.

3.8. COROLÁRIO. *Seja $L|k$ uma extensão Galoisiana finita com L sendo estritamente pitagórico. Então, existe $t \in \mathbb{N}$ tal que $[L : k] = 2^t$.*

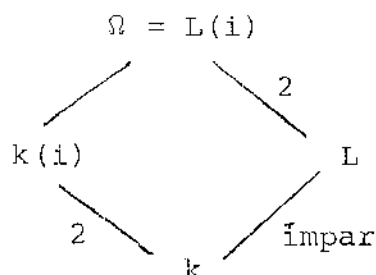
DEMONSTRAÇÃO. Pelo lema 4, se $\tilde{P}$ é um cone de L , então, o número de extensões de $k \cap \tilde{P} = P$ a L é 2^t para algum $t \in \mathbb{N}$. Em virtude da observação feita acima segue-se o resultado.

Por um 2-Sylow corpo de uma extensão Galoisiana $L|K$, possivelmente finita, entenderemos o corpo fixo de um 2-Sylow subgrupo de $G(L|K)$, ([21], pág. 47).

Seja $L|k$ uma extensão de corpos tal que k é toda, extensão algébrica formalmente real de k contida em L são corpos Euclidianos. Então, k é dito ser *hereditariamente Euclideano* (h.e) com relação a L , ou simplesmente hereditariamente euclideano, se L for o fecho algébrico de k . Tais corpos são um tipo bem especial de corpos hereditariamente pitagóricos e serão estudados no parágrafo 4.

3.9. LEMA. Se k é Euclídeano e h.p relativamente a Ω , então, k é hereditariamente Euclídeano relativamente a Ω e $G(\Omega|k(i))$ é abeliano de ordem ímpar.

DEMONSTRAÇÃO. Seja L um 2-Sylow corpo de $\Omega|k$, então, L é uma extensão de grau ímpar de k (ímpar no sentido de número supernatural), e logo é formalmente real. Claramente, L é h.p relativamente a Ω e, em particular, do fato de $L_2 \subset \Omega$, por (2.8), L é estritamente pitagórico. Agora, k é um corpo Euclídeano, então, por (3.7), L tem uma única ordem. Assim, L é Euclídeano e, sendo $\Omega|L$ uma 2-extensão temos, então, que $\Omega = L(i)$. Consequentemente, o grau $[\Omega:k(i)]$ é ímpar (ver diagrama abaixo).



e $[\Omega:k] = 2n$, onde n é um supernatural ímpar.

Assim, já mostramos que $U = G(\Omega|k(i))$ tem grau ímpar. Vamos agora, mostrar que U é abeliano. Seja σ uma involução qualquer em $G(\Omega|k)$ e $u \in U$. Colocando, $F = \Omega^{\langle \sigma u \rangle}$, por (3.2), temos que $(\sigma u)^2 = 1$ ou F não é formalmente real. No segundo caso o grau $[F:k]$ é par e, daí, $i \in F$, pois caso contrário obtemos que $4 \nmid [F(i):k]$ contradizendo $[\Omega:k] = 2n$, onde n é ímpar. Agora, $i \in F$ é também uma contradição, pois $(\sigma u)(i) = -i$. Então,

$(\sigma u)^2 = 1$, ou seja, $\sigma u \sigma = u^{-1}$ ocorre $\forall u \in U$. Daí, U é abeliano, pois, $u, v \in U \implies \sigma uv \sigma = (uv)^{-1} = v^{-1} u^{-1} = (\sigma v \sigma)(\sigma u \sigma) = \sigma v \sigma \sigma u \sigma = (\sigma u \sigma)^{-1}$, donde $uv = vu$.

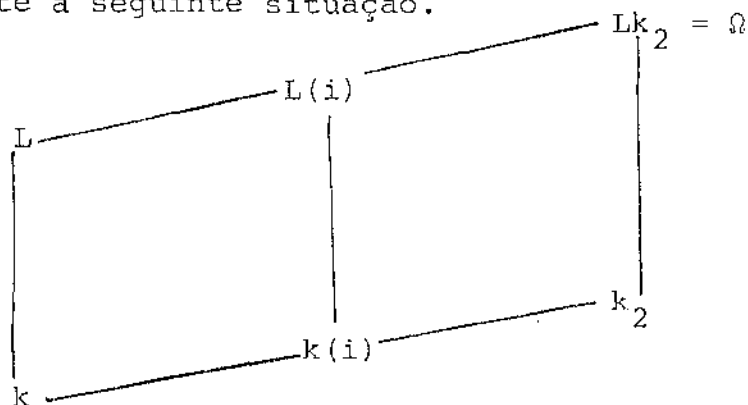
Resta agora, mostrar que, k é h.e. relativamente a Ω . Seja E um corpo intermediário formalmente real de $\Omega|k$ e consideremos um Ω -fecho real k de E . Então, como $\Omega = k(i)$ e $[\Omega : k] = 2n$ com n ímpar, concluímos que E é uma extensão de grau ímpar de k . Por (1.2), $E_2 \subset \Omega$ e, logo E é h.p. relativamente a E_2 e daí, por (2.8), E é estritamente pitagórica. Assim, por (3.7), E tem uma única ordem e E é euclideano. Portanto, k é de fato h.e. relativamente a Ω .

3.10. LEMA. Se k é h.p. relativamente a k_2 , e o grupo de Galois, $G(\Omega|k_2)$ é abeliano, então, $G(\Omega|k(i))$ é abeliano.

DEMONSTRAÇÃO. Observemos primeiramente que $[\Omega : k_2]$ é ímpar, pois se $2 \mid [\Omega : k_2]$, então existe um corpo intermediário L de $\Omega|k_2$ tal que $2 \mid [L : k_2] < \infty$. Como $G(\Omega : k_2)$ é abeliano, $L|k_2$ é extensão normal. $G(L : k_2)$ é também abeliano, então, por recorrência finita, conseguimos uma extensão quadrática de k_2 o que não é possível.

Seja L um 2-Sylow corpo de $\Omega|k$. Desde que $[L : k]$ é ímpar, L é formalmente real, e como $\Omega|L$ é uma 2-extensão, $L_2 = \Omega$. Observemos, também, que $L(i)$ é um 2-Sylow corpo de $\Omega|k(i)$. Do fato de Lk_2 ser um corpo intermediário de $\Omega = L_2|L$, $\Omega|Lk_2$ é uma 2-extensão, sendo $[\Omega : k_2]$ ímpar, concluímos, então, que $[\Omega : k_2]$ e

$[\Omega : Lk_2]$ são relativamente primos. Portanto, $\Omega = Lk_2$ e daí, estamos presente à seguinte situação.



Sendo uma extensão de grau ímpar de K , L deve ser formalmente real. Além disso, observando que, $[L(i) : k(i)]$ é ímpar, e que toda extensão Galoisiana finita de k , contida em k_2 , tem por grau uma potência de 2, concluímos que $L(i) \cap k_2 = k(i)$. Assim, $G(\Omega | L(i)) \approx G(k_2 | k(i))$ é um grupo abeliano e $G(\Omega | k(i)) = G(\Omega | L(i)) \cdot G(\Omega | k_2)$ é o grupo gerado pelos grupos abelianos $W = G(\Omega | k_2)$ e $V = G(\Omega | L(i))$. Portanto, para mostrarmos que $G(\Omega | k(i))$ é abeliano, é suficiente mostrarmos que, $vw = wv$, $\forall v \in V$ e $\forall w \in W$.

Seja σ uma involução arbitrária de $G(\Omega | L)$ e coloquemos $E = k_2 \cap \Omega^\sigma$; $\sigma' = \sigma|_{k_2}$ é também uma involução em $G(k_2 | k)$ e $k_2^{\sigma'} = E$. Então, $[k_2 : E] = 2$ e daí, $k_2 = E(i)$. Por hipótese, $W = G(\Omega | E(i))$ é abeliano e como σ é também uma involução de $G(\Omega | E)$, pelo Lema (3.3), concluímos que $w\sigma w = w^{-1}$ qualquer que seja $w \in W$. Sejam agora, $v \in V$, $w \in W$ e $\sigma \in G(\Omega | L)$ uma involução qualquer. Pelo Lema (3.4), toda extensão não formalmente real de L em $\Omega = L_2$ contém i . Como o subgrupo $\langle \sigma v \rangle$ de $G(\Omega | L)$ é abeliano e

$(\sigma v)(i) = -i$, por (3.2), segue que $\# \langle \sigma v \rangle = 2$, ou seja, σv é uma involução em $G(\Omega|L)$. Daí, conforme já mostramos, $(\sigma v)w(\sigma v) = w^{-1}$ ou $(\sigma v)w(\sigma v)^{-1} = w^{-1}$. Por outro lado, vale também, $\sigma w^{-1}\sigma = w$, isto é, $\sigma((\sigma v)w(\sigma v)^{-1})\sigma = vwv^{-1} = w$. Logo, $vw = wv$ e, portanto, $G(\Omega|k(i))$ é abeliano.

Estamos agora, em condições de demonstrar o teorema principal deste parágrafo, teorema este, que é devido a Becker e que caracteriza de diversas formas os corpos intermediários de k que são h.p relativamente a Ω .

3.11. TEOREMA. (Becker). *Se K é um corpo intermediário formalmente real, da extensão Galoisiana 2-fechada $\Omega|k$, então as seguintes afirmações são equivalentes*

- 1) K é um corpo h.p relativamente a Ω .
- 2) $G(\Omega|K(i))$ é abeliano.
- 3) Toda extensão não formalmente real de K em Ω contém $i=\sqrt{-1}$.
- 4) Toda extensão formalmente real de K em Ω , é a interseção de seus Ω -fechos reais.

DEMONSTRAÇÃO. $1) \Rightarrow 2)$. Em consequência do lema (3.10) basta mostrar que os grupos de Galois, $G(\Omega|K_2)$ e $G(K_2|K(i))$ são abelianos. Fazemos isto, Como K é h.p relativamente a Ω , K é também h.p relativamente a $K_2 \subset \Omega$. Daí, pelo Lema (3.4), $G(K_2|K(i))$ é abeliano. Consideremos agora, um K_2 -fecho real E de K . E , é Euclideano e h.p relativamente a Ω . Então, pelo Lema (3.4), $G(\Omega|E(i)) = G(\Omega|K_2)$ é

abeliano, e, assim, concluimos a implicação.

2) $\rightarrow$ 3). Seja $U = G(\Omega|K(i))$ e σ uma involução em $G(\Omega|K)$. Então, $G(\Omega|K) = \langle \sigma \rangle \cdot U$ é o grupo gerado por σ e U , isto porque $\sigma \notin U$, e como U é abeliano, pelo Lema (3.2), $(\sigma u)^2 = 1$, $\forall u \in U$. Se L é uma extensão não formalmente real de K em Ω , $G(\Omega|L)$ é livre de 2-torção. Por outro lado, $\langle \sigma \rangle \cdot U = \{\sigma u | u \in U\} \cup U$ e, como $G(\Omega|L)$ é subgrupo de $\langle \sigma \rangle \cdot U$, concluimos que $G(\Omega|L) \subset U$, e daí, $K(i) \subset L$, mostrando assim, que $i \in L$.

3) $\rightarrow$ 2). De acordo com o Lema (3.10), é suficiente mostrar que os grupos $G(\Omega|K_2)$ e $G(K_2|K(i))$ são abelianos. Pelo Lema (3.4), $G(K_2|K(i))$ já é abeliano, isto porque $K_2 \subset \Omega$. Para mostrarmos que $G(\Omega|K_2)$ é abeliano, vamos usar o Lema (3.9). Seja E um K_2 -fecho real de K . Por (1.4) E é euclideano e $K_2 = E(i)$. Se L é um corpo formalmente real tal que $E \subset L \subset \Omega$ e F é uma extensão quadrática não formalmente real de L , então, $i \in F$ e, assim, $F = L(i)$. Daí, por (2.4), L é pitagórico, e desse modo, E é h.p relativamente a Ω . Então, pelo Lema (3.9), $G(\Omega|E(i)) = G(\Omega|K_2)$ é abeliano.

2) $\Rightarrow$ 4). Seja L uma extensão formalmente real de K em Ω . Por ser subgrupo de $G(\Omega|K(i))$, $G(\Omega|L(i))$ é também abeliano. Então, se σ é uma involução em $G(\Omega|L)$, temos que $G(\Omega|L) = \langle \sigma \rangle \cdot U$ onde $U = G(\Omega|L(i))$ e, pelo Lema (3.3), $(\sigma u)^2 = 1$, $\forall u \in U$. Então, $G(\Omega|L)$ é gerado pelas involuções σu com $u \in U$ e daí $L = \bigcap_{u \in U} \Omega^{\sigma u}$ é uma interseção de Ω -fechos reais de L . Por outro lado, se k é um Ω -fecho real de L , seja ψ o gerador de $G(\Omega|k)$; ψ é

uma involução de $G(\Omega|L)$ e $G(\Omega|L) = \langle \psi \rangle \cdot U$. Então, $\psi = \sigma_u$ para algum $u \in U$ e, daí, todos os Ω -fechos reais de L são da forma Ω^{σ_u} . Portanto, L é de fato a interseção de todos seus Ω -fechos reais.

4) $\Rightarrow$ 1). Seja L um corpo intermediário formalmente real de $\Omega|K$. Por hipótese L é a interseção de seus Ω -fechos reais que são Euclidianos. Então, L é pitagórico. Portanto, K é h.p relativamente a Ω . Assim, a demonstração está concluída.

4. CARACTERIZAÇÃO DE CORPOS HEREDITARIAMENTE EUCLIDEANOS.

Vamos, neste parágrafo, enunciar e demonstrar o resultado principal sobre corpos h.e que necessitamos no Capítulo IV. Da dos os resultados sobre corpos h.p, anteriormente desenvolvidos, este teorema não passa de uma simples formalidade.

4.1. TEOREMA. (Geyer e Prestel-Ziegler). Se K é um corpo intermediário formalmente real, da extensão Galoísiana 2-fechada $\Omega|K$, então as seguintes afirmações são equivalentes:

- 1) K é h.e relativamente a Ω .
- 2) $G(\Omega|K_2)$ é abeliano e $K_2 = K(i)$.
- 3) $[\Omega : K] = 2 \cdot n$ onde n é um número supernatural ímpar.
- 4) Se E é um corpo intermediário formalmente real K , então $[E : K]$ é ímpar.
- 5) Se E é um corpo intermediário de $\Omega|K(i)$, então, $E(i)$ é quadraticamente fechado.

6) Se F é um corpo intermediário formalmente real de $\Omega|K$, então F tem única ordem.

7) Se $f(X) \in K[X]$ é irredutível e R é um Ω -fecho real de K , então f tem no máximo uma única raiz em R .

DEMONSTRAÇÃO. 1) $\Rightarrow$ 2). Segue de (3.11) ao se notar que $K_2 = K(i)$.

2) $\Rightarrow$ 3). K é Euclideano e, por (3.11), é também h.p relativamente a Ω . Então, por (3.9), $[\Omega : K]$ é ímpar.

3) $\Leftrightarrow$ 4). $\Rightarrow$). Claro $\Leftarrow$). Basta pegar um Ω -fecho real R de K e observar que $\Omega = R(i)$ ((1.4)) e que $[R : K]$ é ímpar.

3) $\Leftrightarrow$ 5). $\Rightarrow$). Seja E um corpo intermediário de $\Omega|K(i)$. Se $E(i)$ não for quadraticamente fechado, então 4 divide $[\Omega : K]$ - uma contradição.

$\Leftarrow$). Seja R um Ω -fecho real de K . Vamos mostrar que $[R : K]$ é ímpar. Se isto não ocorre, então existe um corpo intermediário F de $R|K$ tal que $[F : K]$ é finito e par. Seja E a menor extensão Galoisiana de $K(i)$ contendo $F(i)$ e contida em Ω e consideremos σ como sendo um elemento de ordem 2 de $G(E|K(i))$. Então, $[E : E^\sigma] = 2$ e, como $E^\sigma = E^\sigma(i)$, isto contraria 5).

3) $\Rightarrow$ 6). Seja F um corpo intermediário formalmente real de $\Omega|K$. Se F tiver mais de uma ordem, então existe $a \in F$ tal que $\sqrt{a} \notin F$ e $F(\sqrt{a})$ é formalmente real. Daí, 4 divide $[\Omega : K]$ - uma contradição.

6) $\Rightarrow$ 7). Seja $f(X) \in K[X]$ irredutível e suponhamos que f possua duas raízes α e β em um Ω -fecho real R de K . Então, existe

um K -isomorfismo $\sigma : K(\alpha) \longrightarrow K(\beta)$ tal que $\sigma(\alpha) = \beta$. Como $K(\alpha)$ e $K(\beta)$ possuem únicas ordens, σ é um K -isomorfismo de ordem. Assim, σ estende-se a um K -isomorfismo de ordem $\tilde{\sigma}$ dos fechos reais de $K(\alpha)$ e $K(\beta)$, respectivamente. Agora, $K(\alpha)$ e $K(\beta)$ possuem um mesmo fecho real $\tilde{R}$ de R em um fecho algébrico de R . Logo, σ é o único K -automorfismo de ordem de $\tilde{R}$, ou seja, $\sigma = \text{identidade}$. Assim, $\tilde{\sigma}(\alpha) = \sigma(\alpha) = \alpha = \beta$.

7) $\Rightarrow$ 1). Seja F um corpo intermediário formalmente real de $\Omega|K$. Se F não for um corpo euclideano, então existe $\alpha \in F$ positivo em alguma ordem $\leq$ de F tal que $\alpha \notin F^2$. Então, $F(\sqrt{\alpha})$ é um corpo formalmente real e $x^2 - \alpha$ é um polinômio irreduzível sobre K . Seja R um Ω -fecho real de $(F, \leq)$. Então $\sqrt{\alpha}$ e $-\sqrt{\alpha} \in R$ - uma contradição.

5. EXEMPLOS

Neste parágrafo vamos dar alguns exemplos de corpos hereditariamente pitagóreanos e de corpos h.e. Iniciamos a discussão com alguns exemplos clássicos.

5.1. EXEMPLO. Sejam R um corpo real fechado e $R((X))$ o corpo das séries formais a uma indeterminada. Então, $R((X))$ é um corpo hereditariamente pitagórico relativamente a seu fecho algébrico Ω .

DEMONSTRAÇÃO. R é de característica 0 e, se $k = R((X))$, então $k(\sqrt{-1}) = C((X))$, onde C é um fecho algébrico de R . É um fato bem

conhecido que $\text{Gal}(\Omega | C((X)))$ é pró-cíclico isomorfo a $\hat{\mathbb{Z}} = \varprojlim \frac{\mathbb{Z}}{n\mathbb{Z}}$ (Ver Serre, Local Fields, Springer-Verlag, New York etc., 1979, p. 69). Assim, decorre pelo Teorema (3.1) que $R((X))$ é h.p relativo a Ω . Note-se, que $R((X))$ não é h.e, já que ele possui duas ordens (I.3.8).

5.2. EXEMPLO. Se k é um corpo h.p, relativo a Ω , então existe uma extensão $K|k$ em Ω tal que K é h.e relativo a Ω . (K pode ser real fechado).

DEMONSTRAÇÃO. Seja $G = \text{Gal}(\Omega | k(\sqrt{-1}))$. Então, G é abeliano e daí existe uma decomposição de G na forma $G = H_2 \times H$ onde H_2 é o 2-Sylow subgrupo de G e H é de ordem ímpar (Ver Geyer [11], Satz 1.13, p. 351). Ora, seja F o corpo fixo por H . Se $\text{Gal}(\Omega | k)$ é gerado por G e uma involução σ , então, pelo Lema (3.3), $\sigma\tau = \tau^{-1}$ para todo $\tau \in G$. Assim, $\sigma\tau\sigma = \tau^{-1}$ para todo $\tau \in H$ e, se indicamos $\text{Fix } \sigma$ por R , então, $K = F \cap R$ é gerado por H e σ com $\sigma\tau\sigma = \tau^{-1}$ para todo $\tau \in H$. Portanto, H é um subgrupo normal do grupo $\text{Gal}(\Omega | K)$. Logo, $\text{Gal}(\Omega | K) = H \cup \sigma H$, donde $[F : K] = 2$. Como $\sqrt{-1} \in F$ e $[K(\sqrt{-1}) : K] = 2$ decorre que $F = K(\sqrt{-1})$. Portanto, $\text{Gal}(\Omega | K(\sqrt{-1})) = H$ é um grupo abeliano de ordem ímpar e daí H é h.e.

5.3. EXEMPLO. Seja $k = R((X))$ e $K = \bigcup_{n \geq 0} k(X^{\frac{1}{2^n}}) = \bigcup_{n \geq 0} k((X^{\frac{1}{2^n}}))$. Então k é um corpo h.e relativamente ao seu fecho algébrico Ω .

DEMONSTRAÇÃO. Se $C = k(\sqrt{-1})$, então $k(\sqrt{-1}) = C((X))$. Observe que no Exemplo (5.2), o corpo F é o fecho quadrático de $k(\sqrt{-1})$ em Ω . Ora, sabe-se que para todo número natural n , existe uma única extensão de $C((X))$ de grau n dada por $C((X^{\frac{1}{n}})) = C((X))(X^{\frac{1}{n}})$, onde $C((X^{\frac{1}{n}}))$ denota o corpo de séries formais em $X^{\frac{1}{n}}$ com coeficientes sobre C . Portanto, o fecho quadrático de $k(\sqrt{-1}) = F = \bigcup_{n \geq 0} C((X^{\frac{1}{2^n}}))$ e daí, $K = \bigcup_{n \geq 0} k((X^{\frac{1}{2^n}}))$ é h.e.

Vamos agora procurar dar alguns exemplos de corpos (infinitos) de números algébricos. Para tal, precisamos dos seguintes resultados.

5.4. TEOREMA. (Becker-Bröcker). Seja k um corpo h.p relativo a Ω e suponhamos que k tenha um número finito de ordens. Então, o número de ordens de k é igual a 2^t onde $|\frac{k^*}{k \cdot 2}| = 2^{t+1}$.

DEMONSTRAÇÃO. Referimo-nos ao Teorema 18, p. 122 e a observação que segue na p. 124 de Becker [3].

5.5. TEOREMA. (Geyer). Seja k um corpo formalmente real. Então, as seguintes condições são equivalentes.

1) k é interseção de dois fechos reais de k no seu fecho algébrico.

2) k é h.p e $\text{Gal}(\Omega|k(\sqrt{-1}))$ é cíclico.

3) $\text{Gal}(\Omega|k)$ é um grupo diédrico; isto é, $\text{Gal}(\Omega|k)$ é gerado (topologicamente) por dois elementos σ e τ onde σ é uma involução, τ é de ordem infinita e $\sigma\tau\sigma = \tau^{-1}$.

DEMONSTRAÇÃO. 1) $\Rightarrow$ 3). Seja $k = R_1 \cap R_2$ e sejam σ_1 e σ_2 as involuções que definem R_1 e R_2 . Seja $\tau = \sigma_1\sigma_2$. Então, τ fixa $\sqrt{-1}$. $k = R_1 \cap R_2$ é o corpo fixo por σ_1 e σ_2 ou seja, por τ e σ_1 . Mais ainda, $\sigma_1\tau\sigma_1 = \sigma_1(\sigma_1\sigma_2)\sigma_1 = \sigma_2\sigma_1 = (\sigma_1\sigma_2)^{-1} = \tau^{-1}$. Portanto, o grupo $\text{Gal}(\Omega|k)$ é diédrico.

3) $\Rightarrow$ 2). Observe que se H é o fecho do grupo gerado por τ , então, $\text{Gal}(\Omega|k) = H \cup \sigma H$, e todo elemento de H é uma involução. Logo, $\text{Gal}(\Omega|k(\sqrt{-1})) \subseteq H$, onde Ω é um fecho algébrico de k . Mas, $\text{Gal}(\Omega|k(\sqrt{-1}))$ é de índice 2 em $\text{Gal}(\Omega|k)$. Logo, $\text{Gal}(\Omega|k(\sqrt{-1})) = H$ é cíclico. Daí, resulta 2.

2) $\Rightarrow$ 1). Se $\text{Gal}(\Omega|k(\sqrt{-1}))$ é gerado por τ , e σ é uma involução de $\text{Gal}(\Omega|k)$, então σ e $\sigma\tau$ são duas involuções e daí, $k = \text{Fix}(\sigma, \tau) = \text{Fix}(\sigma, \sigma\tau) = \text{Fix}(\sigma) \cap \text{Fix}(\sigma\tau) = R_1 \cap R_2$, onde R_1 e R_2 são dois fechos reais de k .

Daremos agora um exemplo bem concreto de um corpo de números reais que é h.e.

5.6. EXEMPLO. Sejam R o fecho algébrico do corpo $\mathbb{Q}$ dos números racionais e k um subgrupo de R maximal em relação a exclusão de $\sqrt[3]{2}$ (dentro de R). Então, k é h.e.

DEMONSTRAÇÃO. Por causa de maximalidade k é Euclideano e $|\frac{k'}{k^2}| = 2$. Seja $\alpha = \sqrt[3]{2}$, ω uma raiz terceira primitiva da unidade e $\beta = \omega\alpha$.

Então, $k(\alpha)$ e $k(\beta)$ são corpos ordenados. Seja R_1 um fecho algébrico de $k(\beta)$. Então, $R \cap R_1$ contém k , não pode conter α e é um corpo formalmente real, pois $\omega \notin R_1$. Logo, $k = R_1 \cap R_2$ e k é h.p, (Teorema (3.11)) ou (5.5). Ora, $|\frac{k^*}{k \cdot 2}| = 2$ implica que $k(\sqrt{-1})$ é quadraticamente fechado. Como $\Omega|k(\sqrt{-1})$ é abeliano, isto implica que $\Omega : k(\sqrt{-1})$ é ímpar. Logo, k é h.e.

Os resultados de Geyer e Becker-Bröcker são citados na seguinte proposição.

5.7. PROPOSIÇÃO. *Se k é um corpo de números algébricos h.p relativamente ao fecho algébrico de $\mathbb{Q}$, então k é interseção de dois fechos reais de k . k tem no máximo duas ordens e, k é h.e. se, e somente se k possui uma única ordem.*

DEMONSTRAÇÃO. Um resultado de Geyer que usa a teoria local de corpos de classes (Satz 2.3, p. 357 de [11]), afirma que qualquer subgrupo abeliano de $\text{Gal}(\Omega|\mathbb{Q})$ é cíclico (pró). Assim, em nosso caso $\text{Gal}(\Omega|k(\sqrt{-1}))$ é cíclico. Pelo Teorema 5.5, k é interseção de dois fechos reais de k . Para concluir, observamos que $k(\sqrt{-1})$ possui no máximo uma única extensão quadrática, pois o fecho quadrático de $k(\sqrt{-1})$ é uma extensão (pró)-cíclica de $k(\sqrt{-1})$. Assim, se $F = k(\sqrt{-1})$, então $(F^*/_{F \cdot 2}) \leq 2$ e daí, $|\frac{k^*}{k \cdot 2}| \leq 4$. Pelo Teorema 5.4, o número de ordens de k é no máximo 2. A última afirmativa é clara.

CAPÍTULO IV

CORPOS COM A PROPRIEDADE DE MUDANÇA DE SINAL

Neste capítulo vamos dar uma bela aplicação da teoria de valorizações compatíveis com ordens desenvolvidos no Capítulo I. Um dos resultados básicos da teoria de corpos formalmente reais, afirma que, um polinômio irredutível, sobre um corpo ordenado (K, K_+) , que muda de sinal em K , possui raízes no fecho real de (K, K_+) . Por outro lado, conforme o exemplo (1.2) a recíproca deste resultado não é verdadeira: mais precisamente, se α é um elemento de um fecho real de K , então não é necessário que o polinômio mínimo de α sobre K mude de sinal sobre K .

Neste capítulo, estudaremos tal recíproca, e para isto introduziremos a definição de corpos com a propriedade de mudança de sinal. O ponto culminante do capítulo é o Teorema (2.4), devido a Viswanathan, que caracteriza tais corpos como sendo hereditariamente Euclidianos ou densos em seus respectivos fechos reais.

Fixados um corpo ordenado não arquimediano (K, K_+) e uma valorização ω de K compatível com K_+ , vamos estudar no primeiro parágrafo, condições necessárias do grupo de valores de ω e, no segundo condições necessárias sobre o corpo residual de ω , para que K tenha a propriedade de mudança de sinal.

1. GRUPO DE VALORES E POLINÔMIOS DEFINIDOS.

A proposição abaixo, é um dos resultados fundamentais da teoria de corpos formalmente reais.

1.1. PROPOSIÇÃO. Sejam (K, K_+) um corpo ordenado, e $f(X) \in K[X]$ um polinômio irredutível. Se existem elementos $a, b \in K$ tais que $f(a) \cdot f(b) \notin K_+$, então f possui raízes no fecho real $\tilde{K}$ de (K, K_+) .

Por outro lado, como mostra o exemplo abaixo, a recíproca deste resultado não é verdadeira.

1.2. EXEMPLO. (Bourbaki [6], pag.61, ex. 26). No corpo $K = \mathbb{Q}(X)$, consideremos a ordem lexicográfica. Seja $f(Y) = (Y^2 - X) \cdot (Y^2 - 4X) - 1 = Y^4 - 5XY^2 + 4X^2 - 1 \in \mathbb{Q}(X)[Y]$. Então:

- a) f é irredutível sobre K
- b) f admite raiz no fecho real $\tilde{K}$ de K
- c) $f(\alpha) > 0$, $\forall \alpha \in K$.

De fato: a) As raízes de $f(Y)$ em um fecho algébrico $\bar{K}$ de K são

$\pm \left(\frac{5X \pm \sqrt{9X^2 + 4}}{2} \right)^{1/2}$; $9X^2 + 4$ não é quadrado em K e, desde que, $2, 5X \in K$ concluímos que $f(Y)$ não tem raízes em K . Logo, $f(Y)$ é um polinômio irredutível sobre K .

b) X é positivo em K . Então $\sqrt{X} \in \tilde{K}$, isto é, X é quadrado em $\tilde{K}$. Como $f(\sqrt{X}) = -1$ é negativo e $f(0) = 4X^2 - 1$ é positivo, f muda de sinal em $\tilde{K}$. Assim, por (1.1), f tem raízes em $\tilde{K}$.

c) Sejam $h(X), g(X) \in \mathbb{Q}[X]$, elementos quaisquer com $g(X) \neq 0$, grau $h = n \geq 0$, grau $g = m \geq 0$ e colocamos $\beta = f(h(X)/g(X)) = \frac{(h(X))^4 - 5X(h(X)g(X))^2 + (g(X))^4(4X^2 - 1)}{g(X)^4}$. O único elemento que pode tornar β negativo em K é $-5X(h(X)g(X))^2$ que tem grau $2(n+m)+1$. Temos dois casos:

1º) Se $n \leq m$, então, $2(n+m) + 1 \leq 4m + 1 < 4m + 2 =$ o grau do polinômio $(g(X))^4(4X^2-1)$ que tem coeficiente líder positivo.

2º) Se $0 \leq m < n$, então, $2(n+m) + 1 = 2n + 2m + 1 < 4n =$ o grau de $(h(X))^4$ que tem coeficiente líder positivo.

Daí, concluímos que $\beta > 0$, ou seja, $f(\alpha) > 0$ para todo $\alpha \in K$.

1.3. A partir de agora, salvo menção contrária, assumiremos que (K, K_+) é um corpo ordenado não arquimediano e fixaremos um fecho real $\tilde{K}$ de K . Neste caso, por (II.1.13a) existe uma valorização não trivial ω de K compatível com K_+ . Denotaremos o grupo de valores de tal valorização ω por H e o corpo residual por K_ω . $(K_\omega)_+$ denotará a ordem em K_ω induzida por K_+ . $((K_\omega))_+ = \{b + M_\omega \mid b \in U_\omega \cap K_+ \} \cup \{M_\omega\}$.

1.4. DEFINIÇÃO. Diz-se que um polinômio $f(X) \in K[X]$ é definido sobre K , se $f(a) \in K_+$ para todo $a \in K$. Quando $f(X)$ muda de sinal sobre K , isto é, existem $a, b \in K$ tais que $f(a) \cdot f(b) \notin K_+$, diz-se que $f(X)$ é indefinido sobre K .

Vamos agora, estudar a recíproca da Proposição (1.1). Para isto, daremos a seguinte definição:

1.5. DEFINIÇÃO. Diz-se que o corpo ordenado (K, K_+) tem a *propriedade de mudança de sinal* se, para todo elemento α do fecho real $\tilde{K}$ de K , o polinômio minimal de α sobre K é *índefinido* sobre K .

A proposição abaixo estabelece uma condição suficiente, sobre o grupo de valores H , para a existência de polinômios definidos e irreduzíveis sobre K tendo raízes no fecho real $\tilde{K}$ de K .

1.6. PROPOSIÇÃO. Se $|H/2H| \geq 2$, então existe um polinômio definido e *irreduzível* sobre K , tendo raízes em $\tilde{K}$.

DEMONSTRAÇÃO. Seja $h \in H$ tal que $h < 0$ e h não 2-divisível. Escolhamos $s \in K_+$, tal que $\omega(s) = h$ e seja α o único elemento positivo de $\tilde{K}$ tal que $s = \alpha^4$. Colocando $\beta = \alpha^2$, temos que $s = \beta^2$.

Vamos verificar que $[K(\alpha) : K] = 4$. Para isto, seja $f(X) = X^4 - s \in K[X]$. As raízes de f em $\tilde{K}(i)$ são $\pm\alpha$ e $\pm i\alpha$ e todas estão fora de K , pois, se $\alpha \in K$, então $h = \omega(s) = \omega(\alpha^4) = 2\omega(\alpha^2)$ donde, h é 2-divisível - uma contradição. Como $i\alpha \notin \tilde{K}$ também, $-i\alpha \notin K$ e $i\alpha \notin K$. Assim f não tem raiz em K . Como $\alpha^2 \notin K$ pois, caso contrário, $\omega(\alpha^2) \in H$ e $h = 2\omega(\alpha^2)$, concluímos, então, que f é irreduzível sobre K . Portanto, de fato, $[K(\alpha) : K] = 4$.

Seja $\delta_1 = \beta + \alpha$. Desde que os K -conjugados de α em $\tilde{K}(i)$ são $\alpha, -\alpha, i\alpha$ e $-i\alpha$, concluímos que os K -conjugados de δ_1 em $\tilde{K}(i)$ são $\delta_1, \delta_2 = \beta - \alpha, -\beta + i\alpha$ e $-\beta - i\alpha$. Estes são todos distintos, portanto δ_1 é também um elemento primitivo de $K(\alpha)$ sobre K , isto é, $K(\alpha) = K(\delta_1)$. O polinômio minimal $h(X)$ de δ_1 sobre K , tem somente duas raízes em $\tilde{K}$, a saber δ_1 e δ_2 . Seja $\tilde{\omega}$ a única extensão

de ω a $\tilde{K}$ compatível com $\tilde{K}_+$. Desde que $h = \omega(\alpha^4) = 4\omega(\alpha) < 0$, temos que $\tilde{\omega}(\alpha) < 0$, assim $\tilde{\omega}(\beta) = 2\tilde{\omega}(\alpha) < \tilde{\omega}(\alpha)$. Logo, $\tilde{\omega}(\beta \pm \alpha) = \tilde{\omega}(\beta) = 2\tilde{\omega}(\alpha) = \frac{h}{2} \notin H$. Como $\beta \in \tilde{K}_+$ e $\tilde{\omega}(\beta) < \tilde{\omega}(\pm\alpha)$, pela compatibilidade de $\tilde{\omega}$ com $\tilde{K}_+$, concluimos que, $\delta_1, \delta_2 \in \tilde{K}_+$.

Mostraremos agora, que $h(X)$ é o polinômio requerido. Conforme já mostramos $h(X)$ é irredutível sobre K e tem raiz em $\tilde{K}$. Resta mostrar que h é definido sobre K . Se $b \in K_+$ é tal que $0 < \delta_2 \leq b \leq \delta_1$, então, pela compatibilidade de $\tilde{\omega}$, $\frac{h}{2} = \tilde{\omega}(\delta_1) \leq \tilde{\omega}(b) = \omega(b) = \omega(b) \leq \tilde{\omega}(\delta_2) = \frac{h}{2}$, donde, $h = 2\omega(b)$ - uma contradição. Portanto, $[\delta_2, \delta_1] \cap K = \emptyset$. Sobre $\tilde{K}$, $h(X) = (X^2 + cX + d)(X - \delta_1)(X - \delta_2)$, onde $h_1(X) = X^2 + cX + d$ tem coeficiente líder positivo e não tem raiz em $\tilde{K}$. Assim, $h_1(X)$ é definido sobre K . Como já mostramos que, se $b \in K$, então $b > \delta_2$ e $b > \delta_1$ ou $b < \delta_2$ e $b < \delta_1$, concluimos que, $h(X)$ é definido sobre K .

O próximo resultado, sobre divisibilidade, será usado na demonstração da Proposição (1.8).

1.7. LEMA. *Sejam p um número primo, $h \in H$ um elemento não p -divisível e, $L|K$ uma extensão finita de corpos. Se ω_1 é uma extensão de ω , a uma valorização de L , e $G \supset H$ é o grupo de valores de ω , então, existe um inteiro positivo r tal que h não é p^r -divisível em G .*

DEMONSTRAÇÃO. Desde que 0 é p -divisível, temos que $h \neq 0$. Suponhamos que h seja p^r -divisível em G , para todo $r \geq 1$. Neste caso, para cada $i = 1, 2, \dots$ seja $g_i \in G$ tal que $h = p^i g_i$. Se

$g_i = g_j$ com $i \geq j$, então, $p^i g_i = p^j g_j = p^j g_i$, donde $p^j(g_i - p^{i-j} g_i) = 0$. Como G é livre de torção, segue que, $g_i = p^{i-j} g_i$, donde $i = j$. Assim, os g_i 's são dois a dois distintos.

Desde que $L|K$ é uma extensão finita, G/H é um grupo finito e assim existem inteiros λ, μ com $1 \leq \lambda < \mu$ tais que $g_\mu - g_\lambda \in H$. Logo, se colocarmos $h' = g_\mu - g_\lambda$ obtemos $p^\mu h' = p^\mu g_\mu - p^\mu g_\lambda$, donde, $h = p^\mu g_\mu = p^\mu h' + p^\mu g_\lambda = p^{\mu-\lambda}(p^\lambda g_\lambda - p^\lambda h') = p^{\mu-\lambda}(h + p^\lambda h') = p(p^{\mu-\lambda-1}(h + p^\lambda h')) = p.h''$, onde $h'' = p^{\mu-\lambda-1}(h + p^\lambda h') \in H$. Dessa forma, h é p -divisível - uma contradição.

O próximo resultado estabelece uma primeira conexão entre corpos hereditariamente Euclidianos e corpos com a propriedade de mudança de sinal.

1.8. PROPOSIÇÃO. Se H não for p -divisível para algum primo ímpar p e (K, K_+) não for hereditariamente Euclidiano, então, existe um polinômio irredutível definido sobre K , tendo raízes em $\tilde{K}$.

DEMONSTRAÇÃO. Desde que (K, K_+) não é hereditariamente Euclidiano, existe uma extensão ordenada finita (L, L_+) de (K, K_+) não Euclidiana. Podemos supor, $L = K(s)$ onde $s \in L_+$, $\sqrt{s} \notin L$ e $L \subset \tilde{K}$.

Seja B o fecho integral de A_ω em $K(s)$. Desde que o corpo de frações de B é o fecho algébrico de K em $K(s)$ e $K(s)|K$ é extensão algébrica, segue que $K(s)$ é o corpo de frações de B . Daí, se todo elemento positivo de B for quadrado em $K(s)$, o próprio $K(s)$ seria Euclidiano. Dessa forma, existe $t \in B_+$, tal que $\sqrt{t} \notin K(s)$.

Considereemos, então, $L = K(t)$ como subcorpo ordenado de $\tilde{K}$ onde $t \in L_+ = L \cap \tilde{K}_+$, $\sqrt{t} \notin L$ e t é integral sobre A_ω .

Desde que H não é p -divisível, seja $h \in H$, $h < 0$ e h não p -divisível e seja $y \in \tilde{K}_+$ tal que $\omega(y) = h$. Pelo Lema (1.7) existe um inteiro $r \geq 1$ tal que h não é p^r -divisível em $G = \tilde{\omega}(L)$, onde $\tilde{\omega}$ é a única valorização de K_ω , compatível com $\tilde{K}_+$, que estende ω . O polinômio $X^{p^r} - y \in K[X]$ tem única raiz em $\tilde{K}$, isto porque p^r é ímpar e ainda deste fato, se α é tal raiz, então $\alpha > 0$ em $\tilde{K}$. Desde que $h = \omega(y) = \tilde{\omega}(\alpha^{p^r}) = p^r \tilde{\omega}(\alpha)$ e h não é p^r -divisível em $\tilde{V}(L)$, temos que $\alpha \notin L$. Assim, $L(\alpha)|L$ é uma extensão própria. Do fato de $X^{p^r} - y$ ter somente α como raiz em $\tilde{K}$, concluimos que também o polinômio minimal de α sobre L tem somente α como raiz em $\tilde{K}$, assim, o grau n de α sobre L é também ímpar.

Lembrando que, $\sqrt{t} \notin L = K(t)$, temos $[L(\sqrt{t}) : L] = 2$ e considerando $F = L(\alpha, \sqrt{t}) = K(t)(\sqrt{t}, \alpha) = K(\sqrt{t}, \alpha)$, temos $[F : L] = 2n$, isto porque, 2 e n são primos entre si. Até agora, temos o seguinte diagrama de extensões de corpos.

$$\begin{array}{ccc}
 & F = L(\alpha, \sqrt{t}) = K(\alpha, \sqrt{t}) & \\
 & \swarrow \quad \searrow & \\
 L(\alpha) & & L(\sqrt{t}) \\
 \swarrow \quad \searrow & & \swarrow \quad \searrow \\
 & n \quad 2 & \\
 & L = K(t) & \\
 & | & \\
 & K &
 \end{array}$$

Podemos observar claramente que, pela construção do corpo L , $L|K$ é uma extensão finita. Então, $F|K$ também o é, e assim, se considerarmos a família $\{K(\alpha + n\sqrt{t})\}_{n \geq 1}$ de corpos intermediários entre K e F , devem existir inteiros c, d com $c > d \geq 1$ tais que $K(\alpha + c\sqrt{t}) = K(\alpha + d\sqrt{t}) = E$ (digamos). Desde que $(c - d)\sqrt{t} = (\alpha + c\sqrt{t}) - (\alpha + d\sqrt{t}) \in E$, tiramos que, $\sqrt{t}$, e logo α , estão em E . Portanto, $E = K(\alpha, \sqrt{t}) = F$, isto é, $\delta = \alpha + c\sqrt{t}$ é um elemento primitivo de F sobre K .

Vamos agora, analisar os K -monomorfismos σ de F em $\tilde{K}$. Um tal σ deve levar α em α e t em um elemento $\sigma(t)$ tal que $\sigma(t) = \sigma(\sqrt{t}^2) = (\sigma(\sqrt{t}))^2$ é raiz positiva, em $\tilde{K}$, do polinômio minimal de t sobre K . Desde que $\sigma|_K = \text{id}$, segue que $\tilde{\omega} \circ \sigma$ é uma valorização de F que estende ω . Pela escolha de t , t é integral sobre A_ω , então, $t \in I_F(A_\omega) \subset A_{\tilde{\omega} \circ \sigma}$, onde $I_F(A_\omega)$ é o fecho integral de A_ω em F , que é a intersecção de todos os anéis de valorização de F que estendem A_ω . Então, $(\tilde{\omega} \circ \sigma)(t) \geq 0$ e daí $\tilde{\omega}(\sigma(t)) = \tilde{\omega}(\sigma(\sqrt{t})^2) = 2\omega(\sigma(\sqrt{t})) \Rightarrow \tilde{\omega}(\sigma(\sqrt{t})) = \frac{(\tilde{\omega} \circ \sigma)(t)}{2} \geq 0$. Por outro lado, $\tilde{\omega}(\alpha) = \frac{h}{p^r} < 0$, então $(\tilde{\omega} \circ \sigma)(\delta) = (\tilde{\omega} \circ \sigma)(\alpha + c\sqrt{t}) = \tilde{\omega}(\alpha + c\sigma(\sqrt{t})) = \tilde{\omega}(\alpha) = \frac{h}{p^r}$ pois $\tilde{\omega}(c\sigma(\sqrt{t})) = \tilde{\omega}(c) + \tilde{\omega}(\sigma(\sqrt{t})) = 0 + \tilde{\omega}(\sigma(\sqrt{t})) \geq 0$.

Se $f(X)$ é o polinômio minimal de δ sobre K , então $f(X)$ é de grau par (ver diagrama) e daí, $f(X)$ possui somente um número par de raízes em $\tilde{K}$, digamos, $\delta_1 < \delta_2 < \dots < \delta_{2\mu}$. Desde que $\alpha > 0$ e $\tilde{\omega}(\alpha) < \tilde{\omega}(\pm c\sigma(\sqrt{t}))$ para qualquer K -monomorfismo σ de F em $\tilde{K}$, concluimos, pela compatibilidade de $\tilde{\omega}$ com $\tilde{K}_+$, que $\alpha \geq \pm c(\sqrt{t}) = \sigma(c\sqrt{t})$ donde, $\sigma(\alpha \pm (\sqrt{t})) = \sigma(\delta) \geq 0$. Assim, os conjugados δ_i de

δ de $\tilde{K}$ são todos positivos em $\tilde{K}$. O intervalo $[\delta_1, \delta_{2\mu}]$ de $\tilde{K}$ é disjunto de K pois, se $z \in K$ é tal que $0 < \delta_1 \leq z \leq \delta_{2\mu}$, então, $\frac{h}{p^r} = \tilde{\omega}(\delta_{2\mu}) \leq \tilde{\omega}(z) \leq \tilde{\omega}(\delta_1) = \frac{h}{p^r}$, donde, h é p^r -divisível em H - uma contradição.

Sobre $\tilde{K}$, $f(X) = (X-\delta_1)(X-\delta_2) \dots (X-\delta_{2\mu})f_1(X)$, onde $f_1(X)$ não tem raiz em $\tilde{K}$ e tem coeficiente líder positivo. Então, $f_1(a) > 0$ para todo $a \in K$ e, para todo $a \in K$ temos que $a > \delta_i$, $i = 1, \dots, 2\mu$ ou $a < \delta_i$, $i = 1, \dots, 2\mu$. Portanto, $f(a) > 0$, $\forall a \in K$ e assim, $f(X)$ é um polinômio procurado.

1.9. OBSERVAÇÃO. Lembremo-nos de que, se um grupo H for p -divisível para todo primo p , então, H é divisível. Isto pode ser visto da seguinte maneira. Se $h \in H$ e r é um inteiro positivo, seja $r = p_1 p_2 \dots p_s$ a decomposição de r em fatores primos, onde os p_i 's não precisam ser distintos. Existe $h_1 \in H$ tal que $h = p_1 h_1$. Existe $h_2 \in H$ tal que $h_1 = p_2 h_2$ e assim, por recorrência finita, se $h_i = p_{i+1} h_{i+1}$ existe $h_{i+2} \in H$ tal que $h_{i+1} = p_{i+2} h_{i+2}$, $i = 1, \dots, s-1$. Então, $h = (p_1 p_2 \dots p_s) h_s = r h_s$.

O resultado seguinte estabelece uma condição, sobre o grupo de valores, para que um corpo com a propriedade de mudança de sinal seja hereditariamente Euclideano.

1.10. TEOREMA. Sejam (K, K_+) um corpo ordenado não arquimediano, ω uma valorização não trivial de K , compatível com K_+ e H o grupo de valores de ω . Se H não é divisível e K tem a propriedade de

mudança de sinal, então K é hereditariamente Euclídeano.

DEMONSTRAÇÃO. Desde que K possui a propriedade de mudança de sinal, pela Proposição (1.6), H é 2-divisível. Agora, H não é divisível, então, por (1.9), existe um primo ímpar p tal que H não é p -divisível. Então, pela Proposição (1.8), (K, K_+) é hereditariamente Euclídeano.

2. CORPOS RESIDUAIS E POLINÔMIOS DEFINIDOS.

No parágrafo 1 foram construídos polinômios definidos irreduzíveis sobre K , usando-se propriedades do grupo de valores. Neste parágrafo, continuando com tal estudo, serão obtidas condições suficientes para a existência de tais polinômios, usando-se propriedades do corpo residual. Como consequência desse estudo, seguirá uma caracterização de corpos com a propriedade de mudança de sinal.

Neste parágrafo, continuaremos com as hipóteses e notações fixadas em (1.3).

Para a Proposição (2.2), necessitamos do seguinte resultado básico, a respeito de corpos formalmente reais.

2.1. Seja $s \in K_+$ tal que $s \notin K^2$. Se $\alpha \in K$ é tal que $\alpha^4 = s$; então $[K(\alpha) : K] = 4$. Mais ainda, se $x \in K_+^*$; então $K(\alpha) = K(\alpha^2 + x\alpha)$ e os K -conjugados de $\alpha^2 + x\alpha$ em $\tilde{K}$ são $\delta_1 = \alpha^2 + x\alpha$ e $\delta_2 = \alpha^2 - x\alpha$.

DEMONSTRAÇÃO. α e $\alpha^2 \notin K$ pois, caso contrário, $s = (\alpha^2)^2 \in K^2$. Como $i\alpha \notin K$, segue também que $i\alpha \notin K$. Assim, o polinômio $X^4 - \alpha^4$ não tem raízes em K . Por outro lado, $X^4 - \alpha^4 = (X^2 - \alpha^2)(X + \alpha^2) \notin K[X]$, então, $X^4 - s$ é irreduzível sobre K e assim $[K(\alpha) : K] = 4$.

Para a segunda afirmação, notemos que existem quatro K -monomorfismos de $K(\alpha)$ em $\tilde{K}(i)$, a saber, $\alpha \rightarrow \alpha$, $\alpha \rightarrow -\alpha$, $\alpha \rightarrow i\alpha$ e $\alpha \rightarrow -i\alpha$. Assim, os K -conjugados de $\alpha^2 + \alpha x$ em $\tilde{K}(i)$ são $\alpha^2 + \alpha x$, $\alpha^2 - \alpha x$, $-\alpha^2 + i\alpha x$ e $-\alpha^2 - i\alpha x$. Tais conjugados são dois a dois distintos, então, $[K(\alpha^2 + \alpha x) : K] = 4$. Como $K(\alpha^2 + \alpha x) \subset K(\alpha)$ segue, então, que $K(\alpha) = K(\alpha^2 + \alpha x)$.

2.2. PROPOSIÇÃO. Sejam (K, K_+) um corpo ordenado não arquimediano e ω , H , H_ω , $(K_\omega)_+$ como em (1.3). Se o corpo residual K_ω não for Euclidiano, com respeito a ordem $(K_\omega)_+$, então existe um polinômio definido irreduzível sobre K tendo raízes em $\tilde{K}$.

DEMONSTRAÇÃO. Seja $\bar{s} = s + M_\omega \in (K_\omega)_+$ um elemento positivo que não é quadrado em K_ω . Então, $s \in U_\omega \cap K_+$ e claramente $s \notin K^2$. Sejam, α o único elemento positivo de $\tilde{K}$ tal que $\alpha^4 = s$ e x um elemento positivo de K tal que $\omega(x) > 0$. Com tais escolhas, por (2.1) $[K(\alpha) : K] = 4$, $K(\alpha^2 + \alpha x) = K(\alpha)$ e os K -conjugados de $\alpha^2 + x$ são $\delta_1 = \alpha^2 + \alpha x$ e $\delta_2 = \alpha^2 - \alpha x$. Assim, se $f(X)$ é o polinômio minimal de δ_1 sobre K , então, δ_1 e δ_2 são suas únicas raízes em $\tilde{K}$.

Seja $\tilde{\omega}$ a única valorização de $\tilde{K}$ compatível com $\tilde{K}_+$ estendendo ω . Então, $\tilde{\omega}(\delta x) = \tilde{\omega}(\alpha) + \tilde{\omega}(x) = \omega(x) > 0$ e, dessa forma, $\tilde{\omega}(\delta_1) = \tilde{\omega}(\alpha^2 + \alpha x) = \tilde{\omega}(\alpha^2) = 0$. Similarmente, $\tilde{\omega}(\delta_2) = 0$. Pela

compatibilidade de $\tilde{\omega}$ com $\tilde{K}_+$, $0 < \alpha x < \alpha^2$, donde $\alpha^2 + \alpha x = \delta_1 > \alpha^2 - \alpha x = \delta_2 > 0$, (em $\tilde{K}$).

Se $a \in K \cap [\delta_2, \delta_1]$, isto é, $\delta_2 \leq a \leq \delta_1$, então, $0 = \tilde{\omega}(\delta_1) \leq \tilde{\omega}(a) \leq \tilde{\omega}(\delta_2) = 0$, donde $a \in U_\omega \in K_+$. Passando para o corpo residual $\tilde{K}_\omega$ (via $\bar{a}$) com a ordem $(\tilde{K}_\omega)_+$ induzida por $\tilde{K}_+$, obtemos $\alpha^2 = \delta_2 \leq \bar{a} \leq \delta_1 = \alpha^2$, donde $\bar{a} = \alpha^2 \pmod{M_\omega}$. Assim, $\bar{a}^2 = \alpha^2 \pmod{M_\omega} = \bar{s}$, contrariando o fato de $\bar{s}$ não ser quadrado em K_ω . Portanto, $K \cap [\delta_2, \delta_1] = \emptyset$.

Sobre $\tilde{K}$, $f(X) = f_1(X)(X - \delta_2)(X - \delta_1)$, onde $f(X)$ é mônico e irredutível sobre $\tilde{K}$ de grau 2, então, $f_1(a) > 0$, $\forall a \in K$ e como $K \cap [\delta_2, \delta_1] = \emptyset$, concluimos, então, que $f(a) > 0$, $a \in K$. Assim, f é um polinômio procurado.

2.3. LEMA. Sejam ω uma valorização não trivial de K , $\bar{K}$ o fecho algébrico de K e $\alpha \in \bar{K}^*$. Consideremos uma extensão $\bar{\omega}$ de ω a $\bar{K}$ e $L = K(\alpha)$. Então, existe $\beta \in L$ tal que $K(\alpha) = K(\beta)$, onde β é integral sobre A_ω e $\bar{\omega}(\sigma(\beta)) > 0$ para todo K -conjugado $\sigma(\beta)$ de β em K .

DEMONSTRAÇÃO. Desde que $L|K$ é extensão finita, existem, somente, um número finito de extensões de ω a L , digamos, $v_1 \neq v_2, \dots, v_r$. Para cada i , o grupo quociente $v_i(L^*)/\omega(K^*)$ é finito, donde, para cada i , $1 \leq i \leq r$, existe um inteiro positivo n_i e um elemento $a_i \in K^*$, tal que $\omega(a_i) = v_i(a_i) = n_i v_i(\alpha)$. Desse modo, se $v_i(\alpha) \geq 0$, para algum i , então $\omega(a_i) \geq v_i(\alpha)$, se $v_i(\alpha) < 0$, para algum i , então, $\omega(a_i) < v_i(\alpha)$, donde $\omega(a_i^{-1}) > v_i(\alpha)$.

Logo, existe $b \in K^*$ tal que $\omega(b) \geq v_i(\alpha)$, $\forall i = 1, 2, \dots, r$ e assim, se colocarmos $\beta' = b\alpha^{-1}$, teremos que $\beta' \in A_{v_i}$, para $1 \leq i \leq r$. Desse modo, β' é integral sobre A_ω , e claramente, $K(\alpha) = K(\beta')$.

Seja agora σ um K -isomorfismo qualquer de $K(\beta')$ em $\bar{K}$. Então, $\{\sigma(A_{v_i})\}_{1 \leq i \leq r}$ é a família de todos os anéis de valorização de $K(\sigma(\beta'))$ que estendem A_ω e como $\beta' \in A_{v_i}$, $1 \leq i \leq r$, concluímos que $\sigma(\beta')$ é integral sobre A_ω . Assim, $\sigma(\beta')$ está no fecho integral de A_ω em $\bar{K}$, e portanto, $\bar{\omega}(\sigma(\beta')) \geq 0$ para K -conjugado de $\sigma(\beta')$ de β' em $\bar{K}$. Para concluir, seja $x \in K^*$ tal que $\omega(x) > 0$. Então, $\bar{\omega}(\sigma(x\beta')) > 0$ e $K(\beta') = K(x\beta')$; e assim, $\beta = x\beta'$ é um elemento requerido.

2.4. PROPOSIÇÃO. Sejam (K, K_+) um corpo ordenado não arquimédiano e $\omega, H, K_\omega, \tilde{K}, (K_\omega)_+$, como em (1.3). Se (K, K_+) não for hereditariamente Euclidiano e se o corpo residual K_ω tiver uma extensão não trivial de grau ímpar, então, existe um polinômio definido irreduzível sobre K , tendo raízes no fecho real $\tilde{K}$ de (K, K_+) .

DEMONSTRAÇÃO. Sejam, $\bar{K} = \tilde{K}(i)$ o fecho algébrico de K , $\tilde{\omega}$ a única valorização de $\tilde{K}$ compatível com $\tilde{K}$ estendendo ω e $\bar{\omega}$ a única extensão de $\tilde{\omega}$ a $\bar{K}$, (II.2.6). Seja $G(X)$ um polinômio mônico e irreduzível de $K_\omega[X]$ com grau ímpar, $n > 1$ e $g(X) \in A_\omega[X]$ de grau n e mônico tal que $\overline{g(X)} = G(X)$. Seja $g(X) = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$ a fatorização de $g(X)$ em $\bar{K}[X]$. Desde que $g(X) \in A_\omega[X] \subset A_{\bar{\omega}}[X]$ e os α_i 's estão em $\bar{K}$, concluímos que $\alpha_i \in A_{\bar{\omega}}$, $1 \leq i \leq n$. Passando

BC/4831

para o corpo residual $\bar{K}_\omega$, obtemos $G(X) = (X - \bar{\alpha}_1)(X - \bar{\alpha}_2) \dots (X - \bar{\alpha}_n)$, $(\bar{\alpha}_i = \alpha_i + M_\omega^-)$. Agora, $G(X)$ não tem raízes repetidas, pois K_ω tem característica 0, então $\alpha_i \in U_\omega^-$, $1 \leq i \leq n$, e $\alpha_i \neq \alpha_j$ se $1 \leq i \neq j \leq n$.

Assumamos que $K_\omega \subset \tilde{K}_\omega \subset \bar{K}_\omega$ da maneira natural. Sejam $\alpha_1, \alpha_2, \dots, \alpha_s$ as raízes de $g(X)$ em $\tilde{K}$ (note que s é obrigatoriamente ímpar e que $s \geq 1$).

Vamos agora, usar a hipótese de (K, K_+) não ser hereditariamente Euclidiano. Com tal hipótese, pelo Teorema (III.4.1) existe uma extensão ordenada L , de (K, K_+) , de grau par. Temos que $L = K(v)$ para certo $v \in L$ e podemos supor $L \in \tilde{K}$. Daí, pelo Lema (2.3), existe $\beta \in L$ tal que $L = K(\beta)$, onde β é integral sobre A_ω e $\bar{\omega}(\sigma(\beta)) > 0$ para todo K -conjugado $\sigma(\beta)$ de β em $\bar{K}$. É lógico que podemos supor $\beta \in \tilde{K}_+^*$.

Seja α uma raiz, qualquer, de $g(X)$ em $\tilde{K}$, e consideremos o corpo $F = K(\alpha, \beta)$. F é uma extensão formalmente real finita de K . Assim, por um argumento similar ao usado na demonstração de (1.8) concluímos que existe um inteiro $c \geq 1$ tal que $F = K(\delta)$, onde $\delta = \alpha + c\beta$. Dessa forma, os K -conjugados de δ em $\tilde{K}$, são obtidos a partir dos α e β . Sejam $\beta_1, \dots, \beta_t$ os K -conjugados de β em $\tilde{K}$ e consideremos dois índices fixos i, j tais que $1 \leq i \neq j \leq s$; conforme observamos anteriormente $\alpha_i \neq \alpha_j$. Além disso, se $\alpha_i < \alpha_j$, então $\alpha_i + c\beta_\lambda < \alpha_j + c\beta_\mu$ para todos inteiros λ, μ com $1 \leq \lambda, \mu \leq t$. Para ver isso, observemos que $0 < \alpha_j - \alpha_i$ e desde que $\bar{\alpha}_i \neq \bar{\alpha}_j$, $\alpha_j - \alpha_i \in U_\omega^-$. Pela escolha de β , $\bar{\omega}(\beta_\mu) > 0$, $\mu = 1, \dots, t$. Então,

$0 = \tilde{\omega}(\alpha_j - \alpha_i) < \tilde{\omega}(c(\beta_\lambda - \beta_\mu))$, donde pela compatibilidade de $\tilde{\omega}$ com $\tilde{K}_+$, $c(\beta_\lambda - \beta_\mu) < \alpha_j - \alpha_i$, isto é, $\alpha_i + c\beta_\lambda < \alpha_j + c\beta_\mu$. Em particular, a família $\{\alpha_i + c\beta_\lambda\}$, $(1 \leq i \leq s, 1 \leq \lambda \leq t)$ contém s.t elementos distintos e é a família de K-conjugados de $\delta = \alpha + c\beta$ em $\tilde{K}$.

Se $f(X)$ é o polinômio minimal de δ sobre K , então, as raízes de $f(X)$ em $\tilde{K}$, podem ser agrupadas em s-intervalos da seguinte maneira: Primeiro, arranjamos os α_i 's e os β_j 's de tal maneira que $\alpha_1 > \alpha_2 > \dots > \alpha_s$ e $\beta_1 > \beta_2 > \dots > \beta_t$. Então, para certo r fixo entre 1 e s teremos, $\alpha_r + c\beta_t < \alpha_r + c\beta_{t-1} < \dots < \alpha_r + c\beta_1$. Se I_r é o intervalo $[\alpha_r + c\beta_t, \alpha_r + c\beta_1]$ de $\tilde{K}$, então, $I_r \cap K = \emptyset$ para $1 \leq r \leq s$, de fato: se $a \in K \cap I_r$ para certo r , então, pela convexidade de A_ω , concluímos que $a \in A_\omega$ e assim, podemos passar para o corpo residual K_ω , onde obteremos $\overline{\alpha_r + c\beta_t} \leq \overline{a} \leq \overline{\alpha_r + c\beta_1}$. Assim, $\overline{a} = \overline{\alpha_r}$, pois $\tilde{\omega}(c\beta_1) > 0$, $1 \leq i \leq t$ e daí, $\overline{a}$ é a raiz de $G(X)$ em K_ω - uma contradição. Portanto, $I_r \cap K = \emptyset$, $1 \leq r \leq s$.

Relembrando que $K(\beta)|K$ é extensão com grau par, e que $\alpha_i + c\beta_\lambda$, $1 \leq i \leq s$ e $1 \leq \lambda \leq t$ são os K-conjugados de δ em K , temos que t é par. Logo, em cada intervalo I_r , $f(X)$ tem um número par raízes. Se colocarmos $d_{i\lambda} = \alpha_i + c\beta_\lambda$, $1 \leq i \leq s$, $1 \leq \lambda \leq t$, então; sobre $\tilde{K}[X]$, $f(X) = \prod_{i=1}^s \prod_{\lambda=0}^{t-1} (X - d_{i(t-\lambda)}) f_1(X)$, onde

$f_1(X)$ é definido sobre $\tilde{K}$ e, portanto, sobre K . Como $I_r = [c_{r,t}, c_{r,1}] \cap K = \emptyset$, $1 \leq r \leq s$, $d_{r,1} < d_{\mu,t}$ se $1 \leq r < \mu \leq s$ e cada I_r contém um número par de raízes de $f(X)$, concluímos, então, que

$f(X)$ é um polinômio requerido.

O próximo resultado é uma caracterização de corpos que tem a propriedade de mudança de sinal.

2.4. TEOREMA. O corpo ordenado (K, K_+) tem a propriedade de mudança de sinal se, e somente se K é hereditariamente Euclídeano ou K é denso em seu fecho real.

DEMONSTRAÇÃO. $\Leftarrow$) Se (K, K_+) for hereditariamente Euclídeano, então, (III.4.1) garante que (K, K_+) não admite extensão algébrica ordenada de grau par. Daí, se $\alpha \in \tilde{K}$, o polinômio minimal de α , sobre K , tem grau ímpar. Portanto, ele muda de sinal em K .

Suponhamos agora, que K é denso em $\tilde{K}$: Seja $\alpha \in \tilde{K}$ e $f(X)$ seu polinômio minimal sobre K . Se $f(X)$ tem grau ímpar, tudo bem. Então, suponhamos que $f(X)$ tenha grau par. Neste caso, $f(X)$ tem um número par de raízes em $\tilde{K}$ e estas são duas a duas distintas. Suponhamos que $\alpha_1 < \alpha_2 < \dots < \alpha_{2r}$, ($r \geq 1$) sejam tais raízes. Daí, sobre $\tilde{K}[X]$

$$f(X) = (X - \alpha_1) \dots (X - \alpha_{2r}) f_1(X),$$

onde $f_1(X)$ é mônico e irredutível de grau par sobre $\tilde{K}$. Então, $f_1(a) > 0$, $\forall a \in K$. Usando agora o fato de K ser denso em $\tilde{K}$, concluímos que existe $a \in K$ tal que $\alpha_1 < a < \alpha_2$. Portanto, claramente, $f(a) < 0$ e assim, $f(X)$ muda de sinal sobre K .

$\Rightarrow$) Assumamos que (K, K_+) tem a propriedade de mudança de sinal e suponhamos que K não é hereditariamente Euclideano. Vamos mostrar que K é denso em $\tilde{K}$.

Se K_+ for uma ordem arquimediana, a conclusão segue por (II.2.1). Suponhamos, então, que K_+ não é arquimediana. Neste caso, pela Proposição (2.2) K_ω é Euclideano para toda valorização ω de K compatível com K_+ e pela Proposição (2.4) K_ω não admite extensão, não trivial, de grau ímpar. Assim, K_ω é real fechado para toda valorização ω compatível com K_+ . Agora, pelo Teorema (1.10), o grupo de valores de qualquer valorização de K compatível com K_+ é divisível, então, pelo Teorema (II.2.5) K é denso em $\tilde{K}$. Isto mostra o Teorema.

CAPÍTULO V

UM TEOREMA DE KAPLANSKY SOBRE CORPOS REAIS FECHADOS

Neste capítulo, trataremos de um aspecto diferente da teoria de valorizações. Veremos, como uma estrutura de corpo ordenado, se reflete na situação de corpos completos e completamentos de corpos valorizados.

Restringimo-nos a um corpo valorizado (K, v) de posto 1 e perguntamos:

- 1) Se K possui uma estrutura de corpo ordenado, é possível munir o completamento $\hat{K}$ de (K, v) com uma estrutura de corpo ordenado?
- 2) Se $(K, \leq)$ é um corpo real fechado, o que se pode dizer sobre o completamento $(\hat{K}, \hat{v})$ de (K, v) ?

A segunda pergunta é respondida por um teorema devido a Kaplansky (1947). Nossa prova deste teorema (Teorema (4)) é bem simplificada, via um resultado de Prestel (1976) e de um resultado sobre complementamento de um corpo valorizado algebricamente fechado. A segunda pergunta é o resultado (5).

1. PROPOSIÇÃO. (Continuidade de raízes). Sejam (K, v) um corpo valorizado com grupo de valores G_v e $f(X) = X^n + a_1 X^{n-1} + \dots + a_n \in K[X]$ um polinômio tendo n raízes distintas: $x_1, x_2, \dots, x_n$ em K . Sejam

$\gamma \in G_V$ suficientemente grande e $g(X) = X^n + b_1 X^{n-1} + \dots + b_n \in K[X]$ um polinômio tendo suas raízes em K , tal que

$$\tilde{v}(f(X) - g(X)) = \min_{1 \leq i \leq n} \{v(a_i - b_i)\} > \gamma.$$

Então, todas as raízes de $g(X)$ são distintas e mais ainda; para cada raiz y de g , existe exatamente uma raiz x_i de f tal que $v(y - x_i) > \max_{i \neq j} \{v(x_i - x_j)\}$.

DEMONSTRAÇÃO. Sejam $\alpha = \max_{i \neq j} \{v(x_i - x_j) \neq 0\}$, $\beta = \min_{1 \leq i \leq n} \{v(x_i)\}$ e fixemos $\gamma \in G_V$ com $\gamma > n\alpha - \min_{1 \leq i \leq n-1} \{(n-i)\beta\}$ e $\gamma > \max\{0, \beta, n\beta\}$

(note que $\beta \leq \alpha$).

Primeiramente, vamos mostrar, que se $z \in K$ é tal que $\beta \leq v(z - x_i) \leq \alpha$, $\forall i = 1, 2, \dots, n$, então $g(z) \neq 0$.

De fato; se z satisfaz tal condição, então, $v(f(z)) =$

$$= v\left(\sum_{i=1}^n (z - x_i)\right) = \sum_{i=1}^n v(z - x_i) \leq n\alpha. \text{ Do mesmo modo, se } h(X) = f(X) -$$

$$- g(X) \text{ e } \tilde{v}(f(X) - g(X)) > \gamma, \text{ então } v(h(z)) = v\left(\sum_{i=1}^n (a_i - b_i) z^{n-i}\right) \geq$$

$$\geq \min_{1 \leq i \leq n} \{v(a_i - b_i) + (n-i)v(z)\} \geq \gamma + \min_{1 \leq i \leq n} \{(n-i)v(z)\} \geq \gamma +$$

$$+ \min_{1 \leq i \leq n} \{(n-i)\beta\} > n\alpha, \text{ isto porque, se } \beta = v(x_j), \text{ então } v(z) =$$

$$= v(z - x_j + x_j) \geq \min\{v(x_j), v(z - x_j)\} = \beta.$$

Logo, se $\beta \leq v(z - x_i) \leq \alpha$, $\forall i = 1, 2, \dots, n$ e $g(z) = 0$, então $h(z) = f(z)$. Dai, usando as desigualdades $v(f(z)) \leq n\alpha$ e

$v(h(z)) > n(\alpha)$, obtidas acima temos: $n\alpha < v(f(z)) \leq n\alpha$ o que é um absurdo. Assim, se $z \in K$ é tal que $\beta \leq v(z-x_i) \leq \alpha$, $\forall i=1, 2, \dots, n$, então $g(z) \neq 0$.

Vamos agora mostrar que, se existir um índice i tal que $v(z-x_i) < \beta \leq v(x_i)$, então da mesma forma, $g(z) \neq 0$.

De fato; se $z \in K$ satisfaz tal condição, então $v(z-x_i) \leq \beta \leq v(x_j)$, $\forall j = 1, 2, \dots, n$, donde $v(z) = v(z-x_i) < \beta \leq v(x_j)$, $\forall j = 1, 2, \dots, n$ e assim $v(z) = v(z-x_j)$ $\forall j = 1, 2, \dots, n$. Logo,

$$v(f(z)) = v\left(\prod_{i=1}^n (z-x_i)\right) = \sum_{i=1}^n v(z-x_i) = nv(z).$$

Da escolha de γ temos dois casos:

1º CASO. Se $v(z) \geq 0$, então $\gamma + \min_{1 \leq i \leq n} \{(n-i)v(z)\} = \gamma > n\beta > nv(z)$, pois $\beta > v(z)$.

2º CASO. Se $v(z) < 0$, então $\gamma + \min_{1 \leq i \leq n} \{(n-i)v(z)\} =$
 $= \gamma + (n-1)v(z) > \beta + nv(z) - v(z) > \beta + nv(z) - \beta = nv(z).$

Portanto, $v(h(z)) \geq \gamma + \min_{1 \leq i \leq n} \{(n-i)v(z)\} > nv(z) = v(f(z))$; isto mostra que $g(z) \neq 0$.

Logo, segue das duas afirmações que mostramos que: se $y \in K$ é tal que $g(y) = 0$ deve existir um índice i tal que $v(y-x_i) > \alpha$. Para mostrar a unicidade de tal x_i , basta observar que, se $i \neq j$, então $v(y-x_j) = \min\{v(y-x_i), v(x_i-x_j)\} \leq \alpha$.

Para terminar, resta mostrar que g não possui raízes repetidas.

Se, por exemplo, tivermos $v(y-x_1) < \alpha$ para toda raiz y de g , então $g(X) = \prod_y (X-y)$ implicando em $v(g(x_1)) = \sum_y v(y-x_1) \leq n\alpha$.

Por outro lado, temos que $v(x_1-x_i) \geq \min\{v(x_1), v(x_i)\} \geq \min_{1 \leq j \leq n} \{v(x_j)\} = \beta$, $\forall i = 1, 2, \dots, n$. Daí, pelo mesmo argumento usado

na prova da primeira afirmação, segue que $v(g(x_1)) = v(g(x_1)) - f(x_1) = v(h(x_1)) > n\alpha$ - uma contradição. Isto mostra que g não possui raízes repetidas, pois f e g possuem grau n e f só possui raízes simples.

Para o resultado (3) necessitamos de um importante resultado, conhecido como Lema de Krasner. Vamos citá-lo sem fazer sua respectiva demonstração; a mesma pode ser encontrada em Artin [24] ou Endler [9].

2. LEMA. (Lema de Krasner). Sejam (K, v) um corpo valorizado henseliano e $\bar{v}$ um prolongamento de v ao fecho algébrico $\bar{K}$ de K . Além disso, sejam $x, y \in \bar{K}$ tais que $\bar{v}(y-x) > \max_{1 \leq i \leq n} \{v(x_i - x)\}$, onde

$x_1, x_2, \dots, x_n$ são os conjugados de x em $\bar{K}$ distintos de x . Então $K(x, y) \mid K(y)$ é uma extensão de corpos puramente inseparável, e se x é separável sobre K , então $K(x) \subset K(y)$.

3. TEOREMA. (Kurschák). Seja (K, v) um corpo valorizado e algebricamente fechado. Então, se v é de posto 1, o completamento

$(\hat{K}, \hat{v})$ de (K, v) é algebricamente fechado.

DEMONSTRAÇÃO. Seja $f(X) = X^n + a_1 X^{n-1} + \dots + a_n \in \hat{K}[X]$ um polinômio separável e mônico. Sejam $x_1, x_2, \dots, x_n$ as raízes distintas de f em um fecho algébrico $\bar{\hat{K}}$ de $\hat{K}$. O corpo valorizado $(\hat{K}, \hat{v})$ é henseliano, pois v é de posto 1; logo $\hat{v}$ admite um único prolongamento $\bar{\hat{v}}$. Denotemos tal prolongamento, por $\bar{\hat{v}}$. Observemos que, sendo prolongamentos de v , $\hat{v}$ e $\bar{\hat{v}}$ são ambas de posto 1.

Com referência a $(\bar{\hat{K}}, \bar{\hat{v}})$, escolhemos agora γ, α e β da maneira indicada na Proposição (1).

Do fato de K ser denso em $\hat{K}$, para cada i , existe $b_i \in K$ tal que $\hat{v}(b_i - a_i) > \gamma$. Consideremos o polinômio $g(X) = X^n + b_1 X^{n-1} + \dots + b_n \in K[X]$.

Dessa forma, se $y \in K \subset \bar{\hat{K}}$ é uma raiz de g , por (), existe exatamente uma raiz x_i de f tal que $\bar{\hat{v}}(y - x_i) > \alpha > \max_{i \neq j} \{\bar{\hat{v}}(x_i - x_j), 0\}$. Conforme já mencionamos, $(\hat{K}, \hat{v})$ é henseliano.

Então, pelo Lema de Krasner, $\hat{K}(x_i) \subset \hat{K}(y) = \hat{K}$, pois, conforme estamos supondo, K é algebricamente fechado. Daí, necessariamente f é de grau 1.

Suponhamos agora, que f seja mônico, irredutível e inseparável sobre $\hat{K}$. Então, por um resultado bem conhecido existe um polinômio $f_0 \in \hat{K}[X]$ tal que $f(X) = f_0(X^{p^r})$, onde p é a característica de $\hat{K}$, $r \geq 1$ é um inteiro e f_0 é um polinômio irredutível e separável sobre $\hat{K}$.

Daí, usando o caso anterior, concluímos que $\text{grau } f_0 = 1$.
Portanto, $f(X) = X^{p^r} - a$, onde $a \in \hat{K}$.

Existe uma sequência de Cauchy, (a_n) de elementos de K tal que $a = \lim a_n$ e, do fato de K ser algebricamente fechado, para todo $n \geq 1$, existe $b_n \in K$ tal que $b_n^{p^r} = a_n$. Temos $p^r v(b_n - b_m) = v((b_n - b_m)^{p^r}) = v(b_n^{p^r} - b_m^{p^r}) = v(a_n - a_m)$, $\forall m, n$. Assim, (b_n) também é uma sequência de Cauchy em K . Seja $b = \lim b_n \in K$. Então $b^{p^r} = \lim b_m^{p^r} = \lim a_n = a$, donde $f(X) = X^{p^r} - a = X^{p^r} - b^{p^r} = (X-b)^{p^r}$, com $r \geq 1$; mas pegamos inicialmente f irredutível; então isto é uma contradição. Assim $\hat{K}$ só admite polinômios irredutíveis de grau 1 e, portanto, $\hat{K}$ é algebricamente fechado.

4. TEOREMA (Kaplansky). Sejam K um corpo real fechado com cone positivo K_+ , v uma valorização de posto 1 de K e $(\hat{K}, \hat{v})$ o completamento de (K, v) . Então:

- 1) Se K_+ é compatível com v ; $\hat{K}$ é real fechado.
- 2) Se K_+ é não compatível com v ; $\hat{K}$ é algebricamente fechado.

DEMONSTRAÇÃO. (1) Se K_+ é compatível com v , então, por (I.2.6) G_v , o grupo de valores de v , é divisível e K_v , o corpo residual de v , é real fechado. Do fato de v ter posto 1, $(\hat{K}, \hat{v})$ é henseliano. $(\hat{K}, \hat{v})$ é também extensão imediata de (K, v) , então, novamente, por (I.2.6), $\hat{K}$ é real fechado.

(2) Suponhamos agora, que K_+ não seja compatível com v . Neste caso, consideramos a henselização $(\tilde{K}, \tilde{v})$ de (K, v) . Podemos supor que $(\tilde{K}, \tilde{v})$ está contido em $(\hat{K}, \hat{v})$, isto porque, conforme já mencionamos $(\hat{K}, \hat{v})$ é henseliano. Se $\tilde{K} = K$, por (I.2.3), K_+ é compatível com v . Assim, $\tilde{K} = K(i)$ é algebricamente fechado. K é denso no espaço topológico $(\tilde{K}, T_{\tilde{v}})$, pois $(\tilde{K}, T_{\tilde{v}})$ é subespaço topológico de $(\hat{K}, T_{\hat{v}})$. Logo, por (II.1.4), $(\tilde{K}, \tilde{v})$ e (K, v) possuem o mesmo completamento. Pelo Teorema (3) o completamento de $(\tilde{K}, \tilde{v})$ é algebricamente fechado; então, $\hat{K}$ é algebricamente fechado.

5. COROLÁRIO. *Seja (K, v) um corpo valorizado formalmente real de posto 1. Então, o completamento $(\hat{K}, \hat{v})$ tem uma estrutura de corpo ordenado se, e somente se existe uma ordem de K compatível com v .*

DEMONSTRAÇÃO. $\Rightarrow$) Desde que v tem posto 1 $(\hat{K}, \hat{v})$ é henseliano. Assim, se $\hat{K}_+$ é uma ordem de $\hat{K}$, por (I.2.4), $\hat{K}_+$ é compatível com $\hat{v}$. Logo, $\hat{K}_+ \cap K$ é uma ordem de K , compatível com v . $\Leftarrow$) Se K_+ é uma ordem de K compatível com v , então, por (I.1.19), v estende-se a uma única valorização real do fecho real $\tilde{K}$ de K . Daí, pelo Teorema (4), o completamento $\hat{\tilde{K}}$ de $(\tilde{K}, \tilde{v})$ é real fechado. Assim, o completamento de (K, v) é formalmente real.

6. PROPOSIÇÃO. *Sejam K um corpo real fechado com cone positivo K_+ e v uma valorização não trivial de K . Então, o corpo residual K_v , associado a v , é real fechado ou algebricamente fechado e o grupo de valores é divisível.*

DEMONSTRAÇÃO. Se K_+ for compatível com v , por (I.1.20), K_v é real fechado. Dessa forma, suponhamos que K_+ não é compatível com v e vamos mostrar que K_v é algebricamente fechado.

Seja $\tilde{v}$ uma extensão de v a $K(i)$, onde $i = \sqrt{-1}$. Neste caso, $\tilde{v}(i) = 0$ e assim, se $a, b \in K$, $\tilde{v}(a+bi) \geq \min\{v(a), v(b)\}$. Temos dois casos:

1º CASO. Existem elementos $a, b \in K$ tais que $\tilde{v}(a+bi) > \min\{v(a), v(b)\}$. Neste caso, $v(a) = v(b)$ e a, b são não nulos. Temos $v(a+bi) = \tilde{v}(b(ab^{-1}+i)) = v(b) + v(ab^{-1}+i) \geq 0$, pois $\tilde{v}(i) = \tilde{v}(ab^{-1}) = 0$; no entanto, se $v(ab^{-1}+i) = 0$, então $v(a+bi) = v(b)$ o que contraria a propriedade de a e b . Logo, $\tilde{v}(ab^{-1}+i) > 0$, donde $ab^{-1} + M_v = -i + M_v$. Assim, o monomorfismo canônico de K_v em $K(i)_{\tilde{v}}$ é sobrejetor e portanto, K_v é canonicamente isomorfo a $(K(i))_v$. $K(i)$ é algebricamente fechado, pois K é real fechado, logo, $(K(i))_{\tilde{v}}$ e portanto K_v são também algebricamente fechados.

2º CASO. $\tilde{v}(a+bi) = \min\{v(a), v(b)\}$, $\forall a, b \in K$. Neste caso, os corpos residuais K_v e $K(i)_{\tilde{v}}$ não são isomorfos, pois $\tilde{v}(i) = 0$ e, se existir $\alpha \in A_v$ tal que $\alpha + M_v = i + M_v$, então $\alpha - i \in M_v$, donde $0 = \min\{v(\alpha), v(i)\} = v(\alpha - i) > 0$ — um absurdo. Logo, $K(i)_{\tilde{v}}$ é isomorfo ao corpo $K_v(\bar{i})$, onde $\bar{i} = i + M_v$ e $\bar{i} \notin K_v$. Como $K(i)$ é algebricamente fechado, $K(i)_{\tilde{v}}$ também o é; assim, pelo teorema de Artin-Schreier, para corpos reais fechados, concluimos que o corpo residual K_v é real fechado. Daí, por (I.1.18), existe uma ordem de K compatível com v , o que é um absurdo, pois,

conforme estamos supondo K_+ , a única ordem de K , não é compatível com v .

Portanto, o 2º caso não se verifica e assim, K_v é algebricamente fechado.

7. COROLÁRIO. Sejam K um corpo real fechado com ordem arqui-médiana e v é uma valorização não trivial de K . Então o corpo residual K_v é algebricamente fechado.

Daremos agora alguns exemplos para a Proposição (6) e para o Teorema (4).

8. EXEMPLO. Seja $\mathbb{Q}$ o corpo dos números racionais e v_p uma valorização p -ádica de $\mathbb{Q}$. Então, as extensões de v_p ao corpo $\mathbb{R}$ dos números reais e ao fecho real $\tilde{\mathbb{Q}}$, de $\mathbb{Q}$, possuem corpos residuais algebricamente fechados.

9. EXEMPLO. Sejam $\mathbb{R}((X))$ o corpo das séries formais. Por (I.3.8) $\mathbb{R}((X))$ possui uma única valorização real ω e únicas ordens P_1 e P_2 que são compatíveis com ω , (em (I.3.8) ω , P_1 e P_2 são dados explicitamente). ω é uma extensão da valorização ∞ -ádica ω_∞ de $\mathbb{R}(X)$ e P_1 e P_2 são, respectivamente, extensões das ordens $P_1(\infty)$ e $P_2(\infty)$ de $\mathbb{R}(X)$ compatíveis com ω_∞ . Seja $a \in \mathbb{R}$ e consideremos a valorização $(X-a)$ -ádica v_a de $\mathbb{R}(X)$. v_a não é compatível com as ordens $P_1(\infty)$ e $P_2(\infty)$. Daí, se ω_a representa uma extensão de v_a a $\mathbb{R}((X))$, ω_a não é compatível com P_i , $i=1,2$. Denotemos por R o fecho real de $\mathbb{R}((X))$ com respeito à ordem P_1 . Denotemos por ω_a

(resp. ω) uma extensão de ω_a (resp. ω) a R . Então $R_{\tilde{\omega}}$ é real fechado e $R_{\tilde{\omega}_a}$ é algebricamente fechado. Também, por (4), o completamento de $(R, \tilde{\omega})$ é real fechado, enquanto que o de $(R, \tilde{\omega}_a)$ é algebricamente fechado.

BIBLIOGRAFIA

- [1] BANASCHEWSKI , B., Totalgeordment Moduln. Arch. Math. 7, (1957), 430-440.
- [2] BECKER, E., Euklidische Korper und euclidsche Hullen von Korpom. J. reine angew. Math. 268-269, (1974), 41-52.
- [3] BECKER, E., Hereditarily-Pithagoren fields and orderings of higher level, IMPA, Rio de Janeiro, (1978).
- [4] BIGARD. A.; KEINEL, K. e WOLFENSTEN, S., Lectures Notes in Mathematics, Groups et Anneaux Reticules, 608.
- [5] BOURBAKI, N., Algèbre Commutative, Chapitre 6, Paris, (1964).
- [6] BOURBAKI, N., Algèbre Chapitre 6 e 7, Paris, (1964).
- [7] BOURBAKI, N., Topologie Générale. Paris, (1971).
- [8] BRÖCKER, L., Characterization of fans and hereditarily pythagorean fields. Math. Z. (1976), 149-163.
- [9] ENDLER, O., Valuation Theory. Springer, Berlin-Heidelberg , New York, (1972).

- [10] ENGLER, A., Um estudo sobre dependência e composição de anéis de valorização, Tese de Doutorado, IMPA, (1976).
- [11] GEYER, W.D., Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist. J. Number Theory 1, (1969), 346-374.
- [12] JACOBSON, N., Lectures in Abstract Algebra, vol. III, (1964).
- [13] KAPLANSKY, I., Topological methods in valuation theory, Duke Math. J. 14, (1947), 527-541.
- [14] LAM, T.Y., The algebraic Theory Quadratic Forms. Benjamin , (1973).
- [15] LANG. S., The theory of real places, Annals of Math. 57, (1953), 378-391.
- [16] LANG, S., Algebra, Reading, (1965).
- [17] PRESTEL, A., Lectures on formally real fields, IMPA, Rio de Janeiro, (1972).
- [18] PRESTEL, A. and ZIEGLER, M., Erbsich Euklidische Körper, J. reine angew. Math. 274-275, (1975), 196-205.

- [19] RIBEMBOIM, P., Théorie des Valuations, Université de Montreal, (1968).
- [20] RIBEMBOIM, P., L'arithmétique des Corps, Paris, (1972).
- [21] RIBES, L., Introduction of profinite groups and cohomology , Queen's paper in pure and applied mathematics, 24, Kingston, Ontario, (1970).
- [22] VISWANATHAN, T.M., Hahn valuation and (locally) compact rings, J. Algebra 17, (1971), 94-109.
- [23] VISWANATHAN, T.M., Ordered field and sign-changing polynomials, J. reine angew. Math. 296, (1977).
- [24] ARTIN, E., Theory of Algebraic Numbers, Göttingen, 1963.