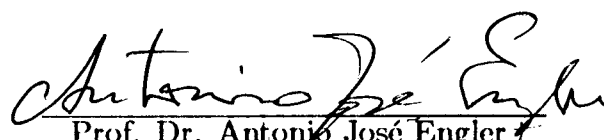


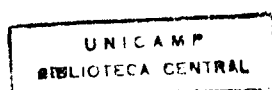
O SUBGRUPO NORMAL ABELIANO MÁXIMO DO PRO-2-GRUPO DE GALOIS

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pelo Sr. João Bosco Nogueira⁶² e aprovada pela Comissão Julgadora.

Campinas, 25 de janeiro de 1993


Prof. Dr. Antonio José Engler
(Orientador)

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para a obtenção do título de DOUTOR em Matemática.



ÍNDICE

Introdução	i
Capítulo I Valorizações	1
§1 Introdução	1
§2 Anéis de valorização 2-henselianos	2
§3 Anéis K^2 -compatíveis — elementos rígidos e básicos	13
Capítulo II Subgrupos Abelianos Máximos de Posto 1	21
§1 Introdução	21
§2 Subgrupos abelianos de posto 1	22
Capítulo III Subgrupos Abelianos de $G(K)$	35
§1 Introdução	35
§2 Subgrupos Abelianos Normais Máximos	36
§3 Subgrupos abelianos de $G(K)$	44
Referências	51

INTRODUÇÃO

Resumo. Neste trabalho mostramos que, para qualquer corpo K , existe um subgrupo abeliano normal máximo do grupo de Galois $G(K)$ de seu fecho quadrático, estabelecemos uma correspondência entre os subgrupos abelianos de $G(K)$ e subgrupos de K^* que contenham o subgrupo dos elementos básicos de K e também novas cotas para o posto máximo atingido pelos subgrupos abelianos de $G(K)$, ou seja, para o invariante $\alpha(K)$ definido por Ware em [W4].

1. Preliminares.

O objeto de estudos do presente trabalho é o grupo de Galois $G(K)$ dos K -automorfismos do fecho quadrático $K(2)$ de um corpo K , onde, salvo menção explícita em contrário, K tem característica diferente de 2. Se K é quadraticamente fechado ou então se K é um corpo real fechado, então $G(K)$ é trivial ou isomorfo a $\mathbb{Z}/2\mathbb{Z}$ respectivamente. Em qualquer outro caso $G(K)$ é um grupo infinito, cujo posto é $|K^*/K^2|$, onde K^* é o grupo multiplicativo de K e K^2 é o subgrupo dos quadrados não nulos de K . Se $G(K)$ é infinito mas $|K^*/K^2| = 2$, então $G(K)$ é isomorfo ao grupo aditivo dos inteiros 2-ádicos e podemos dizer que, ainda neste caso, a estrutura do grupo é simples. Se $|K^*/K^2| \geq 4$, a estrutura de $G(K)$ pode ser bastante complexa e seu estudo demanda essencialmente as técnicas da Cohomologia de Grupos, da Teoria de Formas Quadráticas e Teoria de Valorizações (ver por exemplo [EV] ou ([JW], pg. 393)). Para se fazer um estudo da estrutura de $G(K)$, nos casos mais complexos, é importante conhecer os seus subgrupos abelianos.

Para maior clareza e coerência de exposição, destacamos nesta introdução dois pará-

grafos, sendo que no primeiro deles fizemos uma breve análise de parte da literatura estudada, no que diz respeito às ligações dos temas citados com o presente trabalho, enquanto que no seguinte, procuramos dar uma descrição da maneira pela qual o trabalho se realizou e os principais resultados obtidos.

2. As origens.

Vários autores estudaram as ligações entre Teoria de Valorizações, Formas Quadráticas e Cohomologia de Grupos e as ligações destes temas com a Teoria de Galois. No parágrafo anterior ressaltamos a importância destes assuntos para a Teoria de Galois, no caso do fecho quadrático de um corpo K . Na verdade o emprego destas conexões não se restringe a este último caso. Só a título de exemplo, dado um corpo K de característica diferente de dois, se $\bar{K}$ é o fecho separável de K e $G = G(\bar{K}; K)$, o grupo de Galois de $\bar{K}|K$, Delzant estabelece em [D] uma conexão entre G e a Teoria das Formas Quadráticas sobre K , obtendo um isomorfismo natural entre os anéis de Witt-Grothendieck de G e de K .

No caso do fecho quadrático, se K for “C-corpo” ou de “classe C”, isto é, um corpo rígido (ver definição (I.3.1)) ou, equivalentemente, um corpo cujo anel de Witt $W(K)$ é isomorfo a um anel de grupo $\mathbb{Z}/n\mathbb{Z}[G]$ com $n \geq 0$, Ware mostra em [W] que o grupo de Galois $G(K)$ da extensão $K(2)|K$, onde K é um corpo com $|K^*/K^2| > 2$ que contém todas as raízes 2^n -ésimas de 1, é abeliano, relacionando assim uma estrutura intrínseca da Teoria de Formas Quadráticas com a estrutura de $G(K)$.

Esse tipo de conexão foi ainda estudado por Ware em [W1], [W5] e [W4]. Em [W1] por exemplo, partindo dos trabalhos de Delzant ([D]) e Scharlau ([Sch]), Ware obtém que, se -1 não for quadrado no corpo K , então a estrutura de $G(K)$ determina a do anel de Witt $W(K)$ e, além disso, se K e F são corpos com $G(K) \cong G(F)$ mas com anéis de Witt $W(K)$ e $W(F)$ não isomorfos, então -1 é um quadrado em um dos corpos e é soma de dois quadrados no outro e mostra, ainda nesse trabalho, que um corpo K é

“de classe C” se o grupo $G(K)$ é “quase abeliano”, isto é, existe uma seqüência exata de pro-2-grupos

$$1 \longrightarrow H \longrightarrow G(K) \longrightarrow G(K)/H \longrightarrow 1,$$

sendo H um subgrupo normal fechado de $G(K)$ e ambos, H e $G(K)/H$, forem abelianos (Ware usa o termo *metabeliano* para designar um grupo com esta propriedade). O “Theorem” 4.1 desse artigo estabelece uma equivalência entre o fato de K ser C-corpo e $G(L)$ ser abeliano, onde L é o corpo obtido de K por adjunção de todas as raízes 2^n -ésimas de 1, para $n \geq 1$ e o “Corollary 4.3” descreve as possibilidades para $G(K)$.

No emprego da Teoria de Valorizações, três “*ingredientes*” surgem naturalmente: Elementos Rígidos e Básicos, Anéis 2-henselianos e Anéis *Compatíveis*. Um elemento a do corpo K , $a \notin \pm K^2$ é rígido (o termo *elemento rígido* é de Szymiczek ([Szy])) se a forma quadrática $\langle 1, a \rangle$ só representa elementos de $K^2 \cup aK^2$, onde K^2 é o conjunto dos quadrados não nulos de K . Como observa Ware em [W2], geralmente associados aos elementos rígidos existem anéis de valorização A , com a propriedade de compatibilidade com os quadrados, de forma que os elementos cujos valores não sejam 2-divisíveis são rígidos e, num certo sentido, a “maioria” dos elementos rígidos ocorre assim. Para um anel de valorização A do corpo K , no caso de K ter característica diferente de 2, a compatibilidade mencionada se expressa por $1 + m_A \subseteq K^2$ (onde m_A é o ideal maximal de A), esse conceito é mais forte que 2-henseliano e nos será muito útil. Em [W2] é desenvolvida uma técnica de construção de anéis de valorização compatíveis, a partir de subgrupos de K^* que contenham o grupo dos elementos básicos. Um estudo mais completo dessa técnica é feito em [AEJ], onde os autores obtêm resultados fortes quanto à existência e classificação de anéis de valorização compatíveis que foram fundamentais para o nosso trabalho (para maiores detalhes reportamos o leitor ao §3 do capítulo I).

As principais fontes de consulta utilizadas foram, além dos artigos citados, os livros texto [E] e [Rib] para Teoria de Valorizações, [R] e [S] para grupos profinitos e Cohomologia de Grupos e [L1] para o estudo de Formas Quadráticas.

3. Desenvolvimento do trabalho.

Para nosso trabalho é relevante o fato de o grupo de ramificação de um anel de valorização não diádico ser trivial ([E], 20.18 pg.167) e assim o grupo de inércia ([E], pg. 146) é abeliano. Mostraremos que para a “maior parte” dos corpos o grupo de inércia de um anel de valorização conveniente é o maior subgrupo normal abeliano de $G(K)$.

A base de nossas investigações consistiu na obtenção de anéis de valorização compatíveis, não diádicos, “mínimos”, cujos grupos de inércia associados desempenhassem o papel de “delimitadores” de subgrupos abelianos de $G(K)$. Ele é, quase sempre, o maior subgrupo abeliano normal de $G(K)$. Para isso foi necessário, em primeiro lugar, uma investigação acurada dos anéis de valorização 2-henselianos de K , de forma análoga ao estudo feito em [EE], onde os autores classificam os anéis de valorização henselianos, quanto à ordem dada pela inclusão e a relação desta com a estrutura dos corpos de resíduos. Exemplificando: no nosso trabalho os anéis 2-henselianos cujos corpos de resíduos não sejam quadrático separavelmente fechado formam um conjunto totalmente ordenado pela inclusão, enquanto os que têm corpos de resíduos quadrático separavelmente fechado formam um conjunto dirigido segundo esta ordem (Proposição (I.2.15)). Embora os resultados de [EE] tenham um caráter mais geral, já que os resultados são válidos no fecho algébrico, foi necessário adaptá-los, pois a hipótese 2-henseliano é mais fraca que a hipótese henseliano.

O caso geral teve por base o “Theorem” 3.6 de [W4] (Teorema (III.2.1)): Se K é um corpo com mais de duas classes quadráticas então uma condição necessária e suficiente para que $G(K)$ seja abeliano é que o conjunto dos elementos básicos coincida com o conjunto dos quadrados não nulos de K e que todas as raízes 2^n -ésimas da unidade estejam em K . Usando a existência do anel de valorização “adequado” $\mathcal{O}$ dado por (I.3.7), concluímos que, no caso de K satisfazer as condições equivalentes acima, então $G(K)$ é isomorfo a $G^T(\tilde{\mathcal{O}}; K)$ ou a $G^T(\tilde{\mathcal{O}}; K) \times \mathbb{Z}_2$.

Se $G(K)$ possui um subgrupo abeliano normal de posto pelo menos dois, esse resultado mostra a existência de uma subextensão normal de $K(2)|K$ que possui um anel de valorização 2-henseliano próprio. Adaptando de maneira conveniente a técnica usada por Engler em [En], obtivemos um teorema de descida para anéis de valorização 2-henselianos que, no caso acima, nos permitiu deduzir a existência do anel 2-henseliano no próprio corpo K . Por outro lado, se os subgrupos normais abelianos de $G(K)$ têm posto um é possível descrever, através de geradores e relações, o grupo $G(K)$, caso $G(K)$ não seja abeliano, conforme estabelece o Teorema (II.2.4). Em dois dos três casos descritos pelo Teorema (II.2.4), precisamente naqueles em que K não é formalmente real, foi possível mostrar (Corolário (II.2.5)) que o maior subgrupo abeliano normal de $G(K)$ é o grupo de inércia associado a um anel não diádico.

Finalmente, como aplicação desses resultados, generalizamos resultados de Ware ([W], Theorems B, C) e estabelecemos uma correspondência entre os subgrupos abelianos de $G(K)$ e subgrupos de K^* que contenham o subgrupo dos elementos básicos de K . Obtivemos ainda novas cotas para o posto máximo atingido pelos subgrupos abelianos de $G(K)$, ou seja, para o invariante $a(K)$ (ver Definição (III.3.3)) definido por Ware em [W4].

CAPÍTULO I

VALORIZAÇÕES

1. Introdução.

Neste capítulo adaptamos, de maneira apropriada, alguns resultados de [En], [EE] e de [AEJ] para o estudo de anéis de valorização de um corpo, “*indecompostos*” no fecho quadrático desse corpo (ver [E], Chapter III, pg. 96). Esses anéis serão chamados 2-henselianos (ver Definição (I.2.1) abaixo) e algumas de suas propriedades serão estudadas no próximo parágrafo.

No parágrafo 3 estudamos os anéis de valorização “*compatíveis*” com os quadrados do corpo ou K^2 -compatíveis. Para anéis com corpo de resíduos de característica diferente de 2, as noções de K^2 -compatível e 2-henseliano são equivalentes. Por outro lado, se apenas a característica do corpo de frações do anel é diferente de 2, esses anéis são uma subclasse dos anéis 2-henselianos. De uma maneira geral eles são mais apropriados ao nosso trabalho. Os resultados sobre anéis K^2 -compatíveis decorrem de resultados extremamente fortes contidos em [AEJ] e são essenciais para o trabalho.

Ainda nesse parágrafo estudamos a existência de anéis K^2 -compatíveis em um corpo através do conjunto de seus elementos “*básicos*” (Teorema (I.3.6) e Proposição (I.3.8)).

Notações: Se A é um anel de valorização do corpo K , denotamos por A^* , m_A , $\mathcal{K}_A$ e Γ_A o grupo das unidades, o ideal maximal, o corpo de resíduos e o grupo de valores de A respectivamente. Também denotamos por v_A e ϕ_A a valorização e o *place* canônico respectivamente, associados a A . Se $c(\mathcal{K}_A) \neq 2$, diremos que A é não

diádico.

Denotaremos por K^2 o conjunto dos quadrados não nulos do corpo K . Dado o corpo K , se Ω é o fecho algébrico de K , então o fecho quadrático de K , denotado por $K(2)$, é a reunião de todas as extensões galoisianas de K , com grau potência de 2. $K(2)|K$ é uma extensão galoisiana e denotaremos por $G(K)$ o grupo de Galois $G(K(2); K)$.

2. Anéis de valorização 2-henselianos.

(I.2.1) Definição ([B], [Br]). Um anel de valorização A do corpo K é 2-henseliano se A admite uma única extensão a $K(2)$. Denotamos por $\tilde{A}$ a única extensão de A a $K(2)$ e por $\tilde{v}_A$ a única extensão de v_A a $K(2)$.

Para uma melhor compreensão dos anéis de valorização 2-henselianos, apresentamos uma caracterização desses anéis, devida a Bröcker.

(I.2.2) Proposição (Lema de Hensel [Br] (1.2)). Seja A um anel de valorização do corpo K . Então as seguintes afirmações são equivalentes:

- (a) A é 2-henseliano.
- (b) Para todo polinômio $f(X) \in A[X]$ de grau 2, tal que $\bar{f}(X)$ tenha 2 raízes distintas $\bar{a}$ e $\bar{b}$ em $\mathcal{K}_A$, existem x e y em A , raízes de $f(X)$, tais que $\bar{x} = \bar{a}$ e $\bar{y} = \bar{b}$. ■

Embora as demonstrações de (I.2.3), (I.2.4) e (I.2.5) sejam conhecidas em forma bem mais geral, vamos incluí-las para tornar o texto mais auto-suficiente e também pela

simplicidade das provas no presente caso.

Para cada $b \in K^*$ escolhemos, em $K(2)$, um elemento que denotamos por $b^{1/2}$, que satisfaz $(b^{1/2})^2 = b$.

(I.2.3) Lema (Krasner). *Seja K um corpo com $c(K) \neq 2$, A um anel de valorização 2-henseliano de K , $a \in K^*$ e $\alpha = \widetilde{v}_A(2a^{1/2})$. Se $c \in K^*$ e $\widetilde{v}_A(c^{1/2} - a^{1/2}) > \alpha$, então $K(a^{1/2}) \subseteq K(c^{1/2})$.*

PROVA. Se $a \in K^2$, então $K(a^{1/2}) = K$ e não há nada a provar. Seja $a \in K^* \setminus K^2$ e $\sigma \in \text{aut}(K(c^{1/2}, a^{1/2}); K(c^{1/2}))$. Logo,

$$\sigma(a^{1/2} - c^{1/2}) = \sigma(a^{1/2}) - c^{1/2}.$$

Como A é 2-henseliano, $\widetilde{v}_A \circ \sigma = \widetilde{v}_A$ ([Rib], Théorème 1, pg.166); assim

$$\begin{aligned} \widetilde{v}_A(\sigma(a^{1/2}) - c^{1/2}) &= \widetilde{v}_A(a^{1/2} - c^{1/2}) > \alpha. \\ \widetilde{v}_A(\sigma(a^{1/2}) - a^{1/2}) &= \widetilde{v}_A(\sigma(a^{1/2}) + c^{1/2} - c^{1/2} - (a^{1/2})) \\ &\geq \min\{\widetilde{v}_A(\sigma(a^{1/2}) - (c^{1/2})), \widetilde{v}_A((a^{1/2}) - c^{1/2})\} > \alpha. \end{aligned}$$

Mas $\sigma(a^{1/2}) = a^{1/2}$ ou $-a^{1/2}$. A segunda hipótese nos dá $\widetilde{v}_A(2a^{1/2}) > \alpha$, o que contradiz a escolha de α . Assim $a^{1/2} \in K(c^{1/2})$. ■

O lema a seguir é uma versão da “Proposition” 8 de ([Rib], pg. 195) para anéis 2-henselianos e polinômios de grau dois que acrescentamos para facilitar a leitura.

(I.2.4) Lema ([Rib] Proposition 8, pg. 195). *Sejam K um corpo e A um anel de valorização 2-henseliano de K . Sejam $f(X) = X^2 + a_1X + a_0$ e $g(X) = X^2 + b_1X +$*

b_0 polinômios separáveis de $K[X]$. Se $\gamma \in \Gamma_A$ é suficientemente grande e

$$v_A(f - g) = \min\{v_A(a_1 - b_1), v_A(a_0 - b_0)\} > \gamma,$$

então $f(X)$ é irredutível sobre K se e somente se $g(X)$ o for.

PROVA. Seja L o corpo de raízes do polinômio $f(X)g(X)$. Então $L|K$ é galoisiana finita e, como A é 2-henseliano, A admite um único prolongamento A' a L . Por ([Rib], Théorème 1, pg.166) se σ for um K -automorfismo de L , então $v_{A' \circ \sigma} = v_{A'}$.

Suponha que $f(X)$ tenha raízes x_1 e x_2 em K e seja $\alpha = v_A(x_1 - x_2)$. Sejam y_1 e y_2 as raízes de $g(X)$ em L . Pela propriedade da “continuidade das raízes” ([Rib], Proposition 7, pg. 191) podemos supor que y_1 e y_2 estão enumeradas de maneira que

$$v_{A'}(y_i - x_j) > \alpha \iff i = j, \quad i = 1, 2.$$

Temos então

$$v_{A'}(\sigma(y_i) - x_j) = v_{A'}(\sigma(y_i) - \sigma(x_j)) = v_{A' \circ \sigma}(y_i - x_j) = v_{A'}(y_i - x_j)$$

$\forall i, j = 1, 2$ e portanto y_1 e $y_2 \in K$ e isto encerra a prova. ■

(I.2.5) Corolário. *Todo corpo que contenha 2 anéis de valorização 2-henselianos independentes é quadrático separavelmente fechado.*

PROVA. Seja K um corpo, A e A' anéis de valorização 2-henselianos independentes de K .

1º Caso ($c(K) \neq 2$).

Seja $a \in K^*$, $\gamma > 0$ em Γ_A e $\gamma_1 > 0$ em $\Gamma_{A'}$, satisfazendo

$$\gamma > 2\widetilde{v}_A(2a^{1/2}) \text{ e } \gamma_1 > 2\widetilde{v}_{A'}(2) \geq 0.$$

Como A e A' são independentes existe, pelo Teorema da Aproximação ([E], 11.16, pg. 80), um elemento $d \in K^*$ tal que

$$v_A(d - a) > \gamma \text{ e } v_{A'}(d - 1) > \gamma_1.$$

Como $\gamma_1 > 0$, $v_{A'}(d) = v_{A'}(d - 1 + 1) = \min\{v_{A'}(d - 1), v_{A'}(1)\} = v_{A'}(1) = 0$. Como $(d^{1/2})^2 = d$, segue que $\widetilde{v}_{A'}(d^{1/2}) = 0$, o que implica $\widetilde{v}_{A'}(2d^{1/2}) = \widetilde{v}_{A'}(2) + \widetilde{v}_{A'}(d^{1/2}) = \widetilde{v}_{A'}(2)$. Assim, temos $\gamma_1 > 2\widetilde{v}_{A'}(2d^{1/2})$ que é a hipótese de (I.2.3).

Sejam v a extensão de v_A a $K(a^{1/2})$ e v' a extensão de $v_{A'}$ a $K(d^{1/2})$. Como $1 - d = (1 - d^{1/2})(d^{1/2} + 1)$, temos que

$$v'(1 - d) = v'(1 - d^{1/2}) + v'(d^{1/2} + 1).$$

Se σ for um K -automorfismo de $K(d^{1/2})$, $\sigma \neq id$, então $\sigma(d^{1/2}) = -d^{1/2}$, resultando

$$v'(1 - d^{1/2}) = v'(d^{1/2} + 1)$$

e finalmente $2v'(1 - d^{1/2}) = v'(1 - d) > \gamma_1 > 2v'(2) = 2\widetilde{v}_{A'}(2d^{1/2})$

o que, pelo Lema (I.2.3), implica $d^{1/2} \in K$. Como $a - d = (a^{1/2})^2 - d$, novamente $2v(a^{1/2} - d^{1/2}) = v(a - d) > \gamma > 2v(2a^{1/2})$. Assim, $a^{1/2} \in K$.

2º Caso ($c(K) = 2$).

Queremos mostrar que, se $f(X) = X^2 + X + c$ é um polinômio separável sobre K , então $f(X)$ se fatora em $K[X]$. Para cada $\gamma > 0$ em Γ_A e $\gamma_1 > 0$ em $\Gamma_{A'}$, existe, pelo Teorema da Aproximação, c_1 em K , tal que

$$v_A(c_1) > \gamma \text{ e } v_{A'}(c_1 - c) > \gamma_1.$$

Se γ e γ_1 forem suficientemente grandes, por (I.2.4) $f(X)$, $p(X) = X^2 + X + c_1$ e $q(X) = X^2 + X$ têm, em $K[X]$ o mesmo tipo de fatoração. Portanto f se fatora em K , como

desejado. ■

Neste ponto fazemos um estudo da situação oposta, isto é, dos anéis de valorização anti-2-henselianos, conforme a definição a seguir. Para isto necessitamos da definição de grupo e corpo de decomposição, conforme ([E], pg. 109-110), para o nosso caso. Se D é um anel de valorização de $K(2)$, então o grupo de decomposição de D sobre K é definido por

$$G^Z(D; K) = \{\sigma \in G(K) | \sigma(D) = D\}$$

e o corpo de decomposição de D sobre K , $K^Z(D; K)$, é o corpo fixo de $G^Z(D; K)$. $K^Z(D; K)$ é a 2-henselização de $A = D \cap K$, isto é, a menor subextensão L de $K(2)|K$ tal que o prolongamento $D \cap L$ de A a L é 2-henseliano.

Necessitamos também de um estudo dos grupos de inércia, conforme descrevemos a seguir. Seja D um anel de valorização de $K(2)$, onde K é um corpo. O grupo de inércia de D sobre K (cf. [E], pg.146) pode ser definido por

$$G^T(D; K) = \{\sigma \in G^Z(D; K) | \sigma x - x \in m_D, \forall x \in D\}$$

Se $A = D \cap K$ e

$$\zeta : G^Z(D; K) \longrightarrow G(\mathcal{K}_D; \mathcal{K}_A) = G(\mathcal{K}_A)$$

é o homomorfismo que satisfaz $\phi_D \circ \sigma = \zeta(\sigma) \circ \phi_D$, para todo $\sigma \in G^Z(D; K)$ então, conforme ([E], Theorem 19.1), o núcleo de ζ é exatamente $G^T(D; K)$.

Dado D , anel de valorização de $K(2)$, se $A = D \cap K$ e se $\bar{p}$ é o expoente característico do corpo de resíduos de A , isto é, $\bar{p} = 2$ se $c(\mathcal{K}_A) = 2$ e $\bar{p} = 1$ caso contrário, então existe um homomorfismo “natural” de $G^T(D; K)$ em um grupo de $\bar{p}$ -caracteres do grupo de torsão Γ_D/Γ_A , cujo núcleo é o grupo de ramificação de D sobre K , denotado por $G^V(D; K)$. A seguir faremos uma breve descrição da maneira pela qual esse grupo é construído.

Para cada $\sigma \in G(K)$, a aplicação $x \mapsto \frac{\sigma x}{x}$ é um endomorfismo de $K(2)^*$, cujo núcleo é K^* e temos que esta aplicação induz um homomorfismo de $K(2)^*/K^*$ em D^* , denotado por $\partial\sigma$, que satisfaz

$$\partial(\rho.\sigma) = \partial\rho.(\rho.\partial\sigma), \quad \text{para todos } \rho, \sigma \in G(K)$$

(ver [E], pgs. 157/8).

Por ([E], Theorem (20.5)), para todo $\sigma \in G^T(D; K)$ existe $\tilde{\sigma} \in \text{Hom}(\Gamma_D/\Gamma_A, \mathcal{K}_D)$ (= grupo de caracteres de Γ_D/Γ_A em $\mathcal{K}_D$) tal que o diagrama

$$\begin{array}{ccc} K(2)^*/K^* & \xrightarrow{\partial\sigma} & D^* \\ v_D^* \downarrow & & \downarrow \phi_D^* \\ \Gamma_D/\Gamma_A & \xrightarrow{\tilde{\sigma}} & \mathcal{K}_D \end{array}$$

é comutativo e $\sigma \mapsto \tilde{\sigma}$ é um homomorfismo contínuo

$$\Psi: G^T(D; K) \longrightarrow \text{Hom}(\Gamma_D/\Gamma_A, \mathcal{K}_D).$$

O núcleo de Ψ é precisamente $G^V(D; K)$. Por ([E], (20.18), pg. 167), $G^V(D; K)$ é o único $\bar{p}$ -Sylow subgrupo de $G^T(D; K)$. Em particular, se $\bar{p} = 1$ (por exemplo, se D não for diádico), então $G^V(D; K) = \{id\}$ e conseqüentemente $G^T(D; K)$ é isomorfo a um grupo de caracteres e portanto abeliano.

O corpo de ramificação de D sobre K é o copo fixo de $G^V(D; K)$ e é denotado por $K^V(D; K)$.

A demonstração do teorema (I.2.6) a seguir adota as mesmas linhas da demonstração do Theorem 2.2 de [En].

Como na literatura, se C e C' são subanéis de um anel A , o compósito de C e C' , denotado por $C.C'$ é o menor subanel de A que contem C e C' .

(I.2.6) Teorema. *Sejam K um corpo, C e C' anéis de valorização incomparáveis de $K(2)$ e $D = C.C'$. Então vale:*

$$G^Z(C; K) \cap G^Z(C'; K) = G^T(C; K) \cap G^T(C'; K) = G^T(D; K).$$

PROVA. C e $C' \not\subseteq D \implies G^T(D; K) \subseteq G^T(C; K) \cap G^T(C'; K) \subseteq G^Z(C; K) \cap G^Z(C'; K)$.
Seja E o corpo fixo da interseção $G^Z(C; K) \cap G^Z(C'; K)$, $A = C \cap E$ e $A' = C' \cap E$.
Se C e C' forem independentes, queremos mostrar que $G^Z(C; K) \cap G^Z(C'; K) = \{1\}$.
Da Teoria de Galois, temos que E contém os corpos de decomposição relativos a C e a C' ; logo, A e A' são 2-henselianos. Neste caso, como D é o único prolongamento de $A.A'$ a $K(2)$ e, como A e $A' \subseteq A.A'$, segue que C e $C' \subseteq D$. Portanto $D = K(2)$ e também $A.A' = E$. Assim, por (I.2.5), segue-se que $E = K(2)$, o que termina a prova.

Agora suponha $D = C.C' \neq K(2)$ e seja $B = D \cap E$.

Temos que $\phi_D(C) \cap \phi_D(C') = K_D$,

portanto, pelo caso anterior $G^Z(\phi_D(C); K_B) \cap G^Z(\phi_D(C'); K_B) = \{1\}$.

Mas $\zeta(G^Z(C; K)) \subseteq G^Z(\phi_D(C); K_B)$ e $\zeta(G^Z(C'; K)) \subseteq G^Z(\phi_D(C'); K_B)$.

Portanto temos que $\zeta(G^Z(C; K) \cap G^Z(C'; K)) = \{1\}$. Mas $G^T(D; K)$ é o núcleo de ζ , conforme observação anterior a (I.3.6), ou seja, $G^Z(C; K) \cap G^Z(C'; K) \subseteq G^T(D; K)$. ■

Uma consequência deste último teorema é o seguinte teorema de descida para anéis de valorização 2-henselianos.

(1.2.7) Teorema. *Seja $N|K$ uma extensão normal, com $N \subsetneq K(2)$. Suponha que exista em N um anel de valorização 2-henseliano próprio C tal que $C \cap K$ não seja 2-henseliano. Então existe D , um anel de valorização próprio de N , contendo C , tal que $D \cap K$ é 2-henseliano e $K^T(\tilde{D}; K) \subseteq N$. Além do mais, D pode ser escolhido mínimo no sentido de que $D \subseteq D'$, para todo anel de valorização D' de N tal que $C \subsetneq D'$ e $D' \cap K$ é 2-henseliano.*

PROVA. $G(N) = G(K(2); N) \subseteq G^Z(\tilde{C}; K)$. Se B é um prolongamento de $C \cap K$ a $K(2)$, então existe $\sigma \in G(K)$ tal que $B = \sigma\tilde{C}$ e portanto $G^Z(B; K) = \sigma G^Z(\tilde{C}; K)\sigma^{-1}$. Mas $G(N) \leq G(K)$ e obtemos que $G(N) \subseteq G^Z(B; K)$ também. Desta forma,

$$G(N) \subseteq G^Z(\tilde{C}; K) \cap G^Z(B; K) = G^T(\tilde{C} \cdot B; K),$$

pelo Teorema (1.2.6).

Seja β o conjunto de todos os prolongamentos de $C \cap K$ a $K(2)$ e tome $\tilde{D} = \bigcup \tilde{C} \cdot B$, para todo $B \in \beta$.

Como $\{\tilde{C} \cdot B : B \in \beta\}$ é uma família totalmente ordenada pela inclusão, pois todos esses anéis contêm $\tilde{C}$, temos que $\tilde{D} = \bigcup_{B \in \beta} \tilde{C} \cdot B$ é um anel de valorização de $K(2)$ com ideal maximal $m_D = \bigcap_{B \in \beta} m_{\tilde{C} \cdot B}$. Verifica-se, usando a definição de grupo de inércia (pg. 6) que $G^T(\tilde{D}; K) = \bigcap_{B \in \beta} G^T(\tilde{C} \cdot B; K)$. Segue-se então que $G(N) \subset G^T(\tilde{D}; K)$ e portanto $G^T(\tilde{D}; K) \neq \{1\}$. Logo $\tilde{D} \cap K$ é anel de valorização próprio de K . Por outro lado, $\tilde{D}$ contém todos os K -conjugados de C . Afirmamos que $D = \tilde{D} \cap K$ é o anel de valorização 2-henseliano de K que estamos procurando.

Seja $\tau \in G(K)$. Como $\tilde{D}$ contém C e $\tau^{-1}C$, temos que $\tau\tilde{D}$ contém C . Logo $\tilde{D}$ e $\tau\tilde{D}$ são comparáveis e, sendo K -conjugados, são iguais.

Se D' é um anel de valorização 2-henseliano de N , $C \subseteq D'$ e tal que $D' \cap K$ é anel de valorização 2-henseliano de K , então $\tilde{D}'$ contém todos os prolongamentos de $C \cap K$ a $K(2)$. Concluimos da construção de $\tilde{D}$ que $\tilde{D} \subseteq \tilde{D}'$ e assim $D \subseteq D'$, como queríamos. ■

(1.2.8) Definição. Chamamos um anel de valorização A de K de anti-2-henseliano se $K^Z(D; K) = K(2)$, onde D é uma extensão de A a $K(2)$.

(1.2.9) Proposição. Sejam K um corpo quadrático separavelmente fechado e A um anel de valorização de K . Então $\mathcal{K}_A = \mathcal{K}_A(2)$ e $\Gamma_A = 2\Gamma_A$.

PROVA. Sejam $\mathcal{L}$ extensão de $\mathcal{K}_A$ de grau 2^s e Δ um grupo totalmente ordenado com $\Gamma_A \subseteq \Delta$ e tal que $(\Delta : \Gamma_A) = 2^r$. Conforme ([E], Theorem 27.1, pg. 206), existe $L|K$ separável com grau 2^{s+r} . Logo, $s + r = 0$ e, assim, $\mathcal{L} = \mathcal{K}_A$ e $\Gamma_A = \Delta$. ■

(1.2.10) Definição. Dizemos que A é sem defeito em $K(2)$ se, para todo corpo intermediário $K \subseteq L \subseteq K(2)$, com $[L : K] < \infty$, vale a igualdade fundamental

$$[L : K] = \sum_{D \in \beta(L; A)} e_{D|K} f_{D|K},$$

conforme ([E], pg. 133), onde $e_{D|K}$ é o índice de ramificação ($e_{D|K} = |\Gamma_D / \Gamma_A|$) e $f_{D|K}$ é o grau residual (grau da extensão $\mathcal{K}_D | \mathcal{K}_A$) ([E], pgs. 98 e 99) e $\beta(L; A)$ é o conjunto de todos os prolongamentos de A a L .

(1.2.11) Proposição. Um anel A é anti-2-henseliano se, e somente se, $\mathcal{K}_A = \mathcal{K}_A(2)$, $\Gamma_A = 2\Gamma_A$ e A é sem defeito em $K(2)$. ■

(1.2.12) Proposição ([Br], Lemma 1.3). Sejam A e A' anéis de valorização de K , $A' \subseteq A$. Então $\mathcal{K}_{A'} \cong \mathcal{K}_{\phi_A(A')}$ e A' é 2-henseliano se, e somente se, A e $\phi_A(A')$ são 2-henselianos. ■

(I.2.13) Proposição. *Sejam A e A' anéis de valorização próprios de K . Se A e A' são independentes e A é 2-henseliano, então A' é anti-2-henseliano.*

PROVA. Se L é a 2-henselização de A' , então quaisquer prolongamentos de A e A' a L são independentes. Por (I.2.5) $L = K(2)$. ■

A proposição seguinte é uma generalização parcial do Corolário (I.2.5).

(I.2.14) Proposição ([EE] Proposition). *Sejam B e B' anéis de valorização próprios incomparáveis de K , sendo B' 2-henseliano. Então $\mathcal{K}_B$ é quadraticamente fechado.*

PROVA. Se $A = B \cdot B'$, então $\phi_A(B)$ e $\phi_A(B')$ são independentes e $\phi_A(B')$ é 2-henseliano e, conseqüentemente, $\phi_A(B)$ é anti-2-henseliano por (I.2.13) e $\mathcal{K}_B \cong \mathcal{K}_{\phi_A(B)}$ por (I.2.12) e isto conclui a prova pois $\mathcal{K}_{\phi_A(B)}$ é quadraticamente fechado, por (I.2.11). ■

Seja $\mathcal{H}(K)$ o conjunto de todos os anéis de valorização 2-henselianos do corpo K . Para uma descrição completa de $\mathcal{H}(K)$, procedemos como em [EE] e escrevemos

$$\mathcal{H}(K) = \mathcal{H}_1(K) \cup \mathcal{H}_2(K),$$

onde $\mathcal{H}_1(K) = \{ A \in \mathcal{H}(K) | \mathcal{K}_A \text{ não é quadrático separavelmente fechado} \}$

e $\mathcal{H}_2(K) = \{ A \in \mathcal{H}(K) | \mathcal{K}_A \text{ é quadrático separavelmente fechado} \}.$

As Proposições (I.2.15) e (I.2.16) e o Corolário (I.2.17) refletem propriedades interessantes de $\mathcal{H}(K)$, $\mathcal{H}_1(K)$ e $\mathcal{H}_2(K)$ e são demonstráveis exatamente como em [EE], visto

que os resultados lá utilizados em suas provas também foram obtidos acima para os anéis 2-henselianos ((I.2.9), (I.2.11) e (I.2.14)).

(I.2.15) Proposição ([EE] , Corollary 1).

- (a) *Seja $A \in \mathcal{H}(K)$ e seja C um anel de valorização de K . Se $A \subseteq C$, então $C \in \mathcal{H}(K)$.*
- (b) *$\mathcal{H}_1(K)$ satisfaz (a) e é uma classe totalmente ordenada pela inclusão.*
- (c) *Sejam A e C anéis de valorização de K . Se $A \in \mathcal{H}_2(K)$ e $C \subseteq A$, então $C \in \mathcal{H}_2(K)$. Se A e $C \in \mathcal{H}_2(K)$, então $D = A \cdot C$ é também um elemento de $\mathcal{H}_2(K)$ e portanto $\mathcal{H}_2(K)$ é um conjunto dirigido.*
- (d) *Para todos $A_1 \in \mathcal{H}_1(K)$ e $A_2 \in \mathcal{H}_2(K)$ temos que $A_2 \subsetneq A_1$. ■*

Observação : Em [EE] os autores resumem a propriedade (a) da Proposição anterior, dizendo que $\mathcal{H}(K)$ é uma “upper class” e, analogamente, a primeira parte da propriedade (c), dizendo que $\mathcal{H}_2(K)$ é uma “lower class”.

Como em [EE], obtemos da proposição (I.2.15) que $A_{(1)} = \bigcap A$, para todo $A \in \mathcal{H}_1(K)$, e, se $\mathcal{H}_2(K) \neq \emptyset$, $A_{(2)} = \bigcup A$, para todo $A \in \mathcal{H}_2(K)$, são anéis de valorização de K e satisfazem a seguinte proposição :

(I.2.16) Proposição ([EE] , Corollary 2).

- (a) *$A_{(1)} \in \mathcal{H}(K)$ e $A_{(1)} \in \mathcal{H}_1(K)$ se, e somente se, $\mathcal{H}_1(K)$ possui um menor elemento. Em particular isto ocorre se $\mathcal{H}_2(K)$ é vazio.*
- (b) *Se $\mathcal{H}_2(K)$ é não vazio, então $A_{(2)}$ é o maior elemento de $\mathcal{H}_2(K)$ e temos que $A_{(2)} \subseteq A_{(1)}$, e não existe anel estritamente entre $A_{(1)}$ e $A_{(2)}$. Além disso, $A_{(1)} = A_{(2)}$ se, e somente se, $A_{(1)} \notin \mathcal{H}_1(K)$. ■*

(I.2.17) Corolário.

- (a) *$\mathcal{K}_A$ é quadraticamente fechado para todo anel de valorização A , de K , tal*

que $A \notin \mathcal{H}_1(K)$ e A não seja subanel de $A_{(1)}$.

- (b) Se $\mathcal{H}_2(K) \neq \emptyset$ e A for anel de valorização de K , então $\mathcal{K}_A$ não quadraticamente fechado implica $A \in \mathcal{H}_1(K) \cup \{A_{(2)}\}$. ■

3. Anéis K^2 -compatíveis — elementos rígidos e básicos.

Neste parágrafo usaremos os conceitos de elementos rígidos e básicos, segundo [W2] e [AEJ], isto é, chamaremos um elemento $a \in K$, $a \notin \pm K^2$, *rígido* se $x^2 + ay^2 \in K^2 \cup aK^2$, para todo $x, y \in K$. O elemento a será chamado *birrígido* se a e $-a$ forem rígidos. O conjunto de todos os elementos não birrígidos será chamado conjunto dos básicos e será denotado por $B(K)$ e é um subgrupo de K^* , por ([W2], proposição 2.4). Usaremos também o símbolo $\mathcal{B}$ para $B(K)$. O corpo K será chamado *excepcional* se $B(K) = \pm K^2$ e, ou $-1 \in K^2$ ou então K^2 for aditivamente fechado.

(I.3.1) Definição ([AEJ]). Um anel de valorização A de K é K^2 -compatível se

$$1 + m_A \subseteq K^2.$$

(I.3.2) Observação. Se $c(K) \neq 2$, então um anel de valorização K^2 -compatível é 2-henseliano, segundo ([W2], Lemma 4.3). A recíproca vale se o anel é não diádico, pela proposição (I.2.2).

Em ([AEJ], §2) os autores constroem anéis de valorização K^2 -compatíveis de um corpo K , a partir de subgrupos H de K^* , que satisfaçam

$$\pm K^2 \subseteq \mathcal{B} \subseteq H \subseteq K^*,$$

do seguinte modo: sejam

$$\begin{aligned} O^-(H) &= \{x \in K \mid x \notin H \text{ e } 1+x \in K^2\}; \\ O^+(H) &= \{x \in K^* \mid x \in H \text{ e } xO^-(H) \subseteq O^-(H)\}; \\ O(H) &= O^-(H) \cup O^+(H). \end{aligned}$$

$O(H)$ não é necessariamente um subanel de K , contudo o Theorem 2.16 de [AEJ] estabelece a existência de um subgrupo $\widehat{H}$ de K^* tal que $H \subseteq \widehat{H}$, $(H : \widehat{H}) \leq 2$ e, se $A = O(\widehat{H})$, então A é um anel de valorização K^2 -compatível de K , satisfazendo $A^*K^2 \subseteq \widehat{H}$. Além disso, o teorema afirma que $H = \widehat{H}$, a menos que K seja excepcional.

O §3 de [AEJ] se inicia com o Lemma 3.1 que estabelece que, se $A = O(H)$ é um anel de valorização de K , então $v_A(H)$ não contém subgrupo convexo não trivial de Γ_A . Em seguida, no mesmo parágrafo, é feito um estudo dos anéis K^2 -“coarse” que por conveniência chamamos de “ K^2 -finos”, conforme definição a seguir. Conforme ([AEJ], 3.8), se existe A K^2 -fino, então existe um menor K^2 -fino que, como é único, chamaremos de “o fino”.

(I.3.3) Definição ([AEJ]). Um anel de valorização A de K é “ K^2 -fino” se $v_A(K^2) = v_A(A^*K^2)$ não contém subgrupo convexo não trivial de Γ_A . Ao menor K^2 -fino de K chamaremos de “o fino” e será denotado por $O(K)$ ou simplesmente $\mathcal{O}$.

(I.3.4) Proposição. Assumindo-se $\mathcal{H}_2(K) \neq \emptyset$ e que existe $A_0 \in \mathcal{H}_2(K)$ K^2 -compatível e tal que $A_0 \neq A_{\mathcal{Q}}$ se $A_{\mathcal{Q}}$ é diádico, temos:

- (a) $A \in \mathcal{H}_2(K) \implies A^* \subsetneq K^2$.
- (b) A é K^2 -compatível $\iff A \in \mathcal{H}(K)$.
- (c) Se existe A em $\mathcal{H}_2(K)$ tal que $c(\mathcal{K}_A) \neq 2$ e Γ_A não contém subgrupo isolado 2-divisível não trivial, isto é, A é K^2 -fino, então $A = A_{\mathcal{Q}} = \mathcal{O}$, onde $\mathcal{O}$ é o fino.
- (d) $B = K^2$ e $-1 \in K^2$.

PROVA. Se $K(2) = K$ não há o que demonstrar; assim, assumimos $K \neq K(2)$.

Como $A_0 \subseteq A_{(\mathfrak{A})}$ temos que $m_{A_{(\mathfrak{A})}} \subseteq m_{A_0}$; portanto, $A_{(\mathfrak{A})}$ é K^2 -compatível também.

Observação 1: $\mathcal{H}_2(K)$ está em correspondência bijetora com o conjunto de todos os anéis de valorização de $\mathcal{K}_{A_{(\mathfrak{A})}}$, sendo que $A_{(\mathfrak{A})}$ corresponde a $\mathcal{K}_{A_{(\mathfrak{A})}}$.

Temos dois casos a considerar:

1º Caso. $\mathcal{K}_{A_{(\mathfrak{A})}}$ é extensão algébrica de um corpo finito. Neste caso, pela observação 1, $\mathcal{H}_2(K) = \{A_{(\mathfrak{A})}\}$. Além disso, como $\mathcal{K}_{A_{(\mathfrak{A})}}$ é perfeito e quadrático separavelmente fechado, é quadraticamente fechado e assim $\mathcal{K}_{A_{(\mathfrak{A})}}^2 = \mathcal{K}_{A_{(\mathfrak{A})}}^*$. Por outro lado, $1 + m_{A_{(\mathfrak{A})}} = (1 + m_{A_0})^2$, pois $A_{(\mathfrak{A})}$ é K^2 -compatível e $1 + m_{A_0} \subseteq K^2$. Desses dois fatos e também do fato de $\mathcal{K}_{A_{(\mathfrak{A})}}^*$ ser grupo quociente de $A_{(\mathfrak{A})}^*$ com núcleo $1 + m_{A_{(\mathfrak{A})}}$ resulta $A_{(\mathfrak{A})}^* = (A_{(\mathfrak{A})}^*)^2 \subseteq K^2$. Fica assim provado (a).

Para provar (b), basta lembrar que se $A \in \mathcal{H}(K)$, então $A_{(\mathfrak{A})} \subseteq A$ por (I.2.15)-(d) ($\mathcal{H}_2(K) = \{A_{(\mathfrak{A})}\}$) e, portanto, A é K^2 -compatível. Por ([W2], Lemma 4.3), $c(K) \neq 2$ implica $A \in \mathcal{H}(K)$ se A for K^2 -compatível.

As provas de (c) e (d) serão feitas juntamente com o 2º caso.

2º Caso. Se $\mathcal{K}_{A_{(\mathfrak{A})}}$ não é extensão algébrica de um corpo finito.

Dado $A \in \mathcal{H}(K)$, se $A \in \mathcal{H}_1(K)$ temos $A_{(\mathfrak{A})} \subseteq A$, o que implica $1 + m_A \subseteq 1 + m_{A_{(\mathfrak{A})}} \subseteq K^2$ e A é K^2 -compatível.

A seguir, vamos considerar duas possibilidades: Se $c(\mathcal{K}_{A_{(\mathfrak{A})}}) \neq 2$, então $\mathcal{K}_{A_{(\mathfrak{A})}}$ é quadraticamente fechado e como $A_{(\mathfrak{A})}$ é K^2 -compatível resulta $A_{(\mathfrak{A})}^* \subseteq K^2$, usando o mesmo raciocínio acima para os grupos envolvidos.

Se $A \in \mathcal{H}_2(K)$ então $A^* \subseteq A_{(\mathfrak{A})}^* \subseteq K^2$ e também $1 + m_A \subseteq K^2$ já que $1 + m_A \subseteq A^*$. Assim, A é K^2 -compatível. Logo para o caso $c(\mathcal{K}_{A_{(\mathfrak{A})}}) \neq 2$ estão provados (a) e (b).

Vejamos agora o caso $c(\mathcal{K}_{A_{(\mathfrak{A})}}) = 2$. Como $A_0 \subsetneq A_{(\mathfrak{A})}$, temos que $\phi_{A_{(\mathfrak{A})}}(A_0)$ é $\mathcal{K}_{A_{(\mathfrak{A})}}^2$ -compatível e, pelo Lema (I.3.5), $\mathcal{K}_{A_{(\mathfrak{A})}}^* = \mathcal{K}_{A_{(\mathfrak{A})}}^2$ e, como $A_{(\mathfrak{A})}$ é K^2 -compatível, novamente $A_{(\mathfrak{A})}^* \subseteq K^2$ e

demonstramos (a) e (b) como no caso anterior.

Provas de (c) e (d):

(c) Como existe A K^2 -fino, existe, por ([AEJ] 3.8), $\mathcal{O}$ tal que $\mathcal{O}$ é o fino, com $c(\mathcal{K}_{\mathcal{O}}) \neq 2$. Se $A_{\mathcal{Q}} \subseteq \mathcal{O}$. Seja $\Delta_0 = \bigcup \Delta$, para todo Δ subgrupo isolado de Γ , $\Delta \subsetneq 2\Gamma$, onde $\Gamma = \Gamma_{A_{\mathcal{Q}}}$. Seja $A \supseteq A_{\mathcal{Q}}$ anel de valorização de K tal que $\Gamma_A = \Gamma/\Delta_0$, conforme ([E], Theorem 7.4, pg. 49).

Afirmção. Γ_A não contém subgrupo isolado 2-divisível não trivial.

Sejam Λ subgrupo de Γ_A 2-divisível e $\varphi : \Gamma \longrightarrow \Gamma_A$ a projeção canônica. Então

$$\Delta_0 \subseteq \varphi^{-1}(\Lambda) \subseteq \varphi^{-1}(2\Gamma_A) = \Delta_0 + 2\Gamma = 2\Gamma.$$

Assim, pela construção de Δ_0 , temos $\Delta_0 = \varphi^{-1}(\Lambda)$, ou equivalentemente $\Lambda = \{0\}$.

Se $\mathcal{O} \subseteq A_{\mathcal{Q}}$, $\phi_{A_{\mathcal{Q}}}(\mathcal{O}) \subseteq \mathcal{K}_A$ tem grupo de valores Δ , 2-divisível, por (I.2.9). Mas existe Δ_0 subgrupo de $\Gamma_{\mathcal{O}}$ tal que $\Delta_0 \cong \Delta$ e $\Gamma_{\mathcal{O}}/\Delta_0 \cong \Gamma$. Como $\mathcal{O}$ é o fino, resulta que $\Delta_0 = \{0\}$ e $\mathcal{O} = A_{\mathcal{Q}}$.

Em $\mathcal{K}_A$ temos que $(\phi_A(A_{\mathcal{Q}})^*) \subseteq \mathcal{K}_A^2$ pelo item (a) acima e $\Gamma_{\phi_A(A_{\mathcal{Q}})} \cong \Delta_0$ que é 2-divisível, resultando $\mathcal{K}_A^* = \mathcal{K}_A^2$ também.

Como $c(\mathcal{K}_{\mathcal{O}}) \neq 2$ e $\mathcal{O} \subseteq A$, $c(\mathcal{K}_A) \neq 2$. Assim, $\mathcal{K}_A$ é quadraticamente fechado, o que implica $A \in \mathcal{H}_2(K)$, ou seja, $A_{\mathcal{Q}} = A = \mathcal{O}$ é isto completa a prova de (c) neste caso.

(d) Por ([AEJ], 1.9(1) pg. 5 ou introdução), $\mathcal{B} \subseteq A_{\mathcal{Q}}^* K^2 = K^2$. Mas como $K^2 \subseteq \mathcal{B}$, segue $\mathcal{B} = K^2$. Como -1 é básico, $-1 \in K^2$. ■

(I.3.5) Lema. Se $c(K) = 2$ e A é anel de valorização K^2 -compatível com $A \neq K$, então $K^2 = K^*$.

PROVA. Se $x \in m_A$, então $1+x \in K^2$, o que implica que $x = (1+x)+1 \in K^2 + K^2 \subseteq K^2$. Se $x \notin m_A$ e $x^{-1} \in m_A$, temos que $x^{-1} \in K^2$, ou seja, $x \in K^2$. Se $x \in A^*$ e $y \in m_A$, $y \neq 0$,

então $xy \in m_A$, donde $xy \in K^2$, $y \in K^2$, resultando assim $x \in K^2$. ■

O teorema (I.3.6), a seguir, tem demonstração análoga à da proposição (I.3.4), utilizando ([AEJ] 1.9, 3.8 e 3.9). Esse resultado já foi parcialmente enunciado quando introduzimos $\mathcal{O}$, mas devido à grande importância para nosso trabalho vamos apresentá-lo de maneira mais detalhada.

A proposição (I.3.8) é consequência de (I.3.4) e de (I.3.6) e ambos, (I.3.6) e (I.3.8), são fundamentais para o restante do trabalho.

(I.3.6) Teorema. *Seja K um corpo e suponha que exista A em $\mathcal{H}(K)$ tal que $c(\mathcal{K}_A) \neq 2$ e $\Gamma_A \neq 2\Gamma_A$. Então existe $\mathcal{O}$ (o fino de K) satisfazendo:*

- (a) $\mathcal{B} \subseteq \mathcal{O}^*K^2$ e $(\mathcal{O}^*K^2 : \mathcal{B}) \leq 2$. Além do mais, se K não for excepcional, então $\mathcal{O}^*K^2 = \mathcal{B}$.
- (b) $(\mathcal{K}_{\mathcal{O}}^* : B(\mathcal{K}_{\mathcal{O}})) \leq 2$ e $B(\mathcal{K}_{\mathcal{O}}) = \mathcal{K}_{\mathcal{O}}^*$ se K não for excepcional.
- (c) $\mathcal{O}$ é não diádico e, portanto, $G^T(\tilde{\mathcal{O}}; K)$ é um subgrupo abeliano normal de $G(K)$, de posto igual a $r(K^*/\mathcal{O}^*K^2)$. Mais ainda, $\mathcal{O} \in \mathcal{H}_2(K)$ ou então $\mathcal{H}_2(K) = \emptyset$.
- (d) Todo subgrupo isolado 2-divisível de $\Gamma_{\mathcal{O}}$ é trivial.
- (e) Para todo $A \in \mathcal{H}(K)$ tal que $c(\mathcal{K}_A) \neq 2$ e Γ_A não contém subgrupo isolado 2-divisível não trivial, $\mathcal{O} \subseteq A$.

PROVA. Mostraremos primeiro a existência de um anel de valorização C de K que é K^2 -fino. Seja Δ o subgrupo convexo maximal de $2\Gamma_A$ e C o anel de valorização que contém A e que corresponde a Γ_A/Δ (cf. [E], Theorem 7.4). Por construção, Γ_C satisfaz a condição acima. Como $A \subseteq C$ e A é K^2 -compatível, C é K^2 -compatível, pela observação (I.3.2).

Por ([AEJ], Theorem 3.8), existe o anel $\mathcal{O}$ satisfazendo (d) e (e). ([AEJ], Theorem 3.9) implica que $\mathcal{O}$ satisfaz (a) e ([AEJ], Lemma 4.4) implica $\mathcal{O}$ não diádico. Finalmente, (b) é consequência de (a) e de ([AEJ], Proposition 1.9). ■

A proposição (I.3.7), a seguir, fornece condições suficientes para a existência de um tal anel de valorização A , usando o grupo $\mathcal{B}$.

(I.3.7) Proposição . *Seja K um corpo e suponha que $(K^* : \mathcal{B}) > 2$ ou que $(K^* : \mathcal{B}) = 2$ e K não é excepcional. Então, existe um anel de valorização 2-henseliano não diádico A tal que Γ_A não é 2-divisível.*

PROVA. Seja $H = \mathcal{B}$. Por ([AEJ], Theorem 2.16), existe um subgrupo $\widehat{H}$ de K^* , $H \subseteq \widehat{H}$ tal que $A = O(\widehat{H})$ é um anel de valorização K^2 -compatível de K , que satisfaz $A^* K^2 \subseteq \widehat{H}$. Com as hipóteses da proposição, $\widehat{H} \neq K^*$, e, portanto, $A \neq K$ e Γ_A não é 2-divisível pois, se $x \in K^* \setminus \widehat{H}$ e $\gamma = v_A(x)$, não podemos ter $\gamma = 2v_A(y) = v_A(y^2)$, caso contrário teríamos $xy^{-2} \in A^*$, o que implica $x \in A^* K^2 \subseteq \widehat{H}$, contradizendo a escolha de x .

Suponhamos agora que A seja diádico. Logo, $v_A(2) > 0$ e, como $c(K) \neq 2$, temos $c(K) = 0$. Como, pelo Lemma 3.1 de [AEJ], Γ_A não possui subgrupo convexo 2-divisível não trivial, se Δ for o subgrupo convexo de Γ_A gerado por $v_A(2)$, então $\Delta \not\subseteq 2\Gamma_A$. Por hipótese $\Delta \neq \{0\}$. Assim, estamos em condições de usar a técnica utilizada na demonstração do Lemma 4.4 de [AEJ]. Seja $\delta \in \Delta$, satisfazendo $0 < \delta < v_A(4)$, obtido conforme as observações a seguir.

Observações : (a) se $v_A(2) \notin 2\Gamma_A$, tomamos $\delta = v_A(2)$;

(b) se $v_A(a) \in 2\Gamma_A$ e $\lambda \in \Delta \setminus (\Delta \cap 2\Gamma_A)$ satisfazem $\lambda \leq 2v_A(2)$, tomamos $\delta = \lambda$.

(c) se $v_A(a) \in 2\Gamma_A$ e $\lambda \in \Delta \setminus (\Delta \cap 2\Gamma_A)$ satisfazem $\lambda \leq nv_A(2)$ para $n > 2$, tomamos $\delta = \lambda - (n-2)v_A(2)$.

Seja $e \in K^*$, com $v_A(e) = \delta$. Então $e \in m_A$, $1+e \in 1+m_A \subseteq K^2$ e portanto a forma quadrática $\langle 1, -(1+e) \rangle$ é universal. Pelo Lemma 4.3 de [AEJ], temos $K^* = D(\langle 1, -(1+e) \rangle) \subseteq \{1, e\}(1+m_A)K^2 = K^2 \cup eK^2$. Mas isto contradiz a hipótese da proposição. ■

(I.3.8) Proposição. *Assumindo-se a existência de $\mathcal{O}$ como em (I.3.6), temos:*

(a) Se $\mathcal{O} \in \mathcal{H}_2(K)$ então $\mathcal{O} = A_{\mathcal{O}}$, $\mathcal{B} = K^2$, e $G(K) = G^T(\tilde{\mathcal{O}}; K)$ é um grupo

abeliano.

- (b) Seja $A \in \mathcal{H}(K)$. Se A for não diádico, então é comparável a $\mathcal{O}$. Se $A \subseteq \mathcal{O}$, então $G^I(\tilde{A}; K) = G^I(\tilde{\mathcal{O}}; K)$.

PROVA. (a) Por (I.3.4), se $\mathcal{O} \in \mathcal{H}_\lambda(K)$, temos $\mathcal{O} = A_{\mathcal{O}}$ e $B = K^2$. Como $\mathcal{O}$ é não diádico, por ([E], (20.11)-(a), pg. 161 e Theorem (20.12), pg. 163), $G(K) = G^I(\tilde{\mathcal{O}}; K)$ é um grupo de caracteres e portanto abeliano (ver pg. 6).

(b) Pela Observação (I.3.2), A é K^2 -compatível. Se A e $\mathcal{O}$ fossem incomparáveis, por ([AEJ], Proposition 3.5), $A_{\mathcal{O}}$ conteria ambos e teríamos $\mathcal{O} \in \mathcal{H}_\lambda(K)$ e a igualdade $A_{\mathcal{O}} = \mathcal{O}$ dada pelo item anterior, contra A e $\mathcal{O}$ incomparáveis.

Vejamos o caso $A \subseteq \mathcal{O}$. Por ([AEJ], Theorem 3.8 pg. 461), Γ_A contém um subgrupo 2-divisível não trivial Δ , tal que $\Gamma_{\mathcal{O}} = \Gamma_A/\Delta$. Seja C a imagem de $\tilde{A}$ em $\mathcal{K}_{\mathcal{O}}(2)$. Então $C \cap \mathcal{K}_{\mathcal{O}}$ é a imagem de A em $\mathcal{K}_{\mathcal{O}}$ e tem grupo de valores isomorfo a Δ , portanto 2-divisível. Assim, $C \cap K^T(C; \mathcal{K}_{\mathcal{O}})$ também tem grupo de valores 2-divisível. Como $c(\mathcal{K}_A) \neq 2$ ($\mathcal{K}_A = \mathcal{K}_{\mathcal{O}}(2)$) e $C \cap K^T(C; \mathcal{K}_{\mathcal{O}})$ é anel de valorização 2-henseliano, tendo corpo de resíduos quadraticamente fechado e grupo de valores 2-divisível, segue-se que $K^T(C; \mathcal{K}_{\mathcal{O}}) = \mathcal{K}_{\mathcal{O}}(2)$. Assim, $K^T(\tilde{A}; K) = K^T(\tilde{\mathcal{O}}; K)$ por ([E], 19.13) e isto encerra a prova, pois ambos os anéis são não diádicos. ■

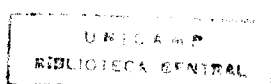
Por coerência de exposição colocamos o próximo resultado neste Capítulo, embora ele só vá ser utilizado no Capítulo III.

(I.3.9) Proposição. *Seja K um corpo satisfazendo:*

- (i) *Existe uma extensão normal própria E de K , $E \subsetneq K(2)$.*
- (ii) *Existe uma extensão F de K , $F \subsetneq E$ tal que F contém um anel de valorização 2-henseliano não diádico C , com $\Gamma_C \neq 2\Gamma_C$.*

Então, K satisfaz as hipóteses do Teorema (I.3.6).

PROVA. $\tilde{C} \cap E$ é anel de valorização 2-henseliano não diádico próprio de E . Por (I.2.7),



existe um anel de valorização próprio D de E , $\tilde{C} \cap E \subseteq D$ tal que $D \cap K$ é anel de valorização 2-henseliano, sendo $D = \tilde{C} \cap E$, ou então $K^T(\tilde{D}; K) \subseteq E$. D é não diádico pois $\tilde{C} \cap E \subseteq D$. Se $D = \tilde{C} \cap E$, a hipótese $\Gamma_C \neq 2\Gamma_C$ nos dá que o grupo de valores de $D \cap K = C \cap K$ não é 2-divisível. Por outro lado, se $D \neq \tilde{C} \cap E$ e $D \cap K$ tiver grupo de valores 2-divisível, também $D \cap K^T(\tilde{D}; K)$ tem grupo de valores 2-divisível. Como D é não diádico, por ([E], Theorem (20.12), pg. 163) $K^T(\tilde{D}; K) = K(2)$, contradizendo $K^T(\tilde{D}; K) \subseteq E \neq K(2)$. Assim, $A = D \cap K$ satisfaz as hipóteses de (I.3.6). ■

(I.3.10) Proposição. *Seja $L|K$ uma extensão de corpos, $L \subseteq K(2)$ e A um anel de valorização de L tal que Γ_A não contenha subgrupo isolado 2-divisível não trivial. Então, $A \cap K$ tem a mesma propriedade.*

PROVA. Seja $C = A \cap K$. Como Γ_A/Γ_C é um grupo com 2-torsão, por ([E], 13.1), segue-se que todo subgrupo isolado 2-divisível não trivial de Γ_C é também subgrupo isolado de Γ_A . ■

CAPÍTULO II

Subgrupos Abelianos Máximos de Posto 1

1. Introdução.

No capítulo III fazemos um estudo dos subgrupos abelianos de $G(K)$ e estabelecemos que, para todo corpo K , $G(K)$ possui um maior subgrupo abeliano normal $\mathfrak{A}$ (III.2.6). Para um tal $\mathfrak{A}$ existem duas opções, ou $\mathfrak{A} \cong G^T(\tilde{\mathcal{O}}; K)$ onde $\mathcal{O}$ é dado pelo Teorema (I.3.6) (se $\mathcal{O}$ é não diádico, lembramos que $G^T(\tilde{\mathcal{O}}; K)$ é um grupo de caracteres), ou então $\mathfrak{A} \cong G^T(\tilde{\mathcal{O}}; K) \times \mathbb{Z}_2$.

Neste capítulo estudamos os corpos K cujos subgrupos abelianos normais têm posto no máximo 1. O Teorema (II.2.5) fornece uma classificação de tais corpos. Esta classificação foi feita utilizando o homomorfismo natural $\varphi : G(K) \longrightarrow \text{Aut}(U)$. Se $\text{Im}(\varphi) \cong \mathbb{Z}_2$, obtemos duas das três possibilidades (a outra delas corresponde a K ser $K(2)$ -pitagórico) e, aplicando o Teorema (I.3.6), deduzimos (Corolário (II.2.6)) que, nesta situação, se K não é $K(2)$ -pitagórico, então $G^T(\tilde{\mathcal{O}}; K)$ é o maior subgrupo abeliano normal de $G(K)$. O Teorema (II.2.5) é complementado com exemplos em (II.2.7). Observamos também que o caso em que a característica de K é dois não é interessante, conforme estabelece o Corolário (II.2.8).

Notações: Usaremos o símbolo $\mathbb{Z}_2$ para denotar o grupo aditivo dos inteiros 2-ádicos (algumas vezes ficará claro o uso da estrutura de anel e não faremos qualquer menção explícita a isto).

Se G é um pro-2-grupo e $S \subseteq G$, denotamos por $\langle S \rangle$ o subgrupo fechado gerado (no sentido topológico) por S e, se S for um conjunto finito, digamos, $S = \{\sigma_1, \dots, \sigma_k\}$, escreveremos $\langle \sigma_1, \dots, \sigma_k \rangle$ no lugar de $\langle \{\sigma_1, \dots, \sigma_k\} \rangle$.

Se K é um corpo e H é um subgrupo de $G = G(K)$, denotaremos por $C(H)$ o centralizador de H em G ,

$$C(H) = \{ g \in G \mid gh = hg, \forall h \in H \}.$$

Se σ é uma involução de $G(K)$ temos $C(\langle \sigma \rangle) = \{ \langle \sigma \rangle \}$, por ([B], cap. II, Theorem 4, pg. 78).

Se G é um pro-2-grupo com H subgrupo normal de G e se S for um subgrupo de G/H , denotaremos por $H \rtimes S$ o produto semidireto $H \rtimes_{\varphi} S$, onde $\varphi : S \longrightarrow \text{Aut}(H)$ é o homomorfismo definido por $\varphi(\bar{g})(x) = gxg^{-1}$, para todo $\bar{g} \in S$ e todo $x \in H$, conforme ([MB], pg. 461).

2. Subgrupos abelianos de posto 1.

(II.2.1) Proposição. *Seja K um corpo tal que $G(K)$ contenha um subgrupo normal $U \cong \mathbb{Z}_2$. Então, uma das alternativas ocorre:*

- (a) *Existe um subgrupo normal U' de $G(K)$ tal que $U \subseteq U' \cong \mathbb{Z}_2$ e $C(U') = U'$, ou então*
- (b) *Existe $g \in C(U)$ e $g \notin U$, tal que $\langle g \rangle \cap U = \{1\}$. Neste caso, $\langle g \rangle \times U \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ é um subgrupo de $G(K)$.*

PROVA. Seja $\mathcal{G} = \{H \mid H \cong \mathbb{Z}_2 \text{ é subgrupo normal de } G(K), H \supseteq U\}$. Pelo Lema de Zorn $\mathcal{G}$ possui um elemento maximal U' .

Seja $\varphi : G(K) \longrightarrow \text{Aut}(U') \cong \text{Aut}(\mathbb{Z}_2)$ o homomorfismo dado por $\varphi(g)(x) = gxg^{-1}$, para todo $g \in G$ e todo $x \in U'$. É imediato que $\text{kernel}(\varphi) = C(U')$. Assumiremos que (a) não ocorre. Se, para todo $g \in C(U')$ com $g \notin U'$, vale que $\langle g \rangle \cap U' \neq \{1\}$, então existe um natural $n \geq 1$ tal que $g^n \in U'$. Assim, $C(U')/U'$ é um grupo de torsão e, como é também um pro-2-grupo, segue-se que a ordem do elemento gU' de $C(U')/U'$ é potência de 2, digamos, 2^s para algum $s \geq 0$. Denotaremos por $\sigma(g)$ este número.

Afirmamos que se $\sigma(g) = 2^s$ com $s > 0$, então $\langle g^{2^s} \rangle = U'$. Se $2^r = (U' : \langle g^{2^s} \rangle)$,

com $r \geq 0$, então $\langle g^{2^r} \rangle = (U')^{2^r}$. Assim, existe $h \in U'$ tal que $g^{2^r} = h^{2^r}$. Como g e h comutam, temos que $(h^{2^{r-s}} g^{-1})^{2^s} = 1$, se $r \geq s$. Se $y = h^{2^{r-s}} g^{-1}$, temos que $\langle g \rangle \subseteq C(\langle y \rangle)$ o que implica que y não é uma involução, conforme foi observado na introdução deste capítulo. Portanto, $y = 1$ e temos que $g = h^{2^{r-s}} \in U'$, o que contradiz $g \notin U'$. Por outro lado, se $s > r$, de maneira análoga obtemos $g^{2^{s-r}} h^{-1} = 1$ e portanto $g^{2^{s-r}} \in U'$, o que contradiz a minimalidade de s , caso tenhamos $r \neq 0$ e então $r = 0$, provando assim a afirmação.

$C(U')/U'$ é pro-2-grupo de torsão. Sendo assim, possui elemento de ordem 2. Tomamos g em $C(U')$ tal que $\phi(g) = 2$. Se, para todo $g' \in C(U')$ tal que $\phi(g') = 2$, vale $\langle g \rangle = \langle g' \rangle$, segue-se que $\langle g \rangle$ é subgrupo normal de $G(K)$. Como $U' = \langle g^2 \rangle \subsetneq \langle g \rangle$, obtemos uma contradição com a maximalidade de U' .

Assim, existem g_1 e g_2 em $C(U')$ tais que $\phi(g_1) = 2 = \phi(g_2)$ e $\langle g_1 \rangle \neq \langle g_2 \rangle$. Seja $h = g_1 g_2 \in C(U')$. Como $h^{\phi(h)} \in U'$ e $g_1 \in C(U')$, temos que $g_1(h^{\phi(h)})g_1^{-1} = h^{\phi(h)}$. Por outro lado, como $g_1^2 \in U'$ e $g_2 g_1^{-1} \in C(U')$, segue-se que $g_1 h g_1^{-1} = g_1 (g_1 g_2) g_1^{-1} = g_1^2 (g_2 g_1^{-1}) = (g_2 g_1^{-1}) g_1^2 = g_2 g_1$ e portanto $g_1 h^{\phi(h)} g_1^{-1} = g_1 (g_1 g_2)^{\phi(h)} g_1^{-1} = (g_2 g_1)^{\phi(h)}$ e temos que $(g_1 g_2)^{\phi(h)} = (g_2 g_1)^{\phi(h)}$.

Agora observamos que $(g_1 g_2)(g_2 g_1) = g_1 g_2^2 g_1 = g_1^2 g_2^2$ e $(g_2 g_1)(g_1 g_2) = g_2 g_1^2 g_2 = g_1^2 g_2^2$, ou seja, $g_1 g_2$ comuta com $g_2 g_1$ e portanto $[(g_1 g_2)(g_2 g_1)^{-1}]^{\phi(h)} = 1$. Além disso, $U' \subseteq C(\langle (g_1 g_2)(g_2 g_1)^{-1} \rangle)$, o que mostra que $(g_1 g_2)(g_2 g_1)^{-1}$ não é involução. Assim, $(g_1 g_2)(g_2 g_1)^{-1} = 1$, ou seja, g_1 comuta com g_2 . Mas, como $\langle g_1^2 \rangle = U' = \langle g_2^2 \rangle$ e $U' = (U')^2 \cup g_1^2 (U')^2$, temos que existe $u \in U'$ tal que $g_2^2 = g_1^2 u^2$ (caso contrário teríamos g_2^2 em $(U')^2$, o que não ocorre pois g_2^2 gera U'). Assim, $(g_2^{-1} g_1 u)^2 = 1$ e novamente isto nos diz que $g_2 = g_1 u$, ou seja, $\langle g_2 \rangle \subseteq \langle g_1 \rangle$.

De maneira análoga obtemos também $\langle g_1 \rangle \subseteq \langle g_2 \rangle$, ou seja, g_1 e g_2 geram o mesmo subgrupo, contradizendo a escolha de ambos. Esta contradição nos mostra que $C(U')/U'$ não pode ser um grupo de torsão e decorre daí a existência de $g \in C(U') \subseteq C(U)$, com $\langle g \rangle \cap U' = \{1\}$ e isto encerra a prova. ■

O próximo teorema dá, como foi dito na introdução do capítulo, uma descrição dos corpos K tais que $G(K)$ satisfaz a condição (a) da última proposição. Para isto neces-

sitamos dos dois lemas seguintes.

(II.2.2) Lema. Seja $G = \langle \tau \rangle \rtimes \langle \sigma \rangle \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$ um grupo não abeliano, com $C(\langle \tau \rangle) = \langle \tau \rangle$. Então todo subgrupo abeliano normal H de G está contido em $\langle \tau \rangle$. Além disso, se $G/H \cong \mathbb{Z}_2$, então $H = \langle \tau \rangle$.

PROVA. Seja λ uma unidade de $\mathbb{Z}_2$ que satisfaz $\sigma \tau \sigma^{-1} = \tau^\lambda$. Como G não é abeliano, $\lambda \neq 1$. Se $\lambda = -1$, então $\sigma^2 \tau \sigma^{-2} = \tau$ e teríamos $\sigma^2 \in C(\langle \tau \rangle)$, contradizendo $C(\langle \tau \rangle) = \langle \tau \rangle$. Isto nos diz que $\lambda \in (\pm 1 + 4\mathbb{Z}_2)$, por ([S], Proposition 8, pg 17). Trocando-se τ por τ^{-1} , se necessário, podemos assumir que $\lambda \in (1 + 4\mathbb{Z}_2)$. Assim, $\lambda \in (1 + 2^n \mathbb{Z}_2) \setminus (1 + 2^{n+1} \mathbb{Z}_2)$, para algum $n \geq 2$.

Afirmção: Para todos $\delta, \gamma \in \mathbb{Z}_2$, $\delta, \gamma \neq 0$, não pode ocorrer $\sigma^\delta \tau^\gamma \sigma^{-\delta} = \tau^\gamma$.

Prova. Inicialmente observamos que $\sigma^\delta \tau^\gamma \sigma^{-\delta} = (\sigma^\delta \tau \sigma^{-\delta})^\gamma = \tau^{\gamma \lambda^\delta}$. Seja $\omega \in (1 + 4\mathbb{Z}_2) \setminus (1 + 8\mathbb{Z}_2)$. Da prova da Proposition 8 de [S], obtemos que ω é um gerador de $(1 + 4\mathbb{Z}_2)$ como $\mathbb{Z}_2$ -módulo, isto é, $\omega^{\mathbb{Z}_2} = (1 + 4\mathbb{Z}_2)$. Resulta então que $\lambda \in (1 + 2^n \mathbb{Z}_2) \setminus (1 + 2^{n+1} \mathbb{Z}_2)$ é também um gerador de $(1 + 2^n \mathbb{Z}_2)$ como $\mathbb{Z}_2$ -módulo e portanto $\lambda^\delta = 1 + 4\mu$ para algum $\mu \in \mathbb{Z}_2, \mu \neq 0$. Supondo agora $\sigma^\delta \tau^\gamma \sigma^{-\delta} = \tau^\gamma$, obtemos $\tau^\gamma = \tau^{\gamma(1+4\mu)}$ e portanto $\tau^{4\mu\gamma} = 1$ e, como esta última igualdade não pode ocorrer, a afirmação fica provada.

Agora, seja $h = \sigma^\alpha \tau^\beta \in H$, $\alpha, \beta \in \mathbb{Z}_2$ e $\lambda = 1 + 4\nu$ com $\nu \in \mathbb{Z}_2$. Então $h^{-1} \sigma h \sigma^{-1} = (\tau^{-\beta} \sigma^{-\alpha})(\sigma \sigma^\alpha \tau^\beta \sigma^{-1}) = \tau^{-\beta} (\sigma \tau \sigma^{-1})^\beta = \tau^{-\beta} \tau^{(\beta+4\nu\beta)} = \tau^{4\nu\beta} \in H \cap \langle \tau \rangle$. Queremos mostrar que $\alpha = 0$. Se α e $\beta \neq 0$, então $H \cap \langle \tau \rangle = \langle \tau^{2^r} \rangle$. Se $\alpha \neq 0$ e $\beta = 0$ também $\tau^{-1} h \tau h^{-1} = \tau^{-1} \sigma^\alpha \tau \sigma^{-\alpha} = \tau^{-1} \tau^{\lambda^\alpha} = \tau^{4\nu} \in H \cap \langle \tau \rangle$, onde $\lambda^\alpha = 1 + 4\nu$ com $\nu \in \mathbb{Z}_2$ e $\nu \neq 0$, como foi calculado anteriormente. Novamente $H \cap \langle \tau \rangle = \langle \tau^{2^r} \rangle$, onde $r \geq 0$ é um inteiro. Portanto, $h \tau^{2^r} = \tau^{2^r} h$, para todo $h \in H$ e então $\tau^{2^r} = h \tau^{2^r} h^{-1} = \sigma^\alpha \tau^{2^r} \sigma^{-\alpha}$, contradizendo a afirmação, se $\alpha \neq 0$. Portanto, $\alpha = 0$ e $H \subseteq \langle \tau \rangle$. Finalmente, se $(\langle \tau \rangle : H) = 2^r$, então $G/H \cong (\mathbb{Z}/2^r \mathbb{Z}) \rtimes \mathbb{Z}_2$. Isto nos diz que, se $G/H \cong \mathbb{Z}_2$, então $H = \langle \tau \rangle$. ■

Na demonstração do próximo lema usaremos argumentos presentes em ([EV], Proposition 4.6).

Para cada $a \in K^\times$ denotamos por $a^{1/2^s}$, uma raiz 2^s -ésima de a , escolhida de forma conveniente, de modo que $(a^{1/2^{s+1}})^2 = a^{1/2^s}$. No caso $a = 1$, chamamos $\varepsilon_s = a^{1/2^s}$, que é uma raiz 2^s -ésima primitiva de 1. Também usamos as notações $i = \varepsilon_2$, $\varepsilon_\infty = \{\varepsilon_n | n \geq 1\}$.

(II.2.3) Definição ([W3]). Um corpo K é um C-corpo se $\mathcal{B} = K^2 \cup -K^2$.

Segundo Ware ([W], §4), uma condição necessária e suficiente para que K seja um C-corpo é que o anel de Witt $W(K)$ seja isomorfo a um anel de grupo do tipo $\mathbb{Z}/n\mathbb{Z}[G]$, onde $n = 0, 2$ ou 4 , e G é um grupo de expoente 2.

(II.2.4) Lema. Seja K um C-corpo não formalmente real tal que $|K^\times/K^2| = 4$ e, para algum $r \geq 2$, $\varepsilon_{r-1} \in K$ e $\varepsilon_r \notin K$. Seja $L = K(\varepsilon_\infty)$. Então

- (a) Se $r = 2$ e $L = K(i)$, então $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$ e podemos escolher geradores σ e τ para as componentes isomorfas a $\mathbb{Z}_2$ tais que $\sigma\tau\sigma^{-1} = \tau^{-1}$.
- (b) Se $r > 2$ ou $L \neq K(i)$, então $G(L; K) \cong \mathbb{Z}_2$. Neste caso, se $r = 2$, então $\varepsilon_3 \in K(i)$.

Antes de iniciar a prova do lema, daremos uma descrição de L , como em ([W1], §4). Podemos escrever $\varepsilon_n = \frac{(\xi_n + i\eta_n)}{2}$ para $n \geq 3$, onde $\xi_n = (\varepsilon_n + \varepsilon_n^{-1})$ e $\eta_n = -i(\varepsilon_n - \varepsilon_n^{-1})$. Portanto, para $n > 3$

$$\xi_n^2 = (\varepsilon_n + \varepsilon_n^{-1})^2 = (\varepsilon_n^2 + \varepsilon_n^{-2} + 2) = (\varepsilon_{n-1} + \varepsilon_{n-1}^{-1} + 2) = \xi_{n-1} + 2$$

e, como $\varepsilon_2 + \varepsilon_2^{-1} = 0$, segue-se que $\xi_3^2 = 2$. De maneira análoga, obtemos $\eta_n^2 = (2 - \xi_{n-1})$, se $n > 3$ e $\eta_3^2 = 2$. Por outro lado, para $n > 3$

$$\xi_n \eta_n = -i(\varepsilon_n + \varepsilon_n^{-1})(\varepsilon_n - \varepsilon_n^{-1}) = -i(\varepsilon_n^2 - \varepsilon_n^{-2}) = -i(\varepsilon_{n-1} - \varepsilon_{n-1}^{-1}) = \eta_{n-1}.$$

Assim, a sequência de corpos definida por $K_2 = K(i)$ e, para $n \geq 3$, $K_n = K_2(\xi_n)$, satisfaz: $K_n \subseteq K_{n+1}$, $K_n = K_2(\eta_n)$ e $L = \bigcup_{n \geq 2} K_n$.

Finalmente, por ([W1], Lemma 4.2), se $L \neq K_2$, então existe $t > 2$ tal que $K_{t-1} = K_2$ e $K_t|K_2$ é a única subextensão quadrática de $L|K_2$. Concluimos que $G(L; K_2) \cong \mathbb{Z}_2$, sempre que $L \neq K_2$.

PROVA DO LEMA:

(a) Por ([W], Corollary 2.10) K_2 é também um C -corpo e, de ([L1], Theorem 3.4, pg. 202) obtemos a seqüência exata

$$1 \longrightarrow \{\pm K^2\} \longrightarrow K^*/K^2 \xrightarrow{\varepsilon} K_2^*/K_2^2 \xrightarrow{N} K^*/K^2,$$

onde ε é o homomorfismo induzido pela inclusão $K^* \hookrightarrow K_2^*$ e N é o homomorfismo induzido pela norma $N_{K_2|K}$. Se $\mathbb{F}_2$ é o corpo com dois elementos, a seqüência acima é uma seqüência exata de $\mathbb{F}_2$ espaços vetoriais e $\dim_{\mathbb{F}_2}(\text{Im}(N)) = 0$ ou 1 , porque K é C -corpo.

Se $\dim_{\mathbb{F}_2}(\text{Im}(N)) = 0$, K^2 seria aditivamente fechado e, como $-1 \notin K^2$, K seria formalmente real, contra a hipótese. Assim, $\dim_{\mathbb{F}_2}(\text{Im}(N)) = 1$ e K_2 também possui quatro classes quadráticas e não é formalmente real.

Por outro lado, temos

$$K^* = (\pm 1)K^2 \cup (\pm a)K^2,$$

para algum $a \in K$. Por ([W], Proposition 1.1), $-1 = c^2 + d^2$ com c e $d \in K$ e, por ([W], Corollary 3.9(1)),

$$K(2) = K_2(\{(c + di)^{1/2^n}, -a^{1/2^n} | n \geq 1\}).$$

Seja $N = K_2(\{(c + di)^{1/2^n} | n \geq 1\})$. O polinômio mínimo de $(c + di)^{1/2^n}$ sobre K é

$$f(X) = [X^{2^n} - (c + di)][X^{2^n} - (c - di)] = X^{2^{n+1}} - 2cX^{2^n} - 1.$$

Observando que $[(c + di)^{1/2^n}(c - di)^{1/2^n}]^{2^n} = -1$, obtemos $(c - di)^{1/2^n} = \varepsilon_{n+1}^j (c + di)^{1/2^n}$ para algum j . Portanto $K_2((c + di)^{1/2^n})$ é a extensão normal de K gerada pelas raízes

de $f(X)$ e, conseqüentemente, N é extensão normal de K . Mostra-se também que $G(N; K) \cong \mathbb{Z}_2$.

Seja agora $F = K(\{a^{1/2^n} | n \geq 1\})$. Por construção, temos $N \cap F = K$ e $N \cdot F = K(2)$.

Seja τ o N -automorfismo que satisfaz $\tau(a^{1/2^n}) = \varepsilon_n a^{1/2^n}$ para todo $n \geq 1$ e σ o F -automorfismo que satisfaz $\sigma((c + di)^{1/2^n}) = (c - di)^{1/2^n}$. Pela construção de τ e σ , obtemos

$$\sigma\tau\sigma^{-1}(\varepsilon_n a^{1/2^n}) = \sigma\tau(\sigma^{-1}(\varepsilon_n) a^{1/2^n}) = \varepsilon_n \sigma(\varepsilon_n a^{1/2^n}) = \varepsilon_n \sigma(\varepsilon_n) a^{1/2^n}.$$

Mas $\sigma|_{K_2} \neq id$ e portanto $\varepsilon_n \sigma(\varepsilon_n) = N_{K_2|K}(\varepsilon_n) = 1$. Como $\tau^{-1}(a^{1/2^n}) = \varepsilon_n^{-1} a^{1/2^n}$ podemos concluir que $\sigma\tau\sigma^{-1} = \tau^{-1}$, o que prova (a).

(b) Já observamos que, se $r > 2$, então $G(L; K) \cong \mathbb{Z}_2$. Para provar a última afirmação, seja $m \geq 2$ um inteiro tal que $\varepsilon_m \in K_2 = K(i)$ e $\varepsilon_{m+1} \notin K_2$. Portanto, como foi observado antes do início da prova, ξ_{m+1} e $\eta_{m+1} \notin K_2$. Suponha que $G(L; K)$ não seja cíclico. Neste caso, $G(L; K) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ e, para todo $n \geq m+1$, $K(\xi_n)$ é uma extensão cíclica de K em L , de grau 2^{n-m} .

K tem exatamente três extensões quadráticas: K_2 , $K(\xi_{m+1})$ e $K(i\xi_{m+1})$, todas elas contidas em L . Seja $N = K(\xi_{m+1})$. Por ([W], Corollary 2.10), N é também C -corpo e possui quatro classes quadráticas por ([W], Theorem 3.2). Portanto N tem três extensões quadráticas, quais sejam, $N(i) = K_2(\xi_{m+1}) = K_{m+1}$, $N(\xi_{m+2}) = K(\xi_{m+2})$ e $N(i\xi_{m+2}) = K(i\xi_{m+2})$. Se $\xi_{m+1}^{1/2} \in K_2(\xi_{m+1})$, então $\xi_{m+1} \in K_2$ contradizendo nossa hipótese. Portanto $N(\xi_{m+1}^{1/2})$ é uma das duas outras extensões de N , as quais são extensões galoisianas de K . Como $\xi_{m+1}^{1/2}$ é raiz do polinômio $X^4 - (2 + \xi_m)$, a hipótese de que $N(\xi_{m+1}^{1/2})$ seja extensão galoisiana de K implica $i \in N(\xi_{m+2})$ ou $i \in N(i\xi_{m+2})$, o que não pode ocorrer, haja visto que $N(i)$, $N(\xi_{m+2})$ e $N(i\xi_{m+2})$ são extensões distintas de K . Desta contradição obtemos $G(L; K) \cong \mathbb{Z}_2$.

Para encerrar a prova, observamos que, se $\varepsilon_3 \notin K_2$, então $2^{1/2} = \xi_3 \notin K_2$ e portanto $K(2^{1/2}) \neq K_2$. Como $K(2^{1/2}) \subsetneq L$, segue-se que K_2 não é a única extensão

quadrática de K em L . Portanto, $G(L; K)$ não é cíclico. ■

(II.2.5) Teorema. *Seja K um corpo tal que $G(K)$ é não abeliano e contém um subgrupo normal U , com $U \cong \mathbb{Z}_2$ e $C(U) = U$. Então K é um C-corpo, $(K^* : K^2) = 4$, $\mathcal{B} = \pm K^2$ ($\neq K^*$) e $G(K) = \langle \tau \rangle \rtimes \langle \sigma \rangle$, onde K , τ e σ satisfazem a uma das condições seguintes:*

- (a) K é $K(2)$ -pitagórico (cf. [B]) ^(*) com 2 ordens, $\sigma^2 = 1$ e $\sigma\tau\sigma = \tau^{-1}$. Neste caso, $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$.
- (b) $-1 \notin K^2$ e existe $m \geq 2$ tal que $\varepsilon_{m+1} \in K(i)$ e $\varepsilon_{m+2} \notin K(i)$. Neste caso, $\sigma\tau\sigma^{-1} = \tau^{2^m-1}$ e $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$.
- (c) Existe $m \geq 2$ tal que $\varepsilon_m \in K$ e $\varepsilon_{m+1} \notin K$. Neste caso, $\sigma\tau\sigma^{-1} = \tau^{2^m+1}$ e $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$.

PROVA. Seja $\varphi : G(K) \longrightarrow \text{Aut}(U) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ o homomorfismo dado por $\varphi(g)(u) = gug^{-1}$, para todo $u \in U$ e $g \in G(K)$. Como $C(U) = U$, temos $\text{Kernel}(\varphi) = C(U) = U$. Temos então que G é metabeliano (cf. [W1]) e, para todo $u \in U$ $gug^{-1} = u^\alpha$ para algum $\alpha \in \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \cong \text{Aut}(U)$.

Por ([W1], Theorem 4.5), K é C-corpo e portanto $\mathcal{B} = \pm K^2$ por ([W], Theorem 1.9). Como $\text{Im}(\varphi) \subseteq \text{Aut}(U)$ temos três casos a serem examinados.

1º caso. $\text{Im}(\varphi) = \{\pm 1\}$.

Tomamos $\sigma \in \varphi^{-1}(-1) \subseteq G(K)$. Então $\sigma u \sigma^{-1} = u^{-1}$ para todo $u \in U$ e $\varphi(\sigma)^2 = 1$ implica $\sigma^2 \in U$. Mas $(\sigma^2)^{-1} = \sigma(\sigma^2)\sigma^{-1} = \sigma^2$, o que implica $\sigma^2 = 1$, ou seja, σ é uma involução de $G(K)$. Assim a sequência exata

$$1 \longrightarrow U \longrightarrow G(K) \longrightarrow \{\pm 1\} \longrightarrow 1$$

é cindida e $G(K)$ é o produto semidireto $U \rtimes \langle \sigma \rangle$. Se τ é um gerador de U , temos então $\sigma\tau\sigma^{-1} = \tau^{-1}$, como queríamos. Além disso, $(K^* : K^2) = 2^{r(G(K))} = 4$.

Do fato de σ e $\sigma\tau$ serem involuções que não estão numa mesma classe de conjugação,

(*) O conceito de corpo $K(2)$ -pitagórico está na introdução do capítulo III.

deduzimos que K é um corpo formalmente real com pelo menos duas ordens distintas ([B], Chapter II, Theorem 4, pg. 78). Como K tem quatro classes quadráticas, K tem exatamente duas ordens e portanto o 1º caso implica (a).

2º caso. $Im(\varphi) \subseteq 1 + 4\mathbb{Z}_2$.

Neste caso $Im(\varphi) \cong \mathbb{Z}_2$ é um pro-2-grupo livre e a seguinte seqüência exata é cindida

$$1 \longrightarrow U \longrightarrow G(K) \longrightarrow \mathbb{Z}_2 \longrightarrow 1.$$

Portanto, $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$ e, assim, $(K^* : K^2) = 2^{r(G(K))} = 4$.

Seja L o corpo obtido de K por adjunção de todas as raízes 2^n -ésimas de 1, para todo $n \geq 1$. Pelo Lema (II.2.4), $G(L; K) \cong \mathbb{Z}_2$. Por ([W1], Theorem 4.1-(2)), $G(L)$ é abeliano e assim, pelo Lema (II.2.2), $G(L) = U$.

Consideremos agora duas possibilidades: $-1 \in K^2$ ou $-1 \notin K^2$. Para cada caso construiremos uma extensão $F|K$ tal que $LF = K(2)$, $L \cap F = K$ e $G(F) \cong \mathbb{Z}_2$.

$$\begin{array}{ccc} & LF = K(2) & \\ & \swarrow \quad \searrow & \\ L & & F \\ & \swarrow \quad \searrow & \\ & K = L \cap F & \end{array}$$

Se $-1 \notin K^2$, então existe $r \geq 3$ tal que $\varepsilon_r \in K(i)$, pelo Lema (II.2.4). Como $K(i)$ é também um C-corpo por ([W], Corollary 2.10) e $G(K)$ não possui subgrupo abeliano de índice dois, existe $s \geq 1$ tal que $\varepsilon_s \notin K(i)$, por ([W], Theorem 3.6). Assim, existe $m \geq 2$ tal que $\varepsilon_{m+1} \in K(i)$ e $\varepsilon_{m+2} \notin K(i)$.

Por outro lado, $K^* = \pm K^2 \cup \pm aK^2$, para algum $a \in K$. Seja $F = K(\{a^{1/2^n} | n \geq 1\})$. Da maneira pela qual $G(K)$ foi descrito, tiramos $LF = K(2)$ e, como $K(i)$ é a única extensão quadrática de K dentro de L e $-1 \notin q(F)$, segue-se que $L \cap F = K$. Temos

assim $G(F) \cong G(L; L \cap F) \cong \mathbb{Z}_2$ e $K(2) = L(\{a^{1/2^n} | n \geq 1\})$.

Por outro lado, também temos $K(2) = F(\varepsilon_\infty)$ e, de $L \cap F = K$, segue que $\varepsilon_{m+1} \in F(i)$ e $\varepsilon_{m+2} \notin F(i)$. Se σ é o F -automorfismo não trivial de $F(i)$, então temos $(\varepsilon_{m+1}\sigma(\varepsilon_{m+1})) \in F$ e $(\varepsilon_{m+1}\sigma(\varepsilon_{m+1}))^{2^{m+1}} = 1$. Portanto, $(\varepsilon_{m+1}\sigma(\varepsilon_{m+1})) = \pm 1$ e $\sigma(\varepsilon_{m+1}) = \pm \varepsilon_{m+1}^{-1}$. De $\sigma(\varepsilon_{m+1}) = \varepsilon_{m+1}^{-1}$ obtemos $\xi_{m+1} \in F$ e, como $\varepsilon_{m+2} \notin F(i)$, temos também $\xi_{m+2} \notin F(i)$. Portanto, $F(\xi_{m+1})$ também é uma extensão quadrática de F em $K(2)$. Mas isto não pode ocorrer pois $G(F)$ é cíclico. Assim, $\sigma(\varepsilon_{m+1}) = -\varepsilon_{m+1}^{-1}$, resultando que $\sigma(\varepsilon_n) = \varepsilon_n^{-1}$, para todo n , $1 \leq n \leq m$. Portanto, existem um F -automorfismo σ e um L -automorfismo τ , tais que $\sigma(\varepsilon_{m+n}) = \varepsilon_{m+n}^{2^m-1}$, e $\tau(a^{1/2^n}) = \varepsilon_n a^{1/2^n}$, para todo $n \geq 1$. Como vale também $\sigma(\varepsilon_n) = (\varepsilon_n)^{2^m-1}$ para todo n , $1 \leq n \leq m$, é imediato que $\sigma\tau\sigma^{-1} = \tau^{2^m-1}$ e obtemos (b).

Vejamos agora o caso $-1 \in K^2$. Se $\varepsilon_m \in K$, e $\varepsilon_{m+1} \notin K$, para $m \geq 2$, então $K^* = K^2 \cup \varepsilon K^2 \cup aK^2 \cup a\varepsilon_m K^2$. Novamente, o corpo $F = K(\{a^{1/2^n} | n \geq 1\})$ tem as propriedades desejadas. Então existe um F -automorfismo σ e um L -automorfismo τ tais que $\sigma(\varepsilon_{m+n}) = \varepsilon_{m+n}^{2^n+1}$ e $\tau(a^{1/2^n}) = \varepsilon_n a^{1/2^n}$, para $n \geq 1$. Outra vez, $\sigma\tau\sigma^{-1} = \tau^{2^m+1}$ e obtemos o caso (c).

3º caso. $Im(\varphi) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Neste caso, Seja $S = \varphi^{-1}(\mathbb{Z}/2\mathbb{Z})$. S é um subgrupo normal de $G(K)$ tal que $U \subseteq S$ e $|\varphi(S)| = 2$. É claro que o centralizador de U em S também é U . Portanto, pelo 1º caso, $S = U \rtimes \langle \sigma \rangle$, para alguma involução $\sigma \in G(K)$. Então K é um corpo formalmente real e, como é C-corpo, $G(K) \cong \mathbb{Z}_2^\alpha \rtimes \mathbb{Z}/2\mathbb{Z}$, por ([B], Theorem 15, pg. 118). Desse modo, se $\alpha \neq 1$, temos uma contradição com $C(U) = U$ e, se $\alpha = 1$, temos uma contradição com $Im(\varphi) = \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. Ou seja, o 3º caso não pode ocorrer e isto encerra a prova. ■

(II.2.6) Corolário. Seja K um corpo tal que $G(K)$ satisfaz (II.2.5) (b) ou (c) e seja $\mathcal{O}$ o anel de valorização cuja existência foi assegurada pelo Teorema (I.3.6). Então $G^T(\tilde{\mathcal{O}}; K)$ é o maior subgrupo abeliano normal de $G(K)$.

PROVA. $G(K)$ satisfaz as hipóteses de (II.2.2) e todo subgrupo abeliano normal de $G(K)$ está contido em $\langle \tau \rangle$.

1º caso. K satisfazendo (b).

Temos que $(K^* : \mathcal{B}) = 2$ e K não é excepcional, por hipótese. Como $\mathcal{B} \neq K^2$, por (I.3.8) $\mathcal{K}_{\mathcal{O}}$ não é quadrático separavelmente fechado e daí, por ([E], Corollary 19.9), $G^T(\tilde{\mathcal{O}}; K)$ é não trivial. Como $\mathcal{O}$ é não diádico, $G^T(\tilde{\mathcal{O}}; K)$ é também abeliano e conseqüentemente, por (II.2.2), isomorfo a $\mathbb{Z}_2$ e está contido em $\langle \tau \rangle$. Seja L o corpo fixo de $\langle \tau \rangle$. Temos $G^T(\tilde{\mathcal{O}}; L) = G^T(\tilde{\mathcal{O}}; K)$ e portanto, $(G(L) : G^T(\tilde{\mathcal{O}}; K))$ não pode ser finito, a menos que seja 1 (cf. [E], Corollary 19.9). Como $G(L) \cong \mathbb{Z}_2$ só tem subgrupos próprios de índice finito, concluímos que $G^T(\tilde{\mathcal{O}}; K) = G(L)$.

2º caso. K satisfazendo (c).

Temos $\mathcal{B} = K^2$ e $(K^* : \mathcal{B}) = 4$. Como $\mathcal{O}$ é não diádico, por (I.3.6), $G^T(\tilde{\mathcal{O}}; K)$ é um subgrupo abeliano e normal de $G(K)$ e portanto contido em $\langle \tau \rangle$. Logo $\mathcal{O} \notin \mathcal{H}_2(K)$ pois $G(K)$ não é abeliano (ver (I.3.8)-(a)). Assim, $\mathcal{O} \in \mathcal{H}_1(K)$ e a prova segue como no caso anterior. ■

(II.2.7) Observações. (a) Por ([EV], Section 5), existem corpos que possuem $G(K)$ como foi descrito em (II.2.5).

(b) No caso (a), pode ou não ocorrer a existência de um anel de valorização 2-henseliano próprio. Por exemplo:

(b)-1. Seja $K = R_1 \cap R_2$, onde R_1 e R_2 são dois fechos reais de $\mathbb{Q}(2^{1/2})$ tais que $2^{1/2} \in q(R_1)$, mas $2^{1/2} \notin q(R_2)$. Denotamos por Ω o fecho algébrico de $\mathbb{Q}$ e por σ_i o único automorfismo não trivial do grupo total de Galois $G(\Omega; R_i)$, $i = 1, 2$. Observando que $G(\Omega; K)$ é gerado por $\{\sigma_1, \sigma_2\}$, concluímos que $G(\Omega : K) \cong \langle \tau \rangle \rtimes \langle \sigma_1 \rangle$, onde $\tau = \sigma_1 \sigma_2$. Assim, o pro-2-grupo quociente maximal $G(K)$ de $G(\Omega; K)$ é isomorfo a $\mathbb{Z}_2 \rtimes \langle \sigma_1 \rangle$ e é do tipo (a). Por outro lado K é um corpo formalmente

real com 2 ordens e por ([B], Theorem 1, pg. 86), é corpo $K(2)$ -pitagórico. Finalmente, para todo anel de valorização C de Ω temos que, ou $K^Z(C; K(i)) = \Omega$, ou então $K^Z(C; K(i))$ é uma extensão finita de $K(i)$ e portanto de K também. Isto é consequência de $G(\Omega; K) = \langle \tau \rangle$ ser um grupo cíclico.

Assumimos então que $K^Z(C; K(i))$ é uma extensão finita de K . Então, por ([En], Theorem 3.7 e Theorem 3.15), existe um anel de valorização henseliano A de K com corpo de resíduos real fechado. Mas isto não é possível, pois $A \cap \mathbb{Q}$ sendo um anel de valorização de $\mathbb{Q}$ tem corpo de resíduos com característica diferente de zero. Assim, $K^Z(C; K(i)) = \Omega$ para todo anel de valorização C de Ω . Portanto, temos também $K^Z(C; K(i)) = K(2)$, para todo anel de valorização C de $K(2)$ e portanto K não possui anel de valorização 2-henseliano.

(b)-2. Por outro lado, se $K = \mathbb{R}((X))$, o corpo de séries de potências sobre $\mathbb{R}$, então K satisfaz o caso (a), $\mathcal{O} = \mathbb{R}[[X]]$ e $G^T(\tilde{\mathcal{O}}; K) = G(K(i))$ é o maior subgrupo abeliano normal de $G(K)$.

Parece bem natural que um pro-2-grupo livre não isomorfo a $\mathbb{Z}_2$ não possa conter um subgrupo abeliano normal não trivial. Para pro-2-grupos livres finitamente gerados isto segue da “Proposition” 3.3 de [Lu].

No próximo Corolário damos, de maneira geral, uma prova simples desse resultado. Obtemos daí que o estudo dos subgrupos abelianos normais de $G(K)$, para corpos com característica dois não é interessante.

(II.2.8) Corolário.

- (a) Se G é um pro-2-grupo livre de posto maior que 1, então $\{1\}$ é o maior subgrupo abeliano normal de $G(K)$.
- (b) Se K for um corpo de característica dois e posto de $G(K)$ maior que 1, então $\{1\}$ é o maior subgrupo abeliano normal de $G(K)$.

PROVA. (a) Se G é um pro-2-grupo livre, por ([HJ], Theorem 10.4), existe um corpo

K tal que $G = G(K)$. Como qualquer subgrupo U de um pro-2-grupo livre é também livre, se U for um subgrupo abeliano e não trivial de G , então $U \cong \mathbb{Z}_2$. Pela Proposição (II.2.1)(b), $C(U) = U$ o que contradiz o Teorema (II.2.5) que descreve U como não sendo livre.

(b) É imediato pois, por ([R] Corollary 3.4, pg. 257) $G(K)$ é pro-2-grupo livre para corpos com característica dois. ■

CAPÍTULO III

SUBGRUPOS ABELIANOS DE $G(K)$

1. Introdução.

No Parágrafo 2 deste capítulo concluímos o estudo dos subgrupos abelianos normais maximais de $G(K)$. O Teorema (III.2.6) estabelece a existência, para todo corpo K , de um maior subgrupo abeliano normal $\mathfrak{U}$ de $G(K)$ e descreve as possibilidades para $\mathfrak{U}$. A descrição de $\mathfrak{U}$, para corpos excepcionais, depende dos conceitos de corpos $K(2)$ -pitagóricos (já citados no capítulo II) ou superpitagóricos que, por sua vez se relacionam com o conceito de “*fan*” conforme descrito abaixo. Nosso ponto de partida foi o Teorema (III.2.1), devido a Ware.

No parágrafo 3, como aplicação, generalizamos para corpos quaisquer, resultados de Ware que relacionam os subgrupos de K^* que contêm $\mathcal{B}$ e os subgrupos abelianos normais de $G(K)$.

Generalizamos também o estudo de subgrupos abelianos de $G(K)$ que não sejam necessariamente normais, também devidos a Ware e obtemos melhores cotas para o invariante $a(K)$ de Ware (ver [W4]).

Notações e conceitos preliminares: Neste capítulo utilizamos as notações dos capítulos anteriores e descrevemos as noções de “*fan*”, corpos $K(2)$ -pitagóricos ou superpitagóricos. Segundo Bröcker ([Br]), que propôs o termo “estritamente pitagórico”, os corpos superpitagóricos foram introduzidos por Diller e Dress em [DD]. Um corpo pitagórico K é superpitagórico se K^2 é um “*fan*”, isto é, se todo subgrupo do grupo multiplicativo K^* , com índice dois e que não contenha -1 , é uma ordem de K . Mais geralmente, uma pre-ordem S do corpo K é um “*fan*” se qualquer subgrupo P de K^* que

contém S e tal que $(K^* : P) = 2$ e $-1 \notin P$ é uma ordem de K .

Se K é um corpo formalmente real e pitagórico, K é $K(2)$ -pitagórico se é hereditariamente pitagórico com respeito a $K(2)$, isto é, dada qualquer subextensão L de $K(2)|K$, L é também pitagórico. Conforme ([B], Theorem 2 pg. 89), uma condição necessária e suficiente para que isto aconteça é K ser superpitagórico, ou seja, K é pitagórico e K^2 é um “fan”.

Por outro lado, conforme ([L2], Corollary 5.16, pg. 46), um corpo formalmente real K é hereditariamente pitagórico com respeito a $K(2)$ se, e somente se, K é formalmente real, pitagórico e, para todo $x \in K$, $x \notin \pm K^2$, x é rígido. Assim, K excepcional com $-1 \notin K^2$ é equivalente a K ser $K(2)$ -pitagórico.

2. Subgrupos Abelianos Normais Máximos.

(III.2.1) Teorema ([W4], Theorem 3.6). *Se K é um corpo com $(K^* : K^2) > 2$, então as seguintes afirmações são equivalentes:*

- (a) $\mathcal{B} = K^2$ e $\varepsilon_n \in K$ para todo $n \geq 1$
- (b) $G(K)$ é um grupo abeliano. ■

(III.2.2) Corolário. *Seja K um corpo que satisfaz as condições equivalentes do teorema anterior. Então K satisfaz as hipóteses do Teorema (I.3.6) e, ou $G(K) = G^T(\tilde{\mathcal{O}}; K)$, ou então $G(K) = G^T(\tilde{\mathcal{O}}; K) \times \mathbb{Z}_2$.*

PROVA. Como $\mathcal{B} = K^2$ e $(K^* : K^2) > 2$, pela Proposição (I.3.7), K possui um anel de valorização 2-henseliano não diádico A tal que Γ_A não é 2-divisível. Aplicando (I.3.6)-(b), temos que $(\mathcal{K}_{\mathcal{O}}^* : \mathcal{B}(\mathcal{K}_{\mathcal{O}})) \leq 2$.

Se $(\mathcal{K}_{\mathcal{O}}^* : \mathcal{K}_{\mathcal{O}}^2) > 2$, como $G(\mathcal{K}_{\mathcal{O}})$ é um quociente de $G(K)$ ([E], Theorem 19.6 pg. 147) que

é abeliano, é também abeliano e teríamos, pelo teorema anterior, $\mathcal{K}_{\mathcal{O}}^2 = B(\mathcal{K}_{\mathcal{O}})$ (K^2 representa o grupo multiplicativo dos quadrados não nulos do corpo K), o que contradiz a primeira desigualdade.

Desse modo, temos $(\mathcal{K}_{\mathcal{O}}^* : \mathcal{K}_{\mathcal{O}}^2) \leq 2$. Se $\mathcal{O}$ tiver corpo de resíduos quadraticamente fechado, então $G(K) = G^T(\tilde{\mathcal{O}}; K)$, se não, a segunda igualdade ocorre. ■

(III.2.3) Lema. *Seja K um corpo com $(K^* : K^2) > 2$ e tal que $G(K)$ contenha um subgrupo abeliano normal não trivial U . Então $\mathcal{B} \neq K^*$.*

PROVA. Se $G(K)$ for abeliano, segue de (III.2.1) que $\mathcal{B} = K^2 \neq K^*$. Suponhamos então que $G(K)$ é não abeliano e $U \cong \mathbb{Z}_2$. Se existe um subgrupo abeliano normal U' de $G(K)$, tal que $U \subseteq U'$, $U' \cong \mathbb{Z}_2$ e $C(U') = U'$, o resultado segue de (II.2.5), caso contrário, pela Proposição (II.2.1)-(b), existe um subgrupo S de $G(K)$ tal que $U \subseteq S$ e $S \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Sejam L e F os corpos fixos de U e S respectivamente. Então $F \subseteq L$ e, como $(F^* : F^2) = 4$ e $G(F) = S$ é abeliano, pelo Teorema (III.2.1) temos também $B(F) = F^2$. Novamente, aplicando a Proposição (I.3.7) e o Teorema (I.3.6) a F , obtemos que $O(F)$ é um anel de valorização 2-henseliano não diádico próprio de F . Observemos que L , F e $O(F)$ satisfazem as hipóteses da Proposição (I.3.9) e portanto $\mathcal{B} \neq K^*$, pelo Teorema (I.3.6)-(a). Suponhamos agora que $r(U) > 1$. Seja E o corpo fixo de U . Nesse caso $B(E) = E^2$ por (III.2.1). Portanto, pela Proposição (I.3.7) e pelo Teorema (I.3.6), obtemos que $O(E)$ é anel de valorização 2-henseliano próprio não diádico de E . Como $F = E$ e $C = O(E)$ satisfazem as condições da Proposição (I.3.9), pelo Teorema (I.3.6)-(a), novamente obtemos $\mathcal{B} \neq K^*$. ■

O Teorema (III.2.4) a seguir é uma generalização do Teorema de Ware para corpos que não sejam de classe C . Observamos que se K não é C -corpo, então K não é excepcional.

(III.2.4) Teorema. Se K não é C -corpo, $(K^* : K^2) > 2$ e $\mathcal{B} \neq K^*$, então K satisfaz as hipóteses do Teorema (I.3.6) e $G^T(\tilde{\mathcal{O}}; K)$ é o maior subgrupo abeliano normal de $G(K)$. Além do mais,

$$r(G^T(\tilde{\mathcal{O}}; K)) = r(K^*/\mathcal{B}).$$

PROVA. Pela Proposição (I.3.7) e pelo Teorema (I.3.6) $G^T(\tilde{\mathcal{O}}; K)$ é um subgrupo abeliano normal de $G(K)$ e por ([E], Theorem 20.12) $r(G^T(\tilde{\mathcal{O}}; K)) = r(\Gamma_{\tilde{\mathcal{O}}}/\Gamma_{\mathcal{O}})$, pois, como $\mathcal{O}$ é não diádico, $G^V(\tilde{\mathcal{O}}; K)$ é trivial. Por outro lado, $\mathcal{O}^*K^2 = \mathcal{B}$, pelo Teorema (I.3.6), acarreta $r(\Gamma_{\tilde{\mathcal{O}}}/\Gamma_{\mathcal{O}}) = r(K^*/\mathcal{B})$.

Agora seja U um subgrupo abeliano normal de $G(K)$. Temos 2 casos a considerar: $r(U) = 1$ e $r(U) > 1$.

1º Caso. $U \cong \mathbb{Z}_2$. Seja F o corpo fixo de U . Por ([E], 19.10) temos que $G^T(\tilde{\mathcal{O}}; F) = G^T(\tilde{\mathcal{O}}; K) \cap U$. O diagrama nº 1 ilustra a situação descrita, com a posição dos corpos fixos desses grupos. Por ([E], Corollary 19.9), sabemos que $(G(F) : G^T(\tilde{\mathcal{O}}; F))$ não pode ser finito, a menos que $G(F) = G^T(\tilde{\mathcal{O}}; F)$. Podemos então concluir que, ou $G^T(\tilde{\mathcal{O}}; K) \cap U = \{1\}$, ou então $U \subseteq G^T(\tilde{\mathcal{O}}; K)$.

Se $G^T(\tilde{\mathcal{O}}; K) \cap U = \{1\}$, o que equivale dizer que $K^T(\tilde{\mathcal{O}}; F) = K(2)$, então obtemos

$$UG^T(\tilde{\mathcal{O}}; K)/G^T(\tilde{\mathcal{O}}; K) \cong U/U \cap G^T(\tilde{\mathcal{O}}; K) \cong U \cong \mathbb{Z}_2$$

Mas

$$UG^T(\tilde{\mathcal{O}}; K)/G^T(\tilde{\mathcal{O}}; K) \cong G(K^T(\tilde{\mathcal{O}}; K); F \cap K^T(\tilde{\mathcal{O}}; K)).$$

Por ([E], Theorem 19.13), este último grupo é isomorfo a $G(\mathcal{K}(2); \mathcal{K})$, onde $\mathcal{K}$ é o corpo de resíduos de $\tilde{\mathcal{O}} \cap (F \cap K^T(\tilde{\mathcal{O}}; K))$. Assim, $\mathbb{Z}_2 \cong G(\mathcal{K}(2); \mathcal{K})$, que é um subgrupo normal de $G(\mathcal{K}_{\mathcal{O}})$.

Afirmamos que $(\mathcal{K}_{\mathcal{O}}^* : \mathcal{K}_{\mathcal{O}}^2) > 2$.

Pela afirmação, as hipóteses do Lema (III.2.3) estão satisfeitas e portanto $B(\mathcal{K}_{\mathcal{O}}) \neq \mathcal{K}_{\mathcal{O}}^*$, o que contradiz o Teorema (I.3.6)(b), pois K é não excepcional. Portanto, $U \subseteq G^T(\tilde{\mathcal{O}}; K)$.

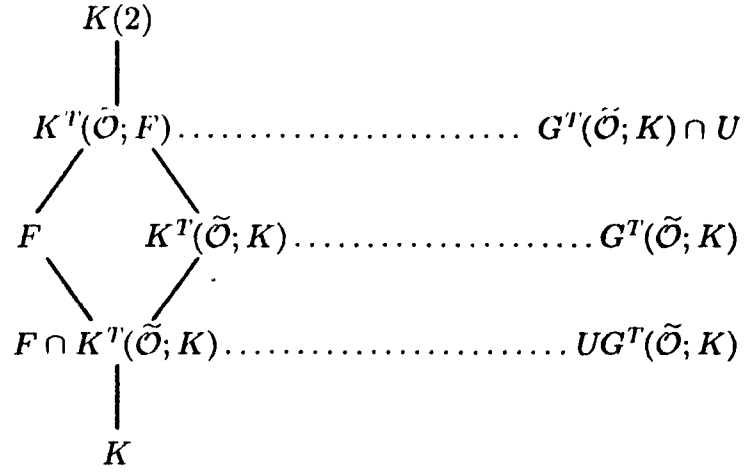


Diagrama nº 1

Prova da afirmação: Se $(\mathcal{K} : \mathcal{K}_{\mathcal{O}}^2) = 1$, então $\mathcal{O} \in \mathcal{H}_2(K)$ e teríamos, pela Proposição (I.3.8), $B = K^2$ e K seria C -corpo, contra a hipótese. Assumindo $(\mathcal{K}^* : \mathcal{K}^2) = 2$, teríamos $G(\mathcal{K}_{\mathcal{O}}) \cong \mathbb{Z}_2$ e portanto $\mathcal{K}$ seria extensão finita de $\mathcal{K}_{\mathcal{O}}$ e $F \cap K^T(\tilde{\mathcal{O}}; K)$ também seria extensão finita de K . Mas $U = G(F)$ e $G^T(\tilde{\mathcal{O}}; K)$ são subgrupos abelianos normais de $G(K)$ cuja interseção é trivial. Assim, $G(F \cap K^T(\tilde{\mathcal{O}}; K)) \cong G(F) \times G^T(\tilde{\mathcal{O}}; K)$ é um grupo abeliano com posto maior que 1. Pelo Teorema (III.2.1), $F \cap K^T(\tilde{\mathcal{O}}; K)$ seria C -corpo. Por ([W], Corollary 2.11), K também seria C -corpo, contra a hipótese. Assim, a afirmação é verdadeira.

2º caso. $r(U) > 1$.

Seja F o corpo fixo de U e $C = \tilde{\mathcal{O}} \cap F$.

(A) Se $C \in \mathcal{H}_2(F)$, então $G(F) = G^T(\tilde{\mathcal{O}}; F) = G(F) \cap G^T(\tilde{\mathcal{O}}; K)$, sendo a primeira igualdade decorrência de (I.2.17)(b) e do fato de C ser não diádico. A segunda decorre de ([E], 19.10-b).

Logo, $U = G(F) \subseteq G^T(\tilde{\mathcal{O}}; K)$.

(B) Assumimos então $C \notin \mathcal{H}_2(F)$.

Seja $A = O(F) \cap K$. Então $c(\mathcal{K}_A) = c(\mathcal{K}_{O(F)}) \neq 2$ e, como o grupo de valores de $O(F)$ não possui subgrupo convexo 2-divisível não trivial, o mesmo acontece com A , pela Proposição (I.3.9).

Se $A \in \mathcal{H}(K)$, então pelo Teorema (I.3.6)(e), $\mathcal{O} \subseteq A$ e então $C \subseteq O(F)$. Portanto, $G^T(\tilde{\mathcal{O}}; F) = G^T(\widetilde{O(F)}; F)$, pela Proposição (I.3.8)-(b), pois $\tilde{\mathcal{O}} = \tilde{C}$. Por outro lado, como $C \notin \mathcal{H}_2(F)$ e $C \subseteq O(F)$, temos $O(F) \notin \mathcal{H}_2(F)$ e assim $G(F) \neq G^T(\widetilde{O(F)}; F)$. Deste modo, $G(F) \cong G^T(\widetilde{O(F)}; F) \times \mathbb{Z}_2$, pelo Corolário (III.2.2) e concluimos com

$$G(F) \cong G^T(\tilde{\mathcal{O}}; F) \times \mathbb{Z}_2.$$

Estamos agora na situação ilustrada pelo diagrama nº 1. Como no 1º caso, seja $\mathcal{K}$ o corpo de resíduos de $\mathcal{O} \cap (F \cap K^T(\tilde{\mathcal{O}}; K))$. Temos $G(\mathcal{K}) \cong \mathbb{Z}_2$ é subgrupo normal de $G(\mathcal{K}_{\mathcal{O}})$. Se $(\mathcal{K}_{\mathcal{O}}^* : \mathcal{K}_{\mathcal{O}}^2) > 2$, então pelo Lema (III.2.3) $B(\mathcal{K}_{\mathcal{O}}) \neq \mathcal{K}_{\mathcal{O}}^*$ o que contradiz o Teorema (I.3.6)-(b) pois K não é excepcional.

Se $(\mathcal{K}_{\mathcal{O}}^* : \mathcal{K}_{\mathcal{O}}^2) = 1$ então, de maneira análoga ao que foi feito no 1º caso, obtemos que K é C -corpo, contra a hipótese. Deste modo, temos $A \notin \mathcal{H}(K)$ e portanto, pelo Teorema (I.2.7) existe um anel de valorização D de F tal que

$$O(F) \subsetneq D \subseteq C, D \cap K \in \mathcal{H}(K) \text{ e } G(F) \subseteq G^T(\tilde{D}; K).$$

Como $O(F) \subsetneq D$ e $O(F)$ não é diádico, o mesmo acontece com D . Portanto $G^T(\tilde{D}; K) = G^T(\tilde{\mathcal{O}}; K)$ pela Proposição (I.3.8)(b). Portanto $U = G(F) \subseteq G^T(\tilde{\mathcal{O}}; K)$. ■

O Teorema (III.2.5), a seguir, generaliza o Teorema (II.2.5)(c) e o Corolário (II.2.6) para C -corpos arbitrários que não contenham todas as raízes 2^n -ésimas da unidade, para $n \geq 1$. Este resultado complementa ([W1], 4.1 e 4.3).

As construções a seguir serão utilizadas na prova do Teorema (III.2.5). Seja K um corpo para o qual exista o anel $\mathcal{O}$, Λ um conjunto com cardinalidade igual a $r(K^*/\mathcal{O}^*T)$.

Afirmamos que existe um conjunto $\{a_\lambda \mid \lambda \in \Lambda\} \subset K^*$ que é uma $\mathbb{F}_2$ base de $K^T(\tilde{\mathcal{O}}; K)$ módulo $(K^T(\tilde{\mathcal{O}}; K))^2$.

Prova da afirmação: É suficiente mostrar que

$$\varphi: K^*/\mathcal{O}^*K^2 \longrightarrow (K^T(\tilde{\mathcal{O}}; K))^*/(K^T(\tilde{\mathcal{O}}; K))^2,$$

definida por $\varphi(x\mathcal{O}^*K^2) = x(K^T(\tilde{\mathcal{O}}; K))^2$ é isomorfismo. Seja $x \in K^*$ com $x = y^2$ para algum $y \in K^T(\tilde{\mathcal{O}}; K)$. Como $\tilde{\mathcal{O}} \cap K^T(\tilde{\mathcal{O}}; K)$ e $\mathcal{O}$ têm o mesmo grupo de valores, $x \in \mathcal{O}^*K^2$, ou seja, φ é injetora. Seja agora $y \in (K^T(\tilde{\mathcal{O}}; K))^*$. A mesma observação sobre os grupos de valores envolvidos implica a existência de x em K^* , com yx^{-1} sendo unidade de $\tilde{\mathcal{O}} \cap K^T(\tilde{\mathcal{O}}; K)$. Como o corpo de resíduos desse último é quadraticamente fechado, existe outra unidade $z \in \tilde{\mathcal{O}} \cap K^T(\tilde{\mathcal{O}}; K)$ tal que $yx^{-1} = z^2$, provando assim a afirmação.

Usaremos a base acima para construir um sistema conveniente de geradores de $G^T(\tilde{\mathcal{O}}; K)$.

Pelo Teorema (1.3.6)-(c), $\mathcal{O}$ é não diádico e portanto $G^V(\tilde{\mathcal{O}}; K)$ é trivial (cf. [E], Corollary 20.18) e portanto $G(K^T(\tilde{\mathcal{O}}; K)) = G^T(\tilde{\mathcal{O}}; K)$ é abeliano. Então por (III.2.1), $\varepsilon_n \in K^T(\tilde{\mathcal{O}}; K)$ para todo $n \geq 1$ e, assim, por ([W], Corollary 3.9-(1)), $K(2)$ é o corpo obtido de $K^T(\tilde{\mathcal{O}}; K)$ por adjunção de todas as raízes 2^n -ésimas de a_λ , para todos $n \geq 1$ e $\lambda \in \Lambda$. Podemos escolher então um sistema de geradores $\{\tau_\lambda \mid \lambda \in \Lambda\}$ do grupo $G^T(\tilde{\mathcal{O}}; K)$ (que é isomorfo a $\mathbb{Z}_2^A$) assim caracterizados: Para cada $\gamma \in \Lambda$,

$$\begin{cases} \tau_\gamma(a_\gamma^{1/2^n}) = \varepsilon_n a_\gamma^{1/2^n}, & \text{para todo } n \geq 1 \\ \tau_\gamma(a_\lambda^{1/2^n}) = a_\lambda^{1/2^n}, & \text{para todo } n \geq 1 \text{ e para todo } \lambda \neq \gamma. \end{cases}$$

Para ver isto, seja $\gamma \in \Lambda$ e E_γ o corpo obtido de $K^T(\tilde{\mathcal{O}}; K)$ por adjunção de todas as raízes 2^n -ésimas de a_λ , para todo $n \geq 1$ e $\lambda \in \Lambda$, com $\lambda \neq \gamma$. $E_\gamma^* = q(E_\gamma) \cup aq(E_\gamma)$ e, novamente por ([W], 3.9-(1)), $G(E_\gamma) \cong \mathbb{Z}_2$ tem gerador τ_γ caracterizado por $\tau_\gamma(a_\gamma^{1/2^n}) = \varepsilon_n a_\gamma^{1/2^n}$, para todo $n \geq 1$. Por construção, $K^T(\tilde{\mathcal{O}}; K) \subseteq \bigcap_{\gamma \in \Lambda} E_\gamma = E$.

Como a imagem de $\{\bar{a}_\lambda = a_\lambda E^2 \mid \lambda \in \Lambda\}$ é $\mathbb{F}_2$ -linearmente independente em E^*/E^2 e $E \mid K^T(\tilde{\mathcal{O}}; K)$ é 2-extensão, concluímos que $E = K^T(\tilde{\mathcal{O}}; K)$. Portanto, $\{\tau_\lambda \mid \lambda \in \Lambda\}$ é um sistema de geradores de $G^T(\tilde{\mathcal{O}}; K)$.

(III.2.5) Teorema. *Seja K um C -corpo não formalmente real tal que $(K^* : K^2) > 2$ para o qual exista $r \geq 1$ com $\varepsilon_r \notin K$. Então, K satisfaz as hipóteses do Teorema (I.3.6) e $G(K) \cong G^T(\tilde{\mathcal{O}}; K) \rtimes \mathbb{Z}_2$. Além do mais, podemos escolher um gerador σ para a componente isomorfa a $\mathbb{Z}_2$ cuja ação sobre o sistema de geradores $\{\tau_\lambda \mid \lambda \in \Lambda\}$ de $G^T(\tilde{\mathcal{O}}; K)$, como foi construído anteriormente, é assim descrita:*

- (a) *Se $-1 \notin K^2$ e $\varepsilon_n \in K(i)$ para todo $i \geq 1$, então $\sigma\tau_\lambda\sigma^{-1} = \tau_\lambda^2$ para todo $\lambda \in \Lambda$. Neste caso, $G(K(i)) \cong G^T(\tilde{\mathcal{O}}; K) \times \mathbb{Z}_2$ é o maior subgrupo abeliano normal de $G(K)$.*
- (b) *Se $-1 \notin K^2$ e existe n tal que $\varepsilon_n \notin K(i)$, então $\sigma\tau_\lambda\sigma^{-1} = \tau_\lambda^{2^{m+1}}$ para todo $\lambda \in \Lambda$, onde m satisfaz: $\varepsilon_{m+1} \in K(i)$ e $\varepsilon_{m+2} \notin K(i)$. Neste caso, $G^T(\tilde{\mathcal{O}}; K)$ é o maior subgrupo abeliano normal de $G(K)$.*
- (c) *Se existe $m \geq 2$ tal que $\varepsilon_m \in K$ e $\varepsilon_{m+1} \notin K$, então $\sigma\tau_\lambda\sigma^{-1} = \tau_\lambda^{2^{m+1}} \forall \lambda \in \Lambda$ e $G^T(\tilde{\mathcal{O}}; K)$ é o maior subgrupo abeliano normal de $G(K)$.*

PROVA. Pela Proposição (I.3.7), K satisfaz as hipóteses do Teorema (I.3.6). Seja $\mathcal{K} = \mathcal{K}_{\mathcal{O}}$. Como K não é formalmente real e $\mathcal{O}$ é 2-henseliano, $\mathcal{K}$ também não é formalmente real. Se $\varepsilon_r \notin K$ e $\varepsilon_{r-1} \in K$ para $r \geq 1$, então vale também que $\varepsilon_r \notin \mathcal{K}$, de acordo com (I.2.2). Primeiramente descreveremos $G(\mathcal{K})$. No caso (c), pelo Teorema (I.3.6)-(b), $(\mathcal{O}^*K^2 : K^2) \leq 2$ e portanto $(\mathcal{K}^* : \mathcal{K}^2) \leq 2$ e, pelo que foi observado, $(\mathcal{K}^* : \mathcal{K}^2) = 2$ e, sendo $\mathcal{K}$ não formalmente real, temos $G(\mathcal{K}) \cong \mathbb{Z}_2$. Nos casos (a) e (b) K não é excepcional e portanto, pelo Teorema (I.3.6) $\mathcal{B} = \mathcal{O}^*K^2$ e $B(\mathcal{K}) = \mathcal{K}^*$. Como $(\mathcal{B} : K^2) = 2$, segue-se de ([AEJ], Proposition 1.9-(2)), que $(\mathcal{K}^* : \mathcal{K}^2) = 2$. Como $[\mathcal{K}(2) : \mathcal{K}]$ não é finito, $G(\mathcal{K}) \cong \mathbb{Z}_2$ também nos casos (a) e (b).

Por ([E], 20.10-(b)) $G(K)/G^T(\tilde{\mathcal{O}}; K) \cong G(\mathcal{K}) \cong \mathbb{Z}_2$. Mas, como $\mathbb{Z}_2$ é pro-2-grupo livre, obtemos $G(K)$ como o produto semidireto $G^T(\tilde{\mathcal{O}}; K) \rtimes \mathbb{Z}_2$, como queríamos.

Para descrever $G(K)$ através de geradores e relações da maneira como foi proposto, seja E o corpo obtido de K por adjunção das raízes 2^n -ésimas de a_λ , para todos $n \geq 1$ e $\lambda \in \Lambda$ escolhidas da maneira como foi descrita antes do Lema (II.2.4), onde $\{a_\lambda \mid \lambda \in \Lambda\} \subseteq K^*$ é obtido da maneira sugerida antes do Teorema. Nos ca-

sos (a) e (b) observamos que $\{a_\lambda \mid \lambda \in \Lambda\} \cup \{-1\}$ é $\mathbb{F}_2$ -base de K^* módulo K^2 , enquanto, no caso (c) $\{a_\lambda \mid \lambda \in \Lambda\} \cup \{\varepsilon_m\}$ é $\mathbb{F}_2$ -base de K^* módulo K^2 . Nos três casos, a única extensão quadrática de K , dentro de $K^T(\tilde{\mathcal{O}}; K)$ não está contida em E . Como $EK^T(\tilde{\mathcal{O}}; K) = K(2)$, obtemos, da Teoria de Galois, $\mathbb{Z}_2 \cong G(K)/G^T(\tilde{\mathcal{O}}; K) \cong G(E)$. Se σ for um gerador de $G(E)$ e $\gamma \in \Lambda$, então $\sigma\tau_\gamma\sigma^{-1}(a_\gamma^{1/2^n}) = \sigma(\varepsilon_n)a_\gamma^{1/2^n}$ para todo $n \geq 1$ e $\sigma\tau_\gamma\sigma^{-1}(a_\lambda^{1/2^n}) = a_\lambda^{1/2^n}$ para todos $n \geq 1$ e $\lambda \neq \gamma$ em Λ . Assim a ação de σ sobre os τ_λ , $\lambda \in \Lambda$ pode ser obtida determinando $\sigma(\varepsilon_n)$ para todo $n \geq 1$. No caso (a), $\sigma(\varepsilon_n) = \varepsilon_n^{-1}$, pois a restrição de σ a $K(i)$ não é trivial. Nos casos (b) e (c), primeiramente observamos que $K^T(\tilde{\mathcal{O}}; K) = K(\varepsilon_\infty)$ e $G(K(\varepsilon_\infty); K)$ é um grupo cíclico. No caso (b), $K(i)$ é a única extensão quadrática de K , que está contida em $K^T(\tilde{\mathcal{O}}; K)$. Portanto $K(2^{1/2}) \subseteq K(i)$ e $\varepsilon_3 \in K(i)$. Seja $m \geq 2$ satisfazendo $\varepsilon_m \in K(i)$ e $\varepsilon_{m+1} \notin K(i)$. Como na prova do 2º caso do Teorema (II.2.5) obtemos $\sigma(\varepsilon_n) = \varepsilon_n^{-1}$ para todo n satisfazendo $1 \leq n \leq m$ e $\sigma(\varepsilon_{m+1}) = -\varepsilon_{m+1}$. Assim, podemos obter σ satisfazendo $\sigma(\varepsilon_n) = \varepsilon_n^{2^m - 1}$ para todo $n \geq 1$. Analogamente, no caso (c) podemos escolher σ tal que $\sigma(\varepsilon_n) = \varepsilon_n^{2^m + 1}$ para todo $n \geq 1$.

Para completar a prova seja U um subgrupo abeliano normal de $G(K)$ e F seu corpo fixo. Se $r(U) > 1$, pelo Teorema (III.2.1), temos que $\varepsilon_\infty \subsetneq F$. Portanto, F contém $K(i)$ no caso (a) e contém $K^T(\tilde{\mathcal{O}}; K)$ nos casos (b) e (c). Portanto, no caso (a), temos $U \subseteq G(K(i))$, enquanto que nos casos (b) e (c), temos $U \subseteq G^T(\tilde{\mathcal{O}}; K)$ como queríamos.

Vejamos agora o caso $U \cong \mathbb{Z}_2$ com $C(U) = U$. Pelo Teorema (II.2.5) o caso (a) não pode ocorrer. Nos casos (b) e (c), pelo Corolário (II.2.6), obtemos que $G^T(\tilde{\mathcal{O}}; K)$ é o maior subgrupo abeliano normal de $G(K)$, como queríamos.

Suponhamos agora que não exista um subgrupo normal U' satisfazendo $U \subsetneq U'$, $U' \cong \mathbb{Z}_2$ e $C(U') = U'$. Pela Proposição (II.2.1), existe um subgrupo V de $G(K)$ com $U \subsetneq V$ e $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Seja M o corpo fixo de V . Pelo Teorema (III.2.1) $\varepsilon_\infty \subset M \subseteq F$ e a prova se completa, como no caso $r(U) > 1$. ■

O próximo teorema pode ser considerado uma síntese do que obtivemos até agora, em termos da existência de subgrupos abelianos normais máximos de $G(K)$, para um corpo K .

(III.2.6) Teorema. *Seja K um corpo tal que $(K^* : K^2) > 2$.*

- (a) $G(K)$ possui um maior subgrupo abeliano normal $\mathfrak{U}$. Além disso, se $\mathcal{B} \neq \pm K^2$ então $r(\mathfrak{U}) = r(K^*/\mathcal{B})$.
- (b) $\mathfrak{U} \cong G^T(\tilde{\mathcal{O}}; K)$ ou então K é um C -corpo tal que $\varepsilon_\infty \in K(i)$. Neste último caso, temos a seguinte classificação:
 - (b)-(1) Se $\varepsilon_\infty \in K$, então $\mathfrak{U} = G(K)$ está descrito no Corolário (III.2.2).
 - (b)-(2) Se K é um corpo não formalmente real tal que $-1 \notin K^2$ e $\varepsilon_\infty \in K(i)$, então $\mathfrak{U} = G(K(i)) \cong G^T(\tilde{\mathcal{O}}; K) \times \mathbb{Z}_2$.
 - (b)-(3) Se K é formalmente real, então $\mathfrak{U} = G(K(i))$ e temos duas possibilidades: $\mathfrak{U} = G^T(\tilde{\mathcal{O}}; K)$ se $\mathcal{K}_C$ tiver uma única ordem, ou então $\mathfrak{U} \cong G^T(\tilde{\mathcal{O}}; K) \times \mathbb{Z}_2$ se $\mathcal{K}_C$ tiver duas ordens.

PROVA. Se $\mathcal{B} = K^*$, então $\mathfrak{U}$ é trivial, pelo Lema (III.2.3). Suponhamos $\mathcal{B} \neq K^*$. Se K não for C -corpo, então as afirmações foram demonstradas no Teorema (III.2.4). Se K for C -corpo não formalmente real tal que $\varepsilon_r \notin K$ para algum $r \geq 1$, então as afirmações foram demonstradas no Teorema (III.2.5). Se K for um C -corpo formalmente real, então (a) segue de ([B], Theorem 1, pg. 86). A prova de (b)-(3) é obtida aplicando-se o Corolário (III.2.2) a $K(i)$. ■

3. Subgrupos abelianos de $G(K)$.

Os resultados obtidos até agora nos permitirão estabelecer uma relação entre subgrupos de K^* contendo $\mathcal{B}$ e os subgrupos abelianos normais U de $G(K)$.

(III.3.1) Teorema. *Seja K um corpo, α um cardinal, e seja $\mathcal{B}_0 = K^2 \cup \varepsilon_m K^2$ se $\mathcal{B} = K^2$ e, para algum $m \geq 2$, $\varepsilon_m \in K$ e $\varepsilon_{m+1} \notin K$ ou, caso contrário, $\mathcal{B}_0 = \mathcal{B}$. Então as seguintes afirmações são equivalentes:*

- (a) *Existe um subgrupo H de K^* contendo $\mathcal{B}_0$ com $r(K^*/H) = \alpha$.*
- (b) *Existe uma seqüência exata cindida*

$$1 \longrightarrow U \longrightarrow G(K) \longrightarrow V \longrightarrow 1$$

de pro-2-grupos com U abeliano e $r(U) = \alpha$.

PROVA. Primeiramente vejamos o caso K sendo C -corpo. Se $\varepsilon_n \in K$ para todo $n \geq 1$, o resultado segue do Teorema (III.2.1). Se $-1 \notin K^2$ e K não é formalmente real, então K é não excepcional e portanto $\mathcal{B} = \mathcal{O}^* K^2$, pelo Teorema (I.3.6)-(a) e $r(G^T(\tilde{\mathcal{O}}; K)) = r(K^* : \tilde{\mathcal{O}}^* K^2)$, pelo Teorema (I.3.6)-(c). A equivalência segue então do Teorema (III.2.5)-(a) e (b). Se existe $m \geq 2$ tal que $\varepsilon_m \in K$ e $\varepsilon_{m+1} \notin K$, a equivalência segue do Teorema (III.2.5)-(c) e da igualdade $\tilde{\mathcal{O}}^* K^2 = K^2 \cup \varepsilon_m K^2$. Se K for formalmente real, então K é $K(2)$ -pitagórico. Por ([B], Theorem 1, pg. 86 e Lemma 2, pg. 87), $G(K) = G(K(i)) \rtimes \langle \sigma \rangle$, onde σ é uma involução e $\sigma \tau \sigma^{-1} = \tau^{-1}$, para todo $\tau \in G(K(i))$. Por ([L1], Theorem 3.4 pg. 202), $r(K(i)^*/(K(i))^2) = r(K^*/\mathcal{B})$ e então obtemos a equivalência.

Agora vejamos o caso K não C -corpo. Neste caso, $\mathcal{B} = \mathcal{O}^* K^2$, pelo Teorema (I.3.6)-(a) e (c). Como foi observado antes do Teorema (III.2.6), todo subconjunto $\{a_\lambda | \lambda \in \Lambda\}$ de K^* que é $\mathbb{F}_2$ -base de K^* módulo $\mathcal{O}^* K^2$ também é $\mathbb{F}_2$ -base de $K^T(\tilde{\mathcal{O}}; K)$ módulo $q(K^T(\tilde{\mathcal{O}}; K))$.

((a) $\implies$ (b)). Seja $A_0 \subset \Lambda$ de cardinalidade α . Seja também $\{a_\lambda | \lambda \in \Lambda\}$, uma $\mathbb{F}_2$ base de K^*/K^2 tal que a imagem $\{a_\lambda | \lambda \in A_0\}$, onde $A_0 \subset \Lambda$ tem cardinalidade α , é uma $\mathbb{F}_2$ -base de K^*/H . Seja ainda L o corpo obtido de $K^T(\tilde{\mathcal{O}}; K)$ por adjunção de todas as raízes 2^n -ésimas de a_λ , para todo $n \geq 1$ e para todo $\lambda \in \Lambda$, $\lambda \notin A_0$.

Afirmamos que $\{a_\lambda | \lambda \in A_0\}$ é uma $\mathbb{F}_2$ -base de L^* módulo L^2 , resultando $r(G(L)) = \alpha$. Sejam $\alpha_1, \dots, \alpha_r$ elementos de A_0 tais que $a_{\alpha_1} \dots a_{\alpha_r} = b^2$, $b \in L$. Assim, existem $\lambda_1, \dots, \lambda_s \in \Lambda \setminus A_0$ e $n \geq 1$ tais que $b \in F$, onde $F = K^T(\{a_{\lambda_1}^{1/2^n}, \dots, a_{\lambda_s}^{1/2^n}\})$,

com $K^T = K^T(\mathcal{O}; K)$. Portanto, $(a_{\alpha_1} \dots a_{\alpha_r}) \in F^2 \cap K^T = \langle a_{\lambda_1} (K^T)^2, \dots, a_{\lambda_s} (K^T)^2 \rangle$, pelo Lema (III.3.2), a seguir, contradizendo a escolha de $\{a_\lambda | \lambda \in \Lambda_0\}$ pois os conjuntos $\{\alpha_1, \dots, \alpha_r\}$ e $\{\lambda_1, \dots, \lambda_s\}$ são disjuntos.

Portanto, $\{a_\lambda | \lambda \in \Lambda_0\}$ é $\mathbb{F}_2$ -linearmente independente módulo L^2 . Aplicando agora ([W], Lemma 3.4) a K^T , obtemos que, para todo $x \in L$, existem $\beta_1, \dots, \beta_r \in \Lambda$ e $n \geq 1$ tais que $x^{1/2} \in N$, onde $N = K^T(\{a_{\beta_1}^{1/2^n}, \dots, a_{\beta_s}^{1/2^n}\})$. Seja $\{\alpha_1, \dots, \alpha_s\} = \{\beta_i | \beta_i \in \Lambda_0\}$ e $M = LN$. Então, $M = L(\{a_{\alpha_1}^{1/2^n}, \dots, a_{\alpha_s}^{1/2^n}\})$ e $x \in M^2 \cap L = \langle a_{\lambda_1} L^2, \dots, a_{\lambda_s} L^2 \rangle$, pelo Lema (III.3.2), a seguir, a afirmação está provada.

Seja $\rho \in G(K)$ e $\lambda \in \Lambda \setminus \Lambda_0$. Então $\rho(a_\lambda^{1/2^n}) = \varepsilon_n^j a_\lambda^{1/2^n}$, para algum j , $1 \leq j \leq 2^n - 1$ e portanto $\rho(L) = L$ e $L|K$ é uma extensão normal.

Seja $E = K(\{a_\lambda^{1/2^n} | n \geq 1, \lambda \in \Lambda_0\})$. Então $L \cap E = K$, $LE = K(2)$ e, se $U = G(L)$, obtemos a seqüência exata cindida

$$1 \longrightarrow U \longrightarrow G(K) \longrightarrow V \longrightarrow 1$$

onde $V \cong G(E)$.

((b) $\implies$ (a)). Pelo Teorema (III.2.5) temos que $U \subseteq G^T(\mathcal{O}; K)$. Portanto, $\alpha \leq \#\Lambda = r(K^*/K^2)$ e então existe um subgrupo H de K^* tal que $r(K^*/H) = \alpha$. ■

(III.3.2) Lema. Seja K um corpo tal que $-1 \in K^2$ e sejam $a_1, \dots, a_r$ elementos de $K \setminus \mathbb{F}_2$ -linearmente independentes módulo K^2 . Seja $L = K(\{a_1^{1/2^n}, \dots, a_r^{1/2^n}\})$, $n \geq 1$ e $a_1^{1/2^n}, \dots, a_r^{1/2^n}$ escolhidos da maneira descrita antes do Lema (II.2.4). Então, $L^2 \cap K = \langle a_1 K^2, \dots, a_r K^2 \rangle$.

PROVA. Por recursão sobre r e n .

(a) Se $a \in K \setminus K^2$ e $L = K(a^{1/2})$, tomando $x \in L^2 \cap K$, isto é, $x = (y_1 + y_2 a^{1/2})^2 = y_1^2 + a y_2^2 + 2 y_1 y_2 a^{1/2} \in K$ temos $y_1 = 0$ ou $y_2 = 0$ e obtemos $x \in K^2 \cup a K^2$.

(b) Seja $a \in K \setminus K^2$ e

$$L_0 = K \subseteq L_1 = K(a^{1/2}) \subseteq \dots \subseteq L_n = L_{n-1}(a^{1/2^n}) = L.$$

Pelo item (a), se $x \in L^2 \cap K \subseteq L^2 \cap L_{n-1}$, obtemos que $x \in L_{n-1}^2 \cup a^{1/2^{n-1}} L_{n-1}^2$. Como $x \in K$, obtemos $x \in L_{n-1}^2 \cap K$ e a prova, no caso $r = 1$, segue por indução sobre n .

(c) A recursão sobre r é análoga à que foi feita em (b), lembrando que

$$K(a_1^{1/2^n}, \dots, a_r^{1/2^n}) = K(a_1^{1/2^n}, \dots, a_{r-1}^{1/2^n})(a_r^{1/2^n}). \blacksquare$$

A pergunta que surge naturalmente nesta altura é sobre os subgrupos abelianos de $G(K)$ que não sejam necessariamente normais em $G(K)$. Em [W4], Ware introduz o novo invariante $a(K)$ para um corpo K , definido por:

(III.3.3) Definição. Se K é um corpo,

$$a(K) = \text{maximum}\{r(U) \mid U \text{ é subgrupo abeliano de } G(K)\}.$$

Este invariante foi estudado por Ware, usando anéis de valorização para obter limitantes para $a(K)$ ([W4], Corollary 2 do Theorem 1). O Teorema (III.3.4) a seguir melhora esse resultado.

(III.3.4) Teorema. Seja K um corpo tal que $(K^* : K^2) > 2$ e seja

$\mathcal{A} = \{A \mid A \subseteq \mathcal{O} \text{ é um anel de valorização não diádico de } K \text{ com } \Gamma_A \neq 2\Gamma_A\}$. Então:

(a) Se $\mathcal{A} \neq \emptyset$, então

$$\text{maximum}\{r(\Gamma_A/2\Gamma_A) \mid A \in \mathcal{A}\} \leq a(K) \leq \text{maximum}\{r(\Gamma_A/2\Gamma_A) + 1 \mid A \in \mathcal{A}\}.$$

(b) Se $\mathcal{A} = \emptyset$, então $a(K) = 1$.

PROVA. Como $G^T(D; K)$ é um subgrupo abeliano de $G(K)$ de posto $r(\Gamma_A/2\Gamma_A)$, com $A = D \cap K$, a primeira desigualdade é clara.

Seja então V um subgrupo abeliano de $G(K)$, com $r(V) \geq 2$ e L seu corpo fixo. Pelo Corolário (III.2.2), temos que, ou $V = G^T(\widetilde{O(L)}; L)$, ou então $V = G^T(\widetilde{O(L)}; L) \times \mathbb{Z}_2$. Tomando $C = \widetilde{O(K)} \cap L$ segue-se que, ou $V \subseteq G^T(\widetilde{O(L)}; L)$, ou então $V \subseteq G^T(\widetilde{O(L)}; L) \times \mathbb{Z}_2$. Se C e $\widetilde{O}$ forem anéis de valorização não comparáveis, segue da Proposição (I.2.14) que $G^T(\widetilde{O(L)}; K) = G^Z(\widetilde{O(L)}; K)$ e, pelo Teorema (I.2.6),

$$G^Z(\widetilde{O(L)}; K) = G^Z(\widetilde{O(L)}; K) \cap G^Z(\widetilde{O}; K) = G^T(D; K),$$

onde $D = \widetilde{O(L)} \cdot \widetilde{O}$ (isto é, o menor subanel de $K(2)$ que contém $\widetilde{O(L)}$ e $\widetilde{O}$) e vale a primeira igualdade pois $G^Z(\widetilde{O}; K) = G(K)$. Como $\widetilde{O} \subseteq D$, segue-se que $G^T(D; K) \subseteq G^T(\widetilde{O}; K)$. Por outro lado, se $A = \mathcal{O}$ temos que, ou $V \subseteq G^T(\widetilde{O}; K)$, ou então $V \subseteq G^T(\widetilde{O}; K) \times \mathbb{Z}_2$ e portanto $r(V) \leq r(\Gamma_A/2\Gamma_A) + 1$.

Assuma então que C e $\mathcal{O}$ são comparáveis. Se $\mathcal{O} \subseteq C$, tomamos $A = \mathcal{O}$ e, de maneira análoga ao parágrafo anterior, obtemos novamente $r(V) \leq r(\Gamma_A/2\Gamma_A) + 1$.

Finalmente, assumimos $C \subseteq \mathcal{O}$ e tomamos $A = C$. Como $r(V) \geq 2$ e, ou $V \subseteq G^T(\widetilde{O(L)}; K)$, ou então $V \subseteq G^T(\widetilde{O(L)}; K) \times \mathbb{Z}_2$, segue-se que Γ_A não é um grupo 2-divisível, por ([E], Theorem (20.19), pg. 168). Como $G^V(\widetilde{O(L)}; K)$ é trivial ($\widetilde{O(L)}$ é um anel de valorização não diádico), novamente obtemos $r(V) \leq r(\Gamma_A/2\Gamma_A) + 1$, como foi proposto.

(b) Basta mostrar que, se V for um subgrupo abeliano normal não trivial de $G(K)$, então V tem posto 1. Suponha V um subgrupo abeliano com $r(V) \geq 2$ e E seu corpo fixo. Mostraremos que $\widetilde{O(E)} \cap K \in \mathcal{A}$, contra a hipótese $\mathcal{A} = \emptyset$. Pelo Corolário (III.2.2), $G^T(\widetilde{O(E)}; E)$ é não trivial, caso V tenha posto maior que 1. Portanto, o grupo de valores de $\widetilde{O(E)} \cap K^T(\widetilde{O(E)}; E)$ não é 2-divisível, por ([E], Theorem 20.12). Como $K \subseteq K^T(\widetilde{O(E)}; E) \subset K(2)$, o mesmo é verdade para $\widetilde{O(E)} \cap K$, isto é, $\widetilde{O(E)} \cap K \in \mathcal{A}$ e isto encerra a prova. ■

(III.3.5) Exemplos. Seja $K = k((X))^{\Gamma}$ o corpo de série de potências generalizadas sobre o corpo k , com expoentes no grupo $\Gamma = \mathbb{Z} \times \mathbb{Z}$, com ordem lexicográfica, e assumamos $c(k) \neq 2$. É fato conhecido que o anel de valorização $A = k[[X]]^{\Gamma}$ tem grupo de

valores Γ , corpo de resíduos k e $\mathcal{O}$ é anel de valorização henseliano.

(1) Seja k um corpo quadraticamente fechado. Então, por ([AEJ], Proposition 1.5) $\mathcal{B} = K^2$ e $\varepsilon_n \in K$, para todo $n \geq 1$. Então, pelo Teorema (III.2.1), $G(K)$ é um grupo abeliano. Por construção, $\Gamma_A \neq 2\Gamma_A$ e A é não diádico e 2-henseliano (na verdade, A é henseliano). Portanto, A é K^2 -compatível (ver Observação (I.3.2)). Como o corpo de resíduos $\mathcal{K}_A (= k)$ é quadraticamente fechado, para todo anel de valorização A' de K , $A' \subsetneq A$, o grupo de valores de A' contém um subgrupo convexo 2-divisível não trivial. Portanto, pelo Teorema (I.3.6) $A = \mathcal{O}$ e

$$G(K) = G^Z(\tilde{\mathcal{O}}; K) = G^T(\tilde{\mathcal{O}}; K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

(2) Seja k um corpo de característica diferente de dois, $\{\varepsilon_n | n \geq 1\} \subsetneq k$, $G(k) \cong \mathbb{Z}_2$ e $K^Z(C; k) = k(2)$, para todo anel de valorização próprio C de $k(2)$ (por exemplo, seja k o corpo descrito em (II.2.7)(b)-1). Neste caso, temos $A = \mathcal{O}$ e $G^T(D; K) = G^T(\tilde{\mathcal{O}}; K)$, para todo anel de valorização D de $K(2)$, $D \subsetneq \tilde{\mathcal{O}}$.

Por outro lado,

$$G(K)/G^T(\tilde{\mathcal{O}}; K) \cong G(k) \cong \mathbb{Z}_2$$

nos mostra que $G(K)$ é metabeliano. Portanto, K é um C-corpo, conforme ([W1], Theorem 4.5) e, como $\{\varepsilon_n | n \geq 1\} \subsetneq K$, obtemos que $G(K)$ é abeliano, pelo Teorema (III.2.1). Portanto,

$$G(K) = G^T(\tilde{\mathcal{O}}; K) \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

(3) Seja F uma extensão não real de $\mathbb{Q}$, $-1 \notin F^2$ e $\xi_n \in F$, $\forall n \geq 1$ (por exemplo: $F = \mathbb{Q}(\{\sqrt{-3}\} \cup \{\xi_n | n \geq 1\})$, onde ξ_n , $n \geq 1$ foi introduzido na prova do Lema (II.2.4)). Seja k uma extensão de F tal que $F \subseteq k \subset F(2)$ de tal forma que k seja maximal com respeito à exclusão de i . Isto significa que qualquer extensão de k em $F(2)$ contém i . Portanto, $G(k)$ é um grupo cíclico. Como $F \subseteq k$ e F não é formalmente real, temos que $G(k) \cong \mathbb{Z}_2$. Usando o mesmo tipo de argumento do exemplo (2) podemos mostrar

que $G(K)$ é metabeliano e, portanto, K é C -corpo e também $\varepsilon_n \in K(i)$, para todo $n \geq 1$. Portanto, a condição (a) do Teorema (III.2.5) vale para K .

(4) Tomando, no exemplo anterior, F tal que $\xi_m \notin F$, para algum $m \geq 3$ e $\xi_n \in F$, $\forall n$ $1 \leq n \leq m$, o corpo K construído como acima satisfaz a condição (b) do Teorema (III.2.5).

(5) De maneira análoga à construção do exemplo (3), tomamos F um corpo satisfazendo $\varepsilon_m \in F$ e $\varepsilon_{m+1} \notin F$ para algum $m \geq 2$. Seja k um corpo contendo F ($k \subset F(2)$), maximal com respeito à exclusão de ε_{m+1} . Então o corpo K satisfaz a condição (c) do Teorema (III.2.5).

REFERÊNCIAS

- [AEJ] ARASON, J.K., ELMAN, R., e JACOB, B., *Rigid Elements, Valuations, and Realizations of Witt Rings*. J. of Algebra 110 (1987), 449-467.
- [B1] BECKER E., *Euklidische Körper und Euklidische Hüllen von Körpern*. J. Reine Angew. Math. 268-269 (1974), 41-52.
- [B] BECKER, E., *Hereditarily-Pythagorean Fields and Orderings of Higher Level*, Monografias de Matemática 29, IMPA, Rio de Janeiro, 1978.
- [Br] BRÖCKER, L., *Characterization of Fans and Hereditarily-Pythagorean Fields*. Math. Z. 151 (1976), 149-163.
- [D] DELZANT, A., *Definition des Classes de Stiefel-Whitney d'un Module Quadratique de Caractéristique différente de 2*, C.R. Acad. Sci. Paris Ser A-B 255 (1962), 1366-1368.
- [DD] DILLER, J. e DRESS, A., *Zur Galoistheorie Pythagoreischer Körper*. Arch. der Math. 16 (1965), 148-152.
- [E] ENDLER, O., *Valuation Theory*. Berlin-Heidelberg-New York. Springer Verlag 1972.
- [EE] ENDLER, O. e ENGLER, A. J., *Fields with Henselian Valuation Rings*. Math. Z. 152 (1977), 191-193.
- [En] ENGLER, A. J., *Fields with two Incomparable Henselian Valuation Rings*. Manuscripta Math. 23 (1978), 373-385.
- [EV] ENGLER, A. J. e VISWANATHAN, T. M., *Digging Holes in Algebraic Closures à la Artin I*. Math. Ann. 265 (1983), 263-271.
- [JW] JACOB, B. e WARE, R., *A Recursive Description of the Maximal Pro-2-Group Via Witt Rings*. Math. Z. 200 (1989), 379-396.
- [HJ] HARAN, D. e JARDEN, M., *The Absolute Galois Group of a Pseudo Real Closed Field*. Annali Scuola Normale Superiore, Pisa Serie IV, Vol. XII, N° 3 (1985), 449-489.
- [L1] LAM, T. Y., *The Algebraic Theory of Quadratic Forms*. Benjamin, New York, 1973.
- [L2] LAM, T. Y., *Orderings, Valuations and Quadratic Forms*. CBMS, N° 52 AMS,

1983.

- [Lu] LUBOTZKI, A., *Combinatorial Group Theory for Pro-p-Groups*. J. Pure and Appl. Algebra 25 (1982), 311-325.
- [MB] MAC LANE, S. e BIRKHOFF, G., *Algebra*. The Macmillan Company – New York – Collier – Macmillan Limited – London 1967.
- [Rib] RIBENBOIM, P. *Théorie des Valuations*. Les Presses de L'Université de Montréal – Montréal 1965.
- [R] RIBES, L., *Introduction of Profinite Groups and Galois Cohomology*. Queen's Papers in Pure and Applied Math. 24, Queen's University, Kingston, 1970.
- [Sch] SCHARLAU, W., *Quadratische Formen und Galois Cohomologie*. Invent. Math. 4 (1967), 238-264.
- [S] SERRE, J-P., *Cours D'Arithmétique*. Presses Universitaires de France – Paris, 1970.
- [Szy] SZYMICZEK, K., *Quadratic Forms over Fields*. Dissert. Math. Rozprawy Mat. 52 (1977).
- [W] WARE, R., *When Are Witt Rings Group Rings? II*. Pac. J. Math. 76 (1978), 541-564.
- [W1] WARE, R., *Quadratic Forms and Profinite-2-Groups*. J. Algebra 58 (1979), 227-237.
- [W2] WARE, R., *Valuation Rings and Rigid Elements in Fields*. Can. J. Math. 33 (1981), 1338-1355.
- [W3] WARE, R., *Quadratic Forms and Pro-2-Groups III-Rigid Elements and Semidirect Products*. Comm. in Alg. 13 (1985), 1713-1736.
- [W4] WARE, R., *Stability in Witt Rings and Abelian Subgroups of Pro-2-Groups*. Rocky Mountain J. of Math. 19 (1989), 985-995.
- [W5] WARE, R., *Quadratic Forms and Pro-2-Groups II: The Galois Group of the Pythagorean Closure of a Formally Real Field*. J. of Pure and App. Algebra 30 (1983), 95-107.