UNIVERSIDADE ESTADUAL DE CAMPINAS
Instituto de Matemática, Estatística e Computação Científica - IMECC
Departamento de Matemática

Elementos Rígidos, Valorizações e Estrutura de Anéis de Witt

Tese de Doutorado

Angelo Papa Neto

Orientador: Prof. Dr. Antonio José Engler

Campinas - 2007

Elementos Rígidos, Valorizações e Estrutura de Anéis de Witt

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Angelo Papa Neto e aprovada pela comissão julgadora.

Campinas, 14 de 09 de 2002

Prof. Dr. Antonio José Engler
(orientador)

Banca Examinadora:

1. Prof. Dr. Antonio José Engler
2. Prof.ª Dr.ª Dessislava Hristova Kochloukova
3. Prof. Dr. Fernando Eduardo Torres Orihuela
4. Prof.ª Dr.ª Ires Dias
5. Prof.ª Dr.ª Rosali Brusamarello

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, IMECC-UNICAMP, como requesito parcial para obtenção do Título de DOUTOR em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues

Papa Neto, Angelo

P197e Elementos rígidos, valorizações e estrutura de anéis de Witt / Angelo Papa Neto -- Campinas, [S.P. :s.n.], 2007.

Orientador : Antonio José Engler

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Formas quadráticas. 2. Corpos formalmente reais. 3. Witt, Anéis de. I. Engler, Antonio José. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Rigid elements, valuations and structure of Witt rings.

Palavras-chave em inglês (Keywords): 1. Quadratic forms.2. Formally real fields. 3. Witt rings.

Área de concentração: Álgebra

Titulação: Doutor em Matemática

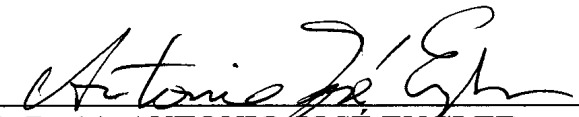
Banca examinadora: Prof. Dr. Antonio José Engler (IMECC-UNICAMP)
Profa. Dra. Dessislava Hristova Kochloukova (IMECC-UNICAMP)
Prof. Dr. Fernando Eduardo Torres Orihuela (IMECC-UNICAMP)
Profa. Dra. Ires Dias (UFSCar)
Profa. Dra. Rosali Brusamarello (UEM)

Data da defesa: 12/09/2007

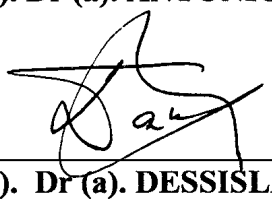
Programa de pós-graduação: Doutorado em Matemática

Tese de Doutorado defendida em 12 de setembro de 2007 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

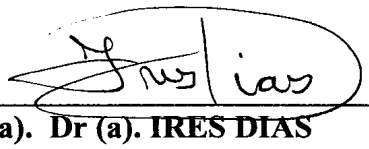


Prof. (a). Dr (a). ANTONIO JOSÉ ENGLER

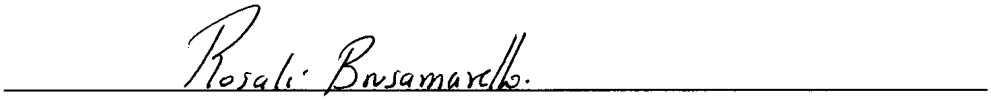


Prof. (a). Dr (a). DESSISLAVA HRISTOVA KOCHLOUKOVA

Prof. (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA



Prof. (a). Dr (a). IRES DIAS



Prof. (a) Dr. (a). ROSALI BRUSAMARELLO

À Sueli e ao Pedro, meus dois tesouros.

Agradecimentos

Esta tese, definitivamente, não é um trabalho solitário e não seria realizada sem o apoio de várias pessoas. É claro que os erros que porventura nela estejam contidos são de inteira responsabilidade do autor.

Em primeiro lugar, gostaria de agradecer ao Centro Federal de Educação Tecnológica do Ceará, onde sou professor desde 1997, pelo apoio durante o afastamento. À Universidade Estadual de Campinas, pelo suporte financeiro através do Programa Piloto de Bolsas para Instrutores Graduados (BIG).

Ao professor Antonio José Engler, meu orientador, com quem aprendi o assunto deste trabalho e também muitas lições sobre como escrever matemática, agradeço, sobretudo, pela paciência e atenção com que se dedicou ao difícil trabalho de orientação.

Aos professores, alunos e funcionários do IMECC, que sempre mantiveram um clima de cordialidade e cooperação, sem o qual seria impossível desenvolver um trabalho de pesquisa. Aos professores Plamen Emilov Koshlukov, Fernando Eduardo Torres Orihuela e Paulo Roberto Brumatti, pelos excelentes cursos nos quais muito aprendi sobre álgebra.

Aos meus amigos Francisco Odair Vieira de Paiva, Paulo Cesar Cavalcante de Oliveira e Luiz Antonio da Silva Medeiros que nos receberam em sua casa, quando de nossa chegada a Campinas. Cabe aqui um agradecimento especial ao Odair, pela pessoa especial que ele é, sempre pronto a ajudar de modo alegre e desprendido.

Aos meus colegas da álgebra, principalmente os mais próximos: Ronie Peterson Dario, Fabio Alexandre de Matos e Maurício de Araújo Ferreira, pela convivência fraterna no período em que estudamos juntos.

À minha família, em especial aos meus pais Nicolino Papa e Dagmar Alves Papa, pela educação que me deram, mais do que por palavras, pelo exemplo. Também pelo período em que, resignadamente, suportaram a ausência do filho.

Ao meu amado filho Pedro Espindola Papa, que nestes seus dois primeiros anos de vida tanto nos tem surpreendido com sua incrível inteligência e espirituosidade, e com sua presença tem banhado de luz os meus dias.

Finalmente, meu agradecimento maior, à minha querida esposa Sueli Espindola Papa, companheira dos bons e maus momentos, a pessoa que acompanhou mais de perto todo o desenvolvimento da tese, nos seus momentos mais alegres e também nos mais sofridos. Sem seu apoio constante, sua disposição e seu sacrifício nas horas difíceis, jamais teria conseguido realizar este intento. A ela dedico, humildemente, este trabalho.

Resumo

Um corpo ordenado é uma estrutura algébrica similar à do corpo dos números reais. No entanto, ao contrário dos reais, um corpo arbitrário F pode admitir mais de uma ordem, inclusive um número infinito e não enumerável de ordens. A cada elemento x do corpo F podemos associar uma forma quadrática binária $\langle 1, x\rangle$, chamada 1-forma de Pfister. Os elementos de $\dot{F} = F \setminus \{0\}$ representados por $\langle 1, x\rangle$ constituem um grupo que chamamos grupo de valores da forma e denotamos por $D\langle 1, x\rangle$. Um elemento $d \in \dot{F}$ é chamado *rígido* se $D\langle 1, d\rangle = \dot{F}^2 \cup d\dot{F}^2$, onde $\dot{F}^2$ é o subgrupo de $\dot{F}$ formado pelos quadrados. Um elemento d é dito birígido se d e $-d$ são rígidos. O presente trabalho tem como objetivo principal obter um teorema de estrutura para o anel de Witt (das classes de equivalência de formas quadráticas) de um corpo ordenado F admitindo um elemento rígido que não é birígido e que é negativo em relação a pelo menos uma das ordens do corpo. Mais precisamente, obtemos uma decomposição do anel de Witt de F como produto de anéis de Witt de duas extensões $H|F$ e $K|F$, ambas contidas no fecho quadrático de F. Os anéis de Witt de H e K têm estrutura mais simples que a do anel de Witt de F. Obtemos os corpos H e K construíndo subgrupos R_d e S_d associados ao elemento rígido d e exigindo que valha uma propriedade de decomposição: $\dot{F} = R_d \cdot S_d$. O corpo H é uma henselização de F relativa a um anel de valorização $(A, \mathfrak{m}_A)$ de F tal que $R_d = (1 + \mathfrak{m}_A)\dot{F}^2$. O corpo K é pitagórico e tem espaço de ordens X_K homeomorfo ao espaço X/S_d das ordens de F que contêm S_d. Obtemos ainda uma condição necessária e suficiente para que ocorra a decomposição $\dot{F} = R_d \cdot S_d$, que depende do grupo de valores e do corpo de resíduos do anel de valorização A.

Abstract

An ordered field is an algebraic structure like the field of real numbers. However, while the field of real numbers have only one ordering, an arbitrary ordered field F may have more than one ordering, and also a infinite and uncountble number of orderings is allowed. To each element $x \in \dot{F}$ one can associate an binary quadratic form $\langle 1, x\rangle$, called Pfister 1-fold form. The set of elements in $\dot{F} = F \setminus \{0\}$ which are represented by $\langle 1, x\rangle$ is a group $D\langle 1, x\rangle$, called value group of $\langle 1, x\rangle$. An element $d \in \dot{F}$ is called *rigid* if $D\langle 1, d\rangle = \dot{F}^2 \cup d\dot{F}^2$, where $\dot{F}^2$ denotes the subgroup of squares in $\dot{F}$. An element d is called birigid if d and $-d$ are both rigid. The main purpose of this thesis is to prove an structure theorem for Witt ring (of equivalence classes of quadratic forms) of an ordered field F with a rigid element which is not birigid and is negative in at least one ordering of F, that is, we get a decomposition of the Witt ring of F as a product of Witt rings of extensions $H|F$ and $K|F$, both inside the quadratic closure of F. The Witt rings of H and K have a simpler structure than Witt ring of F. We get fields H and K by builting subgroups R_d and S_d associated to the rigid element d and making the addicional assumption that $\dot{F} = R_d \cdot S_d$ holds. The field H is a henselization of F relative to a valuation ring $(A, \mathfrak{m}_A)$ of F such that $R_d = (1 + \mathfrak{m}_A)\dot{F}^2$. The pythagorean field K has space of orderings X_K homeomorphic to X/S_d, the space of orderings of F which contain S_d. Moreover, we settle an necessary and sufficient condiction to decomposition $\dot{F} = R_d \cdot S_d$ holds, relative to value group and residue field of valuation ring A.

Sumário

Lista Parcial de Símbolos

Capítulo 1

Introdução

Iniciamos esta introdução deixando claro que tudo o que escrevemos refere-se ao caso **característica $\neq 2$**, tanto para corpos como para anéis. Além disso, para tornar a leitura do trabalho mais dinâmica, *para toda função $X \to Y$ de um conjunto X em um conjunto Y, iremos escrever $X \hookrightarrow Y$ e $X \twoheadrightarrow Y$ para indicar injetividade e sobrejetividade, respectivamente.*

Em [5] R. Bos demonstrou, usando métodos puramente elementares, que para anéis de Witt abstratos a existência de uma decomposição em produto direto ocorre desde que o anel inicial contenha elementos de um tipo especial que são chamados de *rígidos* (definição na página 12). Contudo ele precisou de uma hipótese de 'finitude' muito forte. O resultado de Bos nos leva naturalmente a questionar se para anéis de Witt de corpos (portanto concretos[1]) podemos obter, com a mesma condição de existência de elementos rígidos, essa decomposição onde as parcelas correspondam a anéis de Witt de extensões do corpo dado. Resultados desse tipo vêm sendo pesquisados há muito tempo e têm como meta obter uma redução na complexidade dos problemas definidos sobre o corpo inicial. Mais precisamente, se decompomos o anel de Witt $W(F) \simeq W(H) \times W(K)$ de um corpo F através de duas extensões com propriedades aritméticas mais simples, $H|F$ e $K|F$, podemos tratar problemas que envolvam formas quadráticas sobre F através de H e K. Por essa razão é muito importante obter "boas" extensões H e K que realizem as parcelas de uma dada decomposição.

Esse problema de "realização" é bastante difícil. Arason et al. [1] abordaram com algum sucesso essa questão. Eles trabalharam na pergunta: *Sabendo-se que para dois*

[1] Ainda não é conhecido se todo anel de Witt abstrato pode ser realizado como anel de Witt de um corpo.

anéis de Witt abstratos R e S existe um corpo F tal que $W(F) \simeq R \times S$, existirão extensões H e K de F tais que $W(H) \simeq R$ e $W(K) \simeq S$? Observemos que para essa decomposição atender aos objetivos de redução de problemas devemos também exigir que o seguinte diagrama seja comutativo

$$\begin{array}{ccc} W(F) & \longrightarrow & R \times S \\ \downarrow & & \downarrow \\ W(H) & \longrightarrow & R \end{array} \tag{1.0.1}$$

onde a flecha vertical da esquerda é induzida pela extensão de escalares e a flecha da direita é o homomorfismo associado ao produto na categoria dos anéis de Witt abstratos.

Claramente um diagrama semelhante com K no lugar de H e S no lugar de R também deve ocorrer. Arason et al. [1] tiveram sucesso em realizar uma das parcelas, digamos R, assumindo também a existência de elemento rígido x em R cujo negativo $-x$ também fosse rígido (*birígido*). Não puderam contudo obter uma realização de S. Outros autores também trabalharam nesse problema de realização. Ver, por exemplo, I. Efrat [9]; embora Efrat tenha optado pelo uso da liguagem de estruturas quaterniônicas.

Nosso principal resultado (Teorema 5.26 e seu Corolário 5.28) estabelece que para um corpo F contendo um elemento rígido existe uma decomposição $W(F) \simeq W(H) \times W(K)$, onde H admite um anel de valorização 2-henseliano e K é um corpo pitagórico. Nossos métodos diferem dos métodos de Bos e são da mesma natureza dos de [1]. A partir de um elemento rígido (mas não birígido) construímos um anel de valorização conveniente cuja 2-henselização nos fornece H. Dessa forma podemos obter duas reduções para problemas envolvendo formas quadráticas. A primeira quando consideramos o problema em cada um dos corpos H e K e a segunda quando passamos de H para o corpo de resíduos do anel de valorização 2-henseliano de H. Essa segunda redução pode ser sintetizada através da afirmação de que $W(H) \simeq W(k)[G]$ é um anel de grupo com coeficientes no anel de Witt do corpo de resíduos k do anel de valorização e o grupo G é 2-elementar, determinado pelo grupo de valores do anel de valorização. A redução ao corpo de resíduos de um anel de valorização 2-henseliano é um resultado essencialmente devido a T.A. Springer (veja Lam [22], página 37) que marca a origem da conexão entre valorizações e formas quadráticas (veja Lam, op. cit., página v).

Como Bos, tivemos que assumir uma condição adicional à existência do elemento rígido: assumimos restrições para o grupo de valores e o corpo de resíduos do anel de valorização. Pudemos mostrar contudo que, reciprocamente, uma decomposição de $W(F)$ com as propriedades encontradas tornam essas restrições necessárias. Observamos

também que nossos resultados representam uma contribuição para a chamada *Conjectura do Tipo Elementar* que propõe que se o anel de Witt de um corpo for Noetheriano ele poderá ser decomposto através de um número finito de etapas envolvendo produto direto e extensões como anel de grupo a partir de três anéis básicos $W(\mathcal{L})$, onde $\mathcal{L}$ é um corpo algebricamente fechado, um corpo real fechado, ou finalmente, um corpo local (ver página 136).

A seguir, teceremos em linhas gerais e de modo informal o conteúdo dos capítulos do trabalho. O início de cada capítulo traz uma descrição detalhada de seu conteúdo.

O Capítulo 2 trata das extensões normais e pitagóricas de um corpo formalmente real F. Nele definimos o fecho de F relativo a uma pré-ordem T de F, denotado por F_T, e mostramos que uma extensão normal e pitagórica $K|F$ é sempre do tipo $K = F_T$. Essa é uma contribuição original do nosso trabalho.

No Capítulo 3 estudamos propriedades dos elementos *rígidos* em um corpo F, reproduzindo alguns resultados de [5] que serão necessários ao desenvolvimento do trabalho. Estaremos particulamente interessados em subgrupos especificos R_d, S_d e T_d do grupo multiplicativo $\dot{F}$ do corpo F associados a um elemento rígido d e em suas propriedades. Mostramos, por exemplo, que S_d e T_d são pré-ordens de F (Corolário 3.14, item (2) e Proposição 3.17, respectivamente).

No Capítulo 4 construimos, a partir de elementos rígidos do corpo F e usando resultados do Capítulo 3, um anel de valorização de F com propriedades adequadas a nosso objetivo principal, que é a decomposição do anel de Witt de F. Em particular, esse anel de valorização tem extensão única ao fecho pitagórico de F relativo à pré-ordem S_d.

Finalmente, no Capítulo 5 está a contribuição principal deste trabalho. Nele abordamos, usando o material desenvolvido ao longo do trabalho, o problema da decomposição do anel de Witt em produto direto como descrito acima. Antes, neste mesmo capítulo, construimos um corpo pitagórico $K \supset F$ com propriedades adequadas aos nosso propósitos. Uma das propriedades importantes desse corpo é que há uma bijeção entre o conjunto das ordens de F contendo S_d e o conjunto das ordens de K. O anel de Witt do corpo K vem a ser um dos fatores da decomposição de $W(F)$ no Teorema 5.26.

Incluímos também, em uma série de apêndices, alguns fatos básicos sobre a Teoria de Galois infinita, corpos ordenados, pré-ordens e formas quadráticas. Nestes apêndices, incluímos as demonstrações apenas dos resultados para os quais não encontramos referências facilmente consultáveis. Embora não seja possível produzir um texto autosuficiente esse material poderá facilitar a leitura deste trabalho para os não especialistas

no assunto. Mantivemos, sempre que possível, os argumentos em nível elementar. Essa escolha reduz o uso de referências e ao mesmo tempo evidencia o processo evolutivo ocorrido com o tema. Resultados que no passado representaram contribuições significativas têm hoje, depois de muitos anos de trabalho envolvendo muitos pesquisadores, uma apresentação simples e acessível a um iniciante no doutorado. Um fato natural em matemática mas que só ocorre com teorias cuja importância no desenvolvimento da matemática mantêm o interesse dos pesquisadores buscando sua melhor compreensão.

Capítulo 2

Extensões normais pitagóricas e a construção de fechos

2.1 Extensões normais pitagóricas e a construção de fechos

Neste capítulo, estudaremos extensões normais e pitagóricas de um corpo formalmente real F. Definiremos o fecho quadrático e o fecho pitagórico de um corpo F e veremos que os dois conceitos coincidem se F não é formalmente real. Mais geralmente, definiremos o fecho F_T de um corpo formalmente real F relativo a uma pré-ordem T como uma generalização natural do fecho pitagórico de F de tal forma que, quando $T = \sum \dot{F}^2$, F_T coincida com o fecho pitagórico de F (veja a Definição 2.8). Veremos também que o fecho F_T pode ser caracterizado como uma interseção de corpos euclidianos e mostraremos que $F_T|F$ é uma extensão formalmente real, normal e pitagórica (Proposição 2.9) e que vale a recíproca, isto é, toda extensão formalmente real, normal e pitagórica de F contida no seu fecho quadrático é realizada como o fecho de F relativo a uma pré-ordem T (Teorema 2.12). Esse resultado, bem como a definição de F_T, são contribuições originais deste trabalho.

Um corpo L é dito *quadraticamente fechado* quando todo elemento de L é o quadrado de um outro elemento de L, isto é, $L^2 = L$. Exemplos imediatos são os corpos algebricamente fechados. Dado um corpo F, o seu *fecho quadrático* $F(2)$ é o menor corpo quadraticamente fechado contendo F, ou seja, se $L \supset F$ é quadraticamente fechado, então $L \supset F(2)$. Em particular, isto implica a igualdade $F(2)^2 = F(2)$. O Lema 2.1

abaixo nos ajudará a tornar a definição de fecho quadrático mais precisa.

Lema 2.1 ([23], Exercício 8, p.23) *Se $\{F_i : i \in I\}$ é uma família de subcorpos de um corpo K e $F = \bigcap_{i\in I} F_i \subseteq K$, então a aplicação natural $\dot{F}/\dot{F}^2 \to \prod_{i\in I} \dot{F}_i/\dot{F}_i^2$ é injetiva.*

Demonstração. Seja $x \in \dot{F}$ tal que $x \in \dot{F}_i^2$ para todo $i \in I$. Para cada $i \in I$ existe $x_i \in \dot{F}_i$ tal que $x = x_i^2$. Se $i, j \in I$, então $x_i^2 = x = x_j^2$, o que implica $x_j = \pm x_i$, para qualquer par de índices $i, j \in I$. Assim, se $j \in I$ (fixado) é tal que $x = x_j^2$, então $x_j = \pm x_i \in F_i$, para todo $i \in I$, ou seja, $x_j \in \bigcap_{i\in I} F_i = F$ e $x = x_j^2 \in F^2$. ■

O Lema 2.1 acima mostra que, se $\{F_i : i \in I\}$ é uma família de corpos quadraticamente fechados (isto é, $\dot{F}_i/\dot{F}_i^2 = \{1\}$ para todo $i \in I$) então $F = \bigcap_{i\in I} F_i$ também é quadraticamente fechado. A partir desse fato, podemos redefinir $F(2)$ da seguinte maneira: se F_{alg} é um fecho algébrico de F, tomemos a família formada pelos subcorpos de F_{alg} que são quadraticamente fechados. Então $F(2)$ é a interseção de todos os corpos dessa família:

$$F(2) = \bigcap_{\substack{L=L^2 \\ L\subset F_{alg}}} L \tag{2.1.1}$$

Seja $L \supset F$ um corpo quadraticamente fechado e $\sigma : L \to F_{\text{alg}}$ um F-homomorfismo. Como $L = L^2$, temos que $\sigma(L) = \sigma(L^2) = \sigma(L)^2$ e $\sigma(L)$ também é quadraticamente fechado. Como $F(2)$ é a interseção de todos os corpos quadraticamente fechados contidos em F_{alg}, $F(2)$ é extensão normal de F .

Outra forma de ver o fecho quadrático de um corpo F é construi-lo "de baixo para cima" a partir de F. Uma 2-*extensão* de F é uma extensão $K|F$ contida no fecho quadrático $F(2)$. A Proposição 2.2 abaixo esclarece a relação entre $F(2)$ e 2-extensões de F. Lembremos que estamos considerando apenas corpos cuja característica é diferente de 2.

Proposição 2.2 *Dado um corpo F, definimos uma família de corpos $\{F_n\}_{n\geq 0}$ pondo $F_0 = F$ e $F_{n+1} = F_n(\{\sqrt{a} \mid a \in F_n\})$. Então cada F_n é uma 2-extensão de F e $F(2) = \bigcup_{n\geq 1} F_n$.*

Demonstração. Como $\{F_n\}$ é uma família totalmente ordenada de corpos, a reunião $K = \bigcup_{n\geq 1} F_n$ também é um corpo. Se $x \in K$ então $x \in F_n$ para algum n e $\sqrt{x} \in F_{n+1} \subset K$. Logo, K é quadraticamente fechado e $F(2) \subseteq K$.

Por outro lado, para todo $x \in F$, $\sqrt{x} \in F(2)$, logo $F_1 \subset F(2)$. Supondo que $F_n \subset F(2)$, então $\sqrt{x} \in F(2)$ para todo $x \in F_n$, logo $F_{n+1} \subset F(2)$. Assim, $K \subseteq F(2)$ e isso conclui a demonstração. ■

Para toda 2-extensão $L|F$, temos $L(2) = F(2)$. De fato, como L é uma 2-extensão de F, temos as inclusões: $F \subset L \subset F(2)$. Tomando os fechos quadráticos destes corpos, obtemos $F(2) \subseteq L(2) \subseteq F(2)$ o que implica a igualdade desejada.

Se $L|F$ é uma 2-extensão *finita*, então a teoria de Galois garante a existência de uma torre de corpos

$$F = F_0 \subset F_1 \subset \cdots \subset F_n = L \tag{2.1.2}$$

onde, para cada $1 \leq i \leq n$, $[F_i : F_{i-1}] = 2$. Isso ocorre porque o fecho normal N de $L|F$ é tal que $|G(N|F)| = 2^r$, $r \geq 1$.

Exemplos:

(1) O fecho quadrático de $\mathbb{R}$ é $\mathbb{C}$. De fato, como $-1 \notin \mathbb{R}^2$, $\mathbb{R}$ não é quadraticamente fechado. Por outro lado, $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ é quadraticamente fechado. Uma vez que $[\mathbb{C} : \mathbb{R}] = 2$, o fecho quadrático de $\mathbb{R}$ tem que ser $\mathbb{C}$. Em geral, E é um corpo euclidiano (veja a definição na página 120) se, e somente se, $E(\sqrt{-1})$ é quadraticamente fechado (Teorema B.13).

(2) O fecho quadrático de $\mathbb{Q}$ é o conjunto dos números *construtíveis com régua e compasso*.

(3) O corpo $F = \bigcup_{n\geq 1} \mathbb{F}_5(\sqrt[2^n]{2})$ é quadraticamente fechado, logo é o fecho quadrático de $\mathbb{F}_5$. Para mostrar isso, devemos observar que, em $\mathbb{F}_5$, $0 = 0^2$, $1 = 1^2$, $4 = 2^2$ e $3 = 2^{-1}$. Logo, todo elemento de $\mathbb{F}_5$ é um quadrado em $F_1 = \mathbb{F}_5(\sqrt{2})$. Podemos verificar diretamente que, em F_1, o único elemento que não é um quadrado é "essencialmente"[1], $\sqrt{2}$. Obtemos, então, $\mathbb{F}_5 \subset F_1 \subset F_1(\sqrt[4]{2}) = F_2$ e em F_2 o único elemento que não é um quadrado é "essencialmente", $\sqrt[4]{2}$. Continuando com esse processo, obtemos $F_n = F_{n-1}(\sqrt[2^n]{2})$, para todo $n \geq 2$. Agora, se $x \in F$ então

[1]Por exemplo: $1 + 3\sqrt{2} \notin F_1^2$, mas $1 + 3\sqrt{2} = 3(1 + \sqrt{2})\sqrt{2}$ e $3(1 + \sqrt{2}) = (4 + \sqrt{2})^2 \in F_1^2$. Logo, se $F_2 = F_1(\sqrt[4]{2})$, temos: $\sqrt{2} \in F_2^2$ e $1 + 3\sqrt{2} \in F_2^2$.

$x \in F_n$, para algum $n \geq 1$. Se $x \notin F_n^2$ então $x \in F_{n+1}^2 \subset F^2$. Assim $x \in F^2$, ou seja $F = F^2$.

Chamamos um F-automorfismo $\sigma \in G(F(2)|F)$ de *involução* quando ele tem ordem dois, ou seja, quando $\sigma^2 = 1$ e $\sigma \neq 1$, onde $1 : F(2) \to F(2)$ é a aplicação identidade. Se σ é uma involução, então $\langle\sigma\rangle = \{1, \sigma\}$ é um subgrupo fechado de $G(F(2)|F)$ na topologia de Krull em $G(F(2)|F)$ (veja o Apêndice A, página 111). Denotamos por E_σ o corpo fixo $F(2)^{\{1,\sigma\}}$, isto é:

$$E_\sigma = F(2)^{\{1,\sigma\}} = \{x \in F(2)|\sigma(x) = x\} \tag{2.1.3}$$

Podemos verificar que o Teorema B.13 aplica-se ao corpo E_σ. Mais precisamente, $E_\sigma(\sqrt{-1})$ é quadraticamente fechado e, portanto, E_σ é euclidiano.

Um corpo K é dito *pitagórico* quando toda soma finita de quadrados é um quadrado, isto é, quando $\sum K^2 = K^2$ (veja a notação na página 115). Observe que é suficiente exigir que $1+y^2$ seja um quadrado, para todo $y \in K$. Na Proposição 2.3 abaixo, veremos que a propriedade de ser pitagórico "desce" para extensões finitas.

Proposição 2.3 (Diller - Dress) *Seja $K|F$ uma extensão finita, onde K é pitagórico. Então F também é pitagórico.*

Demonstração ([23], p.269). Vamos usar indução sobre $n = [K : F]$. O caso $n = 1$ é imediato. Suponhamos, então, que $n > 1$. Se F não fosse pitagórico, existiria um elemento $a = 1 + b^2 \notin F^2$ e teríamos $L = F(\sqrt{a}) \subset K$. Como $[K : L] < n$, a hipótese de indução garantiria L pitagórico.

Tomemos agora $x := a + \sqrt{a}$. Sendo L pitagórico, teríamos: $2x = 2(a + \sqrt{a}) = b^2 + 1 + a + 2\sqrt{a} = b^2 + (1 + \sqrt{a})^2 \in L^2$. Como $2 \in L^2$, teríamos $x \in L^2$ e, daí, $N_{L|F}(x) \in F^2$. Por outro lado, $N_{L|F}(x) = a^2 - a = a(a-1) = ab^2 \notin F^2$, contradição. ■

Exemplos de Corpos Pitagóricos:

(1) Um corpo quadraticamente fechado L é pitagórico. De fato, $L^2 \subseteq \sum L^2 \subseteq L = L^2$ implica $\sum L^2 = L^2$.

(2) Se K é pitagórico e não é formalmente real, então K é quadraticamente fechado. De fato, dado $x \in K$, podemos escrever $x = (\frac{x+1}{2})^2 + (-1)(\frac{x-1}{2})^2$ (lembre-se que $car(K) \neq 2$). Como $-1 \in \sum K^2$, temos $x \in K^2 + (-1)K^2 \subseteq \sum K^2 = K^2$,

mostrando que $K = K^2$. Baseados neste fato, a partir daqui *chamaremos de pitagóricos apenas os corpos pitagóricos que também são formalmente reais.*

(3) Todo corpo F real fechado é pitagórico. Isso será provado mais adiante, no parágrafo imediatamente após o Lema 2.7.

(4) Se F_i são subcorpos de um corpo Ω, sendo F_i pitagórico para todo i, então $K = \bigcap_i F_i$ também é pitagórico. Com efeito, dados $x, y \in K$, considere a soma $x^2 + y^2$. Para cada i, existe $z_i \in F_i$ tal que $z_i^2 = x^2 + y^2$. para cada par de índices i, j, temos: $z_i = \pm z_j$. Para um i_0 fixado, temos $z_{i_0} \in \bigcap F_i = K$ e $z_{i_0}^2 = x^2 + y^2$. Observemos que isso é similar ao que já foi feito no Lema 2.1.

O Exemplo (4) acima mostra que, dado um corpo F, faz sentido a noção de menor corpo pitagórico contendo F. De fato, esse corpo minimal é obtido como a interseção de todos os corpos pitagóricos contidos no fecho algébrico F_{alg} de F. Devemos observar que a família $\{F_i\}_{i\in I}$ dos subcorpos pitagóricos de F_{alg} não é vazia, pois o próprio F_{alg} é pitagórico. Denotamos $\bigcap_{i\in I} F_i = F_\pi$, e chamamos esse corpo de *fecho pitagórico* de F. Novamente pelo Exemplo (4) acima, F_π é pitagórico e é evidentemente o menor (em relação à inclusão) dentre todos os F_i. Em particular, como $F(2)$ é pitagórico, temos $F_\pi \subset F(2)$, isto é, F_π é uma 2-extensão de F.

Uma conseqüência imediata da Proposição 2.3 acima é que, se F é um corpo não pitagórico, então $F_\pi|F$ é uma extensão infinita.

Dados um corpo pitagórico $K \supset F$ e um F-homomorfismo $\sigma : K \to F_{\text{alg}}$, temos $\sum \sigma(\dot{K})^2 = \sigma(\sum \dot{K}^2) = \sigma(\dot{K}^2) = \sigma(\dot{K})^2$, ou seja, $\sigma(K)$ também é pitagórico. Como F_π é a interseção de todos os corpos pitagóricos contidos em F_{alg}, segue-se que $F_\pi|F$ é uma extensão normal.

Acabamos de estabelecer um modo de construir F_π "de cima para baixo". Assim como fizemos para o fecho quadrático de um corpo, vamos agora construir F_π "de baixo para cima", o que é útil para fazermos demonstrações por recorrência. Note a semelhança com a Proposição 2.2.

Proposição 2.4 *Dado um corpo F, definimos uma família de corpos $\{F_n\}_{n\geq 0}$ pondo $F_0 = F$ e $F_{n+1} = F_n(\{\sqrt{a} \mid a \in \sum \dot{F}_n^2\})$. Então cada $F_n \subset F_\pi$ e $F_\pi = \bigcup_{n\geq 1} F_n$.*

Demonstração. A família de corpos $\{F_n\}$ é totalmente ordenada, logo a reunião $K = \bigcup_{n\geq 1} F_n$ também é um corpo. Se $x \in K$ então $x \in F_n$ para algum n. Logo, $1 + x^2 \in \sum \dot{F}_n^2$ e $1 + x^2 \in \dot{F}_{n+1}^2 \subset \dot{K}^2$. Assim, K é pitagórico e $F_\pi \subseteq K$.

Por outro lado, $\sum \dot{F}^2 \subset \sum \dot{F}_\pi^2 = \dot{F}_\pi^2$. Logo, dado $s \in \sum \dot{F}^2$ temos $F(\sqrt{s}) \subset F_\pi$. Conseqüentemente, $F_1 \subset F_\pi$. Supondo que $F_n \subset F_\pi$ para algum $n \geq 1$, temos $\sum \dot{F}_n^2 \subset \sum \dot{F}_\pi^2 = \dot{F}_\pi^2$, o que implica $F_n(\sqrt{s}) \subset F_\pi$ para todo $s \in \sum \dot{F}_n^2$ e, daí, $F_{n+1} \subset F_\pi$. Isso mostra que $K \subseteq F_\pi$. ■

No artigo [17], página 178, Griffin define o fecho pitagórico de F usando a construção feita acima. Vale mencionar que, neste mesmo artigo (e na mesma página) Griffin mostra que, para todo $n \geq 0$, $F_{n+1}|F_n$ é uma extensão normal com grupo de Galois $G(F_{n+1}|F_n)$ isomorfo ao produto direto de cópias de $\mathbb{Z}/2\mathbb{Z}$. Contudo, não usaremos este resultado aqui.

Seja T é uma pré-ordem de F e $K|F$ uma extensão de corpos, com K formalmente real. Seguindo a definição da página 117, dizemos que T estende-se a K quando existe uma pré-ordem T_K de K tal que $T_K \cap F = T$.

No caso da extensão $F_\pi|F$, a pré-ordem $\sum \dot{F}^2$ estende-se a $\dot{F}_\pi^2$. De fato, como F_π é pitagórico, $\dot{F}_\pi^2$ é a pré-ordem fraca de F_π. Pelo Teorema B.7, temos: $F_\pi^2 \cap F = (\bigcap_{Q \in X_{F_\pi}} Q) \cap F$, onde X_{F_π} indica, como definido na página 115, o conjunto das ordens de F_π. Agora, o Lema B.9 e a construção de F_π "de baixo para cima" garantem que todas as ordens de F estendem-se[2] para F_π. Assim, temos $(\bigcap_{Q \in X_{F_\pi}} Q) \cap F = \bigcap_{Q \in X_{F_\pi}} (Q \cap F) = \bigcap_{P \in X_F} P = \sum \dot{F}^2$. Portanto, $\dot{F}_\pi^2 \cap F = \sum \dot{F}^2$. O resultado a seguir é bem conhecido e é uma conseqüência desta última igualdade.

Proposição 2.5 ([23], Corolário 4.6, p.258) *Se F é formalmente real, então F_π também é formalmente real.*

Demonstração. No exemplo (2) acima, vimos que um corpo pitagórico que não é formalmente real, é quadraticamente fechado. Portanto, basta mostrarmos que $-1 \notin F_\pi^2$. Por hipótese, $-1 \notin \sum \dot{F}^2$. Por outro lado, $-1 \in F_\pi^2$ implicaria $-1 \in F_\pi^2 \cap F = \sum \dot{F}^2$ e isso conclui a demonstração. ■

Sendo $F_\pi|F$ uma extensão galoisiana, podemos obter alguma informação sobre o grupo de Galois $G(F_\pi|F)$, dada na Proposição 2.6 abaixo, que é um corolário imediato da Proposição 2.3.

Proposição 2.6 *Dado um corpo F, o grupo de Galois $G(F_\pi|F)$ é trivial ou livre de torção.*

[2] Não necessariamente de modo único!

Demonstração. Suponhamos que exista $\sigma \in G = G(F_\pi|F)$ com $\sigma^n = 1$ para algum $n \geq 1$. Seja H o subgrupo de G gerado por σ e K o corpo fixo de H. Então $[F_\pi : K] = |H| = n < \infty$. Pela Proposição 2.3, K é pitagórico e, pela minimalidade do fecho, $K = F_\pi$ e $n = 1$, o que mostra que $\sigma = 1$. ■

Lema 2.7 *Se F é formalmente real mas a extensão quadrática $F(\sqrt{a})$ não é formalmente real, então $-a \in \sum \dot{F}^2$.*

Demonstração. Como $F(\sqrt{a})$ não é formalmente real, nenhuma ordem de F estende-se a esse corpo. Assim, pelo Lema B.9, $a \notin P$ para todo $P \in X_F$, o que implica $-a \in P$, para todo $P \in X_F$. Logo, $-a \in \bigcap P = \sum \dot{F}^2$. ■

Usando o resultado acima, vamos mostrar, como prometido no Exemplo (3), página 5, que todo corpo real fechado é pitagórico. De fato, como F é real fechado, em particular é formalmente real. Se existisse $x = 1 + y^2 \notin F^2$, então $F(\sqrt{x})$ seria uma extensão algébrica própria de F e, portanto, não seria formalmente real (pela definição de corpo real fechado, na página 119). Pelo Lema 2.7, existiriam $z_i \in F$ tais que $\sum {z_i}^2 = -x = -1 - y^2$, isto é, $-1 = y^2 + \sum {z_i}^2 \in \sum \dot{F}^2$ e F não seria formalmente real, contradição. Logo, todo elemento do tipo $1 + y^2$ é um quadrado em F, isto é, F é pitagórico.

Tendo construído o fecho quadrático e o fecho pitagórico de um corpo formalmente real F, faz sentido perguntar se há algum tipo de fecho relacionado a uma pré-ordem arbitrária T de F. Ao contrário do que fizemos nos dois casos anteriores, começaremos construindo um tal fecho "de baixo para cima" para depois seguirmos o caminho oposto.

A idéia é considerar, como fizemos antes, uma família $\{F_n\}_{n\geq 0}$ de corpos definidos recursivamente pondo $F_0 = F$, $F_1 = F(\{\sqrt{t} \,|\, t \in T\})$ e assim por diante. O interessante é que, a partir de F_2, a construção é similar à do fecho pitagórico, dada na Proposição 2.4. Para explicar esse fato devemos lembrar que, pelo Teorema B.7, $T = \bigcap_{P\in X/T} P$. Pelo Lema B.9, as ordens de F que estendem-se a F_1 são exatamente aquelas contidas em X/T. Procedendo de modo análogo ao que fizemos no parágrafo imediatamente anterior à Proposição 2.5, vemos que

$$(\sum \dot{F}_1^2) \cap F = (\bigcap_{Q\in X_{F_1}} Q) \cap F = \bigcap_{Q\in X_{F_1}} (Q \cap F) = \bigcap_{P\in X/T} P = T.$$

Assim, $F_2 = F_1(\{\sqrt{s} \mid s \in \sum \dot{F}_1^2\})$ e, a partir desse ponto, a construção é a mesma da Proposição 2.4. Essa argumentação justifica a definição a seguir.

Definição 2.8 *Dada uma pré-ordem T em F, definimos:*

(a) $F_1 = F(\{\sqrt{t} | t \in T\})$.

(b) F_T *é o fecho pitagórico de* F_1.

Chamamos F_T de fecho pitagórico de F em relação a T, ou, simplesmente, T-fecho.

Proposição 2.9 *O corpo F_T é formalmente real, pitagórico e T estende-se a $\dot{F}_T^2$, isto é, $\dot{F}_T^2 \cap F = T$. Além disso, se $K \supset F$ é pitagórico e $\dot{K}^2 \cap F = T$, então $F_T \subset K$.*

Demonstração. É imediato que F_T é pitagórico, uma vez que F_T é o fecho pitagórico de F_1. As ordens de F que se estendem a F_1 são exatamente aquelas que contêm T. De fato, se P é uma ordem de F tal que $P \not\supset T$, então existe $t \in T \smallsetminus P$. Pelo Lema B.9, P não se estende a $F(\sqrt{t})$ e, portanto, não se estende a F_1. Reciprocamente, se $P \supset T$, então, novamente pelo Lema B.9, P estende-se a $F(\sqrt{t})$, para todo $t \in T$ e, portanto, estende-se a F_1. Podemos então concluir que $\sum \dot{F}_1^2 \cap F = T$. Como F_T é o fecho pitagórico de F_1, das observações feitas imediatamente antes da Proposição 2.5 vem que $\dot{F}_T^2 \cap F_1 = \sum \dot{F}_1^2$. Logo, $\dot{F}_T^2 \cap F = \sum \dot{F}_1^2 \cap F = T$. Como F_1 é formalmente real, F_T também é formalmente real, pela Proposição 2.5. Finalmente, se K é pitagórico e $\dot{K}^2 \cap F = T$, então $\sqrt{t} \in K$ para todo $t \in T$, o que implica $F_1 \subset K$. Logo, sendo K pitagórico, temos $K \supset (F_1)_\pi = F_T$. ■

Como prometido, exibiremos agora um modo de construir F_T "de cima para baixo". De fato, temos a seguinte caracterização do T-fecho F_T como uma interseção de corpos euclidianos (para a definição de corpo euclidiano, veja a página 120):

Proposição 2.10 *Seja F um corpo formalmente real e T uma pré-ordem em F. Então $F_T = \bigcap_{E \in \mathcal{E}} E$, onde $\mathcal{E} = \mathcal{E}_T = \{E \mid F \subseteq E \subseteq F(2)$, E é euclidiano e $E^2 \cap F \supset T\}$. A extensão $F_T|F$ é galoisiana.*

Demonstração. ($\subseteq$) Seja E um corpo euclidiano com $F \subset E \subset F(2)$ e $E^2 \cap F \supset T$. Sabemos que E^2 é uma (a única) ordem em E. Logo, $E^2 \cap F$ é uma ordem em F contendo T.

Dado $t \in T \subset E^2 \cap F$, temos $\sqrt{t} \in E$. Assim, $F(\sqrt{t}) \subset E$, para todo $t \in T$, o que implica que $F_1 \subset E$. Como E é pitagórico e $F_1 \subset E$, o fecho pitagórico de F_1 está contido em E, ou seja $F_T \subseteq E$ para todo E em $\mathcal{E}$. Portanto, $F_T \subseteq \bigcap_{E\in\mathcal{E}} E$.

($\supseteq$) Suponha que $F_T \subsetneq \bigcap_{E\in\mathcal{E}} E$. Então, existe um elemento $a \in F_T$ tal que $F_T \subsetneq F_T(\sqrt{a}) \subseteq \bigcap_{E\in\mathcal{E}} E$. Assim, $\sqrt{a} \in E$, para todo $E \in \mathcal{E}$, donde $a \in E^2 \cap F_T$, para todo $E \in \mathcal{E}$. Agora, dada uma ordem Q em F_T, temos que $Q \cap F \supset T$, pois $Q \supset F_T^2$ e $F_T^2 \cap F = T$. Se E é um corpo euclidiano tal que $E^2 \cap F_T = Q$, então $E^2 \cap F = Q \cap F \supset T$, logo $E \in \mathcal{E}_T$. Assim, toda ordem de F_T é induzida pela ordem de um corpo euclidiano pertencente a $\mathcal{E}_T$. Como $a \in E^2 \cap F_T$, para todo $E \in \mathcal{E}_T$, temos que $a \in \bigcap_{Q\in X_{F_T}} Q = \sum F_T^2 = F_T^2$. Mas isso contradiz a hipótese $F_T \subsetneq F_T(\sqrt{a})$, e, assim, temos a igualdade procurada.

Para mostrarmos a última afirmação devemos observar que, para cada $E \in \mathcal{E}$ e $\sigma \in G(F(2)|F)$, é imediato que $\sigma(E) \in \mathcal{E}$. Logo $\sigma(F_T) \subset F_T$ e $F_T|F$ é uma extensão normal, logo galoisiana[3]. ■

Quando $T = P$ é uma ordem, todas as ordens[4] do corpo F_P estendem P. Neste caso, podemos reescrever o resultado da Proposição 2.10 como: $F_P = \bigcap_{E\in\mathcal{E}} E$, onde $\mathcal{E} = \{E|$ $F \subseteq E \subseteq F(2)$, E é euclidiano e $E^2 \cap F = P\}$. Um corpo euclidiano E é dito *fecho euclidiano* de (F, P) quando $F_P \subset E$. Cada corpo euclidiano $F \subset E \subset F(2)$ é um fecho euclidiano em relação à ordem $E^2 \cap F$. Devemos notar ainda que, se $P \in X/T$, isto é, P é uma ordem contendo a pré-ordem T, então $F_T \subseteq F_P$, a igualdade ocorrendo se e somente se $T = P$. Temos ainda o seguinte resultado:

Corolário 2.11 *Com as notações estabelecidas acima,* $F_T = \bigcap_{P\in X/T} F_P$.

Demonstração. Pelas observações feitas acima, basta provar a inclusão "$\supseteq$". Se $x \in F_P$, para todo $P \in X/T$, então $x \in E$ para todo corpo euclidiano E tal que $E^2 \cap F \in X/T$, isto é, $E^2 \cap F \supset T$. Logo, pela Proposição 2.10, $x \in F_T$. ■

Estabelecemos no Teorema 2.12 a seguir a recíproca da Proposição 2.9. Lembremos que, de acordo com o Exemplo 2 da página 4, para nós, um corpo pitagórico também é

[3]Todas as extensões são separáveis pois os corpos envolvidos têm sempre característica zero.

[4]Como $F_P^2 \cap F = P$, num primeiro momento poderíamos pensar que F_P^2 é uma ordem, mas isso não é verdade. Como F_P é pitagórico, $F_P^2 = \sum \dot{F}_P^2$ é a pré-ordem fraca de F_P. Logo $\bigcap Q = F_P^2$, onde $Q \in X_{F_P}$. O que ocorre é que $Q \cap F = P$ para toda ordem Q de F_P, pois a única ordem de F que se estende a F_P é P, mas ela não se estende de modo único.

formalmente real.

Teorema 2.12 *Dado um corpo formalmente real F, uma extensão $K|F$ contida em $F(2)$ é normal e pitagórica se e somente se $K = F_T$, onde $T = \dot{K}^2 \cap F$.*

Demonstração. A necessidade já foi demonstrada na Proposição 2.9. Vamos demonstrar a suficiência.

Como K é pitagórico, $T = \dot{K}^2 \cap F$ é uma pré-ordem de F e $F_T \subseteq K$. Consideremos, agora, $E \in \mathcal{E}_T$, isto é, um corpo euclidiano E tal que $F \subset E \subset F(2)$ e $\dot{E}^2 \cap F \supset T$; denotamos $G(F(2)|E) = \{1, \sigma\}$. Seja P uma ordem de K que estende $\dot{E}^2 \cap F$ e E_1 um corpo euclidiano contendo K tal que $\dot{E}_1^2 \cap K = P$; denotamos $G(F(2)|E_1) = \{1, \sigma_1\}$. Então $\dot{E}_1^2 \cap F = P \cap F = \dot{E}^2 \cap F$. Pela Proposição B.16, existe $g \in G(F(2)|F)$ tal que $\sigma = g\sigma_1 g^{-1}$. Uma vez que $K|F$ é uma extensão normal, $G(F(2)|K)$ é subgrupo normal de $G(F(2)|F)$ e, como $\sigma_1 \in G(F(2)|K)$, temos $\sigma \in G(F(2)|K)$. Isso significa que $E \supset K$, para todo $E \in \mathcal{E}_T$, ou seja, $K \subseteq \bigcap_{E \in \mathcal{E}_T} E = F_T$. Logo, vale a igualdade $K = F_T$, como queríamos. ■

Capítulo 3

Elementos rígidos, birígidos e básicos

Neste capítulo estudamos alguns elementos que aparentemente têm propriedades muito simples. Eles são usualmente denominados "rígidos" e "birígidos". Curiosamente, a presença de um número apropriado de rígidos em um corpo determina fortemente outras propriedades do corpo. O trabalho, neste capítulo, inicia-se com o estudo de elementos rígidos e de como produzir birígidos a partir de rígidos. Em seguida analisamos as propriedades do conjunto dos não-birígidos, que são chamados de "básicos". Logo após, veremos como os elementos rígidos se comportam em relação a 2-extensões, isto é, extensões do corpo dentro do fecho quadrático, como definimos na página 2. Finalizamos o capítulo estudando o comportamento dos subgrupos R_d (veja a Definição 3.3) e $T_d = R_d \cdot \sum \dot{F}^2$ em relação a 2-extensões de F.

Baseados nos resultados obtidos para birígidos e básicos de um corpo F construiremos, no capítulo seguinte, anéis de valorização de F que gozam de uma propriedade de compatibilidade relativa a um subgrupo de $\dot{F}$ (veja a definição na página 49). Veremos que, para subgrupos específicos de $\dot{F}$, essa compatibilidade implica uma propriedade análoga a henselianidade. Classificaremos essa propriedade como henselianidade relativa. Essa é nossa meta principal destes dois capítulos: construir os anéis de valorização compatíveis com subgrupos de $\dot{F}$. Esses anéis serão decisivos para o trabalho feito no Capítulo 5, onde vamos abordar o problema da decomposição do anel de Witt de um corpo em fatores com estrutura mais simples.

3.1 O grupo $D\langle 1,-d\rangle$ com d rígido: apresentação

Nesta seção, introduzimos os conceitos de rigidez e birigidez em um corpo F. Coletamos as propriedades básicas desses elementos, que serão utilizadas em capítulos posteriores. Estamos particularmente interessados no grupo $D\langle 1,-d\rangle$, onde d é rígido. Exibimos ainda uma série de exemplos de elementos rígidos e birígidos.

Seja R um subgrupo do grupo multiplicativo $\dot{F}$ do corpo F e $R^\bullet = R\cup\{0\}$. Dado $x\in F$, o conjunto $R+xR=\{r_1+xr_2\neq 0 | r_1,r_2\in R^\bullet\}$ contém $R\cup xR$. Um elemento $x\in F$ é dito *R-rígido*[1] se $x\notin R$ e $R+xR=R\cup xR$. Se x e $-x$ são ambos R-rígidos, dizemos que x é *R-birígido*.

Quando $R=\dot{F}^2$, dizemos simplesmente que x é *rígido* ou *birígido* ao invés de *$\dot{F}^2$-rígido* ou *$\dot{F}^2$-birígido*, respectivamente. Devemos observar que, neste caso, $R+xR=\dot{F}^2+x\dot{F}^2=D\langle 1,x\rangle$, o subgrupo de $\dot{F}$ formado pelos elementos representados pela forma de Pfister $\langle 1,x\rangle$ (veja o Lema C.8). Assim, x é rígido se, e somente se, a forma $\langle 1,x\rangle$ representa apenas os elementos de $\dot{F}^2\cup x\dot{F}^2$.

Se $d\in F$ é um elemento rígido, a estrutura de $D\langle 1,d\rangle$ é, como vimos, bem simples. Se d é birígido, $D\langle 1,-d\rangle=\dot{F}^2\cup -d\dot{F}^2$ tem uma estrutura similar. No caso em que d é um elemento rígido que não é birígido, a estrutura de $D\langle 1,-d\rangle$ não é tão simples. Lembremos que, pelo Lema C.8, $D\langle 1,-d\rangle$ é subgrupo de $\dot{F}$.

De acordo com o Corolário do Teorema 1 de [8], em um corpo não formalmente real, todo rígido é birígido. Por isso, só faz sentido considerarmos corpos formalmente reais neste trabalho.

Os próximos resultados são devidos a Bos [5]. Vamos apresentar suas demonstrações para conveniência do leitor e por serem de importância crucial para a realização deste trabalho. Suas demonstrações são muito técnicas e levarão o leitor através da montagem de um quebra-cabeças necessário para obtermos os birígidos que serão usados na construção de anéis de valorização no capítulo seguinte.

O Lema 3.1 a seguir é técnico, e será utilizado duas vezes no que se segue. A primeira, na discussão anterior ao Lema 3.2 e a segunda, na demonstração do item (v) da Proposição 3.4.

Lema 3.1 (Bos [5], Lema 1.8) *Sejam $x,d\in\dot{F}$, com d rígido. Então:*

(i) $D\left(\langle 1,d\rangle\otimes\langle 1,x\rangle\right)=\left(D\langle 1,x\rangle\cup dD\langle 1,x\rangle\right)\cup\left(D\langle 1,dx\rangle\cup dD\langle 1,dx\rangle\right)$

[1] Alguns autores permitem a existência de rígidos em R. Isso é óbvio no caso em que R é fechado para soma (por exemplo, se R é uma pré-ordem). Nossa hipótese adicional $x\notin R$ será útil adiante.

(ii) $D\langle 1,x\rangle = (D\langle 1,x\rangle \cap D\langle 1,-d\rangle) \cup x\,(D\langle 1,x\rangle \cap D\langle 1,-d\rangle)$ *ou*
$D\langle 1,dx\rangle = (D\langle 1,dx\rangle \cap D\langle 1,-d\rangle) \cup dx\,(D\langle 1,dx\rangle \cap D\langle 1,-d\rangle)$

Demonstração. $D(\langle 1,d\rangle \otimes \langle 1,x\rangle) = D\langle 1,d,x,dx\rangle = D\left(\langle 1,d\rangle \perp x\langle 1,d\rangle\right)$. Pela Proposição C.10, temos:

$$D\left(\langle 1,d\rangle \perp x\langle 1,d\rangle\right) = \bigcup_{\alpha,\beta\in D\langle 1,d\rangle} D\langle \alpha,\beta x\rangle.$$

Como $D\langle 1,d\rangle = \dot{F}^2 \cup d\dot{F}^2$, esta união é igual a $D\langle 1,x\rangle \cup D\langle 1,dx\rangle \cup D\langle d,x\rangle \cup D\langle d,dx\rangle = (D\langle 1,x\rangle \cup dD\langle 1,x\rangle) \cup (D\langle 1,dx\rangle \cup dD\langle 1,dx\rangle)$, o que demonstra (i).

Como $\langle 1,d\rangle \otimes \langle 1,x\rangle$ é uma 2-forma de Pfister (veja a página 131), $D(\langle 1,d\rangle \otimes \langle 1,x\rangle)$ é um grupo e $D\langle 1,x\rangle \cup dD\langle 1,x\rangle = D\langle 1,x\rangle \cdot D\langle 1,d\rangle$ e $D\langle 1,dx\rangle \cup dD\langle 1,dx\rangle = D\langle 1,dx\rangle \cdot D\langle 1,d\rangle$ são subgrupos, uma das seguintes inclusões ocorre:

$$D\langle 1,x\rangle \cup dD\langle 1,x\rangle \subset D\langle 1,dx\rangle \cup dD\langle 1,dx\rangle \text{ ou}$$

$$D\langle 1,x\rangle \cup dD\langle 1,x\rangle \supset D\langle 1,dx\rangle \cup dD\langle 1,dx\rangle.$$

Suponhamos que valha a primeira dessas inclusões. Temos: $D\langle 1,x\rangle \subset D\langle 1,dx\rangle \cup dD\langle 1,dx\rangle = D\langle 1,dx\rangle \cup xD\langle 1,dx\rangle$. Logo, $D\langle 1,x\rangle = (D\langle 1,x\rangle \cap D\langle 1,dx\rangle) \cup x(D\langle 1,x\rangle \cap D\langle 1,dx\rangle)$. Pelo item (2) da Proposição C.9, temos, finalmente: $D\langle 1,x\rangle = (D\langle 1,x\rangle \cap D\langle 1,-d\rangle) \cup x(D\langle 1,x\rangle \cap D\langle 1,-d\rangle)$ e isso mostra a primeira afirmação em (ii). Substituindo x por dx obtemos a segunda afirmação. De modo similar, podemos obter as mesmas igualdades se considerarmos válida a segunda inclusão, ao invés da primeira. ■

Fixemos $d \in \dot{F}$, rígido, e consideremos $x \in D\langle 1,-d\rangle$. Temos $d \in D\langle 1,-x\rangle$ e, portanto, $d\langle 1,-x\rangle \simeq \langle 1,-x\rangle$. Usando essa simetria, podemos escrever $\langle 1,-x\rangle \otimes d\langle 1,-x\rangle \simeq \langle 1,-x\rangle \otimes \langle 1,-x\rangle \simeq \langle 1,1\rangle \otimes \langle 1,-x\rangle$. Como também temos $\langle 1,-x\rangle \otimes d\langle 1,-x\rangle \simeq \langle 1,d\rangle \otimes \langle 1,-x\rangle$, o item (i) do Lema 3.1 nos diz que

$D(\langle 1,d\rangle \otimes \langle 1,-x\rangle) = (D\langle 1,-x\rangle \cup dD\langle 1,-x\rangle) \cup (D\langle 1,-dx\rangle \cup dD\langle 1,-dx\rangle) = D\langle 1,-x\rangle \cup (D\langle 1,-dx\rangle \cup dD\langle 1,-dx\rangle)$ e

$$D(\langle 1,1\rangle \otimes \langle 1,-x\rangle) = D\langle 1,-x\rangle \cup (D\langle 1,-dx\rangle \cup dD\langle 1,-dx\rangle).$$

Como $-dx \in D\langle 1,-d\rangle$, podemos substituir x por $-dx$ na igualdade acima, para chegarmos em

$$D(\langle 1,1\rangle \otimes \langle 1,dx\rangle) = D\langle 1,dx\rangle \cup (D\langle 1,x\rangle \cup dD\langle 1,x\rangle).$$

Como $D\langle 1,-dx\rangle \cup dD\langle 1,-dx\rangle = D\langle 1,-dx\rangle \cdot D\langle 1,d\rangle$ e $D\langle 1,x\rangle \cup dD\langle 1,x\rangle = D\langle 1,x\rangle \cdot D\langle 1,d\rangle$ são grupos e, como um grupo não é união de dois subgrupos próprios, existem quatro combinações possíveis para descrever $D(2\langle 1,-x\rangle)$ e $D(2\langle 1,dx\rangle)$. Vamos resumir essas quatro possibilidades em duas alternativas:

$$D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle \text{ ou } D(2\langle 1,dx\rangle) = D\langle 1,dx\rangle, \tag{3.1.1}$$

$$\begin{gathered} D(2\langle 1,-x\rangle) = D\langle 1,-dx\rangle \cup dD\langle 1,-dx\rangle \\ \text{e} \\ D(2\langle 1,dx\rangle) = D\langle 1,x\rangle \cup dD\langle 1,x\rangle. \end{gathered} \tag{3.1.2}$$

A seguir veremos que assumindo-se que

$$\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2 \tag{3.1.3}$$

a alternativa (3.1.2) implica (3.1.1). A partir de agora estaremos sempre supondo que a hipótese (3.1.3) vale, e consequentemente, após demonstrar o Lema 3.2, teremos que uma das duas alternativas de (3.1.1) sempre ocorre.

Lema 3.2 (Bos [5], Lema 1.10) *Mantendo as notações anteriores e supondo ainda que $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$, temos:*

$$D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle \text{ } ou \text{ } D(2\langle 1,dx\rangle) = D\langle 1,dx\rangle.$$

Demonstração. Mostraremos que se vale (3.1.2), então (3.1.1) também vale. Assumindo-se (3.1.2) temos em particular, $D\langle 1,1\rangle \subset D\langle 1,x\rangle \cup dD\langle 1,x\rangle$ e $D\langle 1,1\rangle \subset D\langle 1,-dx\rangle \cup dD\langle 1,-dx\rangle$, de onde obtemos:

$$D\langle 1,1\rangle = (D\langle 1,x\rangle \cap D\langle 1,1\rangle) \cup (dD\langle 1,x\rangle \cap D\langle 1,1\rangle), \tag{3.1.4}$$

$$D\langle 1,1\rangle = (D\langle 1,-dx\rangle \cap D\langle 1,1\rangle) \cup (dD\langle 1,-dx\rangle \cap D\langle 1,1\rangle). \tag{3.1.5}$$

Supondo $d \in D\langle 1,x\rangle$, da igualdade (3.1.4) vem que $D\langle 1,1\rangle \subset D\langle 1,x\rangle$ e, como $d \in D\langle 1,x\rangle \cap D\langle 1,d\rangle \overset{C.9(2)}{\subset} D\langle 1,-dx\rangle$, a igualdade (3.1.5) nos diz que $D\langle 1,1\rangle \subset D\langle 1,-dx\rangle$. Juntando essas duas informações, obtemos $D\langle 1,1\rangle \subset D\langle 1,x\rangle \cap D\langle 1,-dx\rangle \overset{C.9(2)}{\subset} D\langle 1,d\rangle$ e, por indução, obtemos $\sum \dot{F}^2 \subset D\langle 1,d\rangle = \dot{F}^2 \cup d\dot{F}^2$, contrariando a nossa hipótese.

Assim, $d \notin D\langle 1,x\rangle$ e, como $d \in D\langle 1,-x\rangle$ e $D\langle 1,-x\rangle \cap D\langle 1,1\rangle \overset{C.9(2)}{\subset} D\langle 1,x\rangle$, concluímos que $d \notin D\langle 1,1\rangle$. Vamos fixar para uso futuro que

$$d \notin D\langle 1,x\rangle, \quad d \notin D\langle 1,1\rangle. \tag{3.1.6}$$

Por C.9, item (2), $D\langle 1,x\rangle \cap D\langle 1,-dx\rangle = D\langle 1,x\rangle \cap D\langle 1,d\rangle = D\langle 1,x\rangle \cap (\dot{F}^2 \cup d\dot{F}^2) = \dot{F}^2 \cup (D\langle 1,x\rangle \cap d\dot{F}^2) = \dot{F}^2$. Logo,

$$D\langle 1,x\rangle \cap D\langle 1,-dx\rangle = \dot{F}^2. \tag{3.1.7}$$

Denotemos $A = D\langle 1,x\rangle \cap dD\langle 1,-dx\rangle$, $B = D\langle 1,x\rangle \cap D\langle 1,1\rangle$, $C = dD\langle 1,x\rangle \cap D\langle 1,1\rangle$, $D = D\langle 1,-dx\rangle \cap D\langle 1,1\rangle$ e $E = dD\langle 1,-dx\rangle \cap D\langle 1,1\rangle$. Podemos escrever $D\langle 1,1\rangle$ como interseção do lado direito das equações (3.1.4) e (3.1.5) para obtemos

$$D\langle 1,1\rangle = (B \cap D) \cup (C \cap D) \cup (B \cap E) \cup (C \cap E). \tag{3.1.8}$$

Podemos simplificar a expressão (3.1.8) acima observando que

1. $B \cap D = (D\langle 1,x\rangle \cap D\langle 1,1\rangle) \cap (D\langle 1,-dx\rangle \cap D\langle 1,1\rangle) = (D\langle 1,x\rangle \cap D\langle 1,-dx\rangle) \cap D\langle 1,1\rangle$. Por (3.1.7), $B \cap D = \dot{F}^2 \cap D\langle 1,1\rangle = \dot{F}^2$,
2. $C \cap D = (dD\langle 1,x\rangle \cap D\langle 1,-dx\rangle) \cap D\langle 1,1\rangle = dA \cap D\langle 1,1\rangle$,
3. $B \cap E = (D\langle 1,x\rangle \cap dD\langle 1,-dx\rangle) \cap D\langle 1,1\rangle = A \cap D\langle 1,1\rangle$ e, finalmente,
4. $C \cap E = (dD\langle 1,x\rangle \cap D\langle 1,1\rangle) \cap (dD\langle 1,-dx\rangle \cap D\langle 1,1\rangle) = d(D\langle 1,x\rangle \cap D\langle 1,-dx\rangle) \cap D\langle 1,1\rangle$. Agora, de acordo com (3.1.6) e (3.1.7), $C \cap E = d\dot{F}^2 \cap D\langle 1,1\rangle = \emptyset$.

Com as simplificações acima, podemos reescrever (3.1.8) como

$$D\langle 1,1\rangle = \dot{F}^2 \cup (D\langle 1,1\rangle \cap A) \cup (D\langle 1,1\rangle \cap dA). \tag{3.1.9}$$

Uma vez que $D\langle 1,1\rangle \neq \dot{F}^2$, a igualdade (3.1.9) implica que $(D\langle 1,1\rangle \cap A) \smallsetminus \dot{F}^2 \neq \emptyset$ ou $(D\langle 1,1\rangle \cap dA) \smallsetminus \dot{F}^2 \neq \emptyset$.

Suponhamos que exista $a \in D\langle 1,1\rangle \cap A$, $a \notin \dot{F}^2$. Então $a \in A = D\langle 1,x\rangle \cap dD\langle 1,-dx\rangle$. Resulta, então, que $a \in D\langle 1,x\rangle$ e $dD\langle 1,-dx\rangle = aD\langle 1,-dx\rangle$. Assim, $A = D\langle 1,x\rangle \cap dD\langle 1,-dx\rangle = aD\langle 1,x\rangle \cap aD\langle 1,-dx\rangle = a\dot{F}^2$, por (3.1.7). Como $a \in D\langle 1,1\rangle$ e $d \notin D\langle 1,1\rangle$, temos $D\langle 1,1\rangle \cap dA = D\langle 1,1\rangle \cap da\dot{F}^2 = \emptyset$. Assim, (3.1.9) se tranforma em

$$D\langle 1,1\rangle = \dot{F}^2 \cup a\dot{F}^2. \tag{3.1.10}$$

Por outro lado, $D(2\langle 1,-x\rangle) = D(\langle 1,1\rangle \perp -x\langle 1,1\rangle)$. Logo (3.1.10) e a Proposição C.10 nos dizem que combinado as quatro possibilidades resultantes de $\dot{F}^2 \cup a\dot{F}^2$ e $-x\dot{F}^2 \cup -xa\dot{F}^2$ vamos obter

$D(\langle 1,1\rangle \perp -x\langle 1,1\rangle) = D\langle 1,-x\rangle \cup D\langle 1,-ax\rangle \cup D\langle a,-x\rangle \cup D\langle a,-ax\rangle = D\langle 1,-x\rangle \cdot (\dot{F}^2 \cup a\dot{F}^2) \cup D\langle 1,-ax\rangle \cdot (\dot{F}^2 \cup a\dot{F}^2)$. Porém, $a \in D\langle 1,1\rangle \cap A \subset D\langle 1,1\rangle \cap D\langle 1,x\rangle \overset{C.9(2)}{\subset} D\langle 1,-x\rangle$ e também $a \in D\langle 1,x\rangle \cap D\langle 1,a\rangle \overset{C.9(2)}{\subset} D\langle 1,-ax\rangle$. Logo, $D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle \cup D\langle 1,-ax\rangle$ é uma união de dois subgrupos. Conseqüentemente, $D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle$ ou $D(2\langle 1,-x\rangle) = D\langle 1,-ax\rangle$. Se vale a última igualdade, temos $d \in D\langle 1,-x\rangle \subset D\langle 1,-ax\rangle$, donde $x, ax \in D\langle 1,-d\rangle$. Do fato de $D\langle 1,-d\rangle$ ser grupo resulta então $a \in D\langle 1,-d\rangle \cap D\langle 1,1\rangle \subset D\langle 1,d\rangle = \dot{F}^2 \cup d\dot{F}^2$. Como $a \notin \dot{F}^2$, temos $a \in d\dot{F}^2$, o que implica $d \in a\dot{F}^2 \subset D\langle 1,1\rangle$ e isso contradiz (3.1.6). Portanto, vale $D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle$.

Se admitirmos a existência de $a \in D\langle 1,1\rangle \cap dA$, com $a \notin \dot{F}^2$, chegaremos, de modo semelhante ao que fizemos acima, a $D(2\langle 1,dx\rangle) = D\langle 1,dx\rangle$. Basta observarmos que dA é obtido a partir de A, substituindo x por $-dx$. ■

Os subgrupos de $\dot{F}$ definidos a seguir terão papel importante em todo o restante do trabalho. A Proposição 3.4 logo abaixo já traz alguns resultados importantes sobre R_d. Já S_d será estudado na próxima seção.

Definição 3.3 *Dado um elemento $d \in \dot{F}$ definimos os seguintes subgrupos de $\dot{F}$, que chamaremos de* radicais associados *a d:*

$$R_d = D\langle 1,-d\rangle \cap \bigcap_{s \in \sum F^2} D\langle 1,-s\rangle \quad e$$

$$S_d = \bigcap_{t \in R_d} D\langle 1,-t\rangle.$$

Proposição 3.4 (Bos [5], Corolário 1.11) *Suponha que $d \in F$ é um elemento rígido. Seja $R = R_d$ e $a \in R$. Então:*

(i) $\sum \dot{F}^2 \subset D\langle 1,-a\rangle$.

(ii) *R é um subgrupo de $D\langle 1,-d\rangle$ e $D\langle 1,-d\rangle = R \cup -dR$.*

Suponha ainda que $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$. Então:

(iii) $D\langle 1,-d\rangle = R \dot{\cup} -dR$ *(união disjunta).*

(iv) $D(2\langle 1,-a\rangle) = D\langle 1,-a\rangle$ *e* $D\langle 1,1\rangle \subset D\langle 1,a\rangle$

(v) $D\langle 1,-ad\rangle = D\langle 1,-a\rangle \cap D\langle 1,-d\rangle$ *e* $D\langle 1,ad\rangle \subset D\langle 1,-d\rangle \cup -D\langle 1,-d\rangle$.

Demonstração. (i) Se $a \in R$, então $a \in D\langle 1,-s\rangle$, para todo $s \in \sum \dot{F}^2$, isto é, $s \in D\langle 1,-a\rangle$, para todo $s \in \sum \dot{F}^2$. Logo $\sum \dot{F}^2 \subset D\langle 1,-a\rangle$.

(ii) $R \subset D\langle 1,-d\rangle$ segue-se imediatamente da definição de R. A partir dessa inclusão, vemos que $-dR \subset -dD\langle 1,-d\rangle = D\langle 1,-d\rangle$. Assim, $R \cup -dR \subset D\langle 1,-d\rangle$. Se $\sum \dot{F}^2 \subset \dot{F}^2 \cup d\dot{F}^2$, então (novamente pela definição de R) $R = D\langle 1,-d\rangle$. Em particular, $-d \in R$ e, neste caso, ocorre a igualdade $D\langle 1,-d\rangle = R = R \cup -dR$.

Iremos supor, agora, que $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$. Seja

$$R' = \{x \in D\langle 1,-d\rangle \mid D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle\}.$$

Pelo Lema 3.2, $D\langle 1,-d\rangle = R' \cup -dR'$. De fato, se $x \in D\langle 1,-d\rangle \setminus R'$, então $D(2\langle 1,dx\rangle) = D\langle 1,dx\rangle$, ou seja, $-dx \in R'$.

Agora, se $x \in R'$, então $D\langle 1,1\rangle \subset D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle$ e, supondo $D(n\langle 1\rangle) \subset D\langle 1,-x\rangle$, temos $D(2n\langle 1\rangle) \subset D(2\langle 1,-x\rangle) = D\langle 1,-x\rangle$. Logo, por indução, $\sum \dot{F}^2 \subset D\langle 1,-x\rangle$ e, daí, $x \in R$. Portanto, $R' \subset R$.

Assim, $D\langle 1,-d\rangle = R' \cup -dR' \subset R \cup -dR \subset D\langle 1,-d\rangle$ e $D\langle 1,-d\rangle = R \cup -dR$. Se $R \cap -dR \neq \emptyset$, então $-d \in R$ e, por (i), $\sum \dot{F}^2 \subset D\langle 1,d\rangle = \dot{F}^2 \cup d\dot{F}^2$, contrariando a hipótese. Isso mostra a validade de (iii).

Como $R\dot{\cup} - dR = R' \cup -dR'$, temos $R = R'$, do contrário, $R' \subsetneq R$ implicaria $\emptyset \neq -dR' \cap R \subset -dR \cap R$, o que não ocorre, como já vimos. Isso mostra a primeira parte de (iv). Temos, em particular, $D\langle 1,1\rangle \subset D\langle 1,-a\rangle$ e, pelo item (2) da Proposição C.9, $D\langle 1,1\rangle \subset D\langle 1,a\rangle$.

Resta mostrar o item (v). Temos $D\langle 1,-ad\rangle \subset D(\langle 1,d\rangle \otimes \langle 1,-a\rangle) = D(\langle 1,-a\rangle \perp d\langle 1,-a\rangle)$. Como $a \in D\langle 1,-d\rangle$ também temos $d \in D\langle 1,-a\rangle$ e, daí, $d\langle 1,-a\rangle \simeq \langle 1,-a\rangle$ e portanto $\langle 1,-a\rangle + d\langle 1,-a\rangle \simeq 2\langle 1,-a\rangle$. Logo, $D\langle 1,-ad\rangle \subset D(2\langle 1,-a\rangle) = D\langle 1,-a\rangle$ e $D\langle 1,-ad\rangle = D\langle 1,-a\rangle \cap D\langle 1,-ad\rangle$. Novamente, pelo item (2) de C.9,

$$D\langle 1,-ad\rangle = D\langle 1,-a\rangle \cap D\langle 1,-d\rangle,$$

o que demonstra a primeira parte de (v).

Para demonstrar a segunda parte de (v), vamos considerar as duas alternativas do item (ii) do Lema 3.1. Consideremos a primeira alternativa com $x = a$: $D\langle 1,a\rangle =$

$(D\langle 1,a\rangle \cap D\langle 1,-d\rangle) \cup a(D\langle 1,a\rangle \cap D\langle 1,-d\rangle)$. Como $a \in D\langle 1,-d\rangle$, temos $aD\langle 1,a\rangle = D\langle 1,a\rangle$, e também $aD\langle 1,-d\rangle = D\langle 1,-d\rangle$. Portanto a reunião colapsa na interseção $D\langle 1,a\rangle \cap D\langle 1,-d\rangle$. Mas, se $D\langle 1,a\rangle = D\langle 1,a\rangle \cap D\langle 1,-d\rangle$, então

$$D\langle 1,a\rangle \subset D\langle 1,-d\rangle. \tag{3.1.11}$$

Considerando-se agora a segunda alternativa do item (ii) do Lema 3.1 para $x = a$, como $adD\langle 1,ad\rangle = D\langle 1,ad\rangle$, temos $D\langle 1,ad\rangle = (D\langle 1,ad\rangle \cap adD\langle 1,-d\rangle) \cup (D\langle 1,ad\rangle \cap D\langle 1,-d\rangle) \subset adD\langle 1,-d\rangle \cup D\langle 1,-d\rangle$. Uma vez que $-ad \in D\langle 1,-d\rangle$, obtemos $adD\langle 1,-d\rangle = (-1)D\langle 1,-d\rangle$, de onde resulta que

$$D\langle 1,ad\rangle \subset D\langle 1,-d\rangle \cup -D\langle 1,-d\rangle. \tag{3.1.12}$$

Do caso (3.1.11) e do fato de que $D\langle 1,1\rangle \subset D\langle 1,a\rangle$ obtemos, usando novamente o item (2) da Proposição C.9, que $D\langle 1,1\rangle = D\langle 1,1\rangle \cap D\langle 1,a\rangle \subset D\langle 1,1\rangle \cap D\langle 1,-d\rangle \subset D\langle 1,d\rangle = \dot{F}^2 \cup d\dot{F}^2$, o que implica, após indução, que $\sum \dot{F}^2 \subset \dot{F}^2 \cup d\dot{F}^2$, contrariando nossa hipótese geral. Concluimos então que (3.1.12) sempre vale, ou seja, $D\langle 1,ad\rangle \subset D\langle 1,-d\rangle \cup -D\langle 1,-d\rangle$. ■

Proposição 3.5 (Bos [5], Lema 2.5) *Seja d rígido (lembrar que estamos assumindo $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$) e $a \in R = R_d$. Então*

$$D\langle 1,ad\rangle \subset R \cdot (F^2 \cup dF^2) = R \cup dR.$$

Demonstração. Pelo item (v) da Proposição 3.4, $D\langle 1,ad\rangle \subset D\langle 1,-d\rangle \cup -D\langle 1,-d\rangle = (R \cup -dR) \cup -(R \cup -dR) = (R \cup dR) \cup -(R \cup dR)$.

O resultado procurado é imediato se $D\langle 1,ad\rangle \cap -(R \cup dR) = \emptyset$. Veremos que mesmo que essa interseção não seja vazia ainda assim o resultado é verdadeiro. Suponhamos então que $D\langle 1,ad\rangle \cap -R(\dot{F}^2 \cup ad\dot{F}^2) \neq \emptyset$. Como $\dot{F}^2 \cup ad\dot{F}^2 \subset D\langle 1,ad\rangle$, temos $D\langle 1,ad\rangle \cap -R \neq \emptyset$. Portanto existe $x \in R$ tal que $-x \in D\langle 1,ad\rangle$.

Mais ainda, $-x \in D\langle 1,ad\rangle = dD\langle a,d\rangle$. Assim, $D\langle 1,-x\rangle \subset D\langle 1,d,a\rangle = D\langle 1,a\rangle \cup D\langle a,d\rangle$. Vamos considerar $\langle 1,d,a\rangle = \langle 1,d\rangle \perp \langle a\rangle$ para podermos aplicar a Proposição C.10. Lembrando que $D\langle 1,d\rangle = \dot{F}^2 \cup d\dot{F}^2$ temos apenas duas possibilidades para $x \in D\langle 1,d\rangle$ e uma para $y \in D\langle a\rangle$ (conforme C.10). Logo $D\langle 1,d,a\rangle = D\langle 1,a\rangle \cup D\langle d,a\rangle$.

Afirmamos que a última união é igual a $D\langle 1,a\rangle \cup D\langle 1,ad\rangle$. De fato, como $a \in R \subset D\langle 1,-d\rangle$, temos $-ad \in -dD\langle 1,-d\rangle = D\langle 1,-d\rangle$, donde $d \in D\langle 1,ad\rangle$.

Juntando as duas conclusões podemos escrever $D\langle 1,-x\rangle \subset D\langle 1,a\rangle \cup D\langle 1,ad\rangle$. Usando novamente que um grupo não pode ser a união de dois subgrupos próprios obtemos finalmente que $D\langle 1,-x\rangle \subset D\langle 1,a\rangle$ ou $D\langle 1,-x\rangle \subset D\langle 1,ad\rangle$.

Suponhamos que valha a segunda inclusão. Pelo item (iv) da Proposição 3.4, $D\langle 1,1\rangle \subset D\langle 1,-a\rangle$ e $D\langle 1,1\rangle \subset D\langle 1,-x\rangle \subset D\langle 1,ad\rangle$. Logo, $D\langle 1,1\rangle \subset D\langle 1,ad\rangle \cap D\langle 1,-a\rangle \subset D\langle 1,d\rangle$, pelo item (2) da Proposição C.9. Novamente, por indução, chegaríamos a $\sum \dot{F}^2 \subset \dot{F}^2 \cup d\dot{F}^2$. Como isso vai contra nossa hipótese geral, obtemos uma contradição.

Da primeira inclusão, $D\langle 1,-x\rangle \subset D\langle 1,a\rangle$, vamos obter, novamente graças ao item (2) da Proposição C.9, que $d \in D\langle 1,-a\rangle \cap D\langle 1,-x\rangle \subset D\langle 1,-a\rangle \cap D\langle 1,a\rangle \subset D\langle 1,1\rangle$. Daí, $-1 \in D\langle 1,-d\rangle = R \cup -dR$, pelo item (iii) da Proposição 3.4. Ainda pela Proposição 3.4, item (iii) sabemos que $d \notin R$. Logo, $-1 \in R$ e $D\langle 1,ad\rangle \subset (R \cup dR) \cup -(R \cup dR) = R \cup dR$, o que encerra a demonstração. ■

Lema 3.6 (Bos [5], corolário 1.4 (i)) *Se $d \in F$ é rígido e $d \notin D(n\langle 1\rangle)$, então, para todo $s \in D(n\langle 1\rangle)$, ds é rígido. Em particular, se $d \notin \sum \dot{F}^2$, então ds é rígido, para todo $s \in \sum \dot{F}^2$.*

Demonstração. Mostraremos primeiramente que, se $x, y \in F$ são rígidos e $1 \notin D\langle x,y\rangle$ então todo elemento de $D\langle x,y\rangle$ é rígido. De fato, se $z \in D\langle x,y\rangle$ então $D\langle 1,z\rangle \subset D\langle 1,x,y\rangle = D\langle 1,y\rangle \cup D\langle x,y\rangle = \dot{F}^2 \cup D\langle x,y\rangle$. Tomemos $H = D\langle 1,xy\rangle$. Então H é um subgrupo de $\dot{F}$ e $D\langle 1,z\rangle \subset \dot{F}^2 \cup xH$. Multiplicando essa última inclusão por z, obtemos $D\langle 1,z\rangle \subset z\dot{F}^2 \cup xzH = z\dot{F}^2 \cup H$, pois $z \in D\langle x,y\rangle = xH$. Assim, temos $D\langle 1,z\rangle \subset \dot{F}^2 \cup xH$ e $D\langle 1,z\rangle \subset z\dot{F}^2 \cup H$. Se $H \cap xH \neq \emptyset$ então existem $u, v \in H$ tais que $u = xv$. Mas isso implica $1 = u^{-1}xv \in xH = D\langle x,y\rangle$, contrariando nossa hipótese. Portanto, $H \cap xH = \emptyset$ e $D\langle 1,z\rangle \subseteq \dot{F}^2 \cup z\dot{F}^2$, o que prova que z é rígido.

Podemos mostrar, por indução, que, se $x_1, \ldots, x_n$ são rígidos e $1 \notin D\langle x_1, \ldots, x_n\rangle$, então todo elemento de $D\langle x_1, \ldots, x_n\rangle$ é rígido.

Finalmente, se $d \notin D(n\langle 1\rangle)$, então $1 \notin D(n\langle d\rangle)$. Se d é rígido, então a afirmação do parágrafo anterior mostra que todo elemento de $dD(n\langle 1\rangle) = D(n\langle d\rangle)$ é rígido. ■

Finalizamos esta seção com uma série de exemplos de elementos rígidos em corpos. Os dois primeiros exemplos fazem uso do conceito de valorização, que só será introduzido

formalmente no próximo capítulo. O primeiro exemplo exibe uma maneira natural de "fabricar" elementos birígidos.

Exemplo 3.7 *Rígidos em um corpo valorizado 2-henseliano.*

Suponhamos que F é um corpo munido de um anel de valorização não trivial 2-henseliano (veja a definição na página 53) A tal que $\Gamma_A \neq 2\Gamma_A$. Vamos mostrar que, se $v_A(d) \notin 2\Gamma_A$, então d é birígido em F.

Seja $y \in D\langle 1, \pm d\rangle$. Queremos mostrar que $y \in \dot{F}^2$ ou $y \in \pm d\dot{F}^2$. Podemos escrever $y = a^2 \pm db^2$, onde $a, b \in F$. Assim, $v_A(y) = v_A(a^2 \pm db^2) \geq \min\{v_A(a^2), v_A(db^2)\}$. Se $v_A(a^2) = v_A(db^2)$, então $v_A(d) = v_A(a^2b^{-2}) \in 2\Gamma_A$. Mas estamos supondo exatamente o contrário. Logo, $v_A(a^2) \neq v_A(db^2)$ e $v_A(y) = \min\{v_A(a^2), v_A(db^2)\}$. Temos, então, dois casos:

$\underline{v_A(y) = v_A(a^2) < v_A(db^2)}$. Neste caso, $\frac{db^2}{y} \in \mathfrak{m}_A$. Logo, $\frac{a^2}{y} = \frac{y \mp db^2}{y} = 1 \mp \frac{db^2}{y} \in 1 + \mathfrak{m}_A \subset \dot{F}^2$ e, daí, $y \in \dot{F}^2$.

$\underline{v_A(y) = v_A(db^2) < v_A(a^2)}$. Neste caso, $\frac{a^2}{y} \in \mathfrak{m}_A$ e, assim como fizemos no primeiro caso, $\frac{\pm db^2}{y} = \frac{y - a^2}{y} = 1 - \frac{a^2}{y} \in 1 + \mathfrak{m}_A \subset \dot{F}^2$, donde $y \in \pm d\dot{F}^2$.

Portanto, $D\langle 1, \pm d\rangle = \dot{F}^2 \cup \pm d\dot{F}^2$, ou seja, d é birígido em F.

Exemplo 3.8 *Rígidos no corpo das séries formais $F = k((X))$.*

O corpo $F = k((X))$ das séries formais sobre um corpo k é o completamento de $K = k(X)$, o corpo das funções racionais sobre k, em relação à topologia definida pela valorização X-ádica $v_X : K \to \mathbb{Z} \cup \{\infty\}$ dada por: $v_X(f) = n$, onde $f = a_nX^n + a_{n+1}X^{n+1} + \cdots + a_mX^m \in k[X]$, $m, n \in \mathbb{Z}$, $n \leq m$, $a_n \neq 0$, e $v_X(\frac{f}{g}) = v_X(f) - v_X(g)$, onde $f, g \in k[X]$.

Como F é completo, o anel de valorização $A_X = k[[X]]$ é henseliano. Em particular, A_X é 2-henseliano. Isso significa que $1 + \mathfrak{m}_X \subset \dot{F}^2$, onde $\mathfrak{m}_X = XA_X$ é o ideal maximal de A_X. Uma vez que $v_X(X) = 1 \notin 2\mathbb{Z}$, o Exemplo 3.7 mostra que X é birígido.

Podemos usar o critério acima para encontrar outros birígidos em F. Por exemplo, $X + f$ é birígido, para todo $f = a_1X + a_2X^2 + \cdots \in \mathfrak{m}_X$, com $a_1 \neq -1$. De fato, $f \in \mathfrak{m}_X$ implica que $f = Xg$, onde $g = a_1 + a_2X + \cdots \in A_X$. Logo, $v_X(X + f) = v_X(X) + v_X(1 + g) = 1 + 0 = 1 \notin 2\mathbb{Z}$. Note que $v_X(1 + g) = 0$, pois, em geral, temos $v_X(1 + g) \geq \min\{v_X(1), v_X(g)\} = 0$. Se $v_X(g) \neq v_X(1) = 0$, então $v_X(1 + g) = 0$. Se, caso contrário, $v_X(g) = 0$, então $1 + g = (1 + a_1) + a_2X + a_3X^2 + \cdots$, com $1 + a_1 \in k \setminus \{0\}$, pois $a_1 \neq -1$. Logo, $v_X(1 + g) = 0$.

Exemplo 3.9 ([3], p.132) *Um corpo admitindo um elemento rígido que não é birígido.*

Vimos no Exemplo 3.8 que o corpo das séries formais $k((X))$ sobre o corpo k admite elementos birígidos. Exibiremos, a seguir, um corpo F, admitindo um elemento rígido que não é birígido.

Seja F_0 um corpo formalmente real contendo exatamente 3 ordens. Por exemplo, $F_0 = \mathbb{Q}(\alpha)$, onde α é uma das três raízes reais do polinômio $f(X) = X^3 - 3X + 1$, irredutível sobre $\mathbb{Q}$. Cada uma das ordens de $\mathbb{Q}(\alpha)$ corresponde a uma imersão de $\mathbb{Q}(\alpha)$ no fecho algébrico $\overline{\mathbb{Q}}$ de $\mathbb{Q}$. Sejam Q_1, Q_2 e Q_3 as três ordens de F_0 e K_i o fecho real de F_0 correspondente à ordem Q_i $(i = 1, 2, 3)$. O corpo $F := \bigcap_{i=1}^{3} K_i$ é pitagórico, pois é interseção de três corpos (reais fechados, logo) pitagóricos. Sejam $P_i = K_i^2 \cap F$ $(i = 1, 2, 3)$ as (únicas) três ordens de F.

Existe um elemento $x \in F$ que é positivo em relação a duas das três ordens e negativo em relação à terceira. De fato, se tal elemento não existisse, então cada elemento $x \in F$ seria positivo em relação às três ordens ou negativo em relação às três e F teria uma só ordem, o que não ocorre. Para explicar esse fato, escrevemos por exemplo, $(+,+,+)$ para indicar que x pertence às três ordens (isto é, $x \in P_1 \cap P_2 \cap P_3$) e, se $x \in (P_1 \cap P_3) \smallsetminus P_2$, escrevemos $(+,-,+)$. Se x não é de um dos "tipos" $(+,+,+)$ ou $(-,-,-)$, então é dos tipos $(+,-,-)$ ou $(-,+,+)$, ou alguma permutação de uma dessas duas configurações. Um x do tipo $(+,+,-)$ é exatamente o que procuramos. Caso x seja do tipo $(-,-,+)$, $-x$ é o elemento que procuramos.

Assim, após uma possível permutação das ordens, podemos supor que $x \in (P_1 \cap P_2) \smallsetminus P_3$. Esse x é nosso candidato a rígido. Para $y \in D\langle 1, x\rangle$, pela escolha de x, temos $y \in P_1 \cap P_2$. Se $y \in P_3$, então $y \in P_1 \cap P_2 \cap P_3 = \sum \dot{F}^2 = \dot{F}^2$ (pois F é pitagórico). Se $y \notin P_3$, então $-y \in P_3$ e, daí, $x^{-1}y = (-x^{-1})(-y) \in P_3$. Logo, $x^{-1}y \in P_1 \cap P_2 \cap P_3 = F^2$, isto é, $y \in x\dot{F}^2$. Portanto, $D\langle 1, x\rangle = \dot{F}^2 \cup x\dot{F}^2$ e x é rígido.

Para mostrarmos que x não é birígido, notemos primeiro que $-x \in P_3$ implica $D_F\langle 1, -x\rangle \subset P_3$ e $x \in P_1 \cap P_2$ implica que $D_F\langle 1, -x\rangle \not\subset P_i$, para $i = 1, 2$. Como F é pitagórico, $D_F\langle 1, -x\rangle$ é uma pré-ordem. Logo $D_F\langle 1, -x\rangle = P_3$.

Se $-x$ fosse rígido, teríamos $(D_F\langle 1, -x\rangle : \dot{F}^2) = 2$. Uma vez que $(\dot{F} : P_3) = 2$ teríamos $(\dot{F} : \dot{F}^2) = 4$. Por outro lado, $\dot{F}^2 = P_1 \cap P_2 \cap P_3$ implica que $(\dot{F} : \dot{F}^2) = 8$.

Exemplo 3.10 *Leques em um corpo F.*

Seja F um corpo formalmente real e T uma pré-ordem em F. A seguir, mostraremos

que existem muitos elementos T-rígidos em F, pelo menos para os casos em que o índice $(\dot{F} : T)$ é pequeno. Para algumas pré-ordens T temos uma situação extrema, onde todo elemento do corpo não pertencente a $\pm T$ é T-rígido. Pré-ordens com essa propriedade foram muito estudadas e mereceram um nome especial ("facher" em alemão, "fan" em inglês, "abanillo" em espanhol, que chamaremos de *leque*). As pré-ordens que vamos construir e investigar são um caso mais fraco, onde podemos ter apenas um elemento d tal que d e $-d$ são T-rígidos, isto é T-birígidos. O mais importante contudo é que vamos construir pré-ordens T e obter birígidos em relação a T a partir de elementos d que são rígidos (em relação a $\dot{F}^2$) mas $-d$ não é rígido. Vamos, a seguir, apresentar o principal resultado sobre os leques, de forma a podermos fazer mais claramente a comparação entre o "caso leque" e o nosso caso. A apresentação do resultado requer alguma preparação. Leitores que estejam familiarizados com a teoria dos leques podem ir diretamente ao resultado de Bröcker (Teorema 3.12), no fim desta secção. Leitores que desejem mais informações sobre os leques devem consultar o parágrafo 5 de [22].

Seja P uma ordem do corpo F. Podemos ver que todo elemento de $\dot{F} \smallsetminus P$ é P-rígido. De fato, se $x \notin P$, então $P \cup xP = P \cup -P = F \supset P + xP \supset P \cup xP$, o que mostra a igualdade $P + xP = P \cup xP$.

Notemos que uma ordem nada mais é do que uma pré-ordem de índice 2 em $\dot{F}$. Assim, o caminho natural a se seguir é considerar o caso em que T é uma pré-ordem tal que $(\dot{F} : T) = 4$. Isto significa que $T = P_1 \cap P_2$, onde P_1 e P_2 são ordens distintas de F. Seja $x \in F \smallsetminus T$ e $y \in T + xT$. Temos dois casos:

$\underline{x \notin P_1 \cup P_2}$. Neste caso, $-x \in P_1 \cap P_2 = T$. Logo, $T + xT = T - T \supset T \cdot D\langle 1, -1\rangle = \dot{F}$. Se x fosse T-rígido, teríamos $\dot{F} = T \cup xT = T \cup -T$ e T seria uma ordem, o que é impossível no nosso caso, pois $(\dot{F} : T) = 4 > 2$. Assim, se $x \notin P_1 \cup P_2$ (o que equivale a $x \in -T$), então x não é T-rígido.

$\underline{x \in P_1 \smallsetminus P_2}$. Como $x \in P_1$, temos $y \in T + xT \subset P_1$. Se $y \in P_2$, então $y \in P_1 \cap P_2 = T$. Se $y \notin P_2$, então $-y \in P_2$. Mas $x \notin P_2$ implica que $-x \in P_2$. Logo, $xy = (-x)(-y) \in P_2$. Como $x, y \in P_1$, temos $xy \in P_1 \cap P_2 = T$ e $y \in xT$. Isso mostra que $y \in T \cup xT$, ou seja, x é T-rígido.

Observando que o caso $x \in P_2 \smallsetminus P_1$ é similar ao caso acima, podemos resumir a discussão acima dizendo que, quando $(\dot{F} : T) = 4$, x é T-rígido se, e somente se, $x \in F \smallsetminus \pm T$.

Uma pré-ordem é chamada de *leque* se todo $x \in F \smallsetminus \pm T$ é T-rígido. Pelo que vimos

acima, toda pré-ordem T tal que $(\dot{F} : T) \leq 4$ é um leque, que denominamos *leque trivial*. A proposição a seguir exibe duas caracterizações de um leque arbitrário.

Proposição 3.11 ([22], Teorema 5.5, p. 40) *Seja $T \subset F$ uma pré-ordem. São equivalentes:*

(1) *T é um leque.*

(2) *Dado um conjunto $S \supseteq T$, se $-1 \notin S$ e S é um subgrupo de $\dot{F}$, então S é uma pré-ordem de F.*

(3) *Dado um conjunto $S \supseteq T$, se $-1 \notin S$ e S é um subgrupo de índice 2 em $\dot{F}$, então S é uma ordem de F.*

Demonstração. (1) $\Rightarrow$ (2): para que S seja uma pré-ordem em F é suficiente que $S + S \subset S$ (pois os outros axiomas são verificados, por hipótese). Sejam $s_1, s_2 \in S$. Para $s_1, s_2 \in T$, temos $s_1 + s_2 \in T \subset S$, pois T é uma pré-ordem. Assim, podemos supor que $s = s_1^{-1}s_2 \notin T$ e escrever $s_1 + s_2 = s_1(1 + s)$. Se $s \in -T \subset -S$, então $-1 \in S$, o que não ocorre, por hipótese. Logo, $s \notin \pm T$ é T-rígido e $1 + s \in T \cup sT \subset S$, o que implica $s_1 + s_2 \in S$.

(2) $\Rightarrow$ (3): imediato.

(3) $\Rightarrow$ (1): para $a \notin \pm T$, $T[a] = T \cup aT$ (veja (B.0.2)) é subgrupo de $\dot{F}$ e $-1 \notin T[a]$; caso contrário, como $-1 \notin T$, teríamos $a \in -T$, o que não ocorre. Podemos escrever $T[a] = \bigcap U$, onde cada U é um subgrupo de índice 2 em $\dot{F}$, contendo $T[a]$ e tal que $-1 \notin U$. Por hipótese, cada U é fechado para a soma. Logo, $T[a] = T \cup aT$ é uma pré-ordem, isto é, $T + aT = T \cup aT$, provando que a é T-rígido. ■

A condição (3) da proposição acima é especialmente importante, pois nos diz que uma pré-ordem é um leque se, e somente se, o conjunto X/T das ordens que contêm T tem o maior número possível de elementos[2]. Por exemplo, se $(\dot{F} : T) = 8$, então $3 \leq |X/T| \leq 4$, onde $|X/T|$ denota o número de elementos de X/T, e T é um leque exatamente quando $|X/T| = 4$. Veremos a seguir que os dois casos possíveis realmente ocorrem.

[2]O que, ao que tudo indica, justifica o nome "leque".

Se $(\dot{F} : T) \geq 8$ a pré-ordem T pode ser ou não um leque. Vamos exibir dois exemplos para esclarecer esse fato. Primeiro, o elemento rígido x obtido no Exemplo 3.9 não pertence a uma das três ordens do corpo F (de fato $x \in (P_1 \cap P_2) \setminus P_3$). Assim, $x \in \dot{F} \setminus \dot{F}^2$, isto é, $-x \notin -\dot{F}^2$, e $-x$ não é rígido, pois x não é birígido. Logo, $\dot{F}^2 = \sum \dot{F}^2$ não é um leque em F.

A seguir, exibiremos um exemplo de um leque T com $(\dot{F} : T) = 8$, ou seja, um leque não trivial. Seja $F = \mathbb{R}((x))((y))$. O corpo F é pitagórico, logo $T = F^2$ é a pré-ordem fraca de F. O $\mathbb{F}_2$-espaço vetorial $\dot{F}/T$ tem base $\{-1, x, y\}$, logo tem 8 elementos. Isso mostra que o índice de T em F é igual a 8. Por outro lado, $X/T = X_F = \{P_1, P_2, P_3, P_4\}$, onde P_i é determinada pelos sinais de x e y em relação a P_i. Existem quatro combinações possíveis: $x, y \in P_1$, $x, -y \in P_2$, $-x, y \in P_3$ e $-x, -y \in P_4$. Logo, o número de ordens que contêm $T = \dot{F}^2$ é o maior possível e, pela observação feita logo após a demonstração da Proposição 3.11, T é um leque.

Embora possam existir leques não triviais, eles sempre se originam de leques triviais, via uma valorização. Este é o conteúdo do teorema abaixo, devido a L. Bröcker e conhecido como teorema da *trivialização de leques*. Citamos o teorema sem demonstração, que pode ser encontrada no artigo original [7] ou no parágrafo 12 do excelente livro de T.Y.Lam [22].

Teorema 3.12 (Bröcker, [7]) *Se T é um leque não trivial, então existe um anel de valorização próprio $(A, \mathfrak{m}_A, k_A)$ de F, tal que $1 + \mathfrak{m}_A \subset T$ e $\overline{T} \subset k_A$ é um leque trivial.*

Devemos observar que a existência de um anel de valorização (não trivial) compatível com uma pré-ordem de F, ou em geral com um subgrupo de $\dot{F}$, é um resultado que depende da existência de um elemento birígido em relação a essa pré-ordem, como veremos no Corolário 4.19. No caso do teorema de Bröcker, a presença de muitos elementos T-rígidos (pois T é um leque) é importante para garantir que $\overline{T}$ é um leque trivial no corpo de resíduos k_A.

Finalizamos a seção com uma conseqüência da Proposição 3.11:

Corolário 3.13 ([22], Corolário 5.6, p.41) *Sejam $F \subset K$ dois corpos. Se T' é um leque em K então $T = T' \cap F$ é um leque em F.*

Demonstração. Seja S como no item (2) da Proposição 3.11. Temos $S \cdot T' \cap F = S$. De fato, se $x \in S \cdot T' \cap F$ então $x = st'$, onde $s \in S$ e $t' \in T'$. Agora $t' = s^{-1}x \in T' \cap F = T \subset S$, logo $x = st' \in S$, pois S é subgrupo de $\dot{F}$. Isso mostra a inclusão $S \cdot T' \subset S$ e a outra inclusão é imediata.

Temos $-1 \notin S \cdot T'$, do contrário -1 pertenceria a $S \cdot T' \cap F = S$ o que não ocorre pela escolha de S. Como $S \cdot T' \supset T'$ é subgrupo de $\dot{K}$ e T' é, por hipótese, um leque, o item (2) da Proposição 3.11 implica que $S \cdot T'$ é uma pré-ordem. Conseqüentemente, $S = S \cdot T' \cap F$ também é uma pré-ordem e, novamente pelo item (2) da Proposição 3.11, T é um leque. ■

3.2 Produzindo birígidos a partir de rígidos

O material exposto nesta seção é, em sua grande maioria, original. Mostramos que, com restrições bem naturais, um elemento rígido d dá origem a um subgrupo R_d de $\dot{F}$ (que já foi definido em 3.3) em relação ao qual d é birígido (veja o item (3) do Corolário 3.14 abaixo). O subgrupo R_d é caracterizado pela propriedade de ser o conjunto dos elementos $x \in \dot{F} \setminus \dot{F}^2$ para os quais $D\langle 1, -x\rangle$ é uma pré-ordem contendo d. De fato, se $x \in \dot{F}$ é tal que $D\langle 1, -x\rangle$ é uma pré-ordem contendo d, então $\sum \dot{F}^2 \subset D\langle 1, -x\rangle$ e $d \in D\langle 1, -x\rangle$. De $\sum \dot{F}^2 \subset D\langle 1, -x\rangle$ vem que $x \in D\langle 1, -s\rangle$, para todo $s \in \sum \dot{F}^2$. De $d \in D\langle 1, -x\rangle$ vem que $x \in D\langle 1, -d\rangle$. Logo, $x \in D\langle 1, -d\rangle \cap \bigcap_{s \in \sum \dot{F}^2} D\langle 1, -s\rangle = R_d$ (veja a definição 3.3).

Reciprocamente, demonstraremos no item (1) do Corolário 3.14 que, para todo $t \in R_d \setminus \dot{F}^2$, $D\langle 1, -t\rangle$ é uma pré-ordem contendo d. Recordemos a definição, dada na página 115: o menor aberto, na topologia de Harrison do espaço de ordens X_F, contendo x é o conjunto $H(x) = \{P \in X_F \text{ ordem de } F \mid x \in P\}$. Mais ainda, de acordo com o Teorema B.7, $\bigcap_{P \in H(x)} P$ é a menor pré-ordem de F contendo x. Logo o fato de $D\langle 1, x\rangle$ ser uma pré-ordem significa que

$$D\langle 1, x\rangle = \bigcap_{P \in H(x)} P.$$

Esse fato é claramente bastante incomum, pois estabelece uma forma de minimalidade para $H(x)$ (ou maximalidade para $D\langle 1, x\rangle$). Temos em geral que

$$\sum \dot{F}^2 + x \sum \dot{F}^2$$

é a menor pré-ordem contendo x, desde que $-x \notin \sum \dot{F}^2$. Dessa forma, para um corpo pitagórico F, valerá sempre que $D\langle 1, x\rangle$ é uma pré-ordem para todo $x \in \dot{F}$ tal que $-x \notin \dot{F}^2$. Logo, F comporta-se como um corpo pitagórico em relação a cada $x \in R_d$, $x \notin \dot{F}^2$. Veremos um pouco mais a frente que há de fato uma ligação entre R_d e "pitagoricidade".

Os outros resultados desta seção são os seguintes: mostramos como produzir, a partir de um elemento rígido d, elementos T_d-birígidos, onde $T_d = R_d \cdot \sum \dot{F}^2$ e $R_d = D\langle 1, -d\rangle \cap \bigcap_{s\in\sum \dot{F}^2} D\langle 1, -s\rangle$ é o radical associado a d. Mostramos, ainda, que T_d e $T_0 = T_d \cup -dT_d$ são pré-ordens de F e que T_0 é a menor pré-ordem que contém $-d$. Finalmente, definimos em (3.2.2) o radical $\mathcal{R}(S)$ associado a um subgrupo S de $\dot{F}$ e coletamos algumas de suas propriedades na Proposição 3.19.

O Corolário 3.14 abaixo, é uma contribuição original do nosso trabalho. Embora seja uma conseqüência imediata dos resultados de [5] que expusemos na seção anterior, não havia ainda aparecido na literatura.

Corolário 3.14 *Seja F um corpo formalmente real admitindo um elemento rígido d que não é birígido. Mantemos, como já foi dito, a hipótese de que $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$. Valem as seguintes afirmações:*

(1) *Para todo $r \in R_d \setminus \dot{F}^2$, $D\langle 1, -r\rangle$ é uma pré-ordem de F.*

(2) *Se $S_d = \bigcap_{r\in R_d} D\langle 1, -r\rangle$, então S_d é uma pré-ordem de F, $d \in S_d$ e $R_d \cap S_d = \dot{F}^2$.*

(3) *d é R_d-birígido.*

Demonstração. Uma vez que $D\langle 1, -r\rangle$ é um subgrupo de $\dot{F}$ contendo $\dot{F}^2$, para verificarmos que é uma pré-ordem[3] temos que mostrar que $D\langle 1, -r\rangle + D\langle 1, -r\rangle \subset D\langle 1, -r\rangle$ e $D\langle 1, -r\rangle \neq \dot{F}$. O primeiro fato decorre do item (iv) da Proposição 3.4, pois dados $x, y \in D\langle 1, -r\rangle$ temos que $x + y \in D(2\langle 1, -r\rangle) = D\langle 1, -r\rangle$. Como $D\langle 1, -r\rangle$ é fechado para soma e $\dot{F}^2 \subset D\langle 1, -r\rangle$, a igualdade $D\langle 1, -r\rangle = \dot{F}$ é equivalente a $-1 \in D\langle 1, -r\rangle$. Esse fato é conseqüência de um procedimento padrão similar ao que pode ser encontrado na Observação (2) da página 115.

Supondo que $-1 \in D\langle 1, -r\rangle$, teríamos $r \in D\langle 1, 1\rangle$. Como $r \in R_d \subset D\langle 1, -d\rangle$, da Proposição C.9, item (2), resultaria que $r \in D\langle 1, 1\rangle \cap D\langle 1, -d\rangle \subset D\langle 1, d\rangle = \dot{F}^2 \cup d\dot{F}^2$, pois d é rígido. Sendo $r \notin \dot{F}^2$, teríamos $r \in d\dot{F}^2$, ou seja, $d \in R_d$. Pelo item (iv) da Proposição 3.4, $D\langle 1, 1\rangle \subset D\langle 1, d\rangle$ e, como já argumentamos outras vezes, chegaríamos por indução a $\sum \dot{F}^2 \subset D\langle 1, d\rangle$, o que contraria nossa hipótese. Portanto, $-1 \notin D\langle 1, -r\rangle$ e $D\langle 1, -r\rangle$ é uma pré-ordem de F.

Para mostrarmos que $R_d \cap S_d = \dot{F}^2$, tomemos $r \in R_d \cap S_d$. Como $R_d \subset D\langle 1, -d\rangle$ e $S_d \subset D\langle 1, -r\rangle$, temos $r \in D\langle 1, -d\rangle$ e $r \in D\langle 1, -r\rangle$, o que implica $r \in D\langle 1, 1\rangle$.

[3] Definição de pré-ordem na página 116.

Logo, $r \in D\langle 1,-d\rangle \cap D\langle 1,1\rangle$ e, pela Proposição C.9, item (2), $r \in D\langle 1,d\rangle = \dot{F}^2 \cup d\dot{F}^2$. Podemos, então, repetir os argumentos do parágrafo anterior para excluir o caso $r \in d\dot{F}^2$ e concluirmos que $r \in \dot{F}^2$.

Pelo item (1) obtemos que S_d é uma pré-ordem como interseção de uma família de pré-ordens. Finalmente, como $R_d \subset D\langle 1,-d\rangle$, temos que $d \in D\langle 1,-r\rangle$, para todo $r \in R_d$.

Vamos, agora, demonstrar a afirmação (3). Dados $x, y \in R_d$, temos: $x + yd = x(1 + x^{-1}yd)$. Pela Proposição 3.5, $1 + x^{-1}yd \in D\langle 1, x^{-1}yd\rangle \subset R_d \cup dR_d$ ($x^{-1}y \in R_d$, pelo item (ii) da Proposição 3.4). Como $x \in R_d$, temos que $x + yd \in R_d \cup dR_d$. Logo, d é R_d-rígido.

Pelo item (iii) da Proposição 3.4, $D\langle 1,-d\rangle = R_d \cup -dR_d$. A seguir, vamos mostrar que $D\langle 1,-d\rangle = R_d - dR_d$ e isso prova que $-d$ é R_d-rígido. A inclusão $D\langle 1,-d\rangle \subset R_d - dR_d$ é clara, pois $\dot{F}^2 \subset R_d$. Reciprocamente, se $x, y \in R_d$, então $x - yd = x(1 - x^{-1}yd)$, onde $x^{-1}y \in R_d$, pois R_d é grupo. Da primeira parte do item (v) da Proposição 3.4, segue-se que $1 - x^{-1}yd \in D\langle 1,-x^{-1}yd\rangle = D\langle 1,-d\rangle \cap D\langle 1,-x^{-1}y\rangle \subset D\langle 1,-d\rangle$. Além disso, $x \in R_d \subset D\langle 1,-d\rangle$ e, já que $D\langle 1,-d\rangle$ é grupo, $x - yd = x(1 - x^{-1}yd) \in D\langle 1,-d\rangle$, ou seja, $R_d - dR_d \subset D\langle 1,-d\rangle$. ■

O Lema 3.15 abaixo mostra que o produto de d por uma soma de quadrados não altera o radical. Esse resultado será usado em vários pontos adiante, por exemplo nas demonstrações da Proposição 3.17 e do Corolário 3.18.

Lema 3.15 *Seja F um corpo formalmente real e não pitagórico. Para todo $s \in \sum \dot{F}^2$, temos que $R_{sd} = R_d$. Em particular, se $d \notin \sum \dot{F}^2$ é rígido, então sd é R_d-birígido.*

Demonstração. De fato, $R_{sd} = D\langle 1,-sd\rangle \cap \bigcap_{w \in \sum F^2} D\langle 1,-w\rangle = D\langle 1,-sd\rangle \cap D\langle 1,-s\rangle \cap \bigcap_{w \in \sum F^2 \smallsetminus \{s\}} D\langle 1,-w\rangle$. Pelo item (2) da Proposição C.9, temos que $D\langle 1,-sd\rangle \cap D\langle 1,-s\rangle = D\langle 1,-d\rangle \cap D\langle 1,-s\rangle$. Portanto

$$R_{sd} = D\langle 1,-d\rangle \cap D\langle 1,-s\rangle \cap \bigcap_{w \in \sum F^2 \smallsetminus \{s\}} D\langle 1,-w\rangle =$$

$$= D\langle 1,-d\rangle \cap \bigcap_{w \in \sum F^2} D\langle 1,-w\rangle = R_d.$$

Suponhamos, agora, que d é um elemento rígido que não é soma de quadrados em F. O Lema 3.6 nos diz que sd é rígido e o item (3) do Corolário 3.14 garante que sd é

R_{sd}-birígido. Como $R_{sd} = R_d$, isso conclui a demonstração. ■

Observação. Recordemos que estamos mantendo como hipótese geral que F é um corpo formalmente real e não pitagórico. Neste caso, temos:

$$\text{se} \quad d \notin \sum \dot{F}^2 \quad \text{então} \quad \sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2. \tag{3.2.1}$$

De fato, se $\sum \dot{F}^2 \subset \dot{F}^2 \cup d\dot{F}^2$, com $\sum \dot{F}^2 \not\subset \dot{F}^2$, teríamos $\sum \dot{F}^2 \cap d\dot{F}^2 \neq \emptyset$, o que implicaria $d \in \sum \dot{F}^2$.

Até o fim desta seção estaremos considerando, salvo menção explícita em contrário, que F **é um corpo formalmente real e não pitagórico e** $d \notin \sum \dot{F}^2$ **é um elemento rígido que não é birígido**. Por R_d e $T_d = \sum \dot{F}^2 \cdot R_d$ denotamos os subgrupos que foram introduzidos no início desta seção. **Estas condições estarão fazendo parte de todos os enunciados apresentados a seguir**.

Proposição 3.16 *A menor pré-ordem (em relação à inclusão) que contém* $-d$ *é* $T_0 = \sum \dot{F}^2 \cdot R_d \cup -d \sum \dot{F}^2 \cdot R_d$.

Demonstração. Lembremos que a menor pré-ordem contendo $-d$ é $T_0 := \sum \dot{F}^2 - d\sum \dot{F}^2$. Dado $t \in T_0$, temos que $t = x - yd$, onde $x, y \in \sum \dot{F}^2$. Logo, $t = x(1 - x^{-1}yd) \in \sum \dot{F}^2 \cdot D\langle 1, -sd\rangle$, onde $s = x^{-1}y \in \sum \dot{F}^2$. Portanto, $T_0 \subset \sum \dot{F}^2 \cdot D\langle 1, -sd\rangle$, onde $s \in \sum \dot{F}^2$.

Agora, o Lema 3.15 garante que sd é R_d-birígido. Assim, $T_0 \subset \sum \dot{F}^2 \cdot D\langle 1, -sd\rangle \subset \sum \dot{F}^2 \cdot (R_d \cup -sdR_d) = \sum \dot{F}^2 \cdot R_d \cup -d \sum \dot{F}^2 \cdot R_d$

Reciprocamente, uma vez que $R_d \subset D\langle 1, -d\rangle$, a multiplicação por $-d$ fornece $-dR_d \subset -dD\langle 1, -d\rangle = D\langle 1, -d\rangle$, ou seja, $R_d \cup -dR_d \subset D\langle 1, -d\rangle$. Isso implica que $\sum \dot{F}^2 \cdot R_d \cup -d\sum \dot{F}^2 \cdot R_d \subset D\langle 1, -d\rangle \cdot \sum \dot{F}^2 \subset \sum \dot{F}^2 - d\sum \dot{F}^2 = T_0$. Logo, $T_0 = \sum \dot{F}^2 \cdot R_d \cup -d\sum \dot{F}^2 \cdot R_d$. ■

Consideremos agora $T_d := \sum \dot{F}^2 \cdot R_d$. Sabemos que T_d é um subgrupo de T_0 de índice ≤ 2. A seguir, vamos mostrar que T_d também é uma pré-ordem.

Proposição 3.17 $T_d = \sum \dot{F}^2 \cdot R_d$ *é uma pré-ordem de* F.

Demonstração. Se $-d \in \sum \dot{F}^2 \cdot R_d$, então $T_d = T_0$ é uma pré-ordem de F. Assim, podemos supor que $-d \notin \sum \dot{F}^2 \cdot R_d$ (isso, de fato, sempre acontece. Veja a observação a seguir).

Para mostrar que T_d é pré-ordem, resta mostrar que T_d é um subconjunto de F fechado para a soma e que $-1 \notin T_d$. Para provar que T_d é aditivamente fechado, basta mostrar que $1 + t \in T_d$, para todo $t \in T_d$, pois T_d é multiplicativamente fechado. Um elemento de T_d é do tipo $t = s\alpha$, onde $s \in \sum \dot{F}^2$ e $\alpha \in R_d$. Uma vez que $s\alpha = t \in T_d \subset T_0$ e, pela Proposição 3.16, T_0 é pré-ordem, temos $1 + s\alpha \in T_0 = T_d \cup -dT_d$. Devemos, então, mostrar que $1 + s\alpha \notin -dT_d$.

Suponha que $1 + s\alpha \in -dT_d = -d\sum \dot{F}^2 \cdot R_d$. Então existem $t' \in \sum \dot{F}^2$ e $\beta \in R_d$ tais que $1 + s\alpha = -dt'\beta$. Logo, $1 + dt'\beta = -s\alpha$. Como d é rígido e $t' \in \sum \dot{F}^2$, dt' é R_d-birígido, pelo Lema 3.15. Assim, $-s\alpha = 1+dt'\beta \in R_d \cup dt'R_d$. Se $-s\alpha \in R_d$, então, como $\alpha \in R_d$, teríamos que $-s \in R_d \subset D\langle 1, -d\rangle$. Isso implicaria que $d \in D\langle 1, s\rangle \subset \sum \dot{F}^2$, o que não ocorre. Por outro lado, $-s\alpha \in dt'R_d$ implicaria $-d \in \sum \dot{F}^2 \cdot R_d$. Mas estamos justamente supondo o contrário. Logo, $1 + t \in T_d$, como queríamos.

Finalmente, $-1 \in T_d$ implicaria $-1 \in T_0$, em contradição com o fato de T_0 ser uma pré-ordem. Logo, $-1 \notin T_d$. ■

Observação. $T_d \neq T_0$ se e somente se $-d \notin T_d = \sum \dot{F}^2 \cdot R_d$, e isso, de fato, acontece. Se $-d \in \sum \dot{F}^2 \cdot R_d$, então existe $s \in \sum \dot{F}^2$ tal que $-sd \in R_d \subset D\langle 1, -w\rangle$, para todo $w \in \sum \dot{F}^2$. Logo, $\sum \dot{F}^2 \subset D\langle 1, sd\rangle = \dot{F}^2 \cup sd\dot{F}^2$, pois sd é rígido. Porém, $\sum \dot{F}^2 \subset \dot{F}^2$ implica que $\sum \dot{F}^2 = \dot{F}^2$ o que não ocorre pois estamos supondo F não-pitagórico. Assim, deveríamos ter $\sum \dot{F}^2 \cap sd\dot{F}^2 \neq \emptyset$, o que implicaria $d \in \sum \dot{F}^2$, que também estamos supondo não ocorrer.

Corolário 3.18 *O elemento d é T_d-birígido.*

Demonstração. Sabemos, pelo item (3) do Corolário 3.14, que d é R_d-birígido. Consideremos $t_1, t_2 \in T_d$ e $y = t_1 + dt_2 = t_1(1 + dt)$, onde $t = t_1^{-1}t_2$. Como $t \in T_d = R_d \cdot \sum \dot{F}^2$, temos $t = rs$, onde $r \in R_d$ e $s \in \sum \dot{F}^2$. Logo $1+dt = 1+r(sd) \in R_d+sdR_d$. Como, pelo Lema 3.15, sd é R_d-birígido, temos que $1 + dt \in R_d \cup sdR_d$ e esta reunião está contida em $T_d \cup dT_d$, pois $s \in \sum \dot{F}^2 \subset T_d$. Uma vez que $t_1 \in T_d$, concluímos que $y \in T_d \cup dT_d$. Isso prova que d é T_d-rígido e, como o argumento continua válido se substituirmos d por $-d$, obtemos o resultado desejado. ■

Motivados pela Definição 3.3 definimos o seguinte *radical associado* a um subgrupo S de $\dot{F}$ que contenha $\dot{F}^2$:

$$\mathcal{R}(S) = \bigcap_{x \in S} D\langle 1, -x\rangle. \tag{3.2.2}$$

Em particular, se $S = \dot{F}$, $\mathcal{R}(S)$ é denominado *radical de Kaplansky* do corpo F e denotado por $R(F)$. O radical de Kaplansky pode ser caracterizado como o subgrupo de $\dot{F}$ formado pelos elementos $x \in \dot{F}$ tais que $\langle 1, -x\rangle$ é universal, isto é, $D\langle 1, -x\rangle = \dot{F}$. Estamos particularmente interessados no caso em que $S = T$, uma pré-ordem de F. Na Proposição a seguir, coletamos algumas propriedades de $\mathcal{R}$.

Proposição 3.19 *O radical $\mathcal{R}$ definido em* (3.2.2) *satisfaz as seguintes propriedades:*

(1) *Se $A \subset B$ são subgrupos de $\dot{F}$ contendo $\dot{F}^2$, então $\mathcal{R}(B) \subset \mathcal{R}(A)$.*

(2) *Se A é um subgrupo de $\dot{F}$ contendo $\dot{F}^2$, então $A \subset \mathcal{R}(\mathcal{R}(A))$.*

(3) *Se $R_0 = \bigcap_{s \in \sum F^2} D\langle 1, -s\rangle$ e S é um subgrupo de R_0 contendo $\dot{F}^2$, temos:*

   (a) $\sum \dot{F}^2 \subseteq \mathcal{R}(R_0) \subseteq \mathcal{R}(S)$, *para todo subgrupo S de R_0.*

   (b) $S \subseteq \mathcal{R}(\mathcal{R}(S)) \subseteq R_0$.

   (c) $\mathcal{R}(\mathcal{R}(R_0)) = R_0$.

(4) *Se $d \in \dot{F}$ é rígido, então $\mathcal{R}(S_d) = R_d$.*

(5) *Se A e B são subgrupos de $\dot{F}$, então $\mathcal{R}(A \cdot B) = \mathcal{R}(A) \cap \mathcal{R}(B)$.*

Demonstração. (1) $\mathcal{R}(B) = \bigcap_{x\in B} D\langle 1, -x\rangle = \left(\bigcap_{x\in A} D\langle 1, -x\rangle\right) \cap \left(\bigcap_{x\in B\smallsetminus A} D\langle 1, -x\rangle\right)$ $\subset \bigcap_{x\in A} D\langle 1, -x\rangle$.

(2) Tomemos $x \in \mathcal{R}(A)$. Temos então: $x \in D\langle 1, -a\rangle$, para todo $a \in A$. Se $x \in D\langle 1, -a\rangle$, então $a \in D\langle 1, -x\rangle$ e isso ocorre para todo $a \in A$. Assim, $A \subseteq D\langle 1, -x\rangle$, para $x \in \mathcal{R}(S)$ arbitrário, o que implica $A \subset \mathcal{R}(\mathcal{R}(A))$.

(3)(a) Para cada $s \in \sum \dot{F}^2$, temos $R_0 \subset D\langle 1, -s\rangle$. Logo $t \in D\langle 1, -s\rangle$, para todo $t \in R_0$, donde $s \in D\langle 1, -t\rangle$ para todo $s \in \sum \dot{F}^2$ e t arbitrário. Isso mostra que $\sum \dot{F}^2 \subseteq D\langle 1, -t\rangle$, para todo $t \in R_0$, ou seja, $\sum \dot{F}^2 \subseteq \mathcal{R}(R_0)$. A outra inclusão segue-se diretamente de (1) e da hipótese $S \subseteq R_0$.

(3)(b) Pelo item (3)(a), $\sum \dot{F}^2 \subseteq \mathcal{R}(S)$. Observando que $R_0 = \mathcal{R}(\sum \dot{F}^2)$, vemos que (1) implica $\mathcal{R}(\mathcal{R}(S)) \subseteq R_0$. A outra inclusão é conseqüência direta do item (2) acima.

(3)(c) Basta tomarmos $S = R_0$ no item (3)(b) acima.

(4) Se $d \notin \sum \dot{F}^2$ é rígido, então $\sum \dot{F}^2[d] = \sum \dot{F}^2 \cup d\sum \dot{F}^2$ e $\mathcal{R}(\sum \dot{F}^2[d]) = \bigcap_{t\in \sum \dot{F}^2 \cup d\sum \dot{F}^2} D\langle 1, -t\rangle = \bigcap_{t\in \sum \dot{F}^2} D\langle 1, -t\rangle \cap D\langle 1, -dt\rangle$. Pela Proposição C.9, item (2),

$D\langle 1,-t\rangle \cap D\langle 1,-dt\rangle = D\langle 1,-t\rangle \cap D\langle 1,-d\rangle$, para todo $t \in \sum \dot{F}^2$. Assim, $\mathcal{R}(\sum \dot{F}^2[d]) = D\langle 1,-d\rangle \cap R_0 = R_d$. Agora, $\mathcal{R}(S_d) = \mathcal{R}(\mathcal{R}(R_d)) = \mathcal{R}(\mathcal{R}(\mathcal{R}(\sum \dot{F}^2[d])))$. Pela segunda parte do item (2) acima, esta última expressão é igual a $\mathcal{R}(\sum \dot{F}^2[d]) = R_d$.

(5) Temos: $\mathcal{R}(A\cdot B) = \bigcap_{a\in A\,,\, b\in B} D\langle 1,-ab\rangle$. Como $1 \in A$, para cada $a' \in A$ e $b' \in B$ temos

$$\mathcal{R}(A\cdot B) = D\langle 1,-b'\rangle \cap D\langle 1,-a'b'\rangle \cap \bigcap_{\substack{a\in A\smallsetminus\{a'\}\\ b\in B\smallsetminus\{b'\}}} D\langle 1,-ab\rangle.$$

Da Proposição C.9, item (2), segue-se que

$$\mathcal{R}(A\cdot B) = D\langle 1,-b'\rangle \cap D\langle 1,-a'\rangle \cap \bigcap_{\substack{a\in A\smallsetminus\{a'\}\\ b\in B\smallsetminus\{b'\}}} D\langle 1,-ab\rangle.$$

Como podemos repetir o argumento acima para cada par de elementos $a \in A$ e $b \in B$, concluimos que $\mathcal{R}(A\cdot B) = \bigcap_{a\in A} D\langle 1,-a\rangle \cap \bigcap_{b\in B} D\langle 1,-b\rangle = \mathcal{R}(A)\cap\mathcal{R}(B)$, como queríamos. ■

Na Proposição 3.20 a seguir calculamos $\mathcal{R}(T_0)$.

Proposição 3.20 *Se T_0 é a pré-ordem definida na Proposição 3.16, então $\mathcal{R}(T_0) = \dot{F}^2$.*

Demonstração. Seja $\mathcal{R}(T_0) = \bigcap_{t\in T_0} D\langle 1,-t\rangle$. Como $T_0 = T_d \cup -dT_d$, temos que $\mathcal{R}(T_0) = \bigcap_{t\in T_d}(D\langle 1,-t\rangle \cap D\langle 1,dt\rangle)$. Pelo item (2) da Proposição C.9, $D\langle 1,-t\rangle \cap D\langle 1,dt\rangle = D\langle 1,-t\rangle \cap D\langle 1,d\rangle$, para todo $t \in T_d$. Logo,

$$\mathcal{R}(T_0) = \left(\bigcap_{t\in T_d} D\langle 1,-t\rangle\right) \cap D\langle 1,d\rangle = \bigcap_{t\in T_d} D\langle 1,-t\rangle \cap (\dot{F}^2 \cup d\dot{F}^2)$$

pois d é rígido. Assim,

$$\mathcal{R}(T_0) = \mathcal{R}(T_d) \cap (\dot{F}^2 \cup d\dot{F}^2). \tag{3.2.3}$$

Em particular, $\mathcal{R}(T_0) \subset \dot{F}^2 \cup d\dot{F}^2$. Como $\mathcal{R}(T_0)$ é subgrupo de $\dot{F}$, podemos tomar $\mathcal{R}(\mathcal{R}(T_0)) = \bigcap_{x\in\mathcal{R}(T_0)} D\langle 1,-x\rangle$. Agora, $x \in \mathcal{R}(T_0)$ implica que $x \in D\langle 1,-t\rangle$, para todo $t \in T_0$. Logo, $T_0 \subset D\langle 1,-x\rangle$. Como x foi tomado arbitrariamente em $\mathcal{R}(T_0)$, temos $T_0 \subset \bigcap_{x\in\mathcal{R}(T_0)} D\langle 1,-x\rangle = \mathcal{R}(\mathcal{R}(T_0))$. Logo, $T_0 \subset \mathcal{R}(\mathcal{R}(T_0))$.

Vamos supor, por absurdo, que $\mathcal{R}(T_0)\cap d\dot{F}^2 \neq \emptyset$. Então, por (3.2.3), $T_0 \subset \mathcal{R}(\mathcal{R}(T_0)) = D\langle 1,-1\rangle \cap D\langle 1,-d\rangle = D\langle 1,-d\rangle$. Por outro lado, o item (iii) da Proposição 3.4 garante que $D\langle 1,-d\rangle = R_d \cup -dR_d \subset \sum \dot{F}^2\cdot R_d \cup -d\sum \dot{F}^2\cdot R_d = T_0$. Portanto, $T_0 = D\langle 1,-d\rangle$.

Como $D\langle 1,-d\rangle = T_0$ é pré-ordem, temos que $\sum \dot{F}^2 \subset D\langle 1,-d\rangle$. Em particular, $D\langle 1,1\rangle \subset D\langle 1,-d\rangle$. Logo, $D\langle 1,1\rangle = D\langle 1,1\rangle \cap D\langle 1,-d\rangle \subset D\langle 1,d\rangle$ pelo item (2) da Proposição C.9. Como d é rígido, $D\langle 1,1\rangle \subset \dot{F}^2 \cup d\dot{F}^2$. Por indução, $\sum \dot{F}^2 \subset \dot{F}^2 \cup d\dot{F}^2$, mas isso contradiz nossa hipótese geral. Logo, $\mathcal{R}(T_0) \cap d\dot{F}^2 = \emptyset$ e, daí, $\mathcal{R}(T_0) \subset \dot{F}^2$. Como a outra inclusão é clara, vale a igualdade. ■

Corolário 3.21 *Mantendo as notações e hipóteses estabelecidas anteriormente, temos* $\mathcal{R}(T_d) \cap d\dot{F}^2 = \emptyset$. *Em particular,* $d \in S_d \setminus \mathcal{R}(T_d)$.

Demonstração. Pela equação (3.2.3), $\dot{F}^2 = \mathcal{R}(T_0) = \mathcal{R}(T_d) \cap (\dot{F}^2 \cup d\dot{F}^2) = (\mathcal{R}(T_d) \cap \dot{F}^2) \cup (\mathcal{R}(T_d) \cap d\dot{F}^2)$. Como $\dot{F}^2 \subset \mathcal{R}(T_d)$ temos: $\mathcal{R}(T_d) \cap \dot{F}^2 = \dot{F}^2$. Logo, $\dot{F}^2 = \dot{F}^2 \cup (\mathcal{R}(T_d) \cap d\dot{F}^2)$ e daí, $\mathcal{R}(T_d) \cap d\dot{F}^2 \subset \dot{F}^2$. Uma vez que $\dot{F}^2 \cap d\dot{F}^2 = \emptyset$, concluímos que $\mathcal{R}(T_d) \cap d\dot{F}^2 = (\mathcal{R}(T_d) \cap d\dot{F}^2) \cap \dot{F}^2 = \mathcal{R}(T_d) \cap (d\dot{F}^2 \cap \dot{F}^2) = \emptyset$. ■

3.3 Estudando o conjunto dos não rígidos

Seja T um subgrupo do grupo multiplicativo $\dot{F}$ do corpo F. Podemos considerar os subconjuntos de $\dot{F}$ formados pelos elementos que <u>não</u> são T-birígidos:

$$B(T) = \{x \in \dot{F} \,|\, x \text{ não é } T\text{-birígido}\}. \tag{3.3.1}$$

Em particular, escrevemos $B = B(\dot{F}^2) = \{x \in F \,|\, x \text{ não é birígido}\}$. Um elemento $x \in B(T)$ é dito *T-básico*. Nesta seção provaremos, seguindo [15], que o conjunto $B(T)$ é um grupo quando T é uma pré-ordem de F.

Vamos denotar $T+aT = \{t_1+at_2 \neq 0 | t_1, t_2 \in T\cup\{0\}\}$, $T+aT+bT = \{t_1+at_2+bt_3 \neq 0 | t_1, t_2, t_3 \in T \cup \{0\}\}$, e assim por diante. No caso em que T é uma pré-ordem, $T + aT$ satisfaz algumas propriedades úteis, que relacionamos a seguir.

Observações:

(1) Se T é uma pré-ordem, então $T + aT$ é um subgrupo de $\dot{F}$, para todo $a \in \dot{F}$. De fato, se $x, y \in T + aT$, podemos escrever $x = t_1 + at_2$ e $y = t_3 + at_4$, onde $t_1, t_2, t_3, t_4 \in T$. Logo, $x^{-1} = x^{-2}x = (x^{-2}t_1) + a(x^{-2}t_2) \in T + aT$ e $xy = (t_1 + at_2)(t_3 + at_4) = (t_1t_3 + a^2t_2t_4) + a(t_1t_4 + t_2t_3) \in T + aT$, pois T é uma pré-ordem.

(2) Supondo ainda que T é uma pré-ordem, temos os seguintes resultados análogos à Proposição C.9:

(a) $b \in T + aT$ implica que $-a \in T - bT$.

(b) $(T + aT) \cap (T + bT) = (T + aT) \cap (T - abT)$.

Em geral, $B(T)$ não é, necessariamente, um grupo. No entanto, a Proposição 3.23 a seguir mostra que, se T é uma pré-ordem, $B(T)$ é grupo. A parte mais difícil dessa demonstração está no Lema 3.22 a seguir.

Lema 3.22 ([15], Lema 5.2A, p. 20) *Seja F um corpo e T uma pré-ordem de F. Se $x, y \in \dot{F}$ são tais que xy é T-birígido, então x é T-birígido ou y é T-birígido.*

Demonstração. Sejam x e y como no enunciado do lema. Sabemos que $xy \notin \pm T$, pois xy é T-birígido. Se um dos elementos está em $\pm T$, o outro é necessariamente T-birígido. Assim, podemos supor que $x, y \notin \pm T$.

Temos o seguinte: $(T+xT)\cdot(T+yT) = T+xyT+xT+yT = (T+xyT)+x(T+xyT)$ (lembremos que $\dot{F}^2 \subset T$). Como xy é T-birígido, $(T + xT) \cdot (T + yT) = (T \cup xyT) + x(T \cup xyT) = (T + xT) \cdot (T \cup yT) \cup (T + yT) \cdot (T \cup xT)$. Observando a igualdade:

$$(T + xT) \cdot (T + yT) = (T + xT) \cdot (T \cup yT) \cup (T + yT) \cdot (T \cup xT)$$

e lembrando que um grupo não pode ser escrito como reunião de dois subgrupos próprios, vemos que ocorre uma das seguintes inclusões:

$$\left.\begin{array}{ccc} (T + xT) \cdot (T \cup yT) & \subset & (T + yT) \cdot (T \cup xT) \\ & \text{ou} & \\ (T + yT) \cdot (T \cup xT) & \subset & (T + xT) \cdot (T \cup yT) \end{array}\right\} (\diamond)$$

Por simetria, podemos assumir que vale a primeira inclusão. Em particular,

$$T + xT = (T + xT) \cap ((T + yT) \cup x(T + yT)) =$$

$$= ((T + xT) \cap (T + yT)) \cup ((T + xT) \cap x(T + yT)).$$

Como $x \in T + xT$ e $T + xT$ é grupo, $x(T + xT) = T + xT$, a última expressão é igual a

$$((T + xT) \cap (T + yT)) \cup x((T + xT) \cap (T + yT)).$$

Pela observação (2)(b) da página 33, a expressão acima é igual a

$$((T + xT) \cap (T - xyT)) \cup x((T + xT) \cap (T - xyT)) =$$

$$= ((T + xT) \cap (T \cup -xyT)) \cup x((T + xT) \cap (T \cup -xyT))$$

pois xy é T-birígido. Como $T \subset T + xT$, obtemos, finalmente:

$$T + xT = (T \cup ((T + xT) \cap -xyT)) \cup (xT \cup x\left((T + xT) \cap -xyT\right)).$$

No entanto, $(T+xT)\cap -xyT = \emptyset$, pois, se existissem $t, t_1, t_2 \in T$ tais que $t_1+xt_2 = -xyt$, teríamos $-x = t_1t_2^{-1} + xytt_2^{-1} \in T + xyT = T \cup xyT$ e, daí, $x \in -T$ ou $y \in -T$, o que contradiz a escolha de x e y. Sendo assim, obtemos, finalmente, $T + xT = T \cup xT$, ou seja, x é T-rígido. Se considerarmos $T - xT$ ao invés de $T + xT$, obteremos que $-x$ é T-rígido. Logo, x é T-birígido. Se vale a outra inclusão em $(\diamond)$, então y é T-birígido. ■

Proposição 3.23 ([15], Corolário 5.3A, p. 21) *Se T é uma pré-ordem, então $B(T)$ é um subgrupo de $\dot{F}$.*

Demonstração. Primeiramente, se $x \in B(T)$, então $x^{-1} = x^{-2}x \in x\dot{F}^2 \subset xT \subset B(T)$, pois $T \subset B(T)$. Consideremos, agora, $x, y \in B(T)$ (isto é, x e y não são T-birígidos). Podemos usar o Lema 3.22 na forma contrapositiva para concluir que $xy \in B(T)$. Portanto, $B(T)$ é subgrupo de $\dot{F}$. ■

3.4 O comportamento de rígidos e não rígidos em relação a 2-extensões

Vamos, agora, estudar o efeito de uma extensão $K|F$ sobre os elementos rígidos de F. Mais precisamente, dada uma extensão $K|F$, tentaremos responder às perguntas:

1) Sob que condições um elemento rígido de F permanece rígido em K?

2) Sob que condições um elemento $x \in F$ que é rígido em K é também rígido em F?

É claro que, uma vez respondidas as duas perguntas acima, obtemos também informações sobre o comportamento dos não rígidos em relação à extensão $K|F$. Obteremos resultados similares aos de [4], mas nos concentraremos no caso de nosso interesse, que é quando a extensão $K|F$ é uma 2-extensão (cf. página 2). Uma resposta aos questionamentos acima, pelo menos para extensões quadráticas, é dada pela Proposição 3.24 a seguir.

Proposição 3.24 (Bos [4], Lema 5.3) *Seja $K = F(\sqrt{a})$ e seja $x \in \dot{F}$. Se x e ax são rígidos em F, então x é rígido em K. Reciprocamente, se x é rígido em K, então x e ax são rígidos em F.*

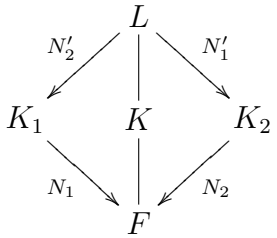
Para demonstrar a Proposição acima, precisamos de alguns resultados, que exibiremos a seguir.

Lema 3.25 *Se $K = F(\sqrt{m})$, $N : K \to F$ é a norma da extensão $K|F$, $G(K|F) = \{1, \sigma\}$ e $x \in K$ é tal que $N(x) = 1$, então existe $u \in K$ tal que $x = \frac{u}{\sigma(u)}$.*

Demonstração. Se $x = -1$, basta tomarmos $u = \sqrt{m}$. Logo, vamos supor que $x \neq -1$. Como $N(x) = x\sigma(x)$, de $N(x) = 1$ segue-se que $\sigma(x) = x^{-1}$. Seja $u = 1 + x \neq 0$. Temos $\sigma(u) = 1 + \sigma(x) = (x + 1)\sigma(x) = u\sigma(x)$. Logo, $\frac{u}{\sigma(u)} = \sigma(x)^{-1} = x$. ■

O Lema 3.25 acima continua válido se $K|F$ for uma extensão cíclica. Além disso, vale a recíproca. Esse resultado mais geral é conhecido como Teorema 90 de Hilbert. A seguir, precisaremos apenas do resultado como foi exposto acima.

Lema 3.26 ([15], Lema 2.3, p.6) *Sejam $a_1, a_2 \in \dot{F} \setminus \dot{F}^2$ tais que $a_1 a_2 \notin \dot{F}^2$. Consideremos as extensões $K_i = F(\sqrt{a_i})$ $(i = 1, 2)$, $L = F(\sqrt{a_1}, \sqrt{a_2})$ e $K = F(\sqrt{a_1} \cdot \sqrt{a_2})$. Denotamos por $N_2' : L \to K_1$, $N_1' : L \to K_2$, $N_1 : K_1 \to F$ e $N_2 : K_2 \to F$ as normas relativas a essas extensões quadráticas (observemos que $N_1 N_2' = N_2 N_1'$ é a norma relativa à extensão $L|F$).*



Se existem $z_i \in K_i$, $i = 1, 2$, tais que $N_1(z_1) = N_2(z_2)$, então existem $z \in L$ e $a \in F$ tais que $N_2'(z) = az_1$ e $N_1'(z) = az_2$.

Demonstração. Seja $G(L|F) = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$ o grupo de Galois de $L|F$, onde $\sigma_1|_{K_2} = id$, $G(K_1|F) = \{1, \sigma_1\}$ e $\sigma_2|_{K_1} = id$, $G(K_2|F) = \{1, \sigma_2\}$. Forçosamente, o corpo fixo de $\sigma_1\sigma_2$ é K. Seja $N' : L \to K$ a norma correspondente, isto é, $N'(w) = w\sigma_1\sigma_2(w)$, onde $w \in L$. Então

$$N'(z_1 z_2^{-1}) = (z_1 z_2^{-1})\sigma_1\sigma_2(z_1 z_2^{-1}) = (z_1 z_2^{-1})\sigma_1(z_1)\sigma_2(z_2)^{-1} =$$

$$= (z_1\sigma_1(z_1))(z_2\sigma_2(z_2))^{-1} = N_1(z_1)N_2(z_2)^{-1} = 1.$$

Pelo Lema 3.25 existe $u \in L$ tal que

$$\frac{z_1}{z_2} = \frac{u}{\sigma_1\sigma_2(u)}. \tag{3.4.1}$$

Seja $z = z_2u \in L$. Temos:

$$z_2\sigma_2(z) = z_2\sigma_2(z_2u) \overset{(3.4.1)}{=} z_2\sigma_2(z_1\sigma_1\sigma_2(u)) = z_2z_1\sigma_1(u) = z_1\sigma_1(z_2u) = z_1\sigma_1(z)$$

Logo, $\frac{\sigma_1(z)}{z_2} = \frac{\sigma_2(z)}{z_1}$. Tomemos, agora, $a := \frac{N_1'(z)}{z_2} \in K_2$. Então $a = \frac{z\sigma_1(z)}{z_2} = \frac{z\sigma_2(z)}{z_1} = \frac{N_2'(z)}{z_1} \in K_1$. Assim, $a \in K_1 \cap K_2 = F$. Além disso, $N_1'(z) = az_2$ e $N_2'(z) = az_1$. ■

Lema 3.27 ([2], Lema 2.1) *Seja $a \in \dot{F} \setminus \dot{F}^2$ e $K = F(\sqrt{a})$. Para todo $b \in \dot{F}$, temos:*

$$D_K\langle 1, b\rangle \cap \dot{F} = D_F\langle 1, b\rangle \cdot D_F\langle 1, ab\rangle$$

Demonstração. Como $a \in \dot{K}$, temos $D_K\langle 1, ab\rangle = D_K\langle 1, b\rangle$, logo

$$D_F\langle 1, b\rangle D_F\langle 1, ab\rangle \subset D_K\langle 1, b\rangle$$

e isto mostra uma das inclusões. Pra mostrar a outra inclusão, tomemos $c \in D_K\langle 1, b\rangle \cap \dot{F}$ e $x, y, z, w \in F$ tais que $c = (x + y\sqrt{a})^2 + b(z + w\sqrt{a})^2 = x^2 + y^2a + z^2b + w^2ab + 2(xy + zwb)\sqrt{a}$. Como $c \in F$, temos

$$xy + zwb = 0 \text{ e} \tag{3.4.2}$$

$$c = x^2 + y^2a + z^2b + w^2ab. \tag{3.4.3}$$

Vamos, primeiramente, supor que $y = 0$. Neste caso, por (3.4.2) $z = 0$ ou $w = 0$. Se $z = 0$, então $c = x^2 + w^2ab \in D_F\langle 1, ab\rangle$. Se $w = 0$, então $c = x^2 + z^2b \in D_F\langle 1, b\rangle$. Observe que $z = w = 0$ está incluido na análise acima. Assim, se $y = 0$, temos $c \in D_F\langle 1, b\rangle D_F\langle 1, ab\rangle$.

Se $y \neq 0$ obtemos, multiplicando (3.4.3) por y^2,

$$cy^2 = (xy)^2 + y^2y^2a + z^2y^2b + w^2y^2ab =$$

$$\overset{(3.4.2)}{=} (-zwb)^2 + y^2y^2a + z^2y^2b + w^2y^2ab =$$

$$= z^2b(w^2b + y^2) + y^2a(y^2 + w^2b) =$$

$$= a(y^2 + (za^{-1})^2 ab)(y^2 + w^2 b).$$

Assim, $\frac{c}{a}y^2 = a(y^2 + (za^{-1})^2 ab)(y^2 + w^2 b) \in D_F\langle 1, b\rangle D_F\langle 1, ab\rangle$, que é um grupo contendo b e ab, logo, contém a (e também a^{-1}). Segue-se que $c \in D_F\langle 1, b\rangle D_F\langle 1, ab\rangle$, como queríamos. ■

Corolário 3.28 ([12], Corolário 2.5, p.8) *Mantendo a notação do Lema* 3.26*, a seguinte seqüência é exata*

$$1 \to \{\dot{F}^2, a_2\dot{F}^2\} \to (D_F\langle 1, -a_1\rangle D_F\langle 1, -a_1a_2\rangle)/\dot{F}^2 \xrightarrow{j} D_{K_2}\langle 1, -a_2\rangle/\dot{K}_2^2 \to$$
$$\xrightarrow{\overline{N}_2} (D_F\langle 1, -a_1\rangle \cap D_F\langle 1, -a_2\rangle)/\dot{F}^2 \to 1$$

Demonstração. Primeiramente, devemos observar que $a_2 \in D_F\langle 1, -a_1\rangle \cdot D_F\langle 1, -a_1a_2\rangle$. Logo, a segunda aplicação da seqüência é bem definida e injetiva. Além disso, pelo Lema 3.27, $D_F\langle 1, -a_1\rangle \cdot D_F\langle 1, -a_1a_2\rangle = D_{K_2}\langle 1, -a_1\rangle \cap F$. Logo, a inclusão $F \subset K_2$ induz a aplicação j. Como $\dot{K}_2 \cap F = \dot{F}^2 \cup a_2\dot{F}^2$, o núcleo de j é exatamente $\{\dot{F}^2, a_2\dot{F}^2\}$.

A seguir, vemos que a imagem de j está contida em $\ker \overline{N}_2$. Resta mostrar, então, que a imagem de $\overline{N}_2$ é $(D_F\langle 1, -a_1\rangle \cap D_F\langle 1, -a_2\rangle)/\dot{F}^2$ e que $\ker \overline{N}_2$ está contido na imagem de j.

Recordando a notação estabelecida no Lema 3.26, vemos que $D_{K_2}\langle 1, -a_1\rangle$ é a imagem de N_1'. Assim, para cada $w \in D_{K_2}\langle 1, -a_1\rangle$, existe $v \in L = K_2(\sqrt{a_1})$ tal que $N_1'(v) = w$. Assim, $N_2(w) = N_2(N_1'(v)) = N_1(N_2'(v)) \in D_F\langle 1, -a_1\rangle \cap D_F\langle 1, -a_2\rangle$ e isso mostra que a norma N_2 de fato induz a aplicação $\overline{N}_2$.

Para mostrarmos a sobrejetividade de $\overline{N}_2$, tomemos $x \in D_F\langle 1, -a_1\rangle \cap D_F\langle 1, -a_2\rangle$. Existem $w_1 \in K_1$ e $w_2 \in K_2$ tais que $N_1(w_1) = x = N_2(w_2)$. Pelo Lema 3.26, existem $w \in L$ e $a \in F$ tais que $N_1'(w) = aw_1$ e $N_2'(w) = aw_2$. Assim, $a^2x = N_2(aw_2) = N_2(N_1'(w))$. Como $N_1'(w) \in D_{K_2}\langle 1, -a_1\rangle$, temos: $x = a^{-2}N_2(N_1'(w)) \in N_2(D_{K_2}\langle 1, -a_1\rangle)$, o que mostra a sobrejetividade de $\overline{N}_2$.

Finalmente, tomando $x \in D_{K_2}\langle 1, -a_1\rangle$ tal que $N_2(x) = y^2 \in \dot{F}^2$, podemos escrever $N_2(\frac{x}{y}) = 1$. Logo, pelo Lema 3.25, existe $u \in K_2$ tal que

$$\frac{x}{y} = \frac{u}{\sigma_2(u)} = \frac{u^2}{N_2(u)}.$$

Logo, $yN_2(u)^{-1} = xu^{-2} \in \dot{F} \cap D_{K_2}\langle 1, -a_1\rangle = D_F\langle 1, -a_1\rangle D_F\langle 1, -a_1a_2\rangle$, pelo Lema 3.27. Assim, $x\dot{K}_2^2 = yN_2(u)^{-1}\dot{K}_2^2 = j(yN_2(u)^{-1}\dot{F}^2)$, mostrando que $\ker \overline{N}_2 \subset \mathrm{Im}(j)$, como

queríamos. ■

Demonstração da Proposição 3.24. Podemos supor que $a \notin F^2$ (do contrário, $K = F$ e não há nada a mostrar). Temos, então $x\dot{F}^2 \cap ax\dot{F}^2 = \emptyset$ e, sendo x e ax rígidos (por hipótese), $D\langle 1, x\rangle \cap D\langle 1, ax\rangle = (\dot{F}^2 \cup x\dot{F}^2) \cap (\dot{F}^2 \cup ax\dot{F}^2) = \dot{F}^2$. Pela Proposição C.9, item (2), $D_F\langle 1, x\rangle \cap D_F\langle 1, -a\rangle = \dot{F}^2$. Vamos usar, agora, o Corolário 3.28, com $a_1 = -x$ e $a_2 = a$, para obtermos a seguinte seqüência exata:

$$1 \to \{\dot{F}^2, a\dot{F}^2\} \to (D_F\langle 1, x\rangle D_F\langle 1, ax\rangle)/\dot{F}^2 \to D_F\langle 1, x\rangle/\dot{K}^2 \to 1.$$

Da seqüência exata acima e da igualdade

$$(D_F\langle 1, x\rangle D_F\langle 1, ax\rangle)/\dot{F}^2 = \{\dot{F}^2, x\dot{F}^2, ax\dot{F}^2, a\dot{F}^2\}$$

(que é conseqüência da rigidez de x e ax em F) segue que $D_K\langle 1, x\rangle/\dot{K}^2 = \{\dot{K}^2, x\dot{K}^2\}$, ou seja, x é rígido em K.

Suponhamos, agora, que x é rígido em K. Fazendo $a_1 = -x$ e $a_2 = a$ na seqüência exata do Corolário 3.28, obtemos $N(D_K\langle 1, x\rangle) = D_F\langle 1, x\rangle \cap D_F\langle 1, -a\rangle$. Por outro lado, $N(D_K\langle 1, x\rangle) \subset \dot{F}^2$, pois x é rígido em K. Logo, $D_F\langle 1, x\rangle \cap D_F\langle 1, -a\rangle = \dot{F}^2$ e, pelo item (2) da Proposição C.9,

$$D_F\langle 1, x\rangle \cap D_F\langle 1, ax\rangle = \dot{F}^2. \tag{3.4.4}$$

Pelo Lema 3.27, temos:

$$(\dot{K}^2 \cup x\dot{K}^2) \cap F = D_K\langle 1, x\rangle \cap F = D_F\langle 1, x\rangle \cdot D_F\langle 1, ax\rangle = \dot{F}^2 \cup a\dot{F}^2 \cup x\dot{F}^2 \cup ax\dot{F}^2.$$

Assim, $D_F\langle 1, x\rangle$ e $D_F\langle 1, ax\rangle$ são subconjuntos de $\dot{F}^2 \cup a\dot{F}^2 \cup x\dot{F}^2 \cup ax\dot{F}^2$. Como $\dot{F}^2 \cup x\dot{F}^2 \subset D_F\langle 1, x\rangle$ e $\dot{F}^2 \cup ax\dot{F}^2 \subset D_F\langle 1, ax\rangle$, a igualdade (3.4.4) nos permite concluir que, de fato, ocorrem $D_F\langle 1, x\rangle = \dot{F}^2 \cup x\dot{F}^2$ e $D_F\langle 1, ax\rangle = \dot{F}^2 \cup ax\dot{F}^2$, ou seja, x e ax são rígidos em F. ■

Corolário 3.29 (Bos [4], Corolário 5.1) *Seja $L|F$ uma 2-extensão finita e seja $x \in \dot{F}$. Se x é rígido em L, então x é rígido em F.*

Demonstração. De acordo com (2.1.2), existe uma torre de corpos $F = F_0 \subset F_1 \subset \cdots \subset F_n = L$, onde $F_{n+1} = F_n(\sqrt{a_n})$, para todo $n \geq 0$ ($a_n \in F_n \smallsetminus F_n^2$). Como x é rígido em L, a Proposição 3.24 garante que x é rígido em F_{n-1}. Repetindo esse processo n vezes, vemos que x é rígido em F. ■

Proposição 3.30 (Bos [4], Proposição 5.2) *Seja $L|F$ uma extensão galoisiana, com $L \subset F(2)$, e seja $x \in \dot{F}$. Suponha que $G(L|F)$ é um grupo de torção. Então, se x é rígido em L, x também é rígido em F.*

Antes de provar a proposição acima, vamos aplicá-la à extensão $F_1|F$, dada no item (a) da Definição 2.8, onde $F_1 = F(\{\sqrt{t}|t \in T\})$. Note que $F_1|F$ é uma extensão normal e $G(F_1|F)$ tem expoente 2, logo, é grupo de torção. No que se segue, adotaremos a seguinte notação, onde F é um corpo e T é uma pré-ordem de F:

$$A_T(F) = \{x \in T \,|\, x \text{ não é rígido}\}. \tag{3.4.5}$$

Em particular, denotamos $A_\pi(F) = \{x \in \sum F^2 \,|\, x \text{ não é rígido}\}$. Convém destacar que $A_T(F)$ e $B(T)$ (definido em (3.3.1)) são conjuntos *distintos* e não há uma relação geral entre eles, apesar de ambos serem formados por elementos não rígidos. Mencionamos ainda que, de acordo com [13], Proposição 3.2, página 28, $A_\pi(F)$ é um subgrupo de $\sum \dot{F}^2$.

Corolário 3.31 $A_T(F) \subseteq A_\pi(F_1) \cap \dot{F}$

Demonstração. A Proposição 3.30 afirma que, se $x \in \dot{F}$ não é rígido em F, então não é rígido em L. Como $T = \sum \dot{F_1}^2 \cap \dot{F}$, segue-se o resultado. ■

Demonstração da Proposição 3.30. Seja S a coleção de todos os corpos N entre F e L tais que x é rígido em N. seja M a interseção de todos esses corpos. Afirmamos que x é rígido em M. De fato, seja $y \in D_M\langle 1, x\rangle$. Então, para todo $N \in S$, $y \in \dot{N}^2 \cup x\dot{N}^2$. Na verdade, temos:

$$\text{para todo } N \in S, y \in \dot{N}^2 \text{ ou, para todo } N \in S, xy \in \dot{N}^2.$$

Se isso não fosse verdade, existiriam $N_1, N_2 \in S$ tais que $y \notin \dot{N_1}^2$ e $xy \notin \dot{N_2}^2$. Então $y \in x\dot{N_1}^2$ e $y \in \dot{N_2}^2$ (se $y \in x\dot{N_2}^2$, então $xy \in \dot{N_2}^2$, o que não ocorre). Como $N_1, N_2 \subset L$, teríamos $y \in x\dot{L}^2$ e $y \in \dot{L}^2$, o que implicaria $x \in L^2$. Mas, por hipótese, x é rígido em L, o que implica $x \notin L^2$.

Agora, $a \in \bigcap_{N \in S} N^2$ implica $a = a_N^2, N \in S$. Logo, $a_{N'} = \pm a_N$, quaisquer que sejam $N, N' \in S$ e isso implica que $a_{N'} \in \bigcap_{N \in S} N$. Portanto, $a = a_N^2 \in (\bigcap_{N \in S} N)^2$. Dessa discussão, segue-se que $\bigcap_{N \in S} N^2 = M^2$. Logo, $y \in \dot{M}^2$ ou $xy \in \dot{M}^2$ e daí, $y \in \dot{M}^2 \cup x\dot{M}^2$, ou seja, y é rígido em M.

Vamos mostrar, agora, que $M = F$. Suponha que $M \neq F$. Então existe um F-automorfismo σ de L que não é a identidade em M. Seja E o corpo fixo de σ. Então $F \subset E \subset L$ e $L|E$ é extensão finita, pois σ tem ordem finita, por hipótese ($G(L|F)$ é grupo de torção).

O Corolário 3.29 mostra que x é rígido em E. Assim, $E \in S$ e $M \subset E$. Isso contradiz o fato de que σ não é a identidade em M. Portanto, $M = F$. Como x é rígido em $M = F$, concluímos a demonstração. ■

No exemplo a seguir, obtemos relações entre $A_\pi(F)$ e $A_T(F)$ e entre $A_T(F)$ e $A_\pi(F_1)$ no caso em que $T = \sum \dot{F}^2[a]$, com a rígido, onde $F_1|F$ é a extensão dada na Definição 2.8. Neste caso particular $F_1|F$ é uma extensão quadrática. Os resultados deste exemplo são similares aos obtidos por Berman em [2], Proposição 2.2.

Exemplo. Seja $a \in F$ tal que $a \notin \sum F^2 \cup -\sum F^2$. Então $T = \sum F^2[a] = \sum F^2 + a\sum F^2$ é uma pré-ordem de F que contém $\sum F^2$ propriamente. Supondo que a é rígido em F, vamos determinar $A_T(F)$.

Primeiramente, afirmamos que, sendo a rígido, $T = \sum F^2 \cup a\sum F^2$. De fato, se $t \in T$, então $t = s_1 + as_2$, onde $s_1, s_2 \in \sum F^2$. Logo, $t = s_1(1 + as)$, onde $s = s_1^{-1}s_2 \in \sum F^2$ e o Lema 3.6 garante que as é rígido. Portanto, $1 + as \in \dot{F}^2 \cup as\dot{F}^2$ e $t = s_1(1 + as) \in \sum F^2 \cup a\sum F^2$.

Sabemos que $\sum F^2 \subseteq T$. Logo, $A_\pi(F) \subseteq A_T(F)$. A seguir, provaremos que no presente caso vale a igualdade. Com efeito, seja $t \in A_T(F)$. Então, pela afirmação acima, $t \in \sum F^2$ ou $t \in a\sum F^2$. Se $t \in a\sum F^2$, então $x = a^{-1}t \in \sum F^2$. Pelo Lema 3.6, $t = ax$ seria rígido, o que não ocorre, por hipótese. Assim, todo $t \in T$ que não é rígido deve, necessariamente, pertencer a $\sum F^2$, ou seja, $A_T(F) \subseteq A_\pi(F)$. Logo, vale a igualdade

$$A_T(F) = A_\pi(F). \tag{3.4.6}$$

Vamos completar a análise do nosso exemplo observando o comportamento dos rígidos sob o efeito da extensão $F_1|F$. No nosso caso, $F_1 = F(\sqrt{a})$ é uma extensão quadrática, onde a é rígido. Em geral, sabemos, pelo Corolário 3.31, que $A_T(F) \subseteq A_\pi(F_1) \cap \dot{F}$.

Afirmamos que, se $T = \sum F^2 \cup a\sum F^2$, então $A_T(F) \cup aA_T(F) = A_\pi(F_1) \cap \dot{F}$. De fato, dado y, $0 \neq y \in aA_T(F)$. Temos que $y = ax$, onde $x \in T = \sum F_1^2 \cap F$ não é rígido em F. Logo, pelo Corolário 3.29, x não é rígido em F_1 (pois $F_1 = F(\sqrt{a})$ é

uma extensão finita). Como $a = (\sqrt{a})^2 \in F_1^2$, $y = ax$ não é rígido em F_1. Ademais, $y = ax \in F_1^2 \sum F_1^2 = \sum F_1^2$. Portanto, $y \in A_\pi(F_1) \cap \dot{F}$.

Da discussão acima, concluímos que $A_T(F) \cup aA_T(F) \subseteq A_\pi(F_1) \cap \dot{F}$. Resta mostrar a outra inclusão. Para tal, utilizaremos a Proposição 3.24 em sua forma contrapositiva: x NÃO é rígido em K implica que x NÃO é rígido em F OU ax NÃO é rígido em F.

Seja $x \in A_\pi(F_1) \cap \dot{F}$. Então $x \in \sum F_1^2 \cap \dot{F} = \dot{T}$ e x não é rígido em $F(\sqrt{a})$. Pela Proposição 3.24, temos dois casos:

(1) x não é rígido em F, o que implica $x \in A_T(F)$

(2) ax não é rígido em F. Neste caso, como $a \in T$ e $TT \subseteq T$, $ax \in A_T(F)$. Mas, $ax \in A_T(F)$ implica $a^2x \in aA_T(F)$, e daí, $x \in aA_T(F)$. Portanto,

$$A_T(F) \cup aA_T(F) = A_\pi(F_1) \cap \dot{F}. \tag{3.4.7}$$

3.5 O comportamento de R_d e T_d em relação a extensões por somas de quadrados

Seja d um elemento rígido, $d \notin \sum \dot{F}^2$, e $s \in \sum \dot{F}^2$. Considere a extensão $K = F(\sqrt{s})$ de F. Já sabemos (pelo Lema 3.6) que ds é rígido e, conseqüentemente, pela Proposição 3.24, d é $\dot{K}^2$-rígido. Denotemos:

$$R_d^F = D_F\langle 1, -d\rangle \cap \bigcap_{w \in \sum F^2} D_F\langle 1, -w\rangle,$$

$$R_d^K = D_K\langle 1, -d\rangle \cap \bigcap_{w \in \sum K^2} D_K\langle 1, -w\rangle.$$

Lembremos que, pelo item (iii) da Proposição 3.4, temos as seguintes igualdades:

$$D_F\langle 1, -d\rangle = R_d^F \cup -dR_d^F \quad \text{e} \quad D_K\langle 1, -d\rangle = R_d^K \cup -dR_d^K. \tag{3.5.1}$$

Podemos ainda aplicar o item (3) do Corolário 3.14 para concluirmos que d é R_d^K-birígido.

Usando a segunda igualdade de (3.5.1), vemos que

$$D_K\langle 1, -d\rangle \cap \dot{F} = (R_d^K \cup -dR_d^K) \cap \dot{F} = (R_d^K \cap \dot{F}) \cup -d(R_d^K \cap \dot{F}). \tag{3.5.2}$$

Por outro lado, o Lema 3.27 implica que

$$D_K\langle 1, -d\rangle \cap \dot{F} = D_F\langle 1, -d\rangle D_F\langle 1, -ds\rangle.$$

Logo, $D_K\langle 1,-d\rangle \cap \dot{F} = (R_d^F \cup -dR_d^F)(R_d^F \cup -dsR_d^F)$ (lembremos que, pelo Lema 3.15, $-ds$ é R_d^F-rígido). Assim,

$$D_K\langle 1,-d\rangle \cap \dot{F} = R_d^F \cup -dsR_d^F \cup -dR_d^F \cup sR_d^F =$$

$$= (R_d^F \cup sR_d^F) \cup -d(R_d^F \cup sR_d^F). \tag{3.5.3}$$

Juntando as igualdades (3.5.2) e (3.5.3), obtemos:

$$(R_d^K \cap \dot{F})\dot{\cup} - d(R_d^K \cap \dot{F}) = (R_d^F \cup sR_d^F)\dot{\cup} - d(R_d^F \cup sR_d^F). \tag{3.5.4}$$

Observemos que as duas reuniões acima são disjuntas. De fato, $-d \notin R_d^K \cap \dot{F}$, já que $-d \notin R_d^K$, devido às propriedades gerais associadas à rigidez de d em K, conforme comentamos no início desta seção. De maneira similar, a rigidez de d e ds em F garantem que $-d$ e $-ds$ não estão em $R_d^F (= R_{ds}^F)$. Portanto, $-d \notin R_d^F \cup sR_d^F$.

Consideremos, agora $x \in R_d^K \cap \dot{F}$. A partir da igualdade (3.5.4), vemos que ou $x \in R_d^F \cup sR_d^F$, ou existe $y \in R_d^F \cup sR_d^F$ tal que $x = -dy$. Vamos, a seguir, mostrar que esse segundo caso não é possível, para concluirmos que $R_d^K \cap \dot{F} \subseteq R_d^F \cup sR_d^F$.

Seja $x = -dy$, com $y \in R_d^F \cup sR_d^F$, e $x \in R_d^K$. Então $dy = -x$ e como $D_K\langle 1,-x\rangle$ é uma pré-ordem de K, temos que

$$D_K\langle 1, dy\rangle = \bigcap_{Q \in H_K(dy)} Q. \tag{3.5.5}$$

Portanto

$$D_K\langle 1, dy\rangle \cap F = \bigcap_{Q \in H_K(dy)} Q \cap F = \bigcap_{P \in H_F(dy)} P, \tag{3.5.6}$$

pois $Q \in H_K(dy)$ se e somente se $Q \cap F = P \in H_F(dy)$ e todas as ordens de F se estendem a K devido a s ser uma soma de quadrados.

Por outro lado, pelo Lema 3.27, temos que

$$D_K\langle 1, dy\rangle \cap F = D_F\langle 1, dy\rangle \cdot D_F\langle 1, dys\rangle. \tag{3.5.7}$$

Pelo Lema 3.15, d e ds são R_d^F-birígidos. Como $y \in R_d^F$, temos

$$D_F\langle 1, dy\rangle \subset R_d^F + dR_d^F = R_d^F \cup dR_d^F \text{ e similarmente}$$

$$D_F\langle 1, dsy\rangle \subset R_d^F + dsR_d^F = R_d^F \cup dsR_d^F. \tag{3.5.8}$$

Juntando as duas últimas equações (3.5.7) e (3.5.8) chegamos a

$$D_K\langle 1, dy\rangle \cap F \subset R_d^F \cup dR_d^F \cup dsR_d^F \cup sR_d^F. \tag{3.5.9}$$

Pelas equações (3.5.6) e (3.5.9) obtemos

$$\sum \dot{F}^2 \subset R_d^F \cup dR_d^F \cup dsR_d^F \cup sR_d^F. \tag{3.5.10}$$

Agora, o Corolário 3.14, item (2), nos diz que S_d^F é uma pré-ordem, $d \in S_d$ e $R_d^F \cap S_d^F = \dot{F}^2$. Usando estes fatos, obtemos:

$$\sum \dot{F}^2 \cap R_d^F \subset S_d^F \cap R_d^F = \dot{F}^2; \tag{3.5.11}$$

$$\sum \dot{F}^2 \cap dR_d^F \subset S_d^F \cap dR_d^F = dS_d^F \cap dR_d^F = d(S_d^F \cap R_d^F) = d\dot{F}^2 \tag{3.5.12}$$

$$\sum \dot{F}^2 \cap sR_d^F \subset S_d^F \cap sR_d^F = sS_d^F \cap sR_d^F = s(S_d^F \cap R_d^F) = s\dot{F}^2 \tag{3.5.13}$$

$$\sum \dot{F}^2 \cap dsR_d^F \subset S_d^F \cap dsR_d^F = dsS_d^F \cap dsR_d^F = ds(S_d^F \cap R_d^F) = ds\dot{F}^2. \tag{3.5.14}$$

Concluímos então que

$$\sum \dot{F}^2 = \sum \dot{F}^2 \cap \left(R_d^F \cup dR_d^F \cup dsR_d^F \cup sR_d^F\right) = \\ \dot{F}^2 \cup d\dot{F}^2 \cup s\dot{F}^2 \cup ds\dot{F}^2 = \left(\dot{F}^2 \cup s\dot{F}^2\right) \cup d\left(\dot{F}^2 \cup s\dot{F}^2\right). \tag{3.5.15}$$

Como $\dot{F}^2 \cup s\dot{F}^2 \subset \sum \dot{F}^2$ obtemos a contradição $\sum \dot{F}^2 \subset \dot{F}^2 \cup d\dot{F}^2$ (ver observação na página 28). Logo $R_d^K \cap F \subset R_d^F \cup sR_d^F$, como queríamos.

Como $R_d^F \subset R_d^K$ e $s \in \dot{K}^2$ temos também $R_d^F \cup sR_d^F \subset R_d^K \cap F$, resultando na igualdade

$$R_d^K \cap F = R_d^F \cup sR_d^F.$$

Acabamos de mostrar a primeira parte da próxima proposição. Lembremos que $T_d^F = R_d^F \cdot \sum \dot{F}^2$ e $T_d^K = R_d^K \cdot \sum \dot{K}^2$.

Proposição 3.32 *Conservando-se todas as notações e hipóteses acima temos:*

(a) $R_d^K \cap F = R_d^F \cup sR_d^F$.

(b) $T_d^K \cap F = T_d^F$.

Demonstração. Só resta provar a segunda afirmação. Sabemos pela Proposição 3.16 que $T_d^K \cup -dT_d^K$ e $T_d^F \cup -dT_d^F$ são as menores pré-ordens de K e F, respectivamente, que contém $-d$. Além disso como s é uma soma de quadrados, toda ordem de F estende-se a K. Decorrem desses fatos as igualdades abaixo:

$$T_d^K \cup -dT_d^K = \bigcap_{Q \in H_K(-d)} Q\,; \qquad T_d^F \cup -dT_d^F = \bigcap_{P \in H_K(-d)} P \tag{3.5.16}$$

$$H_F(-d) = \{\, Q \cap F \mid Q \in H_K(-d)\} \qquad \left(T_d^K \cup -dT_d^K\right) \cap F = T_d^F \cup -dT_d^F \tag{3.5.17}$$

Claramente também vale que

$$\left(T_d^K \cup -dT_d^K\right) \cap F = \left(T_d^K \cap F\right) \cup -d\left(T_d^K \cap F\right). \tag{3.5.18}$$

Juntando agora as equações (3.5.17) com (3.5.18) vamos obter

$$\left(T_d^K \cap F\right) \cup -d\left(T_d^K \cap F\right) = T_d^F \cup -dT_d^F \tag{3.5.19}$$

Novamente, a rigidez de d em F e K implica $d \notin R_d^K$ e $d \notin R_d^F$ pois, por exemplo, se $d \in R_d^F \subset D_F\langle 1, -d\rangle$, teríamos $d \in D_F\langle 1, 1\rangle \subset \sum \dot{F}^2$, o que estamos supondo não ocorrer. Decorre assim de $T_d^F = R_d^F \sum \dot{F}^2$ e $T_d^K = R_d^K \sum \dot{K}^2$ e do Lema 3.15 que $d \notin T_d^K$ e $d \notin T_d^F$, também. Adicionalmente, pelo item (a) desta proposição temos que $T_d^F \subset T_d^K$. Logo

$$\left(T_d^K \cap F\right) \cap -dT_d^F = \emptyset \quad \text{e} \quad -d\left(T_d^K \cap F\right) \cap T_d^F = \emptyset.$$

Concluímos assim que

$$T_d^K \cap F = T_d^F,$$

como queríamos. ■

Capítulo 4

Construção de anéis de valorização apropriados

No presente capítulo estudamos os anéis de valorização que servirão como ferramenta no estudo do anel de Witt de um corpo F que faremos no capítulo seguinte. Na primeira seção definimos e coletamos algumas propriedades dos anéis de valorização que nos serão úteis. Concentramos nossa atenção nos conceitos de compatibilidade e henselianidade de um anel de valorização e concluímos com alguns resultados relacionando esses dois conceitos. Na segunda seção, realizamos a construção de um anel de valorização compatível com uma pré-ordem, que será ferramenta central no nosso estudo posterior sobre a estrutura do anel de Witt de um corpo com elementos rígidos. Como veremos, esse anel de valorização é construído a partir de elementos rígidos no corpo.

4.1 Preliminares sobre anéis de valorização

Reunimos, nesta seção, alguns tópicos sobre valorizações que utilizaremos ao longo do texto. O leitor interessado em maiores detalhes deve consultar os livros citados nas referências: [11], [16], [28]. Enunciamos o Lema de Hensel, em sua versão relativa devida a Bröcker [7] e estudamos com maior detalhe os casos em que a extensão normal é $F(2)|F$ (caso 2-henseliano) ou $F_T|F$, onde T é uma pré-ordem (caso T-henseliano), relacionando os dois casos com a noção de compatibilidade, a ser introduzida em (4.1.1).

Seja F um corpo. Um *anel de valorização* de F é um subanel A de F tal que, dado $x \in F$, temos $x \in A$ ou $x^{-1} \in A$. Como é subanel de um corpo, A é um domínio de integridade. Pela definição, F coincide com o corpo de frações de A.

Dados dois ideais não nulos I e J de A, temos $I \subset J$ ou $J \subset I$. Isto também é uma conseqüência da definição: suponha que $I \not\subset J$, ou seja, que existe $x \in I \setminus J$. Seja $y \in J$, $y \neq 0$. Como $\frac{x}{y} \in F$ temos, por definição, que $\frac{x}{y} \in A$ ou $\frac{y}{x} \in A$. Mas $\frac{x}{y} \in A$ implica que $x = y \cdot \frac{x}{y} \in J$, o que não ocorre, pela escolha de x. Portanto, $\frac{y}{x} \in A$ e $y = x \cdot \frac{y}{x} \in I$.

Pelo que vimos acima, os ideais de A formam uma cadeia, isto é, são totalmente ordenados pela inclusão. Uma conseqüência imediata disso é que A tem um único ideal maximal, ou seja, é um anel local. Este ideal maximal de A é denotado por $\mathfrak{m}_A$. O anel quociente $A/\mathfrak{m}_A$ é, de fato, um corpo, denominado *corpo de resíduos* de A e denotado por k_A. A projeção canônica $\pi_A : A \to k_A$ é dada por $a \mapsto a + \mathfrak{m}_A$. Costumamos denotar $\bar{a} = \pi_A(a)$. Como A é um anel local, as unidades de A são exatamente os elementos de $A \setminus \mathfrak{m}_A$. Estes elementos formam um subgrupo de $\dot{F} = F \setminus \{0\}$, denotado por A^* ou $A^\times$.

O grupo quociente $\Gamma_A = \dot{F}/A^*$ pode ser ordenado da seguinte maneira: dados $\alpha, \beta \in \Gamma_A$, temos $\alpha = xA^*$ e $\beta = yA^*$, onde $x, y \in \dot{F}$. Definimos $\alpha \leq \beta$ se, e somente se, $yx^{-1} \in A$. É um exercício imediato mostrar que $\leq$ é uma relação de ordem. A ordem $\leq$ é linear em Γ_A (ou seja, quaisquer dois elementos de Γ_A são comparáveis por $\leq$). Isso é uma conseqüência direta do fato de que os ideais do anel de valorização A serem totalmente ordenados por inclusão.

Convenciona-se denotar o grupo abeliano ordenado Γ_A aditivamente. Adjuntamos ao grupo Γ_A um símbolo ∞ tal que $\gamma + \infty = \infty + \gamma = \infty$ e $\gamma < \infty$, para todo $\gamma \in \Gamma_A$. O homomorfismo canônico de grupos $v_A : \dot{F} \to \Gamma_A$ dado por $x \mapsto xA^*$ é estendido, por conveniência, a uma aplicação $v_A : F \to \Gamma_A \cup \{\infty\}$, onde $v_A(0) = \infty$ e v_A satisfaz as seguintes propriedades ($x, y \in F$):

(1) $v_A(x) = \infty \Leftrightarrow x = 0$

(2) $v_A(xy) = v_A(x) + v_A(y)$

(3) $v_A(x + y) \geq \min\{v_A(x), v_A(y)\}$

Por definição, $v_A(0) = \infty$. Por outro lado, se $x \neq 0$, então $v_A(x) \in \Gamma_A$ implica que $v_A(x) < \infty$. Logo, vale (1). A propriedade (2) segue-se diretamente do fato de v_A ser um homomorfismo de grupos. Para provar a propriedade (3), podemos assumir que $x + y \neq 0$ e que $v_A(x) \leq v_A(y)$. Pela definição da ordem em Γ_A, $x^{-1}y \in A$. Assim, escrevendo $x + y = x(1 + x^{-1}y)$, temos: $v_A(x + y) = v_A(x) + v_A(1 + x^{-1}y)$ (pela propriedade (2)) e, como $1 + x^{-1}y \in A$, por (a), $v_A(1 + x^{-1}y) \geq 0$. Portanto, $v_A(x + y) \geq v_A(x) = \min\{v_A(x), v_A(y)\}$.

Da definição de $(\Gamma_A, \leq)$, segue-se que:

(a) $A = \{x \in F \mid v_A(x) \geq 0\}$

(b) $\mathfrak{m}_A = \{x \in F \mid v_A(x) > 0\}$

O resultado seguinte é básico e será utilizado por diversas vezes no texto. Para facilitar a referência, o destacamos como um lema.

Lema 4.1 *Se $v_A(x) \neq v_A(y)$, então $v_A(x+y) = min\{v_A(x), v_A(y)\}$*

Demonstração. Podemos assumir que $v_A(x) < v_A(y)$. Supondo que $v_A(x+y) \neq \min\{v_A(x), v_A(y)\}$, temos: $v_A(x+y) > v_A(x)$. Assim, $v_A(x) = v_A((x+y)-y) \geq \min\{v_A(x+y), v_A(y)\} > v_A(x)$, contradição. ■

Na construção que acabamos de fazer, começamos com um anel de valorização e obtivemos, a partir dele, uma aplicação $v_A : F \to \Gamma_A \cup \{\infty\}$. Poderíamos fazer o caminho inverso, começando com uma aplicação $v : F \to \Gamma \cup \{\infty\}$ satisfazendo (1), (2) e (3), e chegando a um anel de valorização $A_v = \{x \in F \mid v(x) \geq 0\}$. No restante do trabalho optamos por falar sempre em anel de valorização, ficando subentendido que, ao tomarmos um anel de valorização A, estamos considerando a família $(A, v_A, \mathfrak{m}_A, \Gamma_A, k_A)$.

Vamos a dois exemplos que servem como preparação para os conceitos que iremos introduzir logo após:

Exemplos:

(1) Seja k um corpo e Γ um grupo abeliano (totalmente) ordenado. O *corpo de séries formais generalizado* $F = k((\Gamma))$ consiste de todas as somas formais $f = \sum_{i\in\Gamma} a_i t^i$, com coeficientes $a_i \in k$, onde t é um símbolo fixado, tais que o *suporte* de f $\text{supp}(f) = \{i \in \Gamma \mid a_i \neq 0\}$ é bem ordenado (isto é, admite um elemento mínimo). A adição em F é definida componente a componente. A multiplicação é definida via $t^i t^j = t^{i+j}$. É pura rotina (ainda que trabalhosa) mostrar que F é, de fato, um corpo.

Em F há uma valorização natural dada por $v(\sum_{i\in\Gamma} a_i t^i) = \min\{i | a_i \neq 0\}$. Se $a_i = 0$ para todo $i \in \Gamma$, isto é, se $\text{supp}(f) = \emptyset$, convenciona-se que $\min\{i | a_i \neq 0\} = \infty$. O anel de valorização associado é $A = k[[\Gamma]] = \{f \in F \mid v(f) \geq 0\}$ e $\mathfrak{m}_A = \{f \in F \mid v(f) > 0\}$.

O corpo de resíduos é $k_A = k$ e o grupo de valores é $\Gamma_A = \Gamma$. Podemos, assim, produzir valorizações que tenham corpo de resíduos e grupo de valores pré-determinados.

Caso particular: $\Gamma = \mathbb{Z}$. Neste caso, $F = k((t))$ é o corpo das séries formais $f = \sum_{i=n}^{\infty} a_i t^i$, onde $n \in \mathbb{Z}$ e $A = k[[t]]$ é o anel das séries formais $f = \sum_{i=n}^{\infty} a_i t^i$, onde $n \in \mathbb{Z}$, $n \geq 0$. O ideal maximal de A é $\mathfrak{m}_A = tA$.

(2) Dado um corpo k, seja $F = k(t)$ o corpo de funções racionais sobre k. Os elementos de $k(t)$ são frações do tipo $\frac{f(t)}{g(t)}$, onde $f, g \in k[t]$ são polinômios na indeterminada t. Dado um polinômio irredutível $p(t) \in k[t]$, podemos escrever, de maneira única, $\frac{f}{g} = p^n \cdot \frac{r}{s}$, onde $r, s \in k[t]$ são tais que $p \nmid r$ e $p \nmid s$. A unicidade dessa representação é garantida por ser $k[t]$ um domínio de fatoração única.

Podemos definir $v_p : F \to \mathbb{Z} \cup \{\infty\}$ pondo $v_p(\varphi) = n$, se $\varphi = p^n \frac{r}{s} \neq 0$ e $v_p(0) = \infty$. A aplicação v_p é uma valorização, denominada *valorização p-ádica* de F. O anel de valorização associado a v_p é a *localização* $A = k[t]_{\mathfrak{p}} = \{\frac{f(t)}{g(t)} \mid p(t) \nmid g(t)\}$, onde $\mathfrak{p} = (p(t))$ é o ideal (primo) gerado por $p(t)$. O corpo de resíduos é $k_A = k[t]_{\mathfrak{p}}/\mathfrak{p}k[t]_{\mathfrak{p}} \simeq k[t]/(p(t))$[1].

Caso particular: o polinômio $p(t) = t - a$ (onde $a \in k$) é irredutível. A valorização $(t-a)$-ádica tem grupo de valores $\Gamma = \mathbb{Z}$, anel de valorização $A = k[t]_{(t-a)}$ e corpo de resíduos $k[t]_{(t-a)}/(t-a)k[t]_{(t-a)} \simeq k$. Note que A consiste exatamente das frações $\frac{f(t)}{g(t)}$ tais que $t - a \nmid g(t)$, isto é, $g(a) \neq 0$. Isso significa que A é o anel das funções *regulares* em a.

Observe que, no exemplo (1) (caso particular), temos: $1 + \mathfrak{m}_A \subset \dot{F}^2$. De fato, $\varphi \in 1 + \mathfrak{m}_A$ implica que $\varphi = 1 + tf(t)$, onde $f(t) \in k[[t]]$. Agora, $\psi \in F^2$ se, e somente se, $\psi = a_n t^n + a_{n+1} t^{n+1} + \cdots$, onde $n = 2m$ e $a_n \in k^2$. De fato, se ψ é dada da maneira acima, onde $a_n = \alpha^2$, podemos construir uma "raiz quadrada"de ψ: $\varphi = b_m t^m + b_{m+1} t^{m+1} + \cdots$, onde $b_m = \alpha$, $b_{m+1} = \frac{a_{n+1}}{2\alpha}$ e, supondo construídos $b_m, b_{m+1}, \ldots, b_{m+l-1}$, encontramos b_{m+l} $(l \geq 2)$ resolvendo a equação

$$a_{n+l} = b_m b_{m+l} + b_{m+1} b_{m+l-1} + \cdots + b_{m+l-1} b_{m+1} + b_{m+l} b_m.$$

A outra implicação é direta. Usando esse critério, vemos que $\varphi \in F^2$. Por outro lado, no exemplo (2) (caso particular), se $a = 1$, temos $t - 1 \in \mathfrak{m}_A$, logo $t = 1 + (t-1) \in 1 + \mathfrak{m}_A$,

[1]Em geral, se R é um anel comutativo com unidade e $\mathfrak{p}$ é um ideal primo de R, então $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ é isomorfo ao corpo de frações do domínio $R/\mathfrak{p}$. Como em $R = k[t]$ todo ideal primo é maximal, $R/\mathfrak{p} = k[t]/(p(t))$ já é um corpo.

mas $t \notin \dot{F}^2$. Portanto, $1 + \mathfrak{m}_A \not\subset \dot{F}^2$.

Compatibilidade.

A principal diferença entre as valorizações do exemplo (1) e do exemplo (2) é que, como vimos acima, no primeiro caso temos $1 + \mathfrak{m}_A \subset \dot{F}^2$, o que não ocorre no segundo caso. Essa "compatibilidade" entre A e um subgrupo de $\dot{F}$ (no caso, $\dot{F}^2$) é uma propriedade importante, como veremos a seguir.

Seja U um subgrupo de $\dot{F}$. Dizemos que o anel de valorização A é *U-compatível* se

$$1 + \mathfrak{m}_A \subset U \tag{4.1.1}$$

No exemplo (1), acima, vimos que $1 + \mathfrak{m}_A \subset U = \dot{F}^2$. Esse é um caso particular de especial importância, que analisaremos com mais detalhe adiante (Proposição 4.11).

Outro caso importante é quando $U = T$, onde T é uma pré-ordem de F. Vimos no capítulo 2 que existe um anel de valorização T-compatível, sempre que T for um "leque" (veja o Teorema 3.12 na página 24). Em particular, se $U = P$, uma ordem de F, o anel de valorização

$$A(P) = \{x \in F \,|\, \text{existe } n \text{ natural tal que } n - x \in P \text{ ou } n + x \in P\}$$

é P-compatível. O resultado a seguir relaciona P-compatibilidade com convexidade:

Proposição 4.2 ([22], Teorema 2.3, p.18) *Se P é uma ordem de F e A é um anel de valorização de F, as seguintes afirmações são equivalentes:*

(i) *A é convexo em relação a P, isto é, se $0 < a < b$ e $b \in A$ então $a \in A$, onde $<$ é a ordem induzida por P.*

(ii) *$\mathfrak{m}_A$ é convexo em relação a P.*

(iii) $1 + \mathfrak{m}_A \subset P$.

Demonstração. Supondo que $0 < a < b \in \mathfrak{m}_A$, temos $0 < b^{-1} < a^{-1}$. Mas $b^{-1} \notin A$, pois $b \in \mathfrak{m}_A$. Logo, por (i), $a^{-1} \notin A$ e isso implica que $a \in \mathfrak{m}_A$. Portanto vale (ii).

Supondo que vale (ii), tomemos $m \in \mathfrak{m}_A$. Se $1 + m \notin P$ teríamos $1 + m < 0$, ou seja $0 < 1 < -m$. Como $0, -m \in \mathfrak{m}_A$, a convexidade de $\mathfrak{m}_A$ implicaria $1 \in \mathfrak{m}_A$, uma contradição. Logo, vale (iii).

Finalmente, suponhamos que $0 < a < b$ e $b \in A$. Se $v_A(a) < v_A(b)$ então $v_A(\frac{b}{a}) > 0$, o que implicaria $\frac{b}{a} \in \mathfrak{m}_A$ e $1 - \frac{b}{a} \in 1 + \mathfrak{m}_A \overset{\text{(iii)}}{\subset} P$. Teríamos, então, $1 - \frac{b}{a} > 0$, isto é,

$a > b$, contradizendo a escolha de a e b. Como $b \in A$, temos $v_A(a) \geq v_A(b) \geq 0$ e isso implica $a \in A$. ■

Corolário 4.3 *Seja P uma ordem de F. A família $\mathcal{F}$ dos anéis de valorização de F compatíveis com P é totalmente ordenada pela inclusão.*

Demonstação. Dados $A, B \in \mathcal{F}$, a Proposição 4.2 implica que A e B são convexos. Suponhamos que $A \not\subset B$ e tomemos $a \in A \setminus B$ com $a > 0$ em relação a P. Consideremos $0 < b \in B$. Como $a \notin B$, não podemos ter $0 < a \leq b$, pois B é convexo. Assim, $0 < b < a \in A$ e, como A é convexo, $b \in A$. Isso mostra que $B \subset A$. ■

Corolário 4.4 *O conjunto dos anéis de valorização de F compatíveis com uma pré-ordem T é totalmente ordenado pela inclusão.*

Demonstração. Se A e B são anéis de valorização de F compatíveis com T, então $1 + \mathfrak{m}_A \subset T$ e $1 + \mathfrak{m}_B \subset T$. Logo, se P é uma ordem de F contendo T, A e B são compatíveis com P. Pelo Corolário 4.3, A e B são comparáveis. ■

Henselianidade.

Seja $K|F$ uma extensão de corpos. Suponha que $A \subset F$ e $B \subset K$ sejam anéis de valorização. Dizemos que B é uma *extensão* de A quando $B \cap F = A$. O teorema de Chevalley abaixo (ou, mais especificamente, seu corolário) garante que um anel de valorização de um corpo F sempre pode ser estendido a um corpo $K \supset F$. Para uma demonstração do Teorema 4.5, veja [27], página 205.

Teorema 4.5 (Chevalley) *Seja K um corpo, $R \subseteq K$ um subanel e $\mathfrak{p} \subset R$ um ideal primo. Então existe um anel de valorização A de K tal que: $R \subseteq A$ e $\mathfrak{m}_A \cap R = \mathfrak{p}$.*

Corolário 4.6 *Se $K|F$ é uma extensão de corpos e A é um anel de valorização de F, então existe um anel de valorização B de K que é extensão de A.*

Demonstração. $A \subset F \subset K$. Logo, o Teorema 4.5 garante a existência de um anel de valorização B de K tal que $A \subset B$ e $\mathfrak{m}_B \cap A = \mathfrak{m}_A$. Devemos mostrar que $B \cap F = A$. A inclusão $\supseteq$ segue-se de $B \supset A$. Para a outra inclusão, tomemos $x \in B \cap F$. Se $x \notin A$, teríamos $x \neq 0$ e $x^{-1} \in \mathfrak{m}_A = \mathfrak{m}_B \cap A$. Logo, teríamos $1 = xx^{-1} \in \mathfrak{m}_B$, contradição! ■

Seja $K|F$ uma extensão algébrica[2] e $B \subset K$ uma extensão do anel de valorização $A \subset F$. Os homomorfismos $A \hookrightarrow B \twoheadrightarrow B/\mathfrak{m}_B = k_B$ e $\dot{F} \hookrightarrow \dot{K} \twoheadrightarrow \dot{K}/B^* \simeq \Gamma_B$ têm núcleos $\mathfrak{m}_B \cap A = \mathfrak{m}_A$ e $B^* \cap \dot{F} = A^*$, respectivamente. Isso nos permite ver $k_A = A/\mathfrak{m}_A$ como subcorpo de k_B e $\Gamma_A \simeq \dot{F}/A^*$ como subgrupo de Γ_B. Podemos, então, definir o *índice de ramificação* $e = e(B|A) = (\Gamma_B : \Gamma_A)$ e o *grau de inércia* $f = f(B|A) = (k_B : k_A)$. Dizemos que B é uma extensão *imediata* de A se $e(B|A) = f(B|A) = 1$. Quando for necessário enfatizar os corpos de frações de A e B, diremos que (K, B) é extensão imediata de (F, A).

Se $K|F$ é uma extensão finita, A é um anel de valorização de F e $\mathcal{B}(K, A)$ é o conjunto dos anéis de valorização de K que estendem A, temos a seguinte *desigualdade fundamental*:

$$[K : F] \geq \sum_{B \in \mathcal{B}(K,A)} e(B|A) \cdot f(B|A). \tag{4.1.2}$$

Uma demonstração deste fato pode ser encontrada em [11], Corolário 17.5, página 128. O anel de valorização A é dito *sem defeito* em K se vale a igualdade em (4.1.2).

De particular interesse é o caso em que o anel de valorização A de F estende-se de modo único para uma extensão normal $N|F$. Uma caracterização desse fato é apresentada no Teorema 4.7 abaixo, que é uma versão devida a L. Bröcker, [7] (1.2), p.151, do resultado conhecido como Lema de Hensel ([28], Teorema 4, p.185).

Originalmente concebido como a principal ferramenta no estudo dos números p-ádicos, o Lema de Hensel foi posteriormente generalizado por W. Krull para anéis de valorização arbitrários. Mais precisamente, a generalização de Krull caracteriza anéis de valorização A de um corpo F que extendem-se de modo único ao fecho algébrico F_{alg} em termos do levantamento de raízes de polinômios a partir do corpo de resíduos de A. Por sua vez, Bröcker [7] observou que a mesma demonstração é válida para uma extensão normal qualquer $N|F$, desde que se assuma uma hipótese adicional sobre os polinômios[3].

Lembremos que para um elemento $a \in A$, denotamos $\bar{a} = \pi_A(a)$ e, se $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, denotamos $\bar{f}(X) = \bar{a}_n X^n + \cdots + \bar{a}_1 X + \bar{a}_0 \in k_A[X]$.

Teorema 4.7 (Lema de Hensel - Bröcker, [7] (1.2)) *Seja F um corpo munido de um anel de valorização A e N uma extensão normal de F. As seguintes afirmações são*

[2]Como estamos interessados em extensões contidas no fecho quadrático de F, o caso em que a extensão $K|F$ é transcendente não está relacionado ao nosso trabalho.

[3]Mais precisamente, devemos supor que $f(X) \in A[X]$ é um polinômio que decompõe-se em fatores lineares em $N[X]$, o que naturalmente sempre acontece em $F_{\text{alg}}[X]$ (veja o item (ii) do Teorema 4.7).

equivalentes.

(i) *A estende-se de modo único para o corpo N.*

(ii) *Seja $f(X) \in A[X]$ um polinômio mônico que decompõe-se em fatores lineares sobre N e $a_0 \in A$ tal que $\bar{a}_0 \in k_A$ é uma raiz simples de $\bar{f}(X)$. Então existe uma raiz $a \in A$ de $f(X)$ tal que $\bar{a} = \bar{a}_0$.*

Um anel de valorização A de F que satisfaz uma das condições acima é denominado N-henseliano.

Seja $N|F$ uma extensão normal com grupo de Galois $G = G(N|F)$. Seja B um anel de valorização de N e $A = B \cap F$. Como fizemos na página 51, denotamos por $\mathcal{B}$ o conjunto dos anéis de valorização de N que estendem A. Por [11], Corolário 14.3, página 106, a aplicação $G \to \mathcal{B}$ dada por $\sigma \mapsto \sigma(B)$ é sobrejetiva. O conjunto

$$G^h(B|F) = \{\sigma \in G \mid \sigma(B) = B\}$$

é um subgrupo de G, denominado *grupo de decomposição* de B sobre F. O corpo fixo relativo a $G^h = G^h(B|F)$:

$$F^h = F^h(B|F) = \{x \in N \mid \sigma(x) = x \text{ para todo } \sigma \in G^h\}$$

é chamado *corpo de decomposição* de B sobre F (cf. [11], p. 110).

Uma *N-henselização* de (F, A) é um par (H, A_H) satisfazendo as seguintes condições (cf. [28], página 175):

(H1) $H|F$ é uma extensão algébrica, $H \subset N$ e $A_H \cap F = A$.

(H2) Se $H \subset L \subset N$ então A_H tem uma única extensão a L.

(H3) Se (H', A'_H) é um par satisfazendo as propriedades (H1) e (H2), então existe um F-isomorfismo τ de H em H' tal que $\tau(A'_H) = A_H$.

Observação 4.8 *De acordo com [28] Teorema 2, página 176, podemos considerar $H = F^h(B|F)$, ou seja, o corpo de decomposição relativo a uma extensão de A para N é uma N-henselização de F. Pela condição (H3), todas as possíveis N-henselizações são F-isomorfas.*

Do Teorema 15.8 de [11], resulta que $(F^h, B \cap F^h)$ é uma extensão imediata de (F, A)

Observação. Sabemos que o fecho quadrático $F(2)$ é uma extensão normal de F (veja a página 2). No caso em que $N = F(2)$, um anel de valorização satisfazendo as condições do Teorema 4.7 é dito 2-*henseliano*. Devemos observar ainda que quando $N = F(2)$ podemos considerar, no item (ii) do Teorema 4.7, f como sendo um polinômio de grau 2. Uma henselização H de F relativa a $N = F(2)$ é chamada 2-henselização.

Pela Proposição 2.9, o T-fecho F_T, definido na página 8, é uma extensão normal de F. Assim, podemos considerar no Teorema 4.7, $N = F_T$. Um anel de valorização A de F é dito T-*henseliano* se A satisfaz uma das condições equivalentes do Teorema 4.7 com $N = F_T$. Uma henselização H de F relativa a $N = F_T$ é chamada de T-henselização. A Proposição 4.9 a seguir apresenta duas caracterizações de um anel de valorização T-henseliano. Uma versão, para o caso $T = \sum \dot{F}^2$ pode ser encontrada em [12], Lema 2.1. Neste caso, consideramos $N = F_\pi$, o fecho pitagórico de F, e dizemos que o anel de valorização é π-henseliano. Uma vez que, para cada pré-ordem T de F, $F_\pi \subset F_T$ (cf. a Definição 2.8), todo anel de valorização T-henseliano também é π-henseliano.

Proposição 4.9 *Para cada anel de valorização A de um corpo F tal que car $k_A \neq 2$, as seguintes condições são equivalentes:*

(i) *A é T-henseliano;*

(ii) $(1 + \mathfrak{m}_A) \cap T \subset F^2$*;*

(iii) *Dados $s, t \in T$ tais que $v_A(t-s) > v_A(s)$, temos: $s \in \dot{F}^2$ se, e somente se, $t \in \dot{F}^2$.*

Demonstração. $(i) \Rightarrow (ii)$ Suponha que A é T-henseliano. Dado $t \in (1 + \mathfrak{m}_A) \cap T$, do fato de t pertencer a $1 + \mathfrak{m}_A$, segue-se que $\overline{X^2 - t} = X^2 - \overline{t} = X^2 - \overline{1}$. Além disso, como $t \in T$, temos que $t \in F_T^2$. Logo, o polinômio $X^2 - t$ decompõe-se em $F_T[X]$ e $\overline{X^2 - t} = (X - \overline{1})(X + \overline{1})$. Portanto, pelo Teorema 4.7, $X^2 - t$ decompõe-se em $F[X]$ e, assim $t \in F^2$.

$(ii) \Rightarrow (i)$ Seja A um anel de valorização de F tal que $(1 + \mathfrak{m}_A) \cap T \subset F^2$. Para uma extensão C de A a F_T, consideremos a T-henselização $F^h = F^h(C|F)$ (veja a página 52). Para provarmos que A é T-henseliano, temos que demonstrar que $F^h = F$.

Suponha que $F^h \neq F$. Então, existe uma subextensão $F \subset L \subset F^h$ tal que $[L : F] = 2$, pois $F \subset L \subset F_T$ e $F_T|F$ é uma extensão obtida a partir de uma torre de extensões multiquadráticas. Portanto, $L = F(\sqrt{x})$, onde $x \in F$ e $x \notin F^2$. Seja $B = C \cap L$. Pela

Observação 4.8, $(F^h, C \cap F^h)$ é uma extensão imediata de (F, A). Logo, o par (L, B) também é uma extensão imediata de (F, A), ou seja, $\Gamma_B = \Gamma_A$ e $k_B = k_A$.

$$\begin{array}{ccc} \left(F^h, C \cap F^h\right) & \Gamma_h & k_h \\ | & = & = \\ (L, B) & \Gamma_B & k_B \\ | & = & = \\ (F, A) & \Gamma_A & k_A \end{array} \tag{4.1.3}$$

Logo, existe $a \in \dot{F}$ tal que $v_B(a) = v_A(a) = v_B(\sqrt{x})$ e assim, $v_B(a^{-1}\sqrt{x}) = 0$, o que implica $a^{-1}\sqrt{x} = u \in U_B$ (onde U_B denota o conjunto das unidades de B). Então, temos a seguinte seqüência de implicações: $\pi_B(u) = \pi_B(a^{-1}\sqrt{x}) \Rightarrow \pi_B(a^{-1}u^{-1}\sqrt{x}) = 1 \Rightarrow \pi_B(a^{-2}u^{-2}x) = 1^2 = 1 \Rightarrow \pi_A(a^{-2}u^{-2}x) = \pi_B(a^{-2}u^{-2}x) = 1 \Rightarrow a^{-2}u^{-2}x \in 1 + \mathfrak{m}_A$.

Portanto, podemos supor que $x \in 1 + \mathfrak{m}_A$ (pois $F(\sqrt{a^{-2}u^{-2}x}) = F(\sqrt{x})$). Uma vez que $L \subset F_T$ e F_T é formalmente real, $L = F(\sqrt{x})$ é, necessariamente, formalmente real. Se $x \notin T$, a pré-ordem T não se estenderia a L e, assim, não se estenderia a F_T. Daí, concluímos que $x \in T$ e, pela hipótese, $x \in (1 + \mathfrak{m}_A) \cap T \subset F^2$, logo $F(\sqrt{x}) = F$, o que contradiz $[L : F] = 2 > 1$. A contradição vem de termos admitido $F^h \neq F$. Assim, devemos ter $F^h = F$ e F é T-henseliano.

$(ii) \Rightarrow (iii)$ Dados $s, t \in T$, suponhamos que $v_A(t - s) > v_A(s)$. Isso implica que $v_A(\frac{t-s}{s}) > 0$. Logo, $ts^{-1} - 1 \in \mathfrak{m}_A$, ou seja, $ts^{-1} \in (1 + \mathfrak{m}_A) \cap T \subset \dot{F}^2$, e daí $t \in s\dot{F}^2$.

$(iii) \Rightarrow (ii)$ Se $t \in (1 + \mathfrak{m}_A) \cap T$, então $v_A(t - 1) > 0 = v_A(1)$, e isso implica que $t \in 1\dot{F}^2$. Portanto, $(1 + \mathfrak{m}_A) \cap T \subset \dot{F}^2$. ■

A Proposição 4.10 a seguir exemplifica como, sob a hipótese de T-henselianidade para um anel de valorização A de F, podemos "levantar" informações do corpo de resíduos k_A para o corpo F. Convém observar que, como $F_T \subset F(2)$, todo anel de valorização 2-henseliano é também T-henseliano[4]. Isso mostra que o resultado abaixo continua válido se A é 2-henseliano.

Proposição 4.10 *Se A é um anel de valorização T-henseliano de F e k_A é formalmente real e pitagórico, então F também é pitagórico.*

Demonstração. Dado $x \in F$, queremos mostrar que $1 + x^2 \in F^2$. Como A é T-henseliano, se $x \in \mathfrak{m}_A$ então $1 + x^2 \in (1 + \mathfrak{m}_A) \cap T \subset F^2$. Podemos, então, supor que

[4]Outra maneira de ver isso é notando que $1 + \mathfrak{m}_A \subset F^2$ implica $(1 + \mathfrak{m}_A) \cap T \subset F^2 \cap T = F^2$, para uma pré-ordem T de F.

$x \notin \mathfrak{m}_A$ e, uma vez que $x = x^{-1}x^2$, podemos supor que $x \in A \setminus \mathfrak{m}_A = A^*$. Como k_A é formalmente real, $\pi_A(1+x^2) \neq 0$. Logo, $\pi_A(1+x^2) = 1 + \pi_A(x)^2 \in \dot{k}_A^2$, pois k_A é pitagórico. Assim, existe $y \in A^*$ tal que $\pi_A(1+x^2) = \pi_A(y^2)$ e isso implica que $(1+x^2)y^{-2} \in (1+\mathfrak{m}_A) \cap T \subset F^2$, donde $1+x^2 \in F^2$. ■

Observação. A Proposição 4.10 mostra que, se F não for pitagórico, o corpo de resíduos de qualquer anel de valorização T-henseliano não poderá ser simultaneamente pitagórico e formalmente real, ou seja, o corpo de resíduos será formalmente real e não pitagórico ou quadraticamente fechado (veja o Exemplo (2) na página 4).

Relação entre compatibilidade e henselianidade.

A seguir indicaremos como as noções de henselianidade e compatibilidade se relacionam. A Proposição 4.11 abaixo mostra que, para um anel de valorização A com car $k_A \neq 2$, a 2-henselianidade, definida na observação logo após o Teorema 4.7, é equivalente à $\dot{F}^2$-compatibilidade, definida em (4.1.1).

Proposição 4.11 ([22], Lema 3.14) *Seja A um anel de valorização de F com car $k_A \neq 2$. Então A é 2-henseliano se e somente se $1 + \mathfrak{m}_A \subset \dot{F}^2$.*

Demonstração.[22] Primeiro suponhamos que A é 2-henseliano. Dado $m \in \mathfrak{m}_A$, mostraremos que $1+m \in \dot{F}^2$. De fato, se $f(X) = X^2 - (1+m) \in A[X]$ então $\bar{f}(X) = X^2 - \bar{1} = (X-\bar{1})(X+\bar{1}) \in k_A[X]$ e, como car $k_A \neq 2$, $\pm\bar{1}$ são raízes simples de $\bar{f}$ em k_A. Além disso, o polinômio quadrático $f(X)$ decompõe-se em fatores lineares sobre $F(2)$. Pelo Teorema 4.7, existe $a \in A$ tal que $f(a) = 0$, ou seja, $1 + m = a^2 \in \dot{F}^2$.

Reciprocamente, suponhamos que $1+\mathfrak{m}_A \subset \dot{F}^2$. Pela observação da página 53, basta verificarmos a validade do item (ii) do Teorema 4.7 para polinômios quadráticos. Mais precisamente, seja $f(X) = X^2 - aX - b \in A[X]$ tal que $\bar{f}(X)$ tem uma raiz simples $\bar{r} \in k_A$, com $r \in A$. Como car $k_A \neq 2$, temos $\frac{1}{2} \in A$ e, após uma mudança de variáveis podemos supor que $a = 0$. Logo, $\bar{f}(X) = X^2 - \bar{b}$ e $\bar{r}^2 = \bar{b} \neq 0$. Seja $m := r^2 - b \in \mathfrak{m}_A$. Como r é uma unidade em A, temos

$$b = r^2(1 - r^{-2}m) \in r^2 \cdot (1 + \mathfrak{m}_A) \subset F^2 \cap A = A^2.$$

Escrevendo $b = c^2$, onde $c \in A$, temos $\bar{r}^2 = \bar{b} = \bar{c}^2$ de modo que $\pm c$ são raízes simples de $f(X)$ em A, uma das quais projeta-se sobre a raiz $\bar{r}$ de $\bar{f}(X)$. ■

Observando-se a Proposição 4.11 acima é de se esperar que haja alguma relação similar entre T-henselianidade e U-compatibilidade, para algum subgrupo U de $\dot{F}$ que de algum modo deve estar relacionado à pré-ordem T. Não devemos esperar uma relação direta entre T-henselianidade e T-compatibilidade, pois, de acordo com o item (ii) da Proposição 4.9, um anel de valorização T-compatível e T-henseliano é, de fato, 2-henseliano.

Lembremos que, no Capítulo 3, página 29, definimos para um subgrupo T de $\dot{F}$ o seguinte subgrupo de $\dot{F}$, que convencionamos chamar de radical:

$$\mathcal{R}(T) = \bigcap_{t \in T} D\langle 1, -t\rangle.$$

Nosso intuito é mostrar que, sob certas condições naturais sobre o corpo F, o radical $\mathcal{R}(T)$ é exatamente o subgrupo U que estamos procurando. Mais precisamente, temos o seguinte resultado.

Teorema 4.12 *Seja F um corpo, T uma pré-ordem de F e $d \in T$ um elemento rígido tal que $\sum \dot{F}^2 \not\subset D\langle 1, d\rangle$. Se A é um anel de valorização $\mathcal{R}(T)$-compatível, então A é T-henseliano.*

Demonstração. Mostraremos primeiro que, sob as hipóteses acima,

$$T \cap \mathcal{R}(T) = \dot{F}^2. \tag{4.1.4}$$

De fato, seja $t \in T \cap \mathcal{R}(T)$. Então $t \in D\langle 1, -t\rangle$ e isso implica que $t \in D\langle 1, 1\rangle$. Por outro lado, como $d \in T$, temos $t \in \mathcal{R}(T) \subset D\langle 1, -d\rangle$. Logo, $t \in D\langle 1, 1\rangle \cap D\langle 1, -d\rangle$ e, pelo item (2) da Proposição C.9, $t \in D\langle 1, d\rangle = \dot{F}^2 \cup d\dot{F}^2$.

Supondo, por absurdo, que $t \in d\dot{F}^2$, obtemos $d \in t\dot{F}^2$. Uma vez que $t \in \mathcal{R}(T) \subset D\langle 1, -d\rangle$ podemos concluir a partir de $d \in D\langle 1, -d\rangle$ que $d \in D\langle 1, 1\rangle$. Como $\sum \dot{F}^2 \subset T$ temos, pelo item (1) da Proposição 3.19, que $\mathcal{R}(T) \subset \mathcal{R}(\sum \dot{F}^2) = R_0$ (conforme a notação estabelecida no item (3) dessa mesma Proposição 3.19). Como $d \in \sum \dot{F}^2$ temos $R_d = R_0$. Logo $d \in R_d$ e, pelo item (iv) da Proposição 3.4, $D\langle 1, 1\rangle \subset D\langle 1, d\rangle$. Por indução, $\sum \dot{F}^2 \subset D\langle 1, d\rangle$, contrariando a hipótese. Portanto, $t \in \dot{F}^2$ e $T \cap \mathcal{R}(T) = \dot{F}^2$.

Agora, se $1 + \mathfrak{m}_A \subset \mathcal{R}(T)$, então $(1 + \mathfrak{m}_A) \cap T \subset T \cap \mathcal{R}(T) = \dot{F}^2$. Logo, pelo item (ii) da Proposição 4.9, A é T-henseliano. ■

O item (4) da Proposição 3.19 garante que $\mathcal{R}(S_d) = R_d$. Logo, obtemos o seguinte resultado:

Corolário 4.13 *Seja d um elemento rígido de F tal que $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$. Sejam R_d e S_d como definidos em 3.3. Se o anel de valorização A de F é compatível com R_d, então A é S_d-henseliano.*

Para algumas pré-ordens T tais que o radical $\mathcal{R}(T)$ é "pequeno" podemos obter, a partir da $\mathcal{R}(T)$-compatibilidade, uma henselianidade "grande", isto é, o anel de valorização estende-se de modo único a uma extensão normal grande de F. Por exemplo, se T_0 é a menor pré-ordem que contém $-d$ (veja a Proposição 3.16) então $\mathcal{R}(T_0) = \dot{F}^2$, como já verificamos na Proposição 3.20. Temos o seguinte Corolário imediato:

Corolário 4.14 (da Proposição 3.20) *Seja A um anel de valorização de F tal que car $k_A \neq 2$. Então A é $\mathcal{R}(T_0)$-compatível se e somente se A é 2-henseliano.*

Demonstração. Pela Proposição 3.20, $\mathcal{R}(T_0) = \dot{F}^2$. Pela Proposição 4.11, segue o resultado. ■

4.2 Construção de valorizações T-compatíveis

Os principais resultados do nosso trabalho são válidos para um corpo F admitindo um elemento rígido d que não é birígido, tal que $d \notin \sum \dot{F}^2$. Já vimos, no Corolário 3.18, que um tal elemento d é T_d-birígido, onde $T_d = R_d \cdot \sum \dot{F}^2$ é uma pré-ordem. Nesta seção construímos um anel de valorização compatível com uma pré-ordem a partir de elementos birígidos em relação a essa pré-ordem (Corolário 4.19). Utilizando esse Corolário, obtemos um anel de valorização compatível com a pré-ordem T_d (Corolário 4.20). Mais ainda, mostraremos na Proposição 4.23 que existe um anel de valorização A de F tal que $R_d = (1 + \mathfrak{m}_A)\dot{F}^2$. Esse anel de valorização será de crucial importância para obtermos os resultados de estrutura para o anel de Witt de F no capítulo seguinte.

A construção que apresentamos apareceu na literatura no início dos anos 80 num trabalho de Roger Ware [34] e vem sendo aperfeiçoada e modificada desde então. A noção de elemento T-rígido (veja a página 12) foi introduzida por Ware também em [34], embora o termo *rígido* tenha sido usado antes em [32], p.29. Essa construção foi motivada principalmente pelo Teorema 3.12 de Bröcker, que garante a existência de um anel de valorização compatível com T, quando T é um leque, isto é, quando há em F uma grande quantidade de elementos T-rígidos. A construção atendendo aos nossos objetivos que faremos a seguir é baseada naquela desenvolvida em [1].

Recordemos que, na página 32, definimos

$$B(T) = \{x \in \dot{F} \,|x \text{ não é } T\text{-birígido}\}.$$

De acordo com a Proposição 3.23 da página 34, se T é uma pré-ordem, $B(T)$ é grupo.

Vamos, a seguir, considerar os conjuntos:

$$\mathcal{O}_1 = \mathcal{O}_1(B(T), T) = \{x \in F | x \notin B(T) \text{ e } 1 + x \in T\} \tag{4.2.1}$$

$$\mathcal{O}_2 = \mathcal{O}_2(B(T), T) = \{x \in B(T) | x\mathcal{O}_1 \subset \mathcal{O}_1\} \tag{4.2.2}$$

$$\mathcal{O}(B(T), T) = \mathcal{O}_1 \cup \mathcal{O}_2 \tag{4.2.3}$$

Supondo que $A = \mathcal{O}(B(T), T)$ é um anel de valorização de F, veremos a seguir que A é T-compatível e não trivial, desde que exista um elemento $d \in F$ que seja T-birígido. Observe que um tal d satisfaz: $d \in \dot{F} \setminus B(T)$, o que implica $B(T) \neq \dot{F}$ (veja o item (3)(b), abaixo).

Proposição 4.15 ([34], Proposição 2.8) *Se $A = \mathcal{O}(B(T), T)$ é um anel de valorização de F, então:*

(1) $A^*T \subset B(T)$

(2) $1 + \mathfrak{m}_A \subset T$

(3) *São equivalentes*

  (a) $A = F$

  (b) $B(T) = \dot{F}$

  (c) $\Gamma_A = 2\Gamma_A$

(4) *car* $k_A \neq 2$

Demonstração. (1) Como $T \subset B(T)$, é suficiente mostrar que $A^* \subset B(T)$. Se $x \notin B(T)$, então x é T-rígido e isso implica $1 + x \in T$ ou $1 + x \in xT$. Suponhamos, primeiro, que $1 + x \in xT$. Como $x \notin B(T)$, certamente $x \notin \mathcal{O}_2$. Assim, se $x \in A$, temos necessariamente, $x \in \mathcal{O}_1$, o que implica $1 + x \in T$. Como $1 + x \in xT$, teríamos $1 + x \in T \cap xT = \emptyset$, contradição ($T \cap xT = \emptyset$ porque $x \notin B(T) \supset T$). Logo, $x \notin A \supset A^*$.

Por outro lado, se $1+x \in T$, então $1+x^{-1} \in x^{-1}T$ e podemos repetir o argumento acima para mostrar que $x^{-1} \notin A$, ou seja, $x \notin A^*$.

(2) Dado $x \in \mathfrak{m}_A$, devemos mostrar que $1+x \in T$. Se $x \in \mathcal{O}_1$, então $1+x \in T$ automaticamente (pela definição de $\mathcal{O}_1$). Logo, podemos supor que $x \in A \setminus \mathcal{O}_1$, ou seja, que $x \in \mathcal{O}_2 \subset B(T)$. Além disso, como $x \in \mathfrak{m}_A$, $x^{-1} \notin A$ e isso implica que existe $y \in \mathcal{O}_1$ tal que $1+x^{-1}y \notin T$, caso contrário, $1+x^{-1}y \in T$, para todo $y \in \mathcal{O}_1$ iria implicar que $x^{-1}y \in \mathcal{O}_1$, para todo $y \in \mathcal{O}_1$, isto é, $x^{-1}\mathcal{O}_1 \subset \mathcal{O}_1$, o que implicaria $x^{-1} \in \mathcal{O}_2 \subset A$. Note que $x^{-1}y \notin B(T)$, pois $x^{-1} \in B(T)$, $y \notin B(T)$ e $B(T)$ é grupo. Assim, $x^{-1}y$ é (T-birígido e, em particular) T-rígido. Logo, $1+x^{-1}y \in T \cup x^{-1}yT$ e, uma vez que $1+x^{-1}y \notin T$, concluímos que $1+x^{-1}y \in x^{-1}yT$. Por outro lado, $T \subset B(T)$ implica que $x^{-1}yT \cap B(T) = \emptyset$, pois $x^{-1}y$ é T-rígido. Portanto,

$$1+x^{-1}y \notin B(T). \tag{4.2.4}$$

Pela escolha de y, temos $y \notin B(T)$, logo $-y \notin B(T)$, pois $-1 \in -T \subset B(T)$. Como estamos supondo que A é um anel, $-y \in A = \mathcal{O}_1 \cup \mathcal{O}_2$. Assim, $-y \in \mathcal{O}_1$, pois $-y \notin B(T)$ implica que $-y \notin \mathcal{O}_2$. Dessa forma, temos $1-y \in T$ e

$$1+x^{-1}y = 1+x^{-1}-x^{-1}+x^{-1}y = (1+x^{-1})+(x^{-1})(1-y) \in (1+x^{-1})T+(-x^{-1})T. \tag{4.2.5}$$

Como $x \in \mathfrak{m}_A$, temos $1+x \in A^*$ e, pelo item (1) acima, $1+x \in B(T)$. Como $x \in B(T)$ e $B(T)$ é grupo,

$$1+x^{-1} = x^{-1}(1+x) \in B(T). \tag{4.2.6}$$

Afirmação: Se $-y \notin T$, então $T+yT \subset B(T) \cup yT$.
Prova da afirmação: dados $t_1, t_2 \in T$ tais que $t_1+yt_2 \notin B(T)$, vamos mostrar que $t_1+yt_2 \in yT$. Pela escolha de t_1 e t_2, t_1+yt_2 é T-birígido, logo $T+(-t_1-yt_2)T \subset T \cup (-t_1-yt_2)T$. Logo, $-yt_2 = t_1-t_1-yt_2 \in T \cup (-t_1-yt_2)T$. Por hipótese, $-y \notin T$. Assim, $-yt_2 \in (-t_1-yt_2)T$, isto é, $t_1+yt_2 \in yT$, o que conclui o prova da afirmação.

Multiplicando a igualdade (4.2.5) por $-x^{-1}$, obtemos

$$(-x^{-1})(1+x^{-1}y) \in T+(-x^{-1})(1+x^{-1})T.$$

Se $x^{-1}(1+x^{-1}) \notin T$, a afirmação acima garante que

$$T+(-x^{-1})(1+x^{-1})T \subset B(T) \cup (-x^{-1})(1+x^{-1})T \subset B(T),$$

a última inclusão é verdadeira pois, como já vimos acima, $-x^{-1}, 1+x^{-1} \in B(T)$. Logo, $1+x^{-1}y \in B(T)$. Mas já vimos em (4.2.4) que $1+x^{-1}y \notin B(T)$. Portanto, $x^{-1}(1+x^{-1}) \in T$ o que implica $\frac{1+x}{x^2} \in T$ e, finalmente, $1+x \in x^2T \subset T$.

(3) ((a)⇒(c)) Imediato, pois neste caso $\Gamma_A = \{0\}$.

(c)⇒(b) $\Gamma_A = 2\Gamma_A$ implica que $\dot{F} = A^*\dot{F}^2$. Como $A^*\dot{F}^2 \subset A^*T$ e, pelo item (1) acima, $A^*T \subset B(T)$, temos: $\dot{F} \subset B(T) \subset \dot{F}$.

(b)⇒(a) $B(F) = \dot{F}$ implica que $\mathcal{O}_1 = \{0\}$, $\mathcal{O}_2 \smallsetminus \{0\} = B(T) = \dot{F}$ e $A = \mathcal{O}_2 = F$.

(4) Uma vez que $1+\mathfrak{m}_A \subset T$, se car $k_A = 2$, então $-2 \in \mathfrak{m}_A$ e $-1 = 1-2 \in 1+\mathfrak{m}_A \subset T$, o que contradiz o fato de T ser uma pré-ordem. ■

Devemos, agora, mostrar que $\mathcal{O}(B(T), T)$, que foi definido em (4.2.3) (página 58) é, de fato, um anel de valorização. Como veremos a seguir, existe uma propriedade chave nessa demonstração (veja (4.2.7)) que nem sempre é satisfeita por T. Para contornar esse problema, usaremos o Lema 4.17 da página 62.

Lema 4.16 *Se $u, v \in \mathcal{O}_1(T)$ são tais que $1-uv \notin T$, então*

(1) $(1-uv)T = -uT = -vT$.

(2) $B(T) = \pm T$ *e portanto T é um leque*[5].

(3) *Dados $x, y \in \mathcal{O}_1(T)$ tais que $x, y \notin vB(T)$, temos $1-xy \in T$.*

Demonstração. (1) Como $u, v \in \mathcal{O}_1(T)$, temos $u, v \notin B(T)$ e $1+u, 1+v \in T$. Assim:

$$1-uv = \begin{cases} 1+u-u-uv = (1+u)-u(1+v) \in T - uT = T \cup -uT \\ 1+v-v-uv = (1+v)-v(1+u) \in T - vT = T \cup -vT \end{cases}$$

Como $1-uv \notin T$, obtemos $1-uv \in -uT \cap -vT$. Logo, $(1-uv)T = -uT = -vT$.

(2) Por definição, $\pm T \subset B(T)$. Suponhamos, por absurdo, que $B(T) \neq \pm T$. Então existe $x \in F \smallsetminus \pm T$ que não é T-birígido. Logo, existem $s, t \in T$ tais que $s+xt \notin T \cup xT$

[5]Definição de leque na página 22.

ou $s - xt \notin T \cup -xT$. Podemos supor que s e t satisfazem $s + xt \notin T \cup xT$, pois a outra situação é análoga. É claro que $s, t \neq 0$. Temos, então $1 + s^{-1}tx \notin T \cup xT$ e podemos substituir x por $s^{-1}tx$, isto é, podemos admitir que $1 + x \notin T \cup xT$. Agora, $-x = 1 - (1 + x) \in T - (1 + x)T$ e $-x \notin T \cup -(1 + x)T$ ($-x \in -(1 + x)T$ é equivalente a $1 + x \in xT$, o que não ocorre). Assim, $1 + x \in B(T)$

Como $-x, -(1 + x) \in B(T)$ e $v \notin B(T)$, temos $-xv, -v(1 + x) \notin B(T)$ (i.e., são birígidos). Logo, $1 + (-xv) = 1 - xv = 1 + v - v(1 + x) = (1 + v) + (-v(1 + x)) \in (T \cup -xvT) \cap (T \cup -v(1 + x)T)$.

Pela escolha de x, $-xvT \cap -v(1 + x)T = \emptyset$ (do contrário, teríamos $1 + x \in xT$, o que não ocorre). Se $-vx \in T$, então $xv \in -T \subset B(T)$ e $v \in B(T)$, contradição. Logo, $-xv \notin T$ e $-xvT \cap T = \emptyset$. Analogamente, $-v(1 + x) \cap T = \emptyset$. Assim, $1 - xv \in T$ e $-xv \in \mathcal{O}_1(T)$.

Uma vez que $1 + x \notin T \cup xT$, temos: $1 + x^{-1} \notin T \cup x^{-1}T$. Além disso, como $B(T)$ é grupo, $x \in B(T)$ implica $x^{-1} \in B(T)$. Podemos então repetir os argumentos acima com x^{-1} e u no lugar de x e v, respectivamente, para obtermos $-x^{-1}u \in \mathcal{O}_1(T)$. Temos ainda, por hipótese, que $1 - (-xv)(-x^{-1}u) = 1 - uv \notin T$. Aplicando-se o item (1) a $-xv$ e $-xu$ resulta $-xvT = (1 - (-xv)(-x^{-1}u))T = (1 - uv)T = -vT$ e isso implica $x \in T$. Contradição.

(3) Sejam $x, y \in \mathcal{O}_1(T)$ tais que $x, y \notin vB(T)$. Suponhamos, por absurdo, que $1 - xy \notin T$. Como $-uT = -vT$, temos $uB(T) = vB(T)$ e $y \notin B(T) \cup uB(T) = B(T) \cup vB(T)$. Assim, $vy^{-1}, uy \notin B(T)$. Logo, $1 - vy^{-1} \in T \cup -vy^{-1}T$. Temos dois casos:

Caso 1: $1 - vy^{-1} \in T$. Como $1 - (-vy^{-1})(-uy) = 1 - uv \notin T$, aplicando-se o item (1) a $-vy^{-1}$ e $-uy$, temos que $(-vy^{-1})T = (-uy)T = (1 - (-vy^{-1})(-uy))T = (1 - uv)T = -uT$, o que implica $y \in uvT = T \subset B(T)$ e, daí, $y \notin \mathcal{O}_1(T)$. Contradição.

Caso 2: $1 - vy^{-1} \in -vy^{-1}T$. Multiplicando por $-vy^{-1}$, obtemos $1 - vy^{-1} \in T$ (podemos, se necessário, substituir v por vw^2, $w \in \dot{F}$). A seguir, observamos que $1 - (-ex)(-e^{-1}y) = 1 - xy \notin T$. Logo, mais uma vez pelo item (1), $(-ex)T = (1 - (-ex)(-e^{-1}y))T = (1 - xy)T = -xT$ e isso implica que $e \in T \subset B(T)$, ou seja, $e \notin \mathcal{O}_1(T)$. Contradição. ■

Lema 4.17 *Suponha que a pré-ordem T de F <u>não</u> satisfaz a seguinte propriedade:*

$$1 - xy \in T \quad \textit{quaisquer que sejam} \quad x, y \in \mathcal{O}_1, \tag{4.2.7}$$

isto é, existem $d, e \in \mathcal{O}_1(T)$ tais que $1 - de \notin T$. Então existe uma pré-ordem T_1 de F tal que $(T_1 : T) = 2$ e T_1 satisfaz (4.2.7). Além disso, $B(T_1) = \pm T_1$ e $\mathcal{O}_1 = \{x \in \mathcal{O} \mid x \notin \pm eT\}$.

Demonstração. Escolhamos e fixemos $d, e \in \mathcal{O}_1(T)$ tais que $1 - de \notin T$. Esses elementos permanecerão fixos no decorrer da demonstração. Consideremos

$$T_1 = T \cup eT. \tag{4.2.8}$$

T_1 é subgrupo de $\dot{F}$ e $F^2 \subset T \subset T_1$. Como $e \in \mathcal{O}_1$, temos $e \notin B(T)$ e e é T-birígido. Em particular, $T_1 = T \cup eT = T + eT$ e $T_1 + T_1 = (T + T) + e(T + T) \subset T + eT = T_1$. Finalmente, $-1 \in T_1$ implica $-1 \in eT$, pois T é pré-ordem. Mas $-1 \in eT$ implica $e \in -T \subset B(T)$, o que contradiz a escolha de e. Assim, $-1 \notin T_1$ e T_1 é uma pré-ordem de F. Além disso, $e \notin T$ implica que $(T_1 : T) = 2$

(1) $\boxed{B(T_1) = \pm T_1}$. Pelo item (2) do Lema 4.16, como T não satisfaz (4.2.7), todo elemento $x \in F \setminus \pm T$ é T-birígido. Consideremos, agora, $x \in F \setminus \pm T_1$ e $a, b \in T_1$. Temos: $x \notin \pm T$ e $ex \notin \pm T$. Logo, x e ex são T-birígidos. Escrevendo $a = e^m\alpha$ e $b = e^n\beta$, onde $m, n \in \{0, 1\}$ e $\alpha, \beta \in T$, obtemos:

$$a \pm xb \in \begin{cases} T \pm xT = T \cup \pm xT, \text{ se } m = n = 0 \\ e(T \pm xT) = eT \cup \pm exT, \text{ se } m = n = 1 \\ T \pm exT = T \cup \pm exT, \text{ se } m = 0, n = 1 \\ e(T \pm e^{-1}xT) = eT \cup \pm xT, \text{ se } m = 1, n = 0 \end{cases}.$$

Portanto, x é T_1-birígido e isso prova que $B(T_1) = \pm T_1$.

(2) $\boxed{\mathcal{O}_1(T_1) = \{x \in \mathcal{O}_1(T) | x \notin \pm eT\}}$. Inicialmente, temos $\{x \in \mathcal{O}_1(T) | x \notin \pm eT\} \subseteq \mathcal{O}_1(T_1)$. De fato, $x \in \mathcal{O}_1(T)$ implica que $x \notin B(T) = \pm T$. Como $x \notin \pm eT$, temos $x \notin \pm(T \cup eT) = \pm T_1$. Além disso, $x \in \mathcal{O}_1(T)$ implica $1 + x \in T \subset T_1$.

Para mostrar a outra inclusão, tomemos $x \in \mathcal{O}_1(T_1)$. Então $x \notin B(T_1) = \pm(T \cup eT)$ e $1 + x \in T_1 = T \cup eT$. Em particular, $x \notin \pm eT$ e $x \notin \pm T = B(T)$, donde $1 + x \in T \cup xT$. Se $1 + x \notin T$, teríamos $1 + x \in eT$ e $1 + x \in xT$. Logo, $x \in xT = eT \subset B(T_1)$, o que não ocorre. Portanto $1 + x \in T$ e $x \in \mathcal{O}_1(T)$, pois $B(T) \subset B(T_1)$ e $x \notin B(T_1)$.

(3) $\boxed{T_1 \text{ satisfaz (4.2.7)}}$. Pelo item (3) do Lema 4.16 e pelo item (2) acima, dados $x, y \in \mathcal{O}_1(T_1)$ quaisquer, $1 - xy \in T \subset T_1$. Logo T_1 satisfaz (4.2.7). ■

Proposição 4.18 *Se T é uma pré-ordem para a qual vale* (4.2.7)*, então $A = \mathcal{O}(B(T), T)$ é um anel de valorização de F.*

Demonstração. Primeiramente, temos $0 \in \mathcal{O}_1$, pois $0 \in F \setminus B(T)$ e $1 + 0 = 1 \in T$. $1 \in \mathcal{O}_2$, pois $1 \in T \subset B(T)$ e $1 \cdot \mathcal{O}_1 \subset \mathcal{O}_1$.

(1) $\boxed{1 + \mathcal{O}_1 \subset \mathcal{O}_2}$. Tomemos $x, y \in \mathcal{O}_1$. Uma vez que $y \in \mathcal{O}_1$, temos $1 + (-y)(1 + y)^{-1} = (1 + y)^{-1} \in T$ e $-y(1 + y)^{-1} \notin B(T)$ (pois $B(T)$ é grupo, $-y \notin B(T)$ e $(1 + y)^{-1} \in T \subset B(T)$). Logo, $-y(1 + y)^{-1} \in \mathcal{O}_1$. Aplicando 4.2.7 a x e $-y(1 + y)^{-1}$ obtemos: $1 + xy(1 + y)^{-1} \in T$. Assim, $1 + (1 + x)y = (1 + y)(1 + \frac{xy}{1+y}) \in T$ e isso implica que $(1 + x)y \in \mathcal{O}_1$ (veja que $(1 + x)y \notin B(T)$). Como $x, y \in \mathcal{O}_1$ são arbitrários, acabamos de mostrar que $1 + x \in \mathcal{O}_2$, para todo $x \in \mathcal{O}_1$, isto é, $1 + \mathcal{O}_1 \subset \mathcal{O}_2$.

(2) $\boxed{A \cdot A \subset A}$. Por definição, $\mathcal{O}_2 \cdot \mathcal{O}_1 \subset \mathcal{O}_1$ e $\mathcal{O}_2 \cdot \mathcal{O}_2 \subset \mathcal{O}_2$. Resta mostrar que $\mathcal{O}_1 \cdot \mathcal{O}_1 \subset A$. Dados $x, y \in \mathcal{O}_1$, vamos considerar dois casos:

(a) $\underline{xy \notin B(T)}$. Neste caso, mostraremos que $\underline{xy \in \mathcal{O}_1}$. Se $-x \in \mathcal{O}_1$ ou $-y \in \mathcal{O}_1$, então (como, por hipótese, vale (4.2.7)) $1 + xy = 1 - x(-y) \in T$, caso $-y \in \mathcal{O}_1$. Como $xy \notin B(T)$, temos $xy \in \mathcal{O}_1$. Devemos, portanto, mostrar que $-x \in \mathcal{O}_1$ ou $-y \in \mathcal{O}_1$. Suponhamos, por absurdo, que valha o contrário, ou seja, $-x, -y \notin \mathcal{O}_1$. Como x e y são T-birígidos, temos: $1 - x \in -xT$ e $1 - y \in -yT$. Por outro lado, como vale (4.2.7), temos: $1 - xy \in T$. Logo, $1 - xy = (1 - x) + x(1 - y) \in T \cap (-xT \cup -xyT) = \emptyset$. Contradição. (observemos que $x \notin B(T)$ implica $-xT \cap T = \emptyset$ e $xy \notin B(T)$ implica $T \cap -xyT = \emptyset$).

(b) $\underline{xy \in B(T)}$. Neste caso, mostraremos que $\underline{xy \in \mathcal{O}_2}$. Dado $a \in \mathcal{O}_1$, temos $-a(1 + a)^{-1} \in \mathcal{O}_1$. De fato, $a \in \mathcal{O}_1$ implica $1 + a \in T \subset B(T)$ e $-a \notin B(T)$. Assim, $-a(1+a)^{-1} \notin B(T)$. Além disso, $1+(-a(1+a)^{-1}) = (1+a)^{-1} \in T$. Logo, $-a(1+a)^{-1} \in \mathcal{O}_1$.

Por (1), $x \in \mathcal{O}_1$ implica que $1 + x \in \mathcal{O}_2$. Logo, como $y \in \mathcal{O}_1$, pela discussão acima, $-y(1 + y)^{-1} \in \mathcal{O}_1$ e $z := (1 + x)(-y)(1 + y)^{-1} \in (1 + x)\mathcal{O}_1 \subset \mathcal{O}_1$. Novamente por (1), temos $1+z \in \mathcal{O}_2$. Como $\mathcal{O}_2\mathcal{O}_2 \subset \mathcal{O}_2$ e $1+y \in \mathcal{O}_2$ resulta que $1-xy = (1+y)(1+z) \in \mathcal{O}_2$.

Tomemos, agora, $a \in \mathcal{O}_1$ arbitrário. Como vimos acima, $-a(1+a)^{-1} \in \mathcal{O}_1$. Assim $(1-xy)(-a)(1+a)^{-1} \in \mathcal{O}_1$. Portanto $1+(1-xy)(-a)(1+a)^{-1} \in T$ e $1+xya = (1+a)(1+(1-xy)(-a)(1+a)^{-1}) \in T$. Uma vez que $xy \in B(T)$ e $a \notin B(T)$, temos $xya \notin B(T)$, o que mostra que $xya \in \mathcal{O}_1$, para $a \in \mathcal{O}_1$, arbitrário, ou seja, $xy \in \mathcal{O}_2$.

(3) $\boxed{\text{Dado } x \in \dot{F},\ x \in A \text{ ou } x^{-1} \in A}$. Em particular, como $-1 \in \dot{F}$ e $-1 \in -T \subset B(T)$, temos $-1 \in \mathcal{O}_2$ e $-\mathcal{O}_1 \subset \mathcal{O}_1$. Vamos mostrar a afirmação dividindo-a em dois casos: primeiro, suponhamos que $x \notin B(T)$. Se $x \notin \mathcal{O}_1$, então $1+x \notin T$ (pela definição de $\mathcal{O}_1$). Como x é T-rígido, $1+x \in xT$ e daí $1+x^{-1} \in T$, o que implica que $x^{-1} \in \mathcal{O}_1$.

Suponhamos, agora, que $x \in B(T)$. Se $x \notin \mathcal{O}_2$, então existe $y \in \mathcal{O}_1$ tal que $xy \notin \mathcal{O}_1$. Como $y \in \mathcal{O}_1$ e $x \in B(T)$, temos $xy \notin B(T)$. Pelo caso anterior, sabemos que $(xy)^{-1} \in \mathcal{O}_1$. Assim, por (2)(b), $x^{-1} = (xy)^{-1}y \in \mathcal{O}_2$.

(4) $\boxed{1+\mathcal{O}_2 \subset A}$. Mais precisamente, dado $x \in \mathcal{O}_2$, $1+x \in \mathcal{O}_1$, se $1+x \notin B(T)$ e $1+x \in \mathcal{O}_2$, se $1+x \in B(T)$. Vamos aos casos:

(a) $\underline{1+x \notin B(T)}$. Temos: $-(1+x) \notin B(T)$, logo $-(1+x)$ é T-birígido. Assim, $-x = 1-(1+x) \in T \cup -(1+x)T$. Se $-x \in -(1+x)T$ teríamos $1+x \in B(T)$, contrário à nossa hipótese (lembremos que $x \in \mathcal{O}_2 \subset B(T)$). Portanto, $1-(1+x) \in T$ e $-(1+x) \in \mathcal{O}_1$. Como $-1 \in \mathcal{O}_2$ (veja o item (3) acima), $1+x = (-1)(-(1+x)) \in \mathcal{O}_2 \cdot \mathcal{O}_1 \subset \mathcal{O}_1$.

(b) $\underline{1+x \in B(T)}$. Como $-1 \in \mathcal{O}_2$ e $x \in \mathcal{O}_2$, temos $-x = (-1)x \in \mathcal{O}_2 \cdot \mathcal{O}_2 \subset \mathcal{O}_2$ (item (2)). Vimos na demonstração do item (2)(b), que $-y(1+y)^{-1} \in \mathcal{O}_1$, para todo $y \in \mathcal{O}_1$. Assim, $(-x)(-y(1+y)^{-1}) \in \mathcal{O}_2 \cdot \mathcal{O}_1 \subset \mathcal{O}_1$ e, portanto, $1+(1+x)y = (1+y)(1+(-x)\frac{-y}{1+y}) \in T$. Como $y \notin B(T)$ e $1+x \in B(T)$, temos $(1+x)y \notin B(T)$. Logo, $(1+x)y \in \mathcal{O}_1$. Acabamos de mostrar que $(1+x)\mathcal{O}_1 \subset \mathcal{O}_1$. Como estamos supondo $1+x \in B(T)$, concluímos que $1+x \in \mathcal{O}_2$

Conclusão: $\underline{A \text{ é um anel de valorização de } F}$. Pelo item (2), $A \cdot A \subset A$. Por (3), $-1 \in \mathcal{O}_2 \subset A$, logo, $-x \in A$, para todo $x \in A$. Para mostrar que A é subanel de F, resta mostrar que $A+A \subset A$. Tomemos $x, y \in A$. Por (3), $xy^{-1} \in A$ ou $yx^{-1} \in A$. Podemos supor, sem perda de generalidade, que $xy^{-1} \in A$. Por (1) e (4), temos $1+xy^{-1} \in A$. Portanto, $x+y = y(1+xy^{-1}) \in A \cdot A \subset A$ (item (2) novamente).

Finalmente, o item (3) mostra que A é um anel de valorização de F. ■

O Corolários 4.19 e 4.20 a seguir garantem a existência de um anel de valorização com propriedades adequadas aos nossos propósitos. Temos que acrescentar ao Corolário 4.19 uma hipótese adicional sobre a pré-ordem T, a saber, $(\dot{F} : T) \geq 8$. Isso se faz necessário porque, caso T não satisfaça (4.2.7), se $(\dot{F} : T) = 4$ a pré-ordem T_1 que vem do Lema 4.17 poderia ser uma ordem, isto é, $T_1 = T \cup eT$ e $\dot{F} = T_1 \cup -T_1$. Se isso acontecesse, teríamos $\dot{F} = T_1 \cup -T_1 \subset B(T_1) \subset \dot{F}$, ou seja, $B(T_1) = \dot{F}$. Pela Proposição 4.15, item (3), o anel de valorização $\mathcal{O}(B(T_1), T_1)$ seria trivial neste caso.

Corolário 4.19 *Seja T uma pré-ordem de F tal que $(\dot{F} : T) \geq 8$. Suponha que exista um elemento T-birígido $d \in F$. Então existe um anel de valorização próprio A de F tal que $\Gamma_A \neq 2\Gamma_A$, car $k_A \neq 2$ e $1 + \mathfrak{m}_A \subset T$.*

Demonstração. Se T satisfaz (4.2.7), então $A = \mathcal{O}(B(T), T)$ é um anel de valorização de F, pela Proposição 4.18. Como d é T-birígido, $d \in \dot{F} \smallsetminus B(T)$, ou seja, $B(T) \neq \dot{F}$. Assim, pela Proposição 4.15, item (3), A é próprio e $\Gamma_A \neq 2\Gamma_A$, enquanto os itens (2) e (4) da mesma proposição garantem que $1 + \mathfrak{m}_A \subset T$ e car $k_A \neq 2$.

Se T não satisfaz (4.2.7), então, o Lema 4.17 garante a existência de uma pré-ordem $T_1 = T \cup eT$ ($e \notin B(T)$) que satisfaz (4.2.7). Como $(T_1 : T) = 2$ e estamos supondo $(\dot{F} : T) \geq 8$, temos $(\dot{F} : T_1) \geq 4$ e $B(T_1) = \pm T_1$ implica que $B(T_1) \neq \dot{F}$. Como $A^*T_1 \subset B(T_1)$, podemos garantir que A é um anel de valorização próprio de F. Podemos, então, repetir o argumento acima para mostrar que $A = \mathcal{O}(B(T_1), T_1)$ satisfaz as conclusões do corolário. A única conclusão que necessita verificação é a compatibilidade: sabemos, de início, que $1 + \mathfrak{m}_A \subset T_1 = T \cup eT$. Supondo $(1 + \mathfrak{m}_A) \cap eT \neq \emptyset$, temos $e \in (1 + \mathfrak{m}_A)T \subset A^*T \subset B(T)$, sendo essa última inclusão justificada pelo item (1) da Proposição 4.15. Mas $e \in B(T)$ contradiz a escolha de e. Logo, $(1 + \mathfrak{m}_A) \cap eT = \emptyset$ e, de fato, $1 + \mathfrak{m}_A \subset T$. ■

No Corolário 4.20 abaixo, obtemos o anel de valorização que necessitamos no caso particular de nosso interesse, quando a pré-ordem considerada é T_d, definida na página 26. Ao contrário do caso mais geral que consideramos acima, aqui não precisamos supor que o índice de T_d em $\dot{F}$ tenha uma cota inferior. Isso se dá porque podemos tratar o caso $(\dot{F} : T_d) = 4$ separadamente. Observemos ainda que T_d não pode ser uma ordem em F, pois $\pm d \notin T_d$. Podemos então garantir que $(\dot{F} : T_d) \geq 4$.

Corolário 4.20 *Seja F um corpo formalmente real e não pitagórico. Se d é um elemento rígido de F tal que $d \notin \sum \dot{F}^2$ e $T_d = R_d \cdot \sum \dot{F}^2$, então existe um anel de valorização A tal que $\Gamma_A \neq 2\Gamma_A$, car $k_A \neq 2$ e $1 + \mathfrak{m}_A \subset T_d$.*

Demonstração. Pela Proposição 3.17, T_d é uma pré-ordem e pelo Corolário 3.18 o elemento d é T_d-birígido. Assim, no caso em que $(\dot{F} : T_d) \geq 8$ podemos aplicar o Corolário 4.19 acima para obtermos um anel de valorização A compatível com a pré-ordem T_d, isto é, tal que $1 + \mathfrak{m}_A \subset T_d$. As outras afirmações seguem-se diretamente do Corolário 4.19.

Suponhamos agora que $(\dot{F} : T_d) = 4$. Então T_d é a interseção de duas ordens. Considerando a extensão $K = F(\sqrt{s})$, onde $s \in \sum \dot{F}^2$, pela Proposição 3.32, item (b), a pré-ordem $T_d^K = R_d^K \cdot \sum \dot{K}^2$ estende $T_d^F = T_d$, isto é, $T_d^F = T_d^K \cap F$. Uma vez que s é uma soma de quadrados, toda ordem de F tem duas extensões ao corpo K (cf. Lema B.9 e comentário posterior). Assim, T_d^K é a interseção de *quatro* ordens de K e, conseqüentemente, $(\dot{K} : T_d^K) \geq 8$. Pelo Corolário 3.18, d é T_d^K-birígido. Podemos então aplicar o Corolário 4.19 para garantirmos a existência de um anel de valorização $B \subsetneq K$ tal que $1 + \mathfrak{m}_B \subset T_d^K$, car $k_B \neq 2$ e $\Gamma_B \neq 2\Gamma_B$. Tomando $A = B \cap F$ vemos que $1 + \mathfrak{m}_A = (1 + \mathfrak{m}_B) \cap F \subset T_d^K \cap F = T_d^F$, car $k_A = \text{car } k_B \neq 2$ e $\Gamma_A \neq 2\Gamma_A$. ■

Finalizamos este capítulo mostrando como é possível obter um anel de valorização A associado a d como no Corolário 4.20 que também seja π-henseliano (logo, S_d-henseliano, como veremos no Corolário 4.24). Esse anel de valorização terá importância crucial no estudo da decomposição de anéis de Witt que faremos no capítulo seguinte.

Fixado $s \in \sum \dot{F}^2$, seja $K = F(\sqrt{s})$. Consideremos as pré-ordens T_d^F e T_d^K como definidas na página 43. Devemos lembrar que estamos supondo $d \notin \sum \dot{F}^2$. Pela Proposição 3.17, sabemos que T_d^F é uma pré-ordem. Como $d \notin \sum \dot{F}^2$, o Lema 3.6 garante que ds também é rígido. Logo, a Proposição 3.24 mostra que d é rígido em K.

Para que T_d^K também seja uma pré-ordem, precisamos verificar que $d \notin \sum \dot{K}^2$. Suponhamos, por absurdo, que $d \in \sum \dot{K}^2$. Então $d = \sum_{i=1}^n (a_i + b_i\sqrt{s})^2$, onde a_i e b_i são elementos de F, para $i = 1, \ldots, n$. Como $d \in F$ teríamos $d = \sum_{i=1}^n a_i^2 + s\sum_{i=1}^n b_i^2 \in \sum \dot{F}^2$, contrariando nossa hipótese geral sobre d. Logo, $d \notin \sum \dot{K}^2$.

Uma vez que $K|F$ é uma extensão finita e F não é pitagórico, a Proposição 2.3 garante que K também não é pitagórico. Logo, pela Observação (3.2.1) da página 28, temos $\sum \dot{K}^2 \not\subset \dot{K}^2 \cup d\dot{K}^2$. Pelo Corolário 3.18, vemos que d é T_d^K-birígido. Podemos então usar o Corolário 4.20 para garantir a existência de um anel de valorização B de K

tal que $\Gamma_B \neq 2\Gamma_B$, car $k_B \neq 2$ e $1+\mathfrak{m}_B \subset T_d^K$, isto é, B é compatível com a pré-ordem $T_d^K = R_d^K \cdot \sum \dot{K}^2$. Seja $A = B \cap F$ anel de valorização de F. Então, pela Proposição 3.32, $1+\mathfrak{m}_A = (1+\mathfrak{m}_B) \cap F \subset T_d^K \cap F = T_d^F$. Além disso, temos:

Proposição 4.21 *Se $K = F(\sqrt{s})$ e A é um anel de valorização de F, temos: $s \in (1+\mathfrak{m}_A)\dot{F}^2$ se e somente se A tem exatamente duas extensões para K.*

Demonstração. A extensão $K|F$ é normal e o polinômio $f(X) = X^2 - s \in F[X]$ fatora-se como $f(X) = (X-\sqrt{s})(X+\sqrt{s})$ em $K[X]$. Além disso, $\bar{f}(X) = X^2 - \bar{1} \in k_A[X]$, pois $s \in 1+\mathfrak{m}_A$. Logo, se a extensão de A para K fosse única, o Teorema 4.7 nos garantiria a existência de um $\alpha \in F$ tal que $f(\alpha) = 0$, isto é, $s = \alpha^2 \in F^2$. Mas isso implicaria que $\sqrt{s} \in F$ e, portanto, $K = F$. Como estamos supondo $F \subsetneq K$, o anel de valorização A tem mais de uma extensão para o corpo K. Logo, A tem *exatamente* duas extensões para o corpo K.

Reciprocamente, suponhamos que A tem duas extensões B_1 e B_2 para K. De acordo com (4.1.2), temos

$$2 \geq e_1 f_1 + e_2 f_2,$$

onde $e_i = (\Gamma_{B_i} : \Gamma_A)$ e $f_i = [k_{B_i} : k_A]$, $i = 1, 2$. Como $e_i \geq 1$ e $f_i \geq 1$, temos também $e_1 f_1 + e_2 f_2 \geq 2$. Logo, ocorre a igualdade

$$2 = e_1 f_1 + e_2 f_2. \tag{4.2.9}$$

A partir da equação (4.2.9) obtemos $e_1 = e_2 = f_1 = f_2 = 1$. Seja $B = B_1$. Uma vez que $\Gamma_B = \Gamma_A$, existe $x \in F$ tal que $v_B(x) = v_B(\sqrt{s})$, logo $x^{-1}\sqrt{s} \in B^*$. Como $k_B = k_A$, existe $u \in A^*$ tal que $\pi_B(u) = \pi_B(x^{-1}\sqrt{s})$, logo $u^{-1}x^{-1}\sqrt{s} \in 1+\mathfrak{m}_B$ e $u^{-2}x^{-2}s \in (1+\mathfrak{m}_B) \cap F = 1+\mathfrak{m}_A$. Como $F(\sqrt{u^{-2}x^{-2}s}) = F(\sqrt{s})$, podemos considerar $s \in 1+\mathfrak{m}_A$. ■

Por outro lado, temos o seguinte resultado:

Proposição 4.22 *Sejam $K = F(\sqrt{s})$, onde $s \in \sum \dot{F}^2$, B um anel de valorização de K compatível com T_d^K e $A = B \cap F$. O anel de valorização B é a única extensão de A para K.*

Demonstração. O grupo de Galois $G = G(K|F) = \{1, \sigma\}$ é gerado pelo automorfismo $\sigma : K \to K$ tal que $\sigma(\sqrt{s}) = -\sqrt{s}$. Como σ é um automorfismo, $\sigma(\sum \dot{K}^2) = \sum \dot{K}^2$. Portanto, decorre da definição de R_d^K que $\sigma(R_d^K) = R_d^K$ ($\sigma(d) = d$, pois $d \in F$). Se

B' é uma extensão de A para K, então $B' = \sigma(B)$ (cf. [11], 14.1, página 105). Assim, $1 + \mathfrak{m}_{B'} = \sigma(1 + \mathfrak{m}_B) \subset \sigma(T_d^K) = \sigma(R_d^K \cdot \sum K^2) = R_d^K \cdot \sum K^2 = T_d^K$, ou seja, B' também é compatível com T_d^K. Sendo ambos compatíveis com uma mesma pré-ordem, o Corolário 4.4 garante que B e B' são comparáveis. Como ambos estendem um mesmo anel de valorização, eles são iguais ([27], Lema A.2.7, p.211). Portanto A tem extensão única ao corpo K. ■

A partir deste ponto, faremos s variar em $\sum \dot{F}^2$. Devemos, então, estabelecer uma notação mais adequada. Para cada $s \in \sum \dot{F}^2 \smallsetminus \dot{F}^2$, denotemos agora $K_s = F(\sqrt{s})$. Vamos denotar por B_s o anel de valorização de K_s cuja existência é garantida pelo Corolário 4.20 e que pela Proposição 4.22 determina um anel de valorização $A_s = B_s \cap F$ de F do qual B_s é o único prolongamento a K_s. Pela Proposição 4.21, $s \notin 1 + \mathfrak{m}_{A_s}$. O Corolário 4.20 garante ainda que $1 + \mathfrak{m}_{B_s} \subset T_d^{K_s}$, $\Gamma_{B_s} \neq 2\Gamma_{B_s}$ e car $k_{B_s} \neq 2$.

Dessa forma, produzimos uma família $\mathcal{A} = \{A_s | s \in \sum \dot{F}^2 \smallsetminus \dot{F}^2\}$ de anéis de valorização tais que $1 + \mathfrak{m}_{A_s} \subset T_d^F$ e $s \notin 1 + \mathfrak{m}_{A_s}$, para todo $s \in \sum \dot{F}^2$. Pelo Corolário 4.4, o conjunto $\mathcal{A}$ é totalmente ordenado pela inclusão.

Proposição 4.23 *A reunião $A = \bigcup_{s \in \sum \dot{F}^2} A_s$ é um anel de valorização próprio de F tal que $(1 + \mathfrak{m}_A) \cap \sum \dot{F}^2 \subset \dot{F}^2$, $d \notin A^* \dot{F}^2$ e $R_d^F = (1 + \mathfrak{m}_A)\dot{F}^2$.*

Demonstração. Se $A = \bigcup_{s \in \sum \dot{F}^2} A_s = F$, então $\bigcup_{s \in \sum \dot{F}^2} A_s^* = F^\times \ni d$. Isso implicaria que $d \in A_s^*$ para algum $s \in \sum \dot{F}^2$. Logo,

$$d \in A_s^* \dot{F}^2 \subset B_s^* \dot{K}_s^2.$$

Porém, pelo item (1) da Proposição 4.15 sabemos que

$$B_s^* \dot{K}_s \subset B(T_d^{K_s}) = \text{ conjunto dos elementos } T_d^{K_s}\text{-básicos},$$

isto é, elementos que não são $T_d^{K_s}$-birígidos. Isso contradiz o fato de d ser $T_d^{K_s}$-birígido. Portanto, $d \notin A^* \dot{F}^2$ e $A \subsetneq F$.

Para cada $s \in \sum \dot{F}^2$, temos $1 + \mathfrak{m}_{A_s} = (1 + \mathfrak{m}_{B_s}) \cap F \subset T_d^{K_s} \cap F = T_d$, logo $1 + \mathfrak{m}_A \subset T_d$.

Para todo $s \in \sum \dot{F}^2 \smallsetminus \dot{F}^2$ temos, pelas Proposições 4.21 e 4.22, $s \notin 1 + \mathfrak{m}_{A_s}$. Como

$$1 + \mathfrak{m}_A = \bigcap_{s \in \sum \dot{F}^2} (1 + \mathfrak{m}_{A_s}),$$

concluimos que

$$(1+\mathfrak{m}_A)\cap\sum\dot{F}^2\subset\dot{F}^2.$$

A seguir vamos concluir, a partir de $d\notin A^*\dot{F}^2$, que d é $(1+\mathfrak{m}_A)\dot{F}^2$-birígido. De fato, seja $x=\alpha^2\pm d\beta^2$, com $\alpha,\beta\in F$. Como $d\notin A^*\dot{F}^2$ temos $v_A(\alpha^2)\neq v_A(d\beta^2)$. Pelo Lema 4.1,

$$v_A(x)=v_A(\alpha^2\pm d\beta^2)=\begin{cases} v_A(\alpha^2) & \text{, se } v_A(\alpha^2)<v_A(d\beta^2) \quad \text{(caso 1)} \\ v_A(t\beta^2) & \text{, se } v_A(\alpha^2)>v_A(d\beta^2) \quad \text{(caso 2)} \end{cases}.$$

Caso 1: $x=\alpha^2\pm d\beta^2=\alpha^2(1\pm\frac{d\beta^2}{\alpha^2})\in(1+\mathfrak{m}_A)\dot{F}^2$.
Caso 2: $x=\alpha^2\pm d\beta^2=\pm d\beta^2(1\pm\frac{\alpha^2}{d\beta^2})\in\pm d(1+\mathfrak{m}_A)\dot{F}^2$.

Assim, $x\in(1+\mathfrak{m}_A)\dot{F}^2\cup\pm d(1+\mathfrak{m}_A)\dot{F}^2$, ou seja, d é $(1+\mathfrak{m}_A)\dot{F}^2$-birígido. Em particular, $D_F\langle 1,-d\rangle\subset(1+\mathfrak{m}_A)\dot{F}^2+(-d)(1+\mathfrak{m}_A)\dot{F}^2=(1+\mathfrak{m}_A)\dot{F}^2\cup(-d)(1+\mathfrak{m}_A)\dot{F}^2$. Assim,

$$R_d^F\subset(1+\mathfrak{m}_A)\dot{F}^2\cup(-d)(1+\mathfrak{m}_A)\dot{F}^2.$$

Por outro lado, se existissem $x\in R_d^F$ e $y\in(1+\mathfrak{m}_A)\dot{F}^2$ tais que $x=-dy$, teríamos $-d=xy^{-1}\in T_d^F$, pois tanto R_d^F como $1+\mathfrak{m}_A$ estão contidos em T_d^F. Mas isso contradiz o fato de d ser T_d^F-birígido. Logo, $R_d\subset(1+\mathfrak{m}_A)\dot{F}^2$.

Para mostrarmos a outra inclusão, notemos que $(1+\mathfrak{m}_A)\dot{F}^2\subset T_d^F$. Pela definição de T_d^F temos que, para cada $x\in(1+\mathfrak{m}_A)\dot{F}^2$, existem $y\in R_d^F$ e $s\in\sum\dot{F}^2$ tais que $x=ys$. Logo $s=xy^{-1}\in(1+\mathfrak{m}_A)\dot{F}^2$, pois $R_d^F\subset(1+\mathfrak{m}_A)\dot{F}^2$. Conseqüentemente, $s\in(1+\mathfrak{m}_A)\dot{F}^2\cap\sum\dot{F}^2=\dot{F}^2$, pela construção de A, donde concluímos que $x\in R_d^F$, como queríamos. ■

Corolário 4.24 *O anel de valorização A, definido na Proposição 4.23 é S_d-henseliano.*

Demonstração. Pela Proposição 4.23, temos $R_d=(1+\mathfrak{m}_A)\dot{F}^2$. Pelo Corolário 4.13, A é S_d-henseliano. ■

No que se segue o anel de valorização A de F π-henseliano e compatível com T_d, definido no enunciado da Proposição 4.23, será denominado *anel de valorização associado* a d e será denotado por A_d .

Capítulo 5

Teorema de estrutura para o anel de Witt $W(F)$

O presente capítulo apresenta os resultados principais do trabalho. O objetivo é obter uma decomposição do anel de Witt $W(F)$ como "produto" de anéis de Witt $W(H)$ e $W(K)$, onde H e K são extensões do corpo F. Esse "produto" de anéis de Witt é definido na primeira seção, onde apresentamos também critérios para garantir a decomposição do anel de Witt de um corpo F como produto de anéis de Witt de duas extensões de F. O Teorema 5.1 fornece um critério para a decomposição de $W(F)$ envolvendo classes de quadrados e o grupo de valores de formas binárias.

Na seção 5.2, Proposição 5.4, mostraremos que a decomposição $R_d \cdot S_d = \dot{F}$ é equivalente à condição:

$$v_A(S_d) = \Gamma_A \quad \text{e} \quad \overline{S}_d^{\times} = \dot{k}_A \tag{5.0.1}$$

A Proposição 5.4 mostra ainda que a decomposição do anel de Witt tem conseqüências sobre o espaço de ordens de F.

Na seção 5.4 obtemos a decomposição do anel de Witt $W(F)$ supondo que vale a condição (5.0.1) onde d é um elemento rígido em F que não é soma de quadrados.

5.1 Produtos de Anéis de Witt

Nesta seção estudaremos critérios para determinar quando o anel de Witt $W(F)$ de um corpo F decompõe-se como produto cartesiano, na categoria dos anéis de Witt, de dois anéis de Witt $W(H)$ e $W(K)$, onde H e K são extensões de F. Convém esclarecer que o produto cartesiano na categoria dos anéis de Witt não coincide com o produto

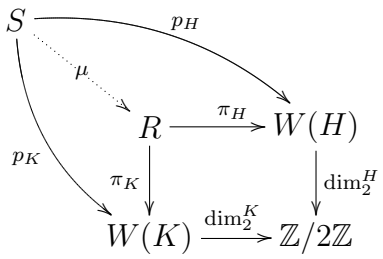
cartesiano na categoria dos anéis. Explicaremos a seguir essa diferença.

Sejam H e K corpos e $W(H)$, $W(K)$ seus anéis de Witt. O produto cartesiano $W(H) \times W(K)$ na categoria dos anéis não é anel de Witt de um corpo. Isso pode ser constatado se observarmos que $(\langle 1\rangle, 0) \in W(H) \times W(K)$ é um idempotente não trivial, isto é, $(\langle 1\rangle, 0)^2 = (\langle 1\rangle, 0)$. Os idempotentes triviais são $1 = (\langle 1\rangle, \langle 1\rangle)$ e $0 = (0, 0)$. Por outro lado, em um anel de Witt de um corpo, os únicos idempotentes são os triviais. Um anel desse tipo é dito *conexo* (veja [23], Teorema 8.6, p.283).

Para remediar essa anomalia, devemos substituir o produto cartesiano usual por um outro produto, de tal modo que $W(H) \times W(F)$ possa ser anel de Witt de algum corpo. Relembremos a definição, para um corpo F, do homomorfismo de anéis $\dim_2 : W(F) \to \mathbb{Z}/2\mathbb{Z}$, dado por $\dim_2(q) := \dim(q) + 2\mathbb{Z}$, para todo $q \in W(F)$, ou seja, a dimensão (da classe de equivalência) de uma forma q tomada módulo 2 (veja a página 131). Se $q = q' \in W(F)$ então $q' \simeq q \perp n\langle 1, -1\rangle$, logo $\dim(q') \equiv \dim(q) \pmod 2$. Isso mostra que $\dim_2$ é bem definido.

Baseados numa propriedade universal do homomorfismo $\dim_2$ acima, definiremos a seguir o produto de $W(H)$ e $W(K)$ na categoria dos anéis de Witt, que denotaremos a princípio por $W(H) \times_2 W(K)$.

O produto $R = W(H) \times_2 W(K)$ é um subanel de $W(H) \times W(K)$ munido de dois homomorfismos de anéis $\pi_H : R \to W(H)$ e $\pi_K : R \to W(K)$ tais que $\dim_2^K \circ \pi_K = \dim_2^H \circ \pi_H$ e tal que, dado um anel S com homomorfismos p_H e p_K, formando um outro diagrama comutativo com os homomorfismos $\dim_2^H : W(H) \to \mathbb{Z}/2\mathbb{Z}$ e $\dim_2^K : W(K) \to \mathbb{Z}/2\mathbb{Z}$, existe um único homomorfismo $\mu : S \to R$ tal que $p_H = \pi_H \circ \mu$ e $p_K = \pi_K \circ \mu$. Por um procedimento padrão inerente à propriedade universal, R é único a menos de isomomorfismo. O diagrama a seguir ilustra o que foi dito acima.



A propriedade universal acima caracteriza $R = W(H) \times_2 W(K)$ como *produto fibrado* de $W(H)$ e $W(K)$ sobre $\mathbb{Z}/2\mathbb{Z}$. Ele é realizado como o subanel do produto usual, na categoria de anéis, formado pelos pares de (classes de) formas quadráticas (q_H, q_K) cujas

dimensões têm a mesma paridade, isto é, $\dim_2(q_H) = \dim_2(q_K)$.

Observemos que o produto fibrado é caracterizado pelo diagrama do tipo "push out" na categoria dos anéis, como descrito acima. Esse tipo de construção é bastante comum. Embora o produto fibrado de grupos seja uma ferramenta útil em geral, convém mencionar que o produto fibrado de anéis de Witt de dois corpos está intimamente relacionado com o produto livre dos grupos de Galois dos fechos quadráticos desses corpos, e não com o produto fibrado desses grupos, como a primeira vista poderíamos supor.

Podemos também verificar que o produto fibrado é conexo, i.e., tem somente idempotentes triviais. Mais ainda, Mieczysław Kula demonstrou em [20], Teorema 3.3, que para cada par de corpos H e K, com um número finito de classes de quadrados, existe um corpo F tal que $W(F) \simeq W(H) \times_2 W(K)$.

No que segue, consideraremos apenas produtos fibrados de anéis de Witt. Assim, não havendo risco de confusão, *usaremos a notação $\times$ (ao invés de $\times_2$) para o produto fibrado.*

Teorema 5.1 *Seja F um corpo com característica $\neq 2$ e H e K duas extensões de F contidas em $F(2)$. Vamos assumir que:*

(1) *As inclusões $F \subset H$ e $F \subset K$ induzem isomorfimo de grupos*

$$\dot{F}/\dot{F}^2 \to \dot{H}/\dot{H}^2 \times \dot{K}/\dot{K}^2;$$

(2) $(D_H\langle 1, x\rangle \cap F) \cap (D_K\langle 1, x\rangle \cap F) \subset D_F\langle 1, x\rangle$, *para todo $x \in \dot{F}$.*

Então as inclusões $F \subset H$ e $F \subset K$ induzem isomorfimo de anéis

$$W(F) \to W(H) \times W(K).$$

Demonstração. Vamos inicialmente considerar a aplicação $\mu : W(F) \to W(H) \times W(K)$ que satisfaz a seguinte condição: dado um elemento $\alpha \in W(F)$ representado pela forma quadrática $\varphi_F = \langle a_1, \ldots, a_n\rangle$ sejam φ_H e φ_K as formas quadráticas sobre H e K, respectivamente, associadas à função quadrática $a_1X_1^2 + \cdots + a_nX_n^2$. Então $\mu(\alpha) = (\alpha_H, \alpha_K)$ onde α_H é a classe de φ_H em $W(H)$ e α_K é a classe de φ_K em $W(K)$ (sempre que não houver risco de confusão vamos omitir os índices H e K nas formas quadráticas).

A funcão μ é um homomorfismo de anéis que pode ser apresentada de forma mais conceitual: como H e K são extensões de F temos naturalmente homomorfismos de anéis $p_H : W(F) \to W(H)$ e $p_K : W(F) \to W(K)$ induzidos pelas inclusões. Os homomorfismos p_H e p_K satisfazem a condição de tornar o quadrado externo do diagrama da página 71 comutativo: $\dim_2 \circ p_H = \dim_2 \circ p_K$. Existe então um único homomorfismo de anéis $\mu : W(F) \to W(H) \times W(K)$ que completa o diagrama: $\pi_H \circ \mu = p_H$ e $\pi_K \circ \mu = p_K$.

Esse homomorfismo μ é nosso candidato ao isomorfismo que torna o teorema verdadeiro. Vejamos inicialmente que μ é sobrejetivo. Dado $(\beta, \gamma) \in W(H) \times W(K)$ sejam $\langle b_1, \ldots, b_m \rangle$ e $\langle c_1, \ldots, c_m \rangle$, formas quadráticas sobre H e K que representam, respectivamente, β e γ. Não devemos nos esquecer que os pares do produto cartesiano $W(H) \times W(K)$ são, por construção, representados por formas quadráticas cujas dimensões têm a mesma paridade. Por essa razão, podemos representar β e γ por duas formas quadráticas de mesma dimensão, acrescentando para isso tantas cópias de $\langle 1, -1 \rangle$ quantas forem necessárias. Devido ao isomorfismo da hipótese de número (1) do teorema, exitem $a_1 \ldots, a_m \in \dot{F}$ tais que $a_i \dot{H}^2 = b_i \dot{H}^2$ e $a_i \dot{K}^2 = c_i \dot{K}^2$, para todo $i = 1, \ldots, m$. Tomando-se então $\alpha \in W(F)$ correspondendo à classe de $\langle a_1, \ldots, a_m \rangle$ vamos obter $\mu(\alpha) = (\beta, \gamma)$, ficando demonstrado que μ é sobrejetiva.

A injetividade de μ corresponde ao item (3) do Lema 5.2 a seguir. ■

Lema 5.2 *Para F, H e K satisfazendo as hipóteses do Teorema 5.1 acima e para uma forma quadrática φ_F definida sobre F, as seguintes conclusões são verdadeiras:*

(1) *Para todo $b \in F$ temos que $b \in D(\varphi_F)$ se e somente se $b \in D(\varphi_H)$ e $b \in D(\varphi_K)$.*

(2) *φ_F é isotrópica se e somente se φ_H e φ_K são isotrópicas.*

(3) *φ_F é hiperbólica se e somente se φ_H e φ_K são hiperbólicas.*

Demonstração. Observemos primeiro que só temos que demonstrar uma das direções em cada um dos três itens, isto é, a necessidade das condições pois a suficiência é clara.

Demonstraremos o primeiro item por indução sobre a dimensão n de φ. A hipótese (1) do Teorema 5.1 garante que o resultado vale para $n = 1$. Infelizmente esse não é o primeiro passo do processo indutivo. Isto é, não podemos deduzir o caso $n = 2$ do caso $n = 1$, mas fica registrado que o resultado vale também para $n = 1$.

Para $n = 2$ basta aplicarmos a hipótese (2) do Teorema 5.1. De fato $c \in D(\langle a, b\rangle_F)$ se $a^{-1}c \in D(\langle 1, a^{-1}b\rangle_F)$, o que pela hipótese (2) ocorre se $a^{-1}c \in D(\langle 1, a^{-1}b\rangle_H)$ e $a^{-1}c \in D(\langle 1, a^{-1}b\rangle_K)$. Multiplicando-se tudo por a vamos obter $a^{-1}c \in D(\langle 1, a^{-1}b\rangle_H)$ e $a^{-1}c \in D(\langle 1, a^{-1}b\rangle_K)$ se e somente se $c \in D(\langle a, b\rangle_H)$ e $c \in D(\langle a, b\rangle_K)$.

Seja agora $\varphi_F = \langle a_1, \dots a_n, a_{n+1}\rangle_F$ e $b \in F$ satisfazendo $b \in D(\varphi_H)$ e $b \in D(\varphi_K)$. Para ser mais preciso sejam $c_1, \dots, c_{n+1} \in H$ e $d_1, \dots, d_{n+1} \in K$ tais que $b = a_1c_1^2 + \cdots a_{n+1}c_{n+1}^2$ e $b = a_1d_1^2 + \cdots a_{n+1}d_{n+1}^2$. Definimos $c_H := a_1c_1^2 + \cdots a_{n+1}c_n^2 \in H$ e $d_K := a_1d_1^2 + \cdots a_{n+1}d_n^2 \in K$. Logo $b = c_H + a_{n+1}c_{n+1}^2$ e $b = d_K + a_{n+1}d_{n+1}^2$.

Pela hipótese (1) exite $a \in F$ tal que $a\dot{H}^2 = c_H\dot{H}^2$ e $a\dot{K}^2 = d_K\dot{K}^2$. Vemos então que $a \in D(\langle a_1, \dots a_n\rangle_H)$ e $a \in D(\langle a_1, \dots a_n\rangle_K)$, resultando pela hipótese de indução que $a \in D(\langle a_1, \dots a_n\rangle_F)$ (†).

Por outro lado, como $b \in D(\langle a, a_{n+1}\rangle_H)$ e $b \in D(\langle a, a_{n+1}\rangle_K)$ temos, pelo caso $n = 2$, que $b \in D(\langle a, a_{n+1}\rangle_F)$ (‡). Juntando-se agora (†) e (‡) concluímos que $b \in D(\langle a_1, \dots a_{n+1}\rangle_F)$, como queríamos. Dessa forma, o item (1) fica demonstrado.

Vejamos agora o item (2). Seja φ_F tal que φ_H e φ_K são isotrópicas (observar que $\dim\varphi \geq 2$). Como φ_H e φ_K são isotrópicas podemos, pelo Teorema C.6, decompô-las sobre H e K nas formas

$$\varphi_H \sim \langle 1, -1\rangle \perp \varphi_H^{'} \qquad \varphi_K \sim \langle 1, -1\rangle \perp \varphi_K^{'} \tag{5.1.1}$$

para convenientes formas quadráticas $\varphi_H^{'}$ e $\varphi_K^{'}$. Uma primeira consequência dessas decomposições é que $1 \in D(\varphi_H)$ e $1 \in D(\varphi_K)$. Pelo item anterior $1 \in D(\varphi_F)$ e podemos decompor $\varphi_F \sim \langle 1\rangle + \Psi_F$ $(*)$ com $1 \leq \dim\Psi_F < \dim\varphi_F$. Aplicando-se o homomorfismo μ nessa última equação obtemos

$$\varphi_H \sim \langle 1\rangle \perp \Psi_H \qquad \varphi_K \sim \langle 1\rangle \perp \Psi_K. \tag{5.1.2}$$

Combinando-se as equações em 5.1.1 e 5.1.2 e aplicando-se o Teorema C.5 vamos obter

$$\Psi_H \sim \langle -1\rangle \perp \varphi_H^{'} \qquad \Psi_K \sim \langle -1\rangle \perp \varphi_K^{'}. \tag{5.1.3}$$

Temos agora que $-1 \in D(\Psi_H)$ e $-1 \in D(\Psi_K)$. Novamente, pelo item anterior vamos concluir que $-1 \in D(\Psi_F)$. Teremos então uma nova decomposição $\Psi_F \sim \langle -1\rangle + \Theta_F$, para uma conveniente forma quadrática Θ_F. Substituindo-se, finalmente, Ψ_F na expressão $(*)$ obtemos $\varphi_F \sim \langle 1, -1\rangle + \Theta_F$. Concluímos assim que φ_F é isotrópica, como desejado.

Chegamos finalmente ao item (3). Neste caso argumentamos por indução sobre a dimensão de φ_F usando o procedimento da demonstração que acabamos de fazer do

item (2). Da conclusão que obtivemos $\varphi_F \sim \langle 1,-1\rangle + \Theta_F$ vemos que φ_H e φ_K são hiperbólicas se e somente se Θ_H e Θ_K são hiperbólicas. Como $\dim\Theta_F = \dim\varphi_F - 2$ resulta da hipótese de indução que Θ_F é hiperbólica. Consequentemente, também φ_F é hiperbólica. ■

5.2 Decomposição em Radicais Associada à Decomposição de $W(F)$

Estabeleceremos nesta seção a equivalência entre a decomposição do anel de Witt $W(F)$ em produto de anéis de Witt de extensões de F e a decomposição do grupo $\dot{F}/\dot{F}^2$ como produto de subgrupos $R_d/\dot{F}^2$ e $S_d/\dot{F}^2$, onde

$$R_d = D_F\langle 1,-d\rangle \cap \left(\bigcap_{t\in\sum \dot{F}^2} D_F\langle 1,-t\rangle \right)$$

e $S_d = \bigcap_{x\in R_d} D_F\langle 1,-x\rangle$. Veremos que estas decomposições guardam uma relação estreita com o comportamento de S_d em relação ao anel de valorização A associado a d, definido na página 69 e que também implicam uma decomposição do espaço de ordens de F como reunião disjunta de dois subespaços. (cf. a Proposição 5.4).

Para conveniência do leitor, recordemos que $D_F\langle 1,-x\rangle$ é pré-ordem para todo $x \in R_d \smallsetminus \dot{F}^2$ (item (1) do Corolário 3.14). Lembremos ainda que, de acordo com o Corolário 3.14, item (2), $R_d \cap S_d = \dot{F}^2$ e $S_d = \bigcap_{x\in R_d} D_F\langle 1,-x\rangle$ também é uma pré-ordem de F e que, pela Proposição 4.23, $R_d = (1+\mathfrak{m}_A)\dot{F}^2$. Note que escrevemos R_d ao invés de R_d^F pois, como trabalharemos apenas no corpo F, não haverá perigo de confusão.

Vamos estabelecer mais algumas notações. Se $\pi_A : A \to k_A = A/\mathfrak{m}_A$ é a projeção canônica, denotamos $\overline{S}_d = \pi_A(S_d \cap A)$ e $\overline{S}_d^{\times} = \overline{S}_d \smallsetminus \{0\} = \pi_A(S_d \cap A^*)$.

Lema 5.3 *Seja F um corpo, d um elemento rígido de F tal que $\sum \dot{F}^2 \not\subset D_F\langle 1,d\rangle$ e A um anel de valorização tal que $R_d = (1+\mathfrak{m}_A)\dot{F}^2$. Então as seguintes afirmações são equivalentes:*

(i) $\overline{S}_d^{\times} = \dot{k}_A$.

(ii) $-1 \in \overline{S}_d^{\times}$.

(iii) $S_d = D_F\langle 1,-x\rangle$, *para algum* $x \in R_d \cap -S_d$.

Mais ainda, para todo $y \in R_d \cap -S_d$, temos que $S_d = D_F\langle 1, -y\rangle$.

Demonstração. A implicação (i) $\Rightarrow$ (ii) é imediata. Suponhamos que vale (ii), i.e., $-1 \in \dot{k}_A = \overline{S}_d^{\times}$. Então existe $s \in S_d$ tal que $\pi_A(s) = -1$, ou seja, $\pi_A(-s) = 1$. Logo, $-s \in 1 + \mathfrak{m}_A \subset R_d$ e $S_d \subset D_F\langle 1, -(-s)\rangle$. Como S_d é fechado para soma e contém $\dot{F}^2$, temos: $D_F\langle 1, s\rangle \subseteq S_d \subseteq D_F\langle 1, s\rangle$. Basta, então, tomarmos $x = -s$ em (iii). Observemos que o argumento acima pode ser repetido para um $y \in R_d \cap -S_d$ arbitrário. Neste caso, $S_d \subseteq D_F\langle 1, -y\rangle$, pois $y \in R_d$ e $D_F\langle 1, -y\rangle \subseteq S_d$, pois $-y \in S_d$. Isso mostra a última afirmação do Lema.

Finalmente, suponhamos que vale (iii). Como $x \in R_d = (1+\mathfrak{m}_A)\dot{F}^2$, podemos escrever $x = ua^2$, onde $u \in 1 + \mathfrak{m}_A$ (ou seja, $\pi_A(u) = 1$) e $a \in \dot{F}^2$. Logo, $S_d = D_F\langle 1, -x\rangle = D_F\langle 1, -u\rangle$. Uma vez que car $k_A \neq 2$, temos $\dot{k}_A = D_{k_A}\langle 1, -1\rangle$. Dado $w \in \dot{k}_A$, existem $a, b \in A^* \subset \dot{F}$ tais que $w = \pi_A(a)^2 - \pi_A(b)^2 = \pi_A(a)^2 - \pi_A(u)\pi_A(b)^2 = \pi_A(a^2 - ub^2)$. Como $a^2 - ub^2 \in D_F\langle 1, -u\rangle \cap A^* = S_d \cap A^*$, temos $w \in \pi_A(S_d \cap A^*) = \overline{S}_d^{\times}$, o que implica $\dot{k}_A \subseteq \overline{S}_d^{\times}$. Como a outra inclusão é clara, vale (i). ■

Como S_d e T_d são pré-ordens de F (veja o Corolário 3.14 e a Proposição 3.17), podemos considerar os conjuntos de ordens $X/S_d = \{P \in X_F \,|\, P \supset S_d\}$ e $X/T_d = \{P \in X_F \,|\, P \supset T_d\}$ (confira a notação na página 117).

Proposição 5.4 *Seja F um corpo, d um elemento rígido de F tal que $\sum \dot{F}^2 \not\subset D_F\langle 1, d\rangle$ e A um anel de valorização tal que $R_d = (1+\mathfrak{m}_A)\dot{F}^2$, com corpo de resíduos k_A e grupo de valores Γ_A. Sejam ainda X/S_d e X/T_d como definidos acima. Considere as seguintes afirmações:*

(1) $\dot{F}/\dot{F}^2 \simeq R_d/\dot{F}^2 \times S_d/\dot{F}^2$ *(produto direto de grupos abelianos).*

(2) $R_d \cdot S_d = \dot{F}$.

(3) $v_A(S_d) = \Gamma_A$ *e* $\overline{S}_d^{\times} = \dot{k}_A$.

(4) $X/T_d \cap X/S_d = \emptyset$.

(5) $X/T_d \dot{\cup} X/S_d = X_F$ *(reunião disjunta).*

Temos as seguintes implicações: (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3), (2) $\Rightarrow$ (4), (4) $\Leftrightarrow$ (5). *Além disso, se $v_A(S_d) = \Gamma_A$, temos* (4) $\Rightarrow$ (3), *ou seja, neste caso as afirmações são equivalentes.*

Demonstração. (1) $\Leftrightarrow$ (2): O item (2) do Corolário 3.14 garante que $R_d \cap S_d = \dot{F}^2$. Logo (2) implica (1). A outra implicação é imediata.

(2) $\Leftrightarrow$ (3): Primeiramente, $v_A(S_d) = \Gamma_A$ implica que $\dot{F} = A^* S_d$. Por outro lado, $\overline{S}_d^{\times} = \dot{k}_A$ implica que $A^* = (1 + \mathfrak{m}_A)S_d$. Logo, sob as duas hipóteses, temos: $\dot{F} = (1 + \mathfrak{m}_A)S_d = R_d S_d$ (pois $R_d = (1 + \mathfrak{m}_A)\dot{F}^2$).

Reciprocamente, dado $a \in A^*$, podemos escrever $a = r \cdot s$, onde $r \in R_d = (1+\mathfrak{m}_A)\dot{F}^2$ (o que implica $\pi_A(r) = \pi_A(\alpha^2)$) e $s \in S_d$. Logo, $\pi_A(a) = \pi_A(r) \cdot \pi_A(s) = \pi_A(\alpha^2) \cdot \pi_A(s) = \pi_A(\alpha^2 \cdot s) \in \pi_A(S_d)$. Portanto $\overline{S}_d^{\times} = \dot{k}_A$. Ademais, dado $x \in \dot{F}$, temos $x = r \cdot s$, com $r \in R_d = (1 + \mathfrak{m}_A)\dot{F}^2 \subset A^*\dot{F}^2$ e $s \in S_d$. Logo, $x = us$ onde $u \in A^*$ e $s \in S_d$ e $v_A(x) = v_A(s) \in v_A(S_d)$. Isso mostra que $v_A(S_d) = \Gamma_A$.

(2) $\Rightarrow$ (4): Se existisse $P \in X/T_d \cap X/S_d$, então $\dot{F} = R_d \cdot S_d = \dot{T}_d \cdot S_d \subset \dot{P} \cdot \dot{P} \subset \dot{P} \subsetneq \dot{F}$, contradição.

(4) $\Leftrightarrow$ (5): Seja $P \in X_F$ e suponhamos que $P \notin X/T_d$, isto é, $T_d \not\subset P$, o que equivale a $R_d \not\subset P$ (pois $T_d = R_d \cdot \sum \dot{F}^2$). Logo, existe $x \in R_d \smallsetminus P$, ou seja, $x \in R_d \cap -P$, o que implica $D\langle 1, -x\rangle \subset P$. Pela definição de S_d (veja o Corolário 3.14), temos: $S_d \subset D\langle 1, -x\rangle$. Assim, $S_d \subset P$, o que significa $P \in X/S_d$. Portanto, $X/T_d \cup X/S_d = X_F$. Se vale (4), essa reunião é disjunta. A recíproca é imediata.

Vamos supor, agora, que vale $v_A(S_d) = \Gamma_A$. Para mostrar que (4) $\Rightarrow$ (3), neste caso, basta mostrar que $\overline{S}_d = k_A$. Supondo o contrário, teríamos $\overline{S}_d \subsetneq k_A$, isto é, $\overline{S}_d$ seria uma pré-ordem de k_A. Isso significa que, para alguma ordem $P \in X/S_d$, teríamos $1+\mathfrak{m}_A \subset P$. Mas, como $T_d = (1 + \mathfrak{m}_A) \cdot \sum \dot{F}^2$, isso implicaria $T_d \subset P$ e $P \in X/T_d \cap X/S_d = \emptyset$, contradição! Portanto, $\overline{S}_d = k_A$. ■

5.3 Construção de um corpo pitagórico

Consideremos, como de costume, F como sendo um corpo formalmente real e d um elemento rígido de F que não é soma de quadrados. Lembremos que S_d é uma pré-ordem de F associada ao elemento d, definida na página 16. O objetivo desta seção é construir uma extensão pitagórica $K|F$, contida no fecho quadrático de F, tal que a

inclusão $F \subset K$ induz um isomorfismo de grupos $\dot{F}/S_d \simeq \dot{K}/\dot{K}^2$ e haja uma bijeção entre X_K, o espaço de ordens de K, e X/S_d, o espaço das ordens de F que contêm S_d. Essa construção é necessária para que obtenhamos mais adiante a decomposição do anel de Witt $W(F)$ como produto cartesiano $W(H) \times W(K)$, onde K é exatamente o corpo que construiremos a seguir e H é uma 2-henselização conveniente de F.

Vamos iniciar nosso estudo trabalhando com uma pré-ordem arbitrária T de F. Podemos munir o conjunto X/T formado pelas ordens de um corpo F que contêm a pré-ordem T com uma estrutura linear da seguinte maneira: cada ordem $P \in X/T$ pode ser identificada com uma função $\chi_P : \dot{F} \to \{\pm 1\}$ definida por $\chi_P(x) = 1$ se $x \in P$ e $\chi_P(x) = -1$ se $x \notin P$. Como $T \subset P = \ker \chi_P$, podemos ver χ_P como um elemento do $\mathbb{F}_2$-espaço vetorial dual $(\dot{F}/T)^*$. Neste contexto, dizer que as ordens $P_1, \ldots, P_n$ são *dependentes* significa simplesmente dizer que $\chi_1 \cdots \chi_n = 1$, onde $P_i = \ker \chi_i$, para cada i, e 1 deve ser entendido como a função $1 : \dot{F} \to \{\pm 1\}$ dada por $x \mapsto 1$. No caso $n = 2$, temos $\chi_1\chi_2 = 1$ se e somente se todo elemento de $\dot{F}$ tem o mesmo sinal em relação a P_1 e P_2, isto é, $P_1 = P_2$.

No caso $n = 3$, sejam P_1, P_2, P_3 ordens em X/T e χ_1, χ_2, χ_3 suas respectivas funções. Se $\chi_1\chi_2\chi_3 = 1$ então $P_1 = P_2 = P_3$. De fato, dado um elemento $x \in \dot{F}$, se $\chi_1(x) = 1$, então $\chi_2(x) = \chi_3(x) = 1$ ou $\chi_2(x) = \chi_3(x) = -1$, mas este último caso implicaria $\chi_1\chi_2\chi_3(-x) = -1$. De modo análogo vemos que, se $\chi_2(x) = 1$, então $\chi_1(x) = \chi_3(x) = 1$ e, se $\chi_3(x) = 1$, então $\chi_1(x) = \chi_2(x) = 1$.

Assim três ordens distintas são sempre independentes. Suponhamos que o produto $\chi_1\chi_2\chi_3$ também é uma ordem, digamos χ_4. Lembrando que $P_i = \ker \chi_i$ $(i = 1, 2, 3, 4)$ vemos que a interseção $S = P_1 \cap P_2 \cap P_3 \cap P_4$ é uma pré-ordem de índice 8 em $\dot{F}$. De acordo com o item (3) da Proposição 3.11 da página 23, S é um leque com 4 elementos. Por essa razão, dizemos que o conjunto $V = \{\chi_1, \chi_2, \chi_3, \chi_4\}$ é um leque com 4 elementos.

Observação: No que segue usaremos o nome **ordem** para indicar tanto o "cone positivo" $P \subset \dot{F}$, como usualmente fazemos, quanto a função $\chi_P : \dot{F} \to \{\pm 1\}$ associada a P. Assim, por exemplo, diremos ora $P \in X_F$, ora $\chi \in X_F$, de acordo com o que for mais conveniente. Enfatizamos porém que nem sempre uma função $\chi : \dot{F} \to \{\pm 1\}$ está associada a uma ordem, por exemplo, para a função dada por $\chi(x) = -1$, qualquer que seja $x \in \dot{F}$, não existe ordem $P \in X_F$ tal que $\chi = \chi_P$.

A importância dos leques com 4 elementos fica evidente no Teorema 5.5 abaixo. Este

Teorema fornece um critério para decidir quando uma função $f \in \mathcal{C}(Y, \{\pm 1\})$, isto é, uma função contínua $f : Y \to \{\pm 1\}$, onde $Y \subset X_F$, é *representada* por um elemento $x \in \dot{F}$, ou seja, quando $f = \hat{x}$, onde $\hat{x} \in \mathcal{C}(Y, \{\pm 1\})$ é a função contínua[1] dada por

$$\hat{x}(\chi) = \chi(x),\ \chi \in Y.$$

Teorema 5.5 (Marshall, [25], Teorema 7.2) *Seja $Y \subset X_F$ um subespaço do espaço das ordens de F e $f \in \mathcal{C}(Y, \{\pm 1\})$. Então $f = \hat{x}$, para algum $x \in \dot{F}$, se e somente se $\sum_{\chi \in V} f(\chi) \equiv 0 (\bmod 4)$ vale para cada leque com 4 elementos $V \subset Y$.*

Usaremos o Teorema 5.5 acima na demonstração do Teorema 5.6 a seguir. Vale observar que uma das direções do Teorema 5.5 pode ser verificada diretamente. De fato, se $f = \hat{x}$ e $V = \{P_1, P_2, P_3, P_4\}$ é um leque, temos três casos a considerar: primeiro, x pode pertencer a duas das ordens e não pertencer às outras duas. Neste caso, $\sum_{i=1}^{4} f(P_i) = 1 + 1 - 1 - 1 = 0$, que é divisível por 4. Se x pertence a três das quatro ordens, então x necessariamente pertence à quarta ordem de V, pois V é um leque. Logo, $\sum_{i=1}^{4} f(P_i) = 1 + 1 + 1 + 1 = 4$. Da mesma forma, se x não pertence a três das quatro ordens, não pode pertencer à quarta ordem e $\sum_{i=1}^{4} f(P_i) = -4$. Logo $\sum_{P \in V} f(P) \equiv 0 (\bmod 4)$ vale sempre que $f = \hat{x}$. O resultado do Teorema 5.5 é relevante porque mostra que somente as funções do tipo $f = \hat{x}$ têm essa propriedade.

Teorema 5.6 *Seja F um corpo formalmente real e T uma pré-ordem de F. Consideremos uma extensão $K|F$ e um subespaço de ordens $Y \subset X_K$ tais que:*

(1) *O corpo K é formalmente real, pitagórico e vale $\bigcap_{Q \in Y} Q = \dot{K}^2$.*

(2) *A aplicação $\rho : Y \to X/T$ induzida pela restrição de ordens é um homeomorfismo.*

Se todo leque com 4 elementos $V \subset X/T$ estende-se a um leque com 4 elementos $W = \rho^{-1}(V) \subset Y$ então o homomorfismo canônico $\varphi : \dot{F}/T \to \dot{K}/\dot{K}^2$ é um isomorfismo e $Y = X_K$.

[1] Consideramos o subespaço $Y \subset X_F$ munido da topologia de Harrison (veja a página 115) e $\{\pm 1\}$ munido da topologia discreta. A propósito, a topologia de Harrison pode ser descrita como a topologia mais fraca de Y que faz com que todas as funções do tipo $\hat{x}$, com $x \in \dot{F}$, sejam contínuas.

Demonstração. Primeiramente, observemos que a partir da bijeção $\rho : Y \to X/T$ podemos obter uma "adjunta" ρ^* dada por:

$$\mathcal{C}(X/T, \{\pm 1\}) \xrightarrow{\rho^*} \mathcal{C}(Y, \{\pm 1\})$$

$$f \longmapsto f \circ \rho$$

Dada $g \in \mathcal{C}(Y, \{\pm 1\})$, a função $f = g \circ \rho^{-1} \in \mathcal{C}(X/T, \{\pm 1\})$ é tal que $\rho^*(f) = g$. Isso mostra que ρ^* é sobrejetiva. Agora, dado $x \in \dot{K}$, seja $f \in \mathcal{C}(X/T, \{\pm 1\})$ tal que $\rho^*(f) = \hat{x}$, isto é, $f \circ \rho = \hat{x}$. Por hipótese, se $V \subset X/T$ é um leque com 4 elementos, então $W = \rho^{-1}(V) \subset Y$ também é um leque com 4 elementos. Logo

$$\sum_{\chi \in V} f(\chi) = \sum_{\xi \in \rho^{-1}(V)} (f \circ \rho)(\xi) = \sum_{\xi \in W} \hat{x}(\xi) \equiv 0 \,(\bmod 4),$$

onde a congruência módulo 4 acima decorre do Teorema 5.5 aplicado a K e $Y \subset X_K$. Usando novamente o Teorema 5.5, vemos que f é representada por algum $y \in \dot{F}$, ou seja, $f = \hat{y}$. Portanto, $\hat{y} \circ \rho = \hat{x}$. Isto significa que as ordens de F que contêm y estão em correspondência biunívoca (via ρ) com as ordens de Y que contêm x. Como $y \in \dot{F} \subset \dot{K}$, podemos considerar y como um elemento de K e escrever $\hat{x} = \hat{y}$, o que é equivalente a $\chi_Q(y^{-1}x) = 1$, para toda ordem $Q \in Y$, isto é, $y^{-1}x \in \bigcap_{Q \in Y} Q = \dot{K}^2$. Isso mostra que $x \in \dot{F}\dot{K}^2$. Conseqüentemente, o homomorfismo $\varphi : \dot{F}/T \to \dot{K}/\dot{K}^2$, induzido pela inclusão $F \subset K$, é sobrejetivo.

Uma vez que $\bigcap_{Q \in Y} Q = \dot{K}^2$ e há uma bijeção entre Y e X/T, temos

$$\dot{K}^2 \cap F = \bigcap_{Q \in Y} Q \cap F = \bigcap_{P \in X/T} P = T$$

e isso prova que φ também é injetivo, logo, um isomorfismo.

Dado $y \in \dot{K}$, pela sobrejetividade de φ existe $x \in \dot{F}$ tal que $y\dot{K}^2 = x\dot{K}^2$. Logo, $\dot{K} \subset \dot{F}\dot{K}^2$ e vale mesmo a igualdade $\dot{K} = \dot{F}\dot{K}^2$ pois a outra inclusão é imediata.

Se P é uma ordem qualquer em X_K, queremos mostrar que $P \in Y$. Primeiramente, temos $\dot{K}^2 \subset P$, o que implica $T = \dot{K}^2 \cap F \subset P \cap F$, ou seja, $P \cap F \in X/T$. Como a restrição de ordens $Y \to X/T$ é sobrejetiva, existe $P' \in Y$ tal que $P' \cap F = P \cap F$. Para $y \in P$, podemos escrever $y = x\alpha^2$, com $x \in F$ e $\alpha \in \dot{K}$. Assim, $x = y\alpha^{-2} \in P \cap F = P' \cap F$ e $y = x\alpha^2 \in P'$. Logo $P \subset P'$ e, como ambas as ordens têm índice 2 em $\dot{K}$, vale a igualdade $P = P'$. ■

Observação 5.7 *Um espaço de ordens, munido da topologia de Harrison, é booleano, isto é, compacto, Hausdorff e totalmente desconexo (cf. página 115). Dessa maneira, se X e Y são espaços de ordens e $\rho : X \to Y$ é contínua e bijetiva, então ρ é um homeomorfismo. Em particular, se $F \subset E \subset F(2)$, S uma pré-ordem de E e $T = S \cap F$, a contração de ordens $\rho : X_E \to X_F$, dada por $\rho(Q) = Q \cap F$ induz uma aplicação contínua $\rho' : X/S \to X/T$ (ver a observação da página 115). Como X/S e X/T são compactos e de Hausdorff, ρ' é um homeomorfismo se for uma bijeção (esse é um resultado da topologia geral, cf. James Dugundji, Topology, Teorema 2.1 (2), p. 226). Por esse motivo, usaremos os termos homeomorfismo e bijeção como sinônimos nesta seção.*

Lema 5.8 *Seja T uma pré-ordem de um corpo F e $\{t_i \mid i \in I\} \subset T$ uma família de representantes de uma $\mathbb{F}_2$-base de $T/\dot{F}^2$. Seja E o corpo obtido a partir de F pela adjunção de exatamente uma raiz de $X^{2^n} - t_i$, escolhida convenientemente[2], para cada $i \in I$ e cada $n \geq 1$. Então E é formalmente real, a função $X_E \to X/T$ dada por $P \mapsto P \cap F$ é um homeomorfismo e $T \subset \dot{E}^2$.*

Demonstração. O corpo E pode ser construído recursivamente usando-se o seguinte procedimento: para cada $i \in I$, denotemos as raízes de $X^2 - t_i$ por $\pm t_{1,i}$. O corpo F_1 é obtido a partir de $F_0 = F$ adjuntando-se, para cada $i \in I$, exatamente uma das raízes de $X^2 - t_i$, digamos $t_{1,i}$. Ou seja, $F_1 = F(\{t_{1,i} \mid i \in I\})$.

Suponhamos construído, para $n \geq 2$, o corpo $F_{n-1} = F_{n-2}(\{t_{n-1,i} | i \in I\})$. Definimos indutivamente $F_n = F_{n-1}(\{t_{n,i} \mid i \in I\})$, onde $t_{n,i}$ é uma das raízes de $X^2 - t_{n-1,i}$, para cada $i \in I$. Dessa forma, obtemos uma cadeia $F = F_0 \subset F_1 \subset F_2 \subset \cdots F_n \subset \cdots$ e definimos $E = \bigcup_{n \geq 0} F_n$. Mostraremos a seguir que o corpo E tem as propriedades requeridas.

Primeiramente, mostraremos que uma ordem $Q_0 = Q$ de F_n tal que $t_{n,i} \in Q$, para todo $i \in I$, tem um único prolongamento em F_{n+1}. No caso $n = 1$, dada uma ordem $Q \in X/T$ afirmamos que, para cada $J \subset I$ finito, existe uma única ordem Q_J de $F_{1,J} = F(\{t_{1,j} \mid j \in J\})$ que estende Q. Mais ainda, podemos escolher as ordens Q_J de modo que, se $J_1 \subset J_2$, então $Q_{J_1} \subset Q_{J_2}$.

Para demonstrarmos a afirmação acima, consideremos inicialmente $J = \{i\}$. Neste caso, toda ordem de X/T tem duas extensões a $F(t_{1,i})$, Q_1 e Q_1', tais que $t_{1,i} \in Q_1$ e $-t_{1,i} \in Q_1'$. Escolhendo, por exemplo, a ordem Q_1, vemos que esta é a única ordem de

[2]Se escolhermos uma raiz $t_{n,i}$ de $X^{2^n} - t_i$, a raiz $t_{n+1,i}$ de $X^{2^{n+1}} - t_i$ deve satisfazer $t_{n+1,i}^2 = t_{n,i}$.

F_1 que estende Q e contém $t_{1,i}$. Agora, o passo de indução: se $J = \{i_1, \ldots, i_n\}$ e Q_m é a única ordem de $F(t_{1,i_1}, \ldots, t_{1,i_m})$ que estende Q e contém $t_{1,i_1}, \ldots, t_{1,i_m}$, escolhemos Q_{m+1} como a única ordem da extensão quadrática $F(t_{1,i_1}, \ldots, t_{1,i_{m+1}})$ de $F(t_{1,i_1}, \ldots, t_{1,i_m})$ que estende Q_m e contém $t_{1,i_{m+1}}$. Dessa forma, obtemos, para cada $J = \{i_1, \ldots i_r\} \subset I$ uma única ordem Q_J de $F_{1,J}$ que estende Q e contém $t_{1,i_1}, \ldots, t_{1,i_r}$. As unicidades determinadas por nossas escolhas implicam que $Q_{J_1} \subset Q_{J_2}$, se $J_1 \subset J_2$.

Assim, o conjunto $\{Q_J \mid J \subset I \text{ finito }\}$ de subconjuntos de F_1 é indutivo[3]. Uma verificação direta mostra que $Q_1 = \bigcup_J Q_J$ é uma ordem de F_1 estendendo Q. Dessa forma, demonstramos que, dada uma ordem $Q \in X/T$, existe uma única ordem Q_1 de F_1 que estende Q e contém $t_{1,i}$, para todo $i \in I$.

Suponhamos, por indução, que Q_n é a única ordem de F_n que estende Q_{n-1} e contém $t_{n,i}$, para todo $i \in I$. Procedendo de modo inteiramente análogo ao caso $n = 1$, podemos mostrar que, para cada $J \subset I$ finito, existe uma única ordem Q_J de $F_{n+1,J} = F_n(\{t_{n+1,j} \mid j \in J\})$ que estende Q_n e contém $t_{n+1,j}$, para todo $j \in J$. Além disso, se $J_1 \subset J_2$ então $Q_{J_1} \subset Q_{J_2}$. Novamente, obtemos um conjunto indutivo $\{Q_J \mid J \subset I \text{ finito}\}$ de subconjuntos de F_{n+1} e, definindo $Q_{n+1} = \bigcup_J Q_J$, podemos verificar diretamente que Q_{n+1} é uma ordem de F_{n+1} estendendo Q_n. Mais ainda, Q_{n+1} é a única ordem de F_{n+1} que estende Q_n e contém $t_{n+1,i}$, para todo $i \in I$.

Considerando uma ordem $Q_0 = Q \in X/T$, para cada $n \geq 1$, seja Q_n a única ordem de F_n satisfazendo as condições:

(1) $Q_n \cap F_{n-1} = Q_{n-1}$;

(2) $t_{n,i} \in Q_n$, para cada $i \in I$.

Novamente por uma verificação direta, vemos que reunião $Q_\infty = \bigcup_{n\geq 1} Q_n$ é uma ordem de E que estende Q. Isso mostra que $X_E \to X/T$, dada por $P \mapsto P \cap F$, é sobrejetiva.

A seguir, mostraremos a injetividade da restrição $X_E \to X/T$. De início, observemos que $t_i \in \dot{F}_1^2$ por construção, logo, $t_i \in \dot{E}^2$ para todo $i \in I$. Como $\{t_i \dot{F}^2 \mid i \in I\}$ é uma $\mathbb{F}_2$-base de $T/\dot{F}^2$, concluímos que $T \subset \dot{E}^2$. Assim, toda ordem P de E contém T e, conseqüentemente, $T \subset P \cap F$, para toda $P \in X_E$, isto é, $P \cap F \in X/T$, para toda ordem P de E. Logo, a imagem da restrição $P \mapsto P \cap F$ está contida em X/T.

Suponhamos que existam ordens $P_1, P_2 \in X_E$ tais que $P_1 \neq P_2$ e $P_1 \cap F = P_2 \cap F$. Como $P_1 \neq P_2$, existe $n \geq 1$ tal que $P_1 \cap F_n \neq P_2 \cap F_n$ e podemos considerar o menor

[3]Ou seja, dados os subconjuntos Q_{J_1} e Q_{J_2} de F_1, existe $Q_{J_1 \cup J_2}$ contendo Q_{J_1} e Q_{J_2}.

$n \geq 1$ com essa propriedade, ou seja, tal que $P_1 \cap F_m = P_2 \cap F_m$, para $0 \leq m < n$. Uma vez que $t_{n-1,i} = t_{n,i}^2 \in \dot{E}^2$, temos $t_{n-1,i} \in P_1 \cap F_{n-1} = P_2 \cap F_{n-1}$, para todo $i \in I$.

Como $P_1 \cap F_n \neq P_2 \cap F_n$ e $P_1 \cap F_{n-1} = P_2 \cap F_{n-1}$, existe uma extensão intermediária $F_{n-1} \subset L \subset F_n$, com $[L : F_{n-1}] < \infty$, tal que $P_1 \cap L \neq P_2 \cap L$. Uma vez que $F_n|F_{n-1}$ é uma extensão multiquadrádica obtida pela adjunção de exatamente uma raiz de cada polinômio $X^2 - t_{n-1,i}$, com $i \in I$, a escolha de L implica que existe $J \subset I$, finito, tal que $L \subset F_{n-1}(J) = F_{n-1}(\{t_{n,j} \mid j \in J\})$. Como $P_1 \cap L \neq P_2 \cap L$, temos $P_1 \cap F_{n-1}(J) \neq P_2 \cap F_{n-1}(J)$.

Chegamos, assim, a uma extensão finita $F_{n-1}(J)|F_{n-1}$ tal que $P_1 \cap F_{n-1} = P_2 \cap F_{n-1}$ e $P_1 \cap F_{n-1}(J) \neq P_2 \cap F_{n-1}(J)$ e que é obtida através da cadeia:

$$F_{n-1} = F_{n-1}(I_0) \subset F_{n-1}(I_1) \subset \cdots \subset F_{n-1}(I_{k-1}) \subset F_{n-1}(I_k) = F_{n-1}(J),$$

onde $\emptyset = I_0 \subset I_1 \subset \cdots \subset I_{k-1} \subset I_k = J$ e cada I_k tem k elementos. Portanto, existe $0 \leq m < k$ tal que $P_1 \cap F_{n-1}(I_m) = P_2 \cap F_{n-1}(I_m)$ e $P_1 \cap F_{n-1}(I_{m+1}) \neq P_2 \cap F_{n-1}(I_{m+1})$, e $F_{n-1}(I_{m+1})$ é uma extensão quadrática de $F_{n-1}(I_m)$, obtida adjuntando-se $t_{n,i}$, onde $\{t_{n,i}\} = I_{m+1} \smallsetminus I_m$. Denotando por $P = P_1 \cap F_{n-1}(I_m) = P_2 \cap F_{n-1}(I_m)$, $P' = P_1 \cap F_{n-1}(I_{m+1})$ e $P'' = P_2 \cap F_{n-1}(I_{m+1})$, temos o seguinte diagrama:

ou seja, as ordens P' e P'' são as duas extensões de P para $F_{n-1}(I_{m+1})$. Como esta é uma extensão quadrática, obtida adjuntando-se $t_{n,i}$, o elemento $t_{n,i}$ não pode pertencer simultaneamente a P' e P'' (veja o Exemplo (3), da página 118). Sem perda de generalidade, podemos supor que $t_{n,i} \notin P'$. Como $t_{n+1,i}^2 = t_{n,i}$, pelo Lema B.9, a ordem P' não se estende para $K = F_{n-1}(I_m)(t_{n+1,i})$. Como $K \subset E$, $P_1 \cap K$ é uma ordem de K que estende $P' = P_1 \cap F_{n-1}(I_{m+1})$. Contradição! Logo, a restrição de ordens $X_E \to X/T$ é injetiva.

Finalmente, pela Observação 5.7, a bijeção $X_E \to X/T$ é um homeomorfismo. ■

A seguir definiremos (Definição 5.10) uma relação de equivalência que será útil na construção do corpo K.

Definição 5.9 *Dizemos que um anel de valorização C de F é* anti-SAP *se k_C é formalmente real e $(\Gamma_C : 2\Gamma_C) \geq 2$; mais ainda, caso k_C tenha ordem única, então $(\Gamma_C : 2\Gamma_C) \geq 4$.*

O nome *anti-SAP* deve-se ao fato de um corpo admitindo um anel de valorização C, como na definição acima e compatível com a pré-ordem fraca, não poder ser SAP. Isso é conseqüência da caracterização de corpos SAP via valorizações (cf. [22], Teorema 16.3, p.121).

A seguir definimos uma relação entre os elementos de X_F.

Definição 5.10 *Duas ordens $P_1, P_2 \in X_F$ são ditas M-equivalentes (notação: $P_1 \sim P_2$) se e somente se $P_1 = P_2$ ou existe um anel de valorização anti-SAP compatível simultaneamente com P_1 e P_2.*

A relação definida acima é reflexiva e simétrica. Isso é claro. Para verificarmos que vale a transitividade, suponhamos que $P_1 \neq P_2$ e $P_1 \sim P_2$ e também $P_2 \neq P_3$ e $P_2 \sim P_3$, onde $P_1, P_2, P_3 \in X_F$. Sejam B e C os anéis de valorização anti-SAP compatíveis respectivamente com os pares P_1, P_2 e P_2, P_3. Os anéis B e C são compatíveis com uma mesma ordem, P_2, logo, pelo Corolário 4.3, são comparáveis. Se $B \subset C$, então $1 + \mathfrak{m}_C \subset 1 + \mathfrak{m}_B \subset P_1$ e, neste caso, C é compatível com P_1 e P_3, ou seja, $P_1 \sim P_3$. Por outro lado, se $C \subset B$, concluímos da mesma maneira que o anel B é compatível com P_1 e P_3, logo $P_1 \sim P_3$.

Definição 5.11 *Chamaremos as classes de equivalência de X_F, determinadas pela relação $\sim$, de componentes conexas de X_F. Dizemos também que um subconjunto Y do espaço de ordens X_F é conexo se Y é uma reunião de componentes conexas de X_F, ou seja, dados $P_1 \in Y$ e $P_2 \in X_F$, se $P_2 \sim P_1$, então $P_2 \in Y$.*

A Proposição a seguir estabelece a ligação entre a relação de equivalência $\sim$ definida acima e os leques com 4 elementos.

Proposição 5.12 *Dadas $P_1, P_2 \in X_F$ com $P_1 \neq P_2$, temos $P_1 \sim P_2$ se e somente se existem $P_3, P_4 \in X_F$ tais que $V = \{P_1, P_2, P_3, P_4\}$ é um leque com 4 elementos.*

Demonstração. Suponhamos, primeiramente, que as ordens P_1 e P_2 pertençam a um leque com 4 elementos V, como descrito no enunciado acima, e tomemos $T = \bigcap_{P \in V} P$. Pelo Teorema 3.12, de Bröcker, existe um anel de valorização não trivial B de F tal que $1 + \mathfrak{m}_B \subset T$ e $\overline{T} = \pi_B(T \cap B^*)$ é uma ordem ou a interseção de duas ordens de k_B. De acordo com o Teorema B.17 de Baer-Krull, o corpo de resíduos $k = k_B$ é formalmente real. Além disso (veja as Observações B.18 e B.19), temos:

$$|X/\overline{T}| \cdot |\Gamma_B/2\Gamma_B| = |X_T^B|, \tag{5.3.1}$$

onde $X/\overline{T} \subset X_k$ é formado pelas ordens de k que contêm $\overline{T}$ e X_T^B indica o conjunto das ordens contidas em X/T compatíveis com B. Se $(\Gamma_B : 2\Gamma_B) = 1$, então $|X/\overline{T}| = |X_T^B| = 4$, contradizendo o fato de $\overline{T}$ ser interseção de, no máximo, duas ordens. Assim, $(\Gamma_B : 2\Gamma_B) \geq 2$. Se $|X_k| = 1$, então $X_k = X/\overline{T}$ e $|X/\overline{T}| = 1$, logo a igualdade em (5.3.1) fornece $|\Gamma_B/2\Gamma_B| = |X_T^B| = 4$. Com isso, vemos que B satisfaz as condições da Definição 5.9, logo é um anel de valorização anti-SAP. Como $1 + \mathfrak{m}_B \subset T \subset P_1 \cap P_2$, temos $P_1 \sim P_2$.

Suponhamos, agora, que P_1 e P_2 sejam duas ordens distintas com $P_1 \sim P_2$. Pela Definição 5.10, existe um anel de valorização anti-SAP B tal que $1 + \mathfrak{m}_B \subset P_1 \cap P_2$. As ordens P_1 e P_2, sendo compatíveis com B, projetam-se sobre ordens $\overline{P}_1$ e $\overline{P}_2$ do corpo de resíduos $k = k_B$. Consideremos o leque trivial $T_0 = \overline{P}_1 \cap \overline{P}_2$. Seja

$$\mathcal{I} = \{P \in X_F \mid 1 + \mathfrak{m}_B \subset P \text{ e } T_0 \subset \overline{P}\}.$$

Se $T = \bigcap_{P \in \mathcal{I}} P$, temos $\overline{T} = T_0$. De fato, como $P_1, P_2 \in \mathcal{I}$, temos $\overline{T} \subseteq \overline{P}_1 \cap \overline{P}_2 = T_0$. Por outro lado, para toda ordem $P \in \mathcal{I}$, $\overline{P} \supset T_0$, logo $\overline{T} \supseteq T_0$. Pela Proposição 5.11(b), p.43, de [22], T é um leque. Como B é anti-SAP, temos que $\mathcal{I}$ tem pelo menos 4 elementos. Podemos, então, tomar uma ordem $P_3 \in \mathcal{I}$ distinta de P_1 e P_2. A pré-ordem $P_1 \cap P_2 \cap P_3$ contém T sendo, pela Proposição 3.11 da página 23, também um leque. Como $P_1 \cap P_2 \cap P_3$ é um subgrupo de índice 8 em $\dot{F}$, existe uma ordem P_4 tal que $P_1 \cap P_2 \cap P_3 \subset P_4$ (veja o parágrafo seguinte à demonstração da Proposição 3.11). Portanto, $V = \{P_1, P_2, P_3, P_4\}$ é um leque com 4 elementos. ■

Definição 5.13 *Consideremos uma extensão $E|F$ tal que $F \subset E \subset F(2)$ e E é formalmente real. Sejam $Y \subset X_E$ e $Z \subset X_F$ subespaços dos espaços de ordens de E e F. Dizemos que $\rho : X_E \to X_F$, dada por $P \mapsto P \cap F$, induz um homeomorfismo fiel $\rho' : Y \to Z$ se:*

(1) *ρ' é uma bijeção;*

(2) *Para todo par $P, Q \in Y$ temos: $P \sim Q$ se e somente se $\rho(P) \sim \rho(Q)$.*

Lema 5.14 *Mantendo a notação estabelecida na Definição 5.13 acima e supondo ainda que ρ' é uma bijeção, as seguintes afirmações são equivalentes:*

(1) *ρ induz um homeomorfismo fiel de Y em Z.*

(2) $V = \{P_1, P_2, P_3, P_4\} \subset Y$ *é um leque com* 4 *elementos se e somente se sua imagem* $\rho(V) = \{\rho(P_1), \rho(P_2), \rho(P_3), \rho(P_4)\} \subset Z$ *é um leque com* 4 *elementos.*

(3) *Todo leque com* 4 *elementos* $W = \{Q_1, Q_2, Q_3, Q_4\} \subset Z$ *estende-se a um leque com* 4 *elementos* $\rho^{-1}(W) = \{\rho^{-1}(Q_1), \rho^{-1}(Q_2), \rho^{-1}(Q_3), \rho^{-1}(Q_4)\} \subset Y$.

Demonstração. (1) $\Leftrightarrow$ (2) segue-se diretamente da Proposição 5.12. (2) $\Rightarrow$ (3) é imediato e (3) $\Rightarrow$ (2) é conseqüencia do Corolário 3.13. ■

Lema 5.15 *Seja* F *um corpo formalmente real,* T *uma pré-ordem de* F *e* B *um anel de valorização de* F *cujo corpo de resíduos* k_B *é formalmente real. Como de costume, vamos denotar por* $\mathfrak{m}_B$ *o ideal maximal de* B.

(1) *Seja* $PO_B = (1 + \mathfrak{m}_B) \sum \dot{F}^2$. PO_B *é uma pré-ordem de* F *e* X/PO_B *é o conjunto de todas as ordens de* F *em relação às quais* B *é compatível. Em particular, se* k_B *é pitagórico, então* $PO_B = (1 + \mathfrak{m}_B)\dot{F}^2$.

(2) *Se* B *é anti-SAP, então* X/PO_B *está contido em uma componente conexa de* X_F.

(3) *Suponhamos que o espaço* X/T *seja conexo e* B *seja um anel de valorização anti-SAP de* F. *Se* $X/PO_B \cap X/T \neq \emptyset$ *então* $X/PO_B \subset X/T$.

(4) *Reciprocamente, se para todo anel de valorização anti-SAP* B *de* F *tivermos* $X/PO_B \subset X/T$, *então* X/T *é conexo.*

Demonstração. (1) Seja $x \in \dot{F}$ tal que $\pi_B(x) \in \sum \dot{k}_B^2$. Existe $s \in \sum \dot{F}^2$ tal que $\pi_B(x) = \pi_B(s)$, logo $\pi_B(s^{-1}x) = 1$, isto é, $s^{-1}x \in 1 + \mathfrak{m}_B$. Conseqüentemente, temos: $x \in (1 + \mathfrak{m}_B) \sum \dot{F}^2 = PO_B$. Por outro lado, se $s \in \sum \dot{F}^2$ então $s = x_1^2 + \cdots + x_n^2$, com $x_i \in \dot{F}$. Podemos supor, sem perda de generalidade, que $v_B(x_1) = \min\{v_B(x_i)\}$, de modo que $\frac{x_i}{x_1} \in B$ para cada i e

$$s = x_1^2 \left(1 + (\frac{x_2}{x_1})^2 + \cdots + (\frac{x_n}{x_1})^2\right).$$

Como k_B é formalmente real, a expressão entre parênteses não pode pertencer a $\mathfrak{m}_B$, logo é uma unidade em B e $2v_B(x_i) \geq 2v_B(x_1) = v_B(s)$. A última desigualdade mostra que, se $s \in B$ então cada $x_i \in B$. Além disso, se $s \in B^*$ então $x_1 \in B^*$. Portanto

$$\pi_B(PO_B \cap B^*) = \sum \dot{k}_B^2. \tag{5.3.2}$$

O conjunto PO_B é fechado para o produto e contém $\dot{F}^2$. Isso é claro. Se $-1 \in PO_B$ então $-1 = us$, com $u \in 1 + \mathfrak{m}_B$ e $s \in \sum \dot{F}^2$. Logo $s \in B^*$ e $-1 \in \sum \dot{k}_B^2$, contradição, pois supomos que k_B é formalmente real. Para demonstrarmos que PO_B é fechado para soma, tomemos $a = u_1 s_1 + u_2 s_2$, com $u_1, u_2 \in 1 + \mathfrak{m}_B$ e $s_1, s_2 \in \sum \dot{F}^2$. Podemos supor, sem perda de generalidade, que $\frac{u_2 s_2}{u_1 s_1} \in B$ (pois B é um anel de valorização). Assim $a = u_1 s_1 (1 + \frac{u_2 s_2}{u_1 s_1})$ e é suficiente considerarmos $a = 1 + us$, com $u \in 1 + \mathfrak{m}_B$ e $s \in \sum \dot{F}^2 \cap B$. Pelo que vimos no parágrafo anterior, $\pi_B(s) \in \sum k_B^2$, logo $\pi_B(a) = 1 + \pi_B(s) \in \sum \dot{k}_B^2$. Usando a igualdade (5.3.2), vemos que existe $t \in PO_B$ tal que $\pi_B(a) = \pi_B(t)$, o que implica $\pi(t^{-1}a) = 1$. Portanto $t^{-1}a \in 1 + \mathfrak{m}_B \subset PO_B$ e, sendo PO_B fechado para o produto, $a \in PO_B$.

Mostramos assim que PO_B é uma pré-ordem de F. É imediato que qualquer ordem P de F compatível com B, isto é, tal que $1 + \mathfrak{m}_B \subset P$, contém PO_B, e vale a recíproca. Logo, X/PO_B coincide com o conjunto das ordens de F compatíveis com B.

Suponha k_B é pitagórico e tome $t = us \in PO_B$, com $u \in 1 + \mathfrak{m}_B$ e $s \in \sum \dot{F}^2$. Como $\pi_B(t) \in \sum \dot{k}_B^2 = \dot{k}_B^2$, existe $w \in \dot{F}^2$ tal que $w^{-1}t \in 1 + \mathfrak{m}_B$. Logo $t \in (1 + \mathfrak{m}_B)\dot{F}^2$ e temos a igualdade $PO_B = (1 + \mathfrak{m}_B)\dot{F}^2$.

(2) Fixada $P_0 \in X/PO_B$, consideremos uma pré-ordem arbitrária $P \in X/PO_B$, $P \neq P_0$. Temos: $1 + \mathfrak{m}_B \subset P_0$ e $1 + \mathfrak{m}_B \subset P$. Pela Definição 5.10, $P \sim P_0$. Assim, X/PO_B está contido na componente conexa de P_0 em X_F.

(3) Seja $P_0 \in X/PO_B \cap X/T$. Pelo item (2), se X_0 é a componente conexa à qual P_0 pertence, então $X/PO_B \subset X_0$. Por outro lado, como X/T é conexo e $P_0 \in X/T$, $X_0 \subset X/T$.

(4) Consideremos $P \in X/T$ e P' uma ordem de F tal que $P' \sim P$. Pela Definição 5.10, existe um anel de valorização anti-SAP B tal que $1 + \mathfrak{m}_B \subset P'$. Logo $P' \in X/PO_B \subset X/T$, o que implica que X/T é conexo. ■

A partir deste ponto, salvo menção explícita em contrário, consideraremos a pré-ordem $T = S_d$ e construiremos um corpo K satisfazendo as condições delineadas no primeiro parágrafo desta seção. Faremos isso utilizando o Teorema 5.6 acima, ou seja, nosso objetivo no que segue é encontrar um corpo K satisfazendo as condições (1) e (2) do Teorema 5.6 e para o qual também valha a condição de que cada leque $V \subset X/S_d$ com 4 elementos possa ser estendido a um leque $W \subset X_K$.

De posse das definições acima podemos descrever em linhas gerais como construiremos o corpo K satisfazendo as condições requeridas: mostraremos (Teorema 5.18, item

(4)) que X/S_d é conexo (no sentido estabelecido acima) e construiremos, para cada componente conexa X_λ contida em X/S_d, uma extensão K_λ de F, de modo que o corpo K irá coincidir com a interseção dos K_λ. No entanto, a construção de K se dará através de aplicações sucessivas da Definição 2.8, obtendo-se em cada passo um fecho relativo a uma determinada pré-ordem do corpo.

Conforme estabelecido no final do Capítulo 4, página 69, chamaremos de A_d a um anel de valorização de F tal que $(1+\mathfrak{m}_A)\dot{F}^2 = R_d$. Assumimos ainda que $\dot{F} = R_d S_d$ o que, de acordo com a Proposição 5.4, implica a decomposição do espaço de ordens $X_F = X/T_d \,\dot\cup\, X/S_d$.

Relembrando a notação que temos usado, nos dois lemas a seguir, Γ_B denota o grupo de valores do anel de valorização B.

Lema 5.16 *Seja B um anel de valorização de F com $A_d \subset B$. Se $\Gamma_B \neq 2\Gamma_B$, então $(1+\mathfrak{m}_B)\dot{F}^2 = R_d$.*

Demonstração. Vamos denotar $A = A_d$. A partir de $A \subset B$ obtemos $1+\mathfrak{m}_B \subset 1+\mathfrak{m}_A$, logo $1+\mathfrak{m}_B \subset R_d$. Afirmamos que todo $x \in \dot{F}$ tal que $v_B(x) \notin 2\Gamma_B$ é R_d-birígido.

De fato, por um lado temos $R_d = (1+\mathfrak{m}_A)\dot{F}^2 \subset A^*\dot{F}^2 \subset B^*\dot{F}^2$, logo $v_B(R_d) \subset 2\Gamma_B$. Por outro lado, temos $1+\mathfrak{m}_B \subset R_d$. Assim, quaisquer que sejam $r_1, r_2 \in R_d$, temos $v_B(r_1) \neq v_B(\pm x r_2)$, do contrário teríamos $v_B(x) \in 2\Gamma_B$, contrariando nossa suposição. Dessa forma, pondo $z = r_1 \pm x r_2$ temos $z = r_1(1+(\pm x)r_2 r_1^{-1}) \in r_1(1+\mathfrak{m}_B) \subset R_d$ se $v_B(\pm x r_2) > v_B(r_1)$. Em contrapartida, se $v_B(\pm x r_2) < v_B(r_1)$, temos

$$z = (\pm x) r_2 (1 + (\pm x)^{-1} r_2^{-1} r_1) \in (\pm x) r_2 (1 + m_B),$$

logo $z \in (\pm x) R_d$.

Usando a decomposição $\dot{F} = R_d S_d$, podemos escrever $x \in \dot{F}$ como $x = re$, com $r \in R_d$ e $e \in S_d$. Assim como x, o elemento e também é R_d-birígido. Uma vez que $e \in S_d$ e $R_d \cap S_d = \dot{F}^2$ (Corolário 3.14, item (2)) o elemento e é rígido[4]. Pela Definição 3.3 da página 16, $e \in S_d$ implica $R_d \subset D\langle 1, -e\rangle$, logo $R_d \subset R_e$.

Uma vez que $r \in R_d \subset B^*\dot{F}^2$, temos $v_B(e) \notin 2\Gamma_B$. Assim, $R_d \cup (-e)R_d \subset R_e \cup (-e)R_e = D\langle 1, -e\rangle$. Por outro lado, decorre também de $v_B(e) \notin 2\Gamma_B$ que e é $(1+\mathfrak{m}_B)\dot{F}^2$-birígido. Logo,

$$D\langle 1, -e\rangle \subset (1+\mathfrak{m}_B)\dot{F}^2 + (-e)(1+\mathfrak{m}_B)\dot{F}^2 = (1+\mathfrak{m}_B)\dot{F}^2 \cup (-e)(1+\mathfrak{m}_B)\dot{F}^2.$$

[4]Lembremos: e é rígido quando $D\langle 1, e\rangle = \dot{F}^2 \cup e\dot{F}^2$.

Portanto, $R_d \subset (1+\mathfrak{m}_B)\dot{F}^2 \cup (-e)(1+\mathfrak{m}_B)\dot{F}^2$. Se existissem $a \in R_d$ e $b \in (1+\mathfrak{m}_B)\dot{F}^2$ tais que $a = -eb$, teríamos $-e = ab^{-1} \in R_d$, pois $1+\mathfrak{m}_B \subset R_d$. Mas isso contradiz a escolha de e. Concluímos, então, que $R_d \subset (1+\mathfrak{m}_B)\dot{F}^2$. Como a outra inclusão é conseqüência da hipótese $A_d \subset B$, temos a igualdade $R_d = (1+\mathfrak{m}_B)\dot{F}^2$. ■

Lema 5.17 *Sejam P uma ordem de F contendo S_d e B um anel de valorização de F compatível com P, isto é, $1+\mathfrak{m}_B \subset P$. Se $A = A_d$ e B forem comparáveis, então $A \subset B$ e $\Gamma_B = 2\Gamma_B$. Mais ainda, se A_d e B não forem comparáveis, então o corpo de resíduos k_B de B é pitagórico.*

Demonstração. Se $B \subset A$, então $1+\mathfrak{m}_A \subset 1+\mathfrak{m}_B \subset P$. Logo $R_d = (1+\mathfrak{m}_A)\dot{F}^2 \subset P$ e, como estamos supondo $S_d \subset P$, teríamos $\dot{F} = R_d S_d \subset P$, contradição.

Dessa forma, para que A e B sejam comparáveis, devemos ter $A \subset B$. Buscando novamente por uma contradição, vamos supor que $\Gamma_B \neq 2\Gamma_B$. Pelo Lema 5.16 acima, obteríamos $R_d = (1+\mathfrak{m}_B)\dot{F}^2$ e isso nos levaria novamente a $R_d \subset P$ e, conseqüentemente, $\dot{F} = R_d S_d \subset P$. Devemos ter, então, $\Gamma_B = 2\Gamma_B$.

De acordo com o Corolário 4.24, o anel de valorização A é S_d-henseliano. Pelas observações feitas na página 53, A também é π-henseliano. Logo, se A e B não forem comparáveis, o Corolário 2.5 de [12] garante que k_B é pitagórico. Isso demonstra a última afirmação. ■

Teorema 5.18 *Seja B um anel de valorização de F compatível com uma ordem P que contém S_d e tal que $\Gamma_B \neq 2\Gamma_B$. Temos então:*

(1) *O corpo de resíduos k_B é pitagórico.*

(2) *$PO_B = (1+\mathfrak{m}_B)\dot{F}^2$ é uma pré-ordem de F e $X/PO_B \subset X/S_d$.*

(3) *$S_d \subset (1+\mathfrak{m}_B)\dot{F}^2$.*

(4) *X/S_d é conexo.*

Demonstração. Uma vez que $\Gamma_B \neq 2\Gamma_B$, o Lema 5.17 acima garante que A_d e B não são comparáveis e k_B é pitagórico. Pelo item (1) do Lema 5.15, $PO_B = (1+\mathfrak{m}_B)\dot{F}^2$ é uma pré-ordem de F. Para concluirmos a demonstração do item (2) suponhamos,

por absurdo, que $X/PO_B \not\subset X/S_d$. Pelo item (5) da Proposição 5.4, existiria $P' \in X/PO_B \cap X/T_d$. Logo, A_d e B seriam compatíveis com P' e, pelo Corolário 4.3, A_d e B seriam comparáveis, gerando uma contradição.

O item (3) é uma conseqüência direta de $X/PO_B \subset X/S_d$. Essa última inclusão é válida para todo B compatível com alguma ordem de X/S_d. Pelo item (4) do Lema 5.15, temos que X/S_d é conexo. ■

Lembremos que o grupo de valores do anel de valorização B de F é dito 2-*divisível* quando $\Gamma_B = 2\Gamma_B$. Usaremos a seguir a notação $F^h(\widehat{B}; F)$ para indicar o corpo de decomposição de uma extensão $\widehat{B}$ de B a $F(2)$, como já fizemos na página 52.

Corolário 5.19 *Seja B um anel de valorização de F compatível com uma ordem P que contém S_d. Assumimos que o grupo de valores de B não é 2-divisível e denotamos por $\widehat{B}$ uma extensão de B a $F(2)$. Então $F^h(\widehat{B}; F)$ é pitagórico e a inclusão $F \subset F^h(\widehat{B}; F)$ induz homomorfismo sobrejetivo $R_d/\dot{F}^2 \to \dot{F}^h(\widehat{B}; F)/\dot{F}^h(\widehat{B}; F)^2$.*

Demonstração. Para simplificar a notação, escrevemos $F^h = F^h(\widehat{B}; F)$. Lembremos que o corpo de decomposição (F^h, B_h), onde $B_h = \widehat{B} \cap F^h$, é uma extensão imediata de (F, B) (cf. página 51 e a Observação 4.8). Isso implica que o corpo de resíduos de $\widehat{B}$ é igual a k_B,o corpo de resíduos de B. De acordo com a Proposição 4.10 e a observação feita no parágrafo imediatamente anterior a essa Proposição, como $\widehat{B} \subset F^h$ é 2-henseliano e seu corpo de resíduos é pitagórico, o corpo F^h também é pitagórico.

Dado $y \in \dot{F}^h$, pelo fato da extensão $F^h|F$ ser imediata temos $v_h(y) \in \Gamma_B$, onde v_h denota a valorização associada a B_h. Logo, existe $x \in \dot{F}$ tal que $v_h(y) = v_h(x)$, ou seja, $v_h(x^{-1}y) = 0$, o que implica $x^{-1}y \in B_h^*$. Agora, se π_h denota a projeção canônica relativa a B_h, temos $\pi_h(x^{-1}y) \in k_B$. Conseqüentemente, existe $u \in B^*$ tal que $\pi_h(x^{-1}y) = \pi_h(u)$. Logo $\pi_h(u^{-1}x^{-1}y) = 1$ e $u^{-1}x^{-1}y \in 1 + \mathfrak{m}_h$, onde $\mathfrak{m}_h$ denota o ideal maximal de B_h. Como B_h é 2-henseliano, temos $u^{-1}x^{-1}y \in 1 + \mathfrak{m}_h \subset (\dot{F}^h)^2$. Portanto $y(\dot{F}^h)^2 = ux(\dot{F}^h)^2$, com $ux \in \dot{F}$. Isso demonstra que a inclusão $F \subset F^h$ induz uma sobrejeção $\dot{F}/\dot{F}^2 \to \dot{F}^h/(\dot{F}^h)^2$. Para finalizar, $ux \in \dot{F} = R_d S_d$ implica que $ux = rs$, com $r \in R_d$ e $s \in S_d$. Pelo item (3) do Teorema 5.18, $S_d \subset (\dot{F}^h)^2$. Logo, $R_d/\dot{F} \to \dot{F}^h/(\dot{F}^h)^2$ também é uma sobrejeção. ■

Lema 5.20 *Seja F um corpo formalmente real e C um anel de valorização de F compatível com alguma ordem de F. Seja $\widehat{C}$ uma extensão de C a $F(2)$ e $F^h = F^h(\widehat{C}; F)$.*

Vamos denotar $C_h = \widehat{C} \cap F^h$ *e* $\mathfrak{m}_h$ *o ideal maximal de* C_h*. Nessas condições, temos:*

(1) $1 + \mathfrak{m}_h \subset (F^h)^{2^n}$*, para todo* $n \geq 0$*.*

(2) *Para todo* $a \in 1 + \mathfrak{m}_C$ *e todo* $n \geq 1$ *o polinômio* $X^{2^n} - a$ *tem uma única raiz em* $1 + \mathfrak{m}_h$*. Mais ainda, se* α *e* α' *são duas raízes de* $X^{2^n} - a$ *em* F^h*, então* $\alpha = \pm\alpha'$*.*

(3) *Se* F^h *for pitagórico então* $X^{2^n} - a$*, com* $a \in 1 + \mathfrak{m}_C$*, tem todas as suas raízes em* $F^h(\sqrt{-1})$*.*

Demonstração. (1) Sabemos que $1 + \mathfrak{m}_h \subset (\dot{F}^h)^2$. Logo, o item (1) vale no caso $n = 1$. Assim, dado $a \in 1 + \mathfrak{m}_h$, existe $b_1 \in \dot{F}^h$ tal que $b_1^2 = a \in 1 + \mathfrak{m}_h$, ou seja, $(b_1 - 1)(b_1 + 1) \in \mathfrak{m}_h$, logo, $b_1 - 1 \in \mathfrak{m}_h$ ou $b_1 + 1 \in \mathfrak{m}_h$. Escolhemos

$$a_1 = \begin{cases} b_1 & \text{se} \quad b_1 - 1 \in \mathfrak{m}_h \\ -b_1 & \text{se} \quad b_1 + 1 \in \mathfrak{m}_h \end{cases}.$$

Dessa forma, $a = a_1^2$ e $a_1 \in 1+\mathfrak{m}_h \subset (\dot{F}^h)^2$, isto é, existe $b_2 \in \dot{F}^h$ tal que $b_2^2 = a_1 \in 1+\mathfrak{m}_h$. Logo $b_2 - 1 \in \mathfrak{m}_h$ ou $b_2 + 1 \in \mathfrak{m}_h$. Procedendo como fizemos acima, podemos escolher $a_2 \in \dot{F}^h$ tal que $a_2^{2^2} = a_1^2 = a$ e $a_2 \in 1 + \mathfrak{m}_h \subset (\dot{F}^h)^2$.

Supondo agora que tenhamos obtido, para $n > 1$, $a_{n-1} \in \dot{F}^h$ tal que $a_{n-1}^{2^{n-1}} = a$ e $a_{n-1} \in 1 + \mathfrak{m}_h$. Como $1 + \mathfrak{m}_h \subset (\dot{F}^h)^2$, existe $b_n \in \dot{F}^h$ tal que $b_n^2 = a_{n-1}$. Repetindo o que já fizemos acima, obtemos $b_n - 1 \in \mathfrak{m}_h$ ou $b_n + 1 \in \mathfrak{m}_h$. Escolhemos então a_n pondo:

$$a_n = \begin{cases} b_n & \text{se} \quad b_n - 1 \in \mathfrak{m}_h \\ -b_n & \text{se} \quad b_n + 1 \in \mathfrak{m}_h \end{cases}$$

de modo que $a_n^{2^n} = a$ e $a_n \in 1 + \mathfrak{m}_h$.

(2) Uma vez que $1+\mathfrak{m}_C \subset 1+\mathfrak{m}_h \subset (\dot{F}^h)^2$, a primeira afirmação do item (2) é imediata. Se α e α' são raízes de $X^{2^n} - a$, temos $(\alpha'\alpha^{-1})^{2^n} = 1$. Como F^h é formalmente real, as únicas 2^n-ésimas raízes da unidade contidas em F^h são -1 e 1. Logo, $\alpha'\alpha^{-1} = \pm 1$ e vale o item (2).

(3) Se K é um corpo pitagórico, então $K(\sqrt{-1})$ contém todas as raízes 2^n-ésimas da unidade. A prova deste fato é elementar e pode ser encontrada, por exemplo, em [6], Lema 4, p.323. Como $F^h(\sqrt{-1})$ contém uma raiz de $X^{2^n} - a$ para $a \in 1 + \mathfrak{m}_C$, conterá também todas as demais raízes. ■

Construção de "fechos" relativos às componentes conexas de S_d

De acordo com o item (4) do Teorema 5.18 o espaço de ordens X/S_d é conexo. Podemos então escrever

$$X/S_d = \dot{\bigcup}_{\lambda\in\Lambda} X_\lambda, \tag{5.3.3}$$

onde Λ é um conjunto possivelmente infinito, não necessariamente enumerável, e cada X_λ é uma componente conexa de X/S_d.

Para cada $\lambda \in \Lambda$ fixemos uma ordem $P_\lambda \in X_\lambda$. Se $P \in X_\lambda$ e $P \neq P_\lambda$, então existe um anel de valorização B_P que é anti-SAP e simultaneamente compatível com P e P_λ. Isso é uma conseqüência da conexidade de X_λ. Como todos os anéis de valorização de $\{B_P \mid P \in X_\lambda \text{ e } P \neq P_\lambda\}$ são compatíveis com P_λ, pelo Corolário 4.3 esse conjunto é totalmente ordenado pela inclusão.

Consideremos, agora, a *envolvente convexa*[5] de $\mathbb{Q}$ em F com relação à ordem P_λ, dada por:

$$B_\lambda = \{x \in F \mid \text{ existe } r \in \mathbb{Q} \text{ tal que } r + x \in P_\lambda \text{ e } r - x \in P_\lambda\}. \tag{5.3.4}$$

Sabemos que B_λ é um anel de valorização de F que está contido em todo anel de valorização de F compatível com P_λ (cf. [22], Teorema 2.6, p.18). Em particular, $B_\lambda \subset B_P$, para toda $P \in X_\lambda$. O ideal maximal de B_λ é dado por

$$\mathfrak{m}_\lambda = \{x \in F \mid r + x \in P_\lambda \text{ e } r - x \in P_\lambda \text{ para todo } r \in \mathbb{Q}\}$$

(cf. [22], Observação 2.7, p.18). Em particular, $1 + x \in P_\lambda$ para todo $x \in \mathfrak{m}_\lambda$, logo $1 + \mathfrak{m}_\lambda \subset P_\lambda$.

Para cada componente X_λ de X/S_d, seja $\mathcal{B}_\lambda$ o conjunto formado pelos anéis de valorização B de F tais que:

(1) B é compatível com alguma ordem $P \in X_\lambda$;

(2) $B_\lambda \subset B$ e, no caso $B_\lambda \neq B$, temos $\Gamma_B \neq 2\Gamma_B$.

Se $\mathfrak{m}_B$ denota o ideal maximal de B, o item (2) acima implica que $1 + \mathfrak{m}_B \subset 1 + \mathfrak{m}_\lambda$. Assim, $1 + \mathfrak{m}_B \subset P_\lambda$ para todo $B \in \mathcal{B}_\lambda$. Aplicando novamente o Corolário 4.3 vemos então que o conjunto $\mathcal{B}_\lambda$ é totalmente ordenado pela inclusão. Além disso, esse conjunto não é vazio, pois $B_\lambda \in \mathcal{B}_\lambda$. Mais ainda, $\mathcal{B}_\lambda$ contém cada um dos anéis B_P considerados acima, caso existam. Quando $X_\lambda = \{P_\lambda\}$, temos $\mathcal{B}_\lambda = \{B_\lambda\}$.

Observemos ainda que para toda ordem $P \in X_\lambda$ existe $B \in \mathcal{B}_\lambda$ tal que $P \in X/PO_B$, basta que tomemos $B = B_P$.

[5]Recordemos que um corpo ordenado tem característica zero, logo contém uma cópia de $\mathbb{Q}$.

Para cada $B \in \mathcal{B}_\lambda$ vamos fixar uma extensão $\widehat{B}$ de B para $F(2)$ escolhida de forma que o conjunto $\widehat{\mathcal{B}}_\lambda$ seja totalmente ordenado pela inclusão. A relação $\widehat{B} \mapsto \widehat{B} \cap F = B$ estabelece uma correspondência biunívoca entre $\widehat{\mathcal{B}}_\lambda$ e $\mathcal{B}_\lambda$. Mantendo a notação usual, escrevemos Γ_B, k_B e $\mathfrak{m}_B$ para o grupo de valores, o corpo de resíduos e o ideal maximal de B, respectivamente.

Para cada $\widehat{B} \in \widehat{\mathcal{B}}_\lambda$ seja $F^h(\widehat{B}; F)$ o corpo de decomposição de $\widehat{B}$ em relação a F, $B_h = \widehat{B} \cap F^h(\widehat{B}; F)$ e $\mathfrak{m}_h$ o ideal maximal de B_h. O par $(F^h(\widehat{B}; F), B_h)$ é extensão imediata do par (F, B) (cf. página 51), logo o grupo de valores e o corpo de resíduos de B_h podem ser tomados como Γ_B e k_B, respectivamente.

Afirmamos que o corpo $F^h = F^h(\widehat{B}; F)$ é pitagórico. De fato, pelo Teorema 5.18, k_B é pitagórico. Se $a \in F^h$, queremos mostrar que $1+a^2$ é um quadrado em F^h. Observando que $1+a^2 = a^2(1+(\frac{1}{a})^2)$ podemos supor que $a \in B_h$. Como B_h é 2-henseliano, podemos aplicar o Teorema 4.7 ao polinômio $p(X) = X^2 - (1 + a^2)$ para concluirmos que uma raiz de $p(X)$ está em F^h, ou seja, $1 + a^2$ é um quadrado em F^h, como queríamos.

Teorema 5.21 *Mantendo-se as notações e convenções introduzidas acima, para cada componente X_λ de X/S_d vamos a seguir construir um corpo K_λ com as seguintes propriedades:*

(1) *K_λ é pitagórico.*

(2) *Para todo $B \in \mathcal{B}_\lambda$, $K_\lambda \subset F^h(\widehat{B}; F)$ e, portanto, $F^h(\widehat{B}; K_\lambda) = F^h(\widehat{B}; F)$.*

(3) *$\dot{K}_\lambda^2 \cap F = S_\lambda = \bigcap_{P \in X_\lambda} P$.*

(4) *A função $\rho = \rho_\lambda : X_{K_\lambda} \to X_F$ dada por $\rho(P) = P \cap F$ é um homeomorfismo fiel de X_{K_λ} em X_λ.*

(5) *$\dot{K}_\lambda = \dot{F} \cdot \dot{K}_\lambda^2$.*

Demonstração. Como já vimos acima, $1 + \mathfrak{m}_B \subseteq 1 + \mathfrak{m}_\lambda \subset P_\lambda$, para todo $B \in \mathcal{B}_\lambda$. Se $P \in X/PO_B$ então P é uma ordem de F compatível com B. Como P_λ também é compatível com B temos $P \sim P_\lambda$ e $P \in X_\lambda$. Assim, $X/PO_B \subset X_\lambda$ e isso implica que

$$S_\lambda = \bigcap_{P \in X_\lambda} P \subset \bigcap_{P \in X/PO_B} P = PO_B,$$

para todo $B \in \mathcal{B}_\lambda$. Pelo item (2) do Teorema 5.18 temos $PO_B = (1 + \mathfrak{m}_B)\dot{F}^2$. Podemos então escolher uma $\mathbb{F}_2$-base $\{s_i\dot{F}^2 \mid i \in I\}$ de $S_\lambda/\dot{F}^2$, com $s_i \in 1 + \mathfrak{m}_B$, para todo $i \in I$ e todo $B \in \mathcal{B}_\lambda$.

Pelo Lema 5.20, para cada $i \in I$ e cada $n \geq 1$, o polinômio $X^{2^n} - s_i$ tem, a menos de sinal, uma única raiz $s_{n,i}$ em $F^h(\widehat{B}; F)$, para cada $B \in \mathcal{B}_\lambda$. Essa unicidade implica que

$$s_{n,i} \in \bigcap_{B \in \mathcal{B}_\lambda} F^h(\widehat{B}; F) \quad \text{para cada} \quad n \geq 1.$$

Assim, se K_1 é o corpo obtido a partir de F pela adjunção de $s_{n,i}$, para cada $n \geq 1$ e cada $i \in I$, temos $K_1 \subset F^h(\widehat{B}; F)$, para todo $B \in \mathcal{B}_\lambda$. Pelo Lema 5.8, K_1 é um corpo formalmente real tal que X_{K_1} é homeomorfo a X_λ e $S_\lambda \subset \dot{K}_1^2$.

Para cada $B \in \mathcal{B}_\lambda$ tomemos $B_1 = B_h \cap K_1$ e denotemos por $\mathfrak{m}_{B,1}$ o ideal maximal de B_1. Como $K_1 \subset F^h(\widehat{B}; F)$ para todo $B \in \mathcal{B}_\lambda$, temos que (K_1, B_1) é uma extensão imediata de (F, B) para todo $B \in \mathcal{B}_\lambda$. Mais ainda, $F^h(\widehat{B}; K_1) = F^h(\widehat{B}; F)$ para todo $B \in \mathcal{B}_\lambda$. Logo B_1 também tem k_B como corpo de resíduos, para cada $B \in \mathcal{B}_\lambda$. Como k_B é pitagórico, $PO_{B_1} = (1 + \mathfrak{m}_{B,1})\dot{K}_1^2$ é uma pré-ordem. Logo $\sum \dot{K}_1^2 \subset PO_{B_1}$.

Aplicando o procedimento acima ao corpo K_1 e à pré-ordem $\sum \dot{K}_1^2$, vamos obter um corpo K_2 tal que $K_2 \subset F^h(\widehat{B}; K_1) = F^h(\widehat{B}; F)$ para todo $B \in \mathcal{B}_\lambda$. Obtemos, também de modo similar ao que foi feito acima, que X_{K_2} é homeomorfo a X_{K_1} e $\sum \dot{K}_1^2 \subset \dot{K}_2^2$.

Repetindo recursivamente esse procedimento, construímos uma cadeia de corpos

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m \subset K_{m+1} \subset \cdots$$

onde, para cada m, $K_m \subset F^h(\widehat{B}; F)$, qualquer que seja $B \in \mathcal{B}_\lambda$. Para $m > 1$, a função $X_{K_m} \to X_{K_{m-1}}$ dada por $P \mapsto P \cap K_{m-1}$ é um homeomorfismo e $\sum \dot{K}_{m-1}^2 \subset \dot{K}_m^2$. No caso $m = 1$, como vimos acima, temos o homeomorfismo $X_{K_1} \to X_\lambda$, dado pela restrição de ordens, e $S_\lambda \subset \dot{K}_1^2$.

Seja agora

$$K_\lambda = \bigcup_{n>1} K_n.$$

Como, para todo $m > 1$, $K_m \subset F^h(\widehat{B}; F)$ para todo $B \in \mathcal{B}_\lambda$, temos $K_\lambda \subset F^h(\widehat{B}; F)$, donde resulta $F^h(\widehat{B}; K_\lambda) = F^h(\widehat{B}; F)$, para todo $B \in \mathcal{B}_\lambda$. Além disso, a função $P \mapsto P \cap F$ é um homeomorfismo de X_{K_λ} em X_λ. De fato, compondo as bijeções $X_{K_m} \to X_{K_{m-1}}$, para cada $2 \leq m \leq n$, e $X_{K_1} \to X_\lambda$, obtemos a bijeção $X_{K_n} \to X_\lambda$, para todo $n \geq 1$, dada pela restrição de ordens. Agora, se $X_{K_\lambda} \to X_\lambda$ não fosse uma bijeção, a restrição $X_{K_n} \to X_\lambda$ não seria uma bijeção para algum $n \geq 1$.

Afirmamos ainda que K_λ é pitagórico. De fato, dado $s = z_1^2 + z_2^2 + \cdots + z_t^2 \in \sum \dot{K}_\lambda^2$ existe $n \geq 1$ tal que $z_1, \ldots, z_t \in K_n$. Logo $s \in \sum \dot{K}_n^2 \subset \dot{K}_{n+1}^2 \subset \dot{K}_\lambda^2$, resultando daí que K_λ é pitagórico.

Sendo K_λ pitagórico, da bijeção entre X_{K_λ} e X_λ obtemos que

$$\dot{K}_\lambda^2 \cap F = \sum \dot{K}_\lambda^2 \cap F = \left(\bigcap_{P \in X_{K_\lambda}} P \right) \cap F = \bigcap_{P \in X_{K_\lambda}} \overbrace{P \cap F}^{Q} = \bigcap_{Q \in X_\lambda} Q = S_\lambda.$$

Com a argumentação acima, ficam demonstrados os três primeiros itens do Teorema. Para completarmos a demonstração do item (4) precisamos mostrar que ρ é fiel, ou seja, dadas $P_1, P_2 \in X_{K_\lambda}$ temos que $P_1 \sim P_2$ se e somente se $\rho(P_1) \sim \rho(P_2)$.

Se $P_1 \sim P_2$ então, pela Proposição 5.12, existem duas ordens $P_3, P_4 \in X_{K_\lambda}$ tais que $V = \{P_1, P_2, P_3, P_4\}$ é um leque com 4 elementos. De acordo com o Corolário 3.13 da página 24, se V é um leque então $W = \rho(V) = \{Q_1, Q_2, Q_3, Q_4\}$, com $Q_i = \rho(P_i) = P_i \cap F$, também é um leque[6]. Como ρ é bijetiva, W tem 4 elementos. Aplicando novamente a Proposição 5.12, vemos que $\rho(P_1) \sim \rho(P_2)$.

Reciprocamente, suponhamos que $Q_1 \sim Q_2$, onde $Q_1, Q_2 \in X_\lambda$. Pela Proposição 5.12, existem $Q_3, Q_4 \in X_\lambda$ tais que $W = \{Q_1, Q_2, Q_3, Q_4\}$ é um leque com 4 elementos. A idéia agora é buscar uma recíproca do Corolário 3.13 para que possamos repetir o argumento usado acima no sentido contrário. Mais precisamente, queremos mostrar que $V = \rho^{-1}(W) = \{P_1, P_2, P_3, P_4\} \subset X_{K_\lambda}$ também é um leque com 4 elementos, onde $P_i = \rho^{-1}(Q_i)$ para cada $i \in \{1, 2, 3, 4\}$. Embora essa recíproca não seja válida em geral, podemos obte-la no nosso caso. Esse é um dos objetivos das construções que temos feito.

Consideremos a pré-ordem $T = Q_1 \cap Q_2 \cap Q_3 \cap Q_4$. A Proposição 5.12 garante a existência de um anel de valorização anti-SAP D de F tal que $1 + \mathfrak{m}_D \subset T$ e $\overline{T} = \pi_D(T \cap D^*)$ é uma ordem ou interseção de duas ordens[7].

Uma vez que $K_\lambda \subset F^h(\widehat{D}; F)$ temos que $(K_\lambda, D_h \cap K_\lambda)$ é uma extensão imediata de (F, D). Logo, $D_\lambda = D_h \cap K_\lambda$ é um anel de valorização anti-SAP com corpo de resíduos k_D e grupo de valores Γ_D. Temos então dois casos:

(1) A pré-ordem $\overline{T} \subset k_D$ é uma ordem e $(\Gamma_D : 2\Gamma_D) = 4$;

(2) A pré-ordem $\overline{T} \subset k_D$ é interseção de duas ordens e $(\Gamma_D : 2\Gamma_D) = 2$.

Em ambos os casos o conjunto das ordens de K_λ compatíveis com D_λ e que projetam-se sobre $\overline{T}$ tem 4 elementos. Uma vez que a restrição ρ é uma bijeção, esse conjunto é for-

[6]Devemos observar que, no Corolário 3.13, descrevemos o leque como uma pré-ordem, justamente a interseção $T' = P_1 \cap P_2 \cap P_3 \cap P_4$.

[7]Na verdade, esse resultado é uma combinação do Teorema 3.12 de Bröcker com o Teorema B.17 de Baer-Krull.

mado, necessariamente, pelas ordens P_1, P_2, P_3, P_4. Denotando por $\mathfrak{m}_\lambda$ o ideal maximal de D_λ, temos $1 + \mathfrak{m}_\lambda \subset T' = P_1 \cap P_2 \cap P_3 \cap P_4$ e $\overline{T'}$ é um leque (trivial) em k_D. Pela Proposição 5.11(b), p.43, de [22], T' também é um leque, ou seja, $V = \{P_1, P_2, P_3, P_4\}$ é um leque, como queríamos.

Finalmente, para demonstrarmos o item (5), basta que apliquemos o Teorema 5.6 com $K = K_\lambda$, $T = S_\lambda$ e $Y = X_{K_\lambda}$. Obtemos, então, que $\varphi : \dot{F}/S_\lambda \to \dot{K}_\lambda/\dot{K}_\lambda^2$ é sobrejetiva, logo $\dot{K}_\lambda = \dot{F} \cdot \dot{K}_\lambda^2$. ■

Observação: o corpo K_λ construido no Teorema 5.21 acima não é único, pois depende de uma família de anéis de valorização $\widehat{\mathcal{B}}_\lambda$ previamente fixada.

Faremos a seguir a construção do corpo pitagórico K do qual necessitamos, que é o objetivo principal desta seção.

Construção do corpo K

Para cada $\lambda \in \Lambda$, fixemos um corpo K_λ como construído no Teorema 5.21. Temos fixada então a família

$$\{K_\lambda \mid \lambda \in \Lambda\}. \tag{5.3.5}$$

Lembremos que, como observamos logo acima, cada corpo K_λ não é único pois depende da escolha de uma família $\widehat{\mathcal{B}}_\lambda$ de anéis de valorização.

Tomemos K_1 como o S_d-fecho de F, conforme a Definição 2.8 da página 8. Uma vez que $S_d \subset S_\lambda$ e $S_\lambda \subset \dot{K}_\lambda^2$, temos que $S_d \subset \dot{K}_\lambda^2$ para cada $\lambda \in \Lambda$. Como K_λ é pitagórico, a Proposição 2.9 garante que $K_1 \subset K_\lambda$, para todo $\lambda \in \Lambda$.

Vamos considerar em K_1 a seguinte pré-ordem:

$$S_1 = \bigcap_{\lambda \in \Lambda} \dot{K}_\lambda^2 \cap K_1,$$

onde a família de corpos $\{K_\lambda \mid \lambda \in \Lambda\}$ foi escolhida e fixada em (5.3.5). Como $S_d = \bigcap_{\lambda\in\Lambda} S_\lambda$ e $S_\lambda = \dot{K}_\lambda^2 \cap F$ para cada $\lambda \in \Lambda$, temos $S_1 \cap F = S_d$.

Vamos agora construir K_2 como sendo o S_1-fecho de K_1. Novamente temos que $S_1 \subset \dot{K}_2^2$ e, para toda ordem P de K_2, $P \cap K_1 \supset \dot{K}_2^2 \cap K_1 = S_1$, logo $P \cap K_1 \in X/S_1$. Além disso, a pré-ordem S_1 foi construida de modo que $S_1 \subset \dot{K}_\lambda^2$, para todo $\lambda \in \Lambda$. Logo, pela Proposição 2.9, $K_2 \subset K_\lambda$ para todo $\lambda \in \Lambda$. Dessa forma, podemos considerar em K_2 a pré-ordem

$$S_2 = \bigcap_{\lambda \in \Lambda} \dot{K}_\lambda^2 \cap K_2.$$

Por construção, temos $S_2 \cap K_1 = S_1$, logo $S_2 \cap F = S_d$.

Supondo construido, para $n > 1$, um corpo pitagórico K_{n-1} munido de uma pré-ordem S_{n-1}, satisfazendo:

(1) $K_{n-1} \subset K_\lambda$, para todo $\lambda \in \Lambda$;

(2) $S_{n-1} = \bigcap_{\lambda\in\Lambda} \dot{K}_\lambda^2 \cap K_{n-1}$;

definimos K_n como o fecho pitagórico de K_{n-1} relativo à pré-ordem S_{n-1}. De modo análogo ao que já fizemos nos casos iniciais, verificamos que as propriedades (1) e (2) acima também valem para K_n e $S_n = \bigcap_{\lambda\in\Lambda} \dot{K}_\lambda^2 \cap K_n$.

Obtemos assim uma cadeia de corpos

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots$$

onde cada K_n é pitagórico e tem uma pré-ordem distinguida S_n ($S_0 = S_d$), satisfazendo as seguintes propriedades:

(a) para todo $\lambda \in \Lambda$, $K_n \subset K_\lambda$ e $S_n \subset \dot{K}_\lambda^2$;

(b) $S_{n-1} \subset \dot{K}_n^2$;

(c) para toda ordem P de K_n, $P \cap K_{n-1} \in X/S_{n-1}$ e $S_n \cap F = S_d$.

Finalmente, definimos o corpo

$$K = \bigcup_{n\geq 0} K_n. \tag{5.3.6}$$

Como cada K_n está contido em todos os K_λ, temos $K \subset K_\lambda$, para todo $\lambda \in \Lambda$. Temos ainda que

$$\bigcap_{\lambda\in\Lambda} \dot{K}_\lambda^2 \cap K = \dot{K}^2. \tag{5.3.7}$$

De fato, se $x \in K \cap \dot{K}_\lambda^2$, para todo $\lambda \in \Lambda$, então $x \in K_n \cap \dot{K}_\lambda^2$, para algum $n \geq 1$ e para todo $\lambda \in \Lambda$. Logo, $x \in S_n \subset \dot{K}_{n+1}^2 \subset \dot{K}^2$. A outra inclusão é imediata.

Se $x \in \sum \dot{K}^2$, então $x \in \sum \dot{K}_n^2$, para algum $n \geq 1$. Logo, x pertence à pré-ordem S_n, para algum $n \geq 1$ e, daí, $x \in S_n \subset \dot{K}_{n+1}^2 \subset \dot{K}^2$. Conseqüentemente, K é pitagórico. Além disso,

$$\dot{K}^2 \cap F = \left(\bigcap_{\lambda\in\Lambda} \dot{K}_\lambda^2 \cap K\right) \cap F = \left(\bigcap_{\lambda\in\Lambda} \dot{K}_\lambda^2 \cap K_n\right) \cap F = S_n \cap F = S_d.$$

Assim, a aplicação $\rho_K : X_K \to X_F$ dada por $\rho_K(P) = P \cap F$ tem imagem contida em X/S_d. A igualdade $\dot{K}^2 \cap F = S_d$ também implica que o homomorfismo canônico $\varphi : \dot{F}/S_d \to \dot{K}/\dot{K}^2$ é injetivo.

Para demonstrarmos a sobrejetividade de φ usaremos o Teorema 5.6. Para tal devemos construir um subconjunto de ordens $Y \subset X_K$ satisfazendo as condições do referido teorema. Para cada $\lambda \in \Lambda$ seja $Y_\lambda \subset X_K$ dado por:

$$Y_\lambda = \{Q \in X_K \mid \text{ existe } Q' \in X_{K_\lambda} \text{ tal que } Q = Q' \cap K\}$$

e $Y = \bigcup_{\lambda\in\Lambda} Y_\lambda$. Esta reunião é disjunta. De fato, se $\lambda, \mu \in \Lambda$, com $\lambda \neq \mu$, e $Q \in Y_\lambda \cap Y_\mu$, então $Q \cap F \in X_\lambda \cap X_\mu = \emptyset$, absurdo!

Temos ainda que

$$\bigcap_{Q\in Y} Q = \bigcap_{\lambda\in\Lambda} \bigcap_{Q\in Y_\lambda} Q = \bigcap_{\lambda\in\Lambda} \bigcap_{Q'\in X_{K_\lambda}} Q' \cap K = \bigcap_{\lambda\in\Lambda} \dot{K}_\lambda^2 \cap K \overset{(5.3.7)}{=} \dot{K}^2,$$

ou seja, $\bigcap_{Q\in Y} Q = \dot{K}^2$.

Seja $W = \{P_1, P_2, P_3, P_4\} \subset X/S_d$ um leque com 4 elementos. Existe $\lambda \in \Lambda$ tal que $W \subset X_\lambda$. Pelo item (4) do Teorema 5.21 e pelo item (3) do Lema 5.14, temos que W estende-se a um leque $\rho_\lambda^{-1}(W) = \{\rho_\lambda^{-1}(P_1), \rho_\lambda^{-1}(P_2), \rho_\lambda^{-1}(P_3), \rho_\lambda^{-1}(P_4)\} \subset X_{K_\lambda}$. Consideremos, então,

$$V = \rho_\lambda^{-1}(W) \cap K = \{\rho_\lambda^{-1}(P_1) \cap K, \rho_\lambda^{-1}(P_2) \cap K, \rho_\lambda^{-1}(P_3) \cap K, \rho_\lambda^{-1}(P_4) \cap K\}.$$

Para cada $i \in \{1, 2, 3, 4\}$ temos, pela definição de Y_λ, que $\rho_\lambda^{-1}(P_i) \cap K \in Y_\lambda \subset Y$. De acordo com o Corolário 3.13, $V \subset Y$ é um leque e como $X_{K_\lambda} \to X_\lambda$ é uma bijeção, V tem 4 elementos. Por sua própria construção, fica claro que V estende W.

Precisamos verificar ainda que $\rho : Y \to X/S_d$ é um homeomorfismo. Esse é o objetivo do Lema 5.22 a seguir.

Lema 5.22 *Mantendo todas as notações estabelecidas acima, temos:*

(1) *O conjunto Y é topologicamente fechado*[8] *em X_K.*

(2) *A restrição de ordens $\rho : Y \to X/S_d$ é um homeomorfismo.*

[8]Topologicamente fechado significa, simplesmente, fechado segundo a topologia de Harrison (cf. página 115) definida em X_K.

Demonstração. Lembrando que existe uma bijeção $\rho_\lambda : X_{K_\lambda} \to X_\lambda$, vamos mostrar que a restrição $\rho : Y_\lambda \to X_\lambda$, dada por $Q \mapsto Q \cap F$ também é uma bijeção. Com efeito, se $P \in X_\lambda$ existe $P_\lambda = \rho_\lambda^{-1}(P) \cap K \in Y_\lambda$ tal que $P_\lambda \cap F = P$, logo ρ é sobrejetiva. Para verificar a injetividade de ρ, consideremos $Q_1, Q_2 \in Y_\lambda$ tais que $Q_1 \cap F = Q_2 \cap F = P \in X_\lambda$. Como $Q_1, Q_2 \in Y_\lambda$, existem $Q_1', Q_2' \in X_{K_\lambda}$ tal que $Q_1' \cap K = Q_1$ e $Q_2' \cap K = Q_2$, logo $Q_1' \cap F = P = Q_2' \cap F$, ou seja, $\rho_\lambda(Q_1') = P = \rho_\lambda(Q_2')$. Sendo ρ_λ injetiva, temos $Q_1' = Q_2'$ e, conseqüentemente, $Q_1 = Q_1' \cap K = Q_2' \cap K = Q_2$.

Uma vez que Y e X/S_d são reuniões disjuntas dos Y_λ e X_λ, respectivamente, com $\lambda \in \Lambda$, e a restrição de ordens estabelece uma bijeção entre Y_λ e X_λ, para cada $\lambda \in \Lambda$, fica claro que a restrição $\rho : Y \to X/S_d$, $P \mapsto P \cap F$, é uma bijeção.

Vamos à demonstração dos itens do Lema.

(1) A restrição $X_{K_\lambda} \to X_K$, dada por $P \mapsto P \cap K$, é contínua e, por serem espaços de ordens, X_{K_λ}, X_K são compactos (cf. página 115). Logo, a imagem Y_λ dessa restrição é um compacto em X_K, em particular, é topologicamente fechada em X_K.

Para mostramos que Y é fechado em X_K é suficiente verificarmos que toda cobertura de Y formada por abertos básicos do tipo $H_K(x) = \{P \in X_K \mid x \in P\}$, com $x \in \dot{K}$, tem subcobertura finita. Consideremos, então, uma cobertura

$$Y = \bigcup_{i \in I} H_K(a_i), \quad \text{com } a_i \in \dot{K}. \tag{5.3.8}$$

Como cada $Y_\lambda \subset Y$ é compacto, existe $I_\lambda \subset I$ *finito* tal que

$$Y_\lambda \subset \bigcup_{i \in I_\lambda} H_K(a_i).$$

Uma vez que $K \subset K_\lambda$ e vale o item (5) do Teorema 5.21, para cada $i \in I_\lambda$ existem $b_i \in \dot{F}$ e $c_i \in \dot{K}_\lambda$ tais que $a_i = b_i c_i^2$. Podemos, então, escrever $c_i^2 = a_i b_i^{-1} \in \dot{K}_\lambda^2 \cap \dot{K}$ e isso implica que $Y_\lambda \subset H_K(c_i^2)$, para todo $i \in I_\lambda$. Logo $H_K(b_i) \cap Y_\lambda \subset H_K(b_i) \cap H_K(c_i^2) \subset H_K(a_i)$. Simetricamente, $b_i = a_i(c_i^{-1})^2$ e $H_K(c_i^2) = H_K((c_i^{-1})^2)$ implicam que $H_K(a_i) \cap Y_\lambda \subset H_K(b_i)$. Portanto,

$$H_K(a_i) \cap Y_\lambda = H_K(b_i) \cap Y_\lambda, \quad \text{para todo } \ i \in I_\lambda \text{ , com } \ \lambda \in \Lambda \text{ arbitrário.} \tag{5.3.9}$$

Dessa forma, a partir a equação (5.3.8), obtemos:

$$Y_\lambda = \bigcup_{i \in I_\lambda} H_K(b_i) \cap Y_\lambda,$$

para cada $\lambda \in \Lambda$. Como vimos no início da demonstração, a restrição de ordens ρ é uma bijeção de Y_λ sobre X_λ. Como $b_i \in \dot{F}$ para cada $i \in I_\lambda$ e $\lambda \in \Lambda$ arbitrário, temos:

$$X_\lambda = \bigcup_{i \in I_\lambda} \rho(H_K(b_i) \cap Y_\lambda) = \bigcup_{i \in I_\lambda} H_F(b_i) \cap X_\lambda.$$

Uma vez que $X/S_d = \bigcup_{\lambda \in \Lambda} X_\lambda$, obtemos:

$$X/S_d \subset \bigcup_{\lambda \in \Lambda} \left(\bigcup_{i \in I_\lambda} H_F(b_i) \right).$$

Sendo X/S_d compacto, existe $\Lambda' \subset \Lambda$ *finito* tal que

$$X/S_d \subset \bigcup_{\lambda \in \Lambda'} \left(\bigcup_{i \in I_\lambda} H_F(b_i) \right).$$

Agora, a bijeção entre Y e X/S_d, dada pela restrição de ordens, garante que

$$Y \subset \bigcup_{\lambda \in \Lambda'} \left(\bigcup_{i \in I_\lambda} H_K(b_i) \right).$$

Combinando-se a inclusão acima com a igualdade dada em (5.3.9), obtemos

$$Y \subset \bigcup_{\lambda \in \Lambda'} \left(\bigcup_{i \in I_\lambda} H_K(a_i) \right)$$

como queríamos.

(2) Como já vimos no início da demonstração, $\rho : Y \to X/S_d$, $P \mapsto P \cap F$, é uma bijeção. Por outro lado, sendo Y compacto e X/S_d Hausdorff, a aplicação $\rho : Y \to X/S_d$ é fechada[9], isto é, se $F \subset Y$ é fechado, então $\rho(F) \subset X/S_d$ é fechado. Assim, a inversa $\rho^{-1} : X/S_d \to Y$ é contínua. Pela Observação 5.7, ρ^{-1} é um homeomorfismo, logo ρ também é um homeomorfismo. ■

Dessa forma, todas as condições do Teorema 5.6 são satisfeitas. Temos então o seguinte resultado:

Teorema 5.23 *Mantendo as notações estabelecidas e lembrando que estamos supondo* $\dot{F} = R_d \cdot S_d$*, temos que a extensão* $K|F$ *definida em* (5.3.6) *satisfaz as seguintes propriedades:*

[9]Citamos novamente James Dugundji, *Topology*, Teorema 2.1 (1), p. 226 como referência para este resultado da topologia geral.

(1) *K é pitagórico.*

(2) *A restrição de ordens $\rho : X_K \to X/S_d$ é um homeomorfismo.*

(3) *Valem os seguintes isomorfismos de grupos: $R_d/\dot{F}^2 \simeq \dot{F}/S_d \simeq \dot{K}/\dot{K}^2$.*

Demonstração. A maior parte das afirmações já foi demonstrada. Devemos notar apenas que, de acordo com o Teorema 5.6, o homomorfismo canônico $\varphi : \dot{F}/S_d \to \dot{K}/\dot{K}^2$ é um isomorfismo e $Y = X_K$. Como já verificamos anteriormente, $\rho : Y \to X/S_d$ é um homeomorfismo, logo a igualdade $Y = X_K$ garante que vale (2). Para completar a demonstração, notemos que a hipótese $\dot{F} = R_d \cdot S_d$ e o item (2) do Corolário 3.14 implicam que $\dot{F}/S_d = R_d \cdot S_d/S_d \simeq R_d/R_d \cap S_d = R_d/\dot{F}^2$. ■

5.4 Teorema de Estrutura para Anéis de Witt

Primeiramente, relembremos algumas hipóteses importantes: como antes, F denota um corpo formalmente real e não pitagórico com um elemento rígido d tal que $d \notin \sum \dot{F}^2$. De acordo com (3.2.1), essas hipóteses implicam $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$. O Corolário 4.20 e a Proposição 4.23 garantem a existência de um anel de valorização A associado a d. Finalmente, R_d e S_d continuarão a denotar os radicais associados a d.

Supondo que $R_d \cdot S_d = \dot{F}$, iremos obter, usando o anel de valorização A associado a d, uma decomposição do anel de Witt $W(F)$ como produto (fibrado, veja a página 71) de anéis de Witt de extensões $H|F$ e $K|F$ contidas no fecho quadrático $F(2)$, de tal modo que $W(H)$ e $W(K)$ têm estruturas mais simples do que $W(F)$. Veja o Teorema 5.26.

Quanto às hipóteses, devemos observar que a hipótese $d \notin \sum \dot{F}^2$ (mais forte do que $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$) é essencial na demonstração do Corolário 3.18, que garante que o elemento d é T_d-birígido. Logo, precisamos desta hipótese para garantir, pelo Corolário 4.20, a existência do anel de valorização A associado a d. Por outro lado, $R_d \cdot S_d = \dot{F}$ é exatamente o item (2) da Proposição 5.4. Isso significa, em particular, que podemos substitui-la por

$$v_A(S_d) = \Gamma_A \text{ e } \overline{S}_d^{\times} = \dot{k}_A \tag{5.4.1}$$

Alguns dos resultados a seguir não dependem dessa hipótese. Assim, não a assumiremos *a priori*, mencionando-a explicitamente nos pontos onde ela for utilizada.

Fixemos uma 2-henselização (H, A_H) de (F, A) (veja a página 52 e também a observação da página 53). Vamos repetir para A_H a notação que usamos para anéis de valorização. No entanto, como a henselização estará fixada daqui por diante omitiremos, por uma questão de simplicidade, os subescritos, isto é, usaremos $\mathfrak{m} = \mathfrak{m}_H$, $\Gamma = \Gamma_H$, $v = v_H$, $k = k_H$, etc., para o ideal maximal, o grupo de valores, a valorização associada, o corpo de resíduos, etc. Observemos que A_H tem extensão única para o fecho quadrático $F(2)$ e car $k \neq 2$, pois car $k_A \neq 2$. Logo, pela Proposição 4.11, $1 + \mathfrak{m} \subset \dot{H}^2$.

Na seção anterior (Teorema 5.23) obtivemos uma extensão $K|F$ que "trivializa" S_d, isto é, tal que $\dot{K}^2 \cap F = S_d$ e "preserva" R_d, isto é, tal que $\dot{K}/\dot{K}^2 \simeq R_d/\dot{F}^2$. A seguir, obteremos uma 2-extensão $H|F$ que tem comportamento similar, mas inverte os papéis de R_d e S_d:

Proposição 5.24 *Seja F um corpo com um elemento rígido d satisfazendo a hipótese $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$ e H como definido acima. Se valem as condições de* (5.4.1)*, então $\dot{H}^2 \cap \dot{F} = R_d$ e $S_d/\dot{F}^2 \overset{\varphi}{\simeq} \dot{H}/\dot{H}^2$ como grupos (em particular, $\dot{H} = S_d \cdot \dot{H}^2$).*

Demonstração. Pelo que vimos acima, $1 + \mathfrak{m} \subset \dot{H}^2$. Logo, $R_d = (1 + \mathfrak{m}_A)\dot{F}^2 \subset (1 + \mathfrak{m})\dot{H}^2 \cap \dot{F} \subset \dot{H}^2 \cap \dot{F}$. Para mostrar a outra inclusão, usaremos o fato de (H, A_H) ser uma extensão *imediata* de (F, A), isto é, $k_A = k$ e $\Gamma_A = \Gamma$.

Seja $x \in \dot{H}^2 \cap \dot{F}$. Podemos escrever $x = y^2$, onde $y \in \dot{H}$. Como $\Gamma = \Gamma_A$, existe $w \in \dot{F}$ tal que $v(y) = v(w)$, onde v denota a valorização associada a A_H. Assim $v(w^{-1}y) = 0$, ou seja, $w^{-1}y \in A_H^*$. Como $k = k_A$, existe $u \in A^*$ tal que $\pi(u) = \pi(w^{-1}y)$, onde $\pi = \pi_H$ é a projeção canônica associada a A_H. Portanto, $\pi(u^{-1}w^{-1}y) = 1$ e daí, $u^{-1}w^{-1}y \in 1 + \mathfrak{m}$. Segue-se que $\dot{F} \ni u^{-2}w^{-2}x = (u^{-1}w^{-1}y)^2 \in (1 + \mathfrak{m}) \cap \dot{F} = 1 + \mathfrak{m}_A$ e isto implica que $x \in (1 + \mathfrak{m}_A)\dot{F}^2 = R_d$.

A seguir, demonstraremos que o homomorfismo de grupos $\varphi : S_d/\dot{F}^2 \to \dot{H}/\dot{H}^2$ dado por $\varphi(x\dot{F}^2) = x\dot{H}^2$ é um isomorfismo. Temos, inicialmente, $y\dot{F}^2 \in \ker\varphi$ se, e somente se, $y \in \dot{H}^2 \cap S_d = (\dot{H}^2 \cap \dot{F}) \cap S_d = R_d \cap S_d = \dot{F}^2$. Isso mostra que φ é injetivo.

Para mostrar a sobrejetividade de φ usamos novamente o fato de $H|F$ ser uma extensão imediata. Não entraremos em detalhes, pois tudo é similar ao que já foi feito acima. Dado $h \in \dot{H}$, existem $z \in \dot{F}$ e $u \in A^* \subset \dot{F}$ tais que $u^{-1}z^{-1}h = w \in 1 + \mathfrak{m}$. Logo, $h = wx$, onde $w \in 1 + \mathfrak{m}$ e $x = uz \in \dot{F}$. Pela Proposição 5.4, (5.4.1) é equivalente a $\dot{F} = R_d \cdot S_d$. Logo, existem $r \in R_d$ e $s \in S_d$ tais que $x = r \cdot s$. Assim, $h = wrs$ e isto implica $hs^{-1} = wr \in (1 + \mathfrak{m}) \cdot R_d \subset \dot{H}^2$ e, portanto, $h\dot{H}^2 = s\dot{H}^2$ e φ é sobrejetivo. ■

Exibimos a seguir um lema técnico que será utilizado na demonstração do Teorema 5.26 logo a seguir. Lembremos que (H, A_H) é uma henselização de (F, A).

Lema 5.25 *Seja $y \in A_H^*$. Se $z \in D_H\langle 1, -y\rangle \cap A_H$ e a forma $\langle 1, -\pi(y)\rangle$ é anisotrópica, então existe $b \in \dot{H}$ tal que $b^2 z \in A_H^*$ e $\pi(b^2 z) \in D_k\langle 1, -\pi(y)\rangle$.*

Demonstração. Podemos escrever $z = \alpha^2 - y\beta^2$, onde $\alpha, \beta \in H$. Seja v a valorização associada ao anel A_H. Temos dois casos a considerar:

Se $v(\alpha) \neq v(\beta)$, podemos supor sem perda de generalidade que $v(\alpha) < v(\beta)$. Logo, $v(\alpha^{-1}\beta) > 0$, isto é, $\alpha^{-1}\beta \in \mathfrak{m}$, onde $\mathfrak{m}$ é o ideal maximal de A_H. Como $y \in A_H$, temos $-y(\alpha^{-1}\beta)^2 \in \mathfrak{m}$. A partir de $z = \alpha^2(1 - y(\alpha^{-1}\beta)^2)$, vemos que $\alpha^{-2}z = 1 - y(\alpha^{-1}\beta)^2 \in 1 + \mathfrak{m}$. Escrevendo $b = \alpha^{-1}$, temos então $\pi(b^2 z) = 1 \in D_k\langle 1, -\pi(y)\rangle$.

Se $v(\alpha) = v(\beta)$, então $\beta \neq 0$. De fato, se $\beta = 0$ teríamos $\alpha = 0$, pois $v(\alpha) = v(\beta)$. Logo, $z = \alpha^2 - y\beta^2 = 0$, o que não é possível, pois $z \in D_H\langle 1, -y\rangle$. A igualdade $v(\alpha) = v(\beta)$ também implica que $\frac{\alpha}{\beta} \in A_H^*$. Logo $z = \beta^2\left(\left(\frac{\alpha}{\beta}\right)^2 - y\right)$, isto é, $\beta^{-2}z = (\frac{\alpha}{\beta})^2 - y$. Assim, $\pi(\beta^{-2}z) \in D_k\langle 1, -\pi(y)\rangle$. Basta, então, escolher $b = \beta^{-1} \in \dot{H}$. ■

Vamos, agora, enunciar e demonstrar o Teorema de estrutura para o anel de Witt do corpo F, satisfazendo nossas hipóteses.

Teorema 5.26 *Seja F um corpo com um elemento rígido $d \notin \sum \dot{F}^2$ e A o anel de valorização de F associado a d. Suponha que valem as condições de* (5.4.1)*:*

$$v_A(S_d) = \Gamma_A \quad e\ \overline{S}_d^{\times} = \dot{k}_A.$$

Então, a henselização H de (F, A) e a extensão $K|F$, dada pelo Teorema 5.23 *são tais que*

$$W(F) \simeq W(H) \times W(K),$$

sendo o isomorfismo induzido pelas inclusões $F \subset H$ e $F \subset K$.

Demonstração. As condições de (5.4.1) são equivalentes à condição (1) da Proposição 5.4:

$$\dot{F}/\dot{F}^2 \simeq R_d/\dot{F}^2 \times S_d/\dot{F}^2.$$

Pela Proposição 5.24 e o Teorema 5.23, obtemos:

$$\dot{F}/\dot{F}^2 \simeq \dot{H}/\dot{H}^2 \times \dot{K}/\dot{K}^2,$$

onde o isomorfismo acima é induzido pelas inclusões $F \subset H$ e $F \subset K$. Logo, vale a hipótese (1) do Teorema 5.1.

A seguir, mostraremos que, sob as condições que assumimos, vale a hipótese (2) do Teorema 5.1, ou seja, mostraremos que vale

$$(D_H\langle 1,-y\rangle \cap \dot{F}) \cap (D_K\langle 1,-y\rangle \cap \dot{F}) \subset D_F\langle 1,-y\rangle \quad \text{para todo} \quad y \in \dot{F} \tag{5.4.2}$$

Suponhamos, primeiro, que $y \in R_d$. Como K é pitagórico, temos

$$D_K\langle 1,-y\rangle = \bigcap_{P \in H_K(-y)} P,$$

onde $H_K(-y)$ é um aberto (e fechado) da topologia de Harrison (veja a página 115).

Se $P \in H_K(-y)$ então $P \cap F \in H_F(-y)$. Reciprocamente, se $Q \in H_F(-y)$, então $S_d \subset D_F\langle 1,-y\rangle \subset Q$ e, pelo item (2) do Teorema 5.23, a ordem Q estende-se a uma ordem P de K. Portanto,

$$D_K\langle 1,-y\rangle \cap F = \bigcap_{P \in H_K(-y)} (P \cap F) = \bigcap_{Q \in H_F(-y)} Q. \tag{5.4.3}$$

Pelo item (1) do Corolário 3.14, $y \in R_d$ implica que $D_F\langle 1,-y\rangle$ é uma pré-ordem. Mais ainda, $D_F\langle 1,-y\rangle$ é a menor pré-ordem de F que contém $-y$. Logo,

$$\bigcap_{Q \in H_F(-y)} Q = D_F\langle 1,-y\rangle. \tag{5.4.4}$$

Juntando as equações (5.4.3) e (5.4.4), temos a igualdade $D_K\langle 1,-y\rangle \cap F = D_F\langle 1,-y\rangle$. Em particular, obtemos a inclusão de (5.4.2) neste caso.

Suponhamos agora que $y \in \dot{F} \smallsetminus R_d$. Pela Proposição 5.24, temos $\dot{H}^2 \cap F = R_d$ e $\dot{H} = S_d \cdot \dot{H}^2$. Para $y \in \dot{F} \smallsetminus R_d$, temos então $y = sh^2$, onde $s \in S_d$ e $h \in \dot{H}$. Logo, $D_H\langle 1,-y\rangle = D_H\langle 1,-s\rangle$ e podemos assumir que $y \in S_d$. Vamos demonstrar que vale a inclusão de (5.4.2) dividindo o problema em dois casos:

Caso 1: $v(y) \notin 2\Gamma$. Isto implica que y é birígido em H, ou seja, vale a igualdade $D_H\langle 1,\pm y\rangle = \dot{H}^2 \cup \pm y\dot{H}^2$. Como $-1 \in \dot{H} = S_d \cdot \dot{H}^2$, existem $s \in S_d$ e $h \in \dot{H}$ tais que $-1 = sh^2$. Assim, $D_H\langle 1,-y\rangle = \dot{H}^2 \cup sy\dot{H}^2$ e $D_H\langle 1,-y\rangle \cap \dot{F} = (\dot{H}^2 \cap \dot{F}) \cup \underbrace{sy}_{\in \dot{F}}(\dot{H}^2 \cap \dot{F}) = R_d \cup syR_d$.

Agora, $-1 = sh^2$ implica $-s = (sh)^2 \in \dot{H}^2 \cap F = R_d$. Assim, $-s \in R_d \subset D_F\langle 1,-y\rangle$, pois $y \in S_d = \mathcal{R}(R_d)$ (veja a Proposição 3.19, item (4)). Temos, então: $-s \in D_F\langle 1,-y\rangle$,

o que implica $s \in D_F\langle -1, y\rangle$ e, daí, $sy \in yD_F\langle -1, y\rangle = D_F\langle -y, y^2\rangle = D_F\langle 1, -y\rangle$. De $y \in S_d$ obtemos $R_d \subset D_F\langle 1, -y\rangle$. Logo $R_d \cup syR_d \subset D_F\langle 1, -y\rangle$, como queríamos.

Caso 2: $v(y) \in 2\Gamma$. Neste caso, $y \in A_H^* \dot{H}^2$. Logo, $y = wh^2$, onde $w \in A_H^*$ e $h \in \dot{H}$. Como $D_H\langle 1, -y\rangle = D_H\langle 1, -w\rangle$, podemos supor desde o início que $y \in A_H^* \cap F = A^*$. Dado $x \in D_H\langle 1, -y\rangle \cap \dot{F}$, queremos mostrar que $x \in D_F\langle 1, -y\rangle$. Como $D_H\langle 1, -y\rangle \cap \dot{F}$ e $D_F\langle 1, -y\rangle$ são subgrupos de $\dot{F}$ contendo $\dot{F}^2$, podemos supor que $x \in A \subset A_H$, caso contrário, poderíamos trabalhar com x^{-1} no lugar de x. Afirmamos que $\langle 1, -\pi(y)\rangle$ é anisotrópica. De fato, se $\langle 1, -\pi(y)\rangle$ fosse isotrópica, teríamos $y \in \dot{k}_A^2$, logo $y \in (1 + \mathfrak{m}_A)\dot{F}^2 = R_d$, contrariando a escolha de y. Pelo Lema 5.25, existe $b \in \dot{H}$ tal que $\pi(b^2x) \in D_k\langle 1, -\pi(y)\rangle = D_{k_A}\langle 1, -\pi(y)\rangle$ (lembremos que $k = k_H = k_A$). Logo, existe $u \in D_F\langle 1, -y\rangle \cap A^*$ tal que $\pi(b^2x) = \pi(u)$, ou seja, $u^{-1}b^2x \in 1 + \mathfrak{m} \subset \dot{H}^2$. Daí, $u^{-1}x \in \dot{H}^2 \cap F = R_d$, pela Proposição 5.24. De acordo com o parágrafo imediatamente anterior ao "Caso 1" acima, estamos admitindo que $y \in S_d$. Portanto, $u^{-1}x \in R_d \subset D_F\langle 1, -y\rangle$ e isso implica $x \in D_F\langle 1, -y\rangle$, como queríamos.

Acabamos de provar que vale (5.4.2). Podemos então usar o Teorema 5.1 para garantir a decomposição $W(F) \simeq W(H) \times W(K)$, onde o isomorfismo é induzido pelas inclusões $F \subset H$ e $F \subset K$. ■

Na demonstração do Teorema 5.26 acima, fica evidente a dualidade "ordem-valorização" na decomposição do anel de Witt $W(F)$. Explicando melhor: os dois corpos que realizam a decomposição são uma henselização e um corpo pitagórico para onde um conjunto de ordens se estende de modo único.

O Lema 5.27 abaixo estabelece a estrutura do anel de Witt de um corpo munido de um anel de valorização 2-henseliano.

Lema 5.27 *Dado um corpo H, suponhamos que existe um anel de valorização 2-henseliano A_H de H, com grupo de valores Γ e corpo de resíduos k. Então $W(H)$ é isomorfo ao anel de grupo $W(k)[G]$, onde $G \simeq \Gamma/2\Gamma$.*

O Lema 5.27 é a generalização de um resultado clássico de T.A. Springer e sua demonstração segue-se do Corolário 4.7 e das observações no início da página 37 de [22].

Obtida a decomposição de $W(F)$ como produto de anéis de Witt de extensões $H|F$ e $K|F$, devemos agora destacar as informações que temos sobre a estrutura de cada um dos "fatores": $W(H)$ e $W(K)$. Para não sobrecarregar o Teorema 5.26, preferimos destacar essas informações no Corolário 5.28 abaixo.

Corolário 5.28 *Admitindo que valem todas as hipóteses do Teorema* 5.26*, temos a decomposição*

$$W(F) \simeq W(H) \times W(K),$$

onde $W(H) \simeq W(k_A)[G]$ *é um anel de grupo, com* k_A *o corpo de resíduos do anel de valorização* A *associado a* d*,* $G \simeq \Gamma_A/2\Gamma_A$ *e* Γ_A *grupo de valores relativo a* A*. Mais ainda, como* K *é pitagórico, o anel* $W(K)$ *é livre de torção.*

Demonstração. A decomposição $W(F) \simeq W(H) \times W(K)$ é o resultado do Teorema 5.26. Como (H, A_H) é uma 2-henselização de (F, A) temos, pelo Lema 5.27, que $W(H) \simeq W(k)[G]$, onde k é o corpo de resíduos e Γ é o grupo de valores do anel de valorização A_H e $G \simeq \Gamma/2\Gamma$. Como $H|F$ é uma extensão imediata, temos $k = k_A$ e $\Gamma = \Gamma_A$. Logo, $W(H) \simeq W(k_A)[G]$ e $G \simeq \Gamma_A/2\Gamma_A$.

Finalmente, como K é um corpo formalmente real e pitagórico, seu grupo de Witt $W(K)$ é livre de torção (cf. Scharlau [31], Teorema 4.10, página 43 e Observação 4.11, página 44). ■

Exibimos, na página 21, Exemplo 3.9, um corpo admitindo um elemento rígido que não é birígido. No entanto, o corpo exibido nesse exemplo é pitagórico. A seguir exibimos um exemplo de corpo formalmente real e *não pitagórico*, admitindo um elemento rígido que não é birígido.

Exemplo 5.29 *Um corpo formalmente real e não pitagórico admitindo um elemento rígido que não é birígido.*

Seja F um corpo formalmente real e não pitagórico. Fixada uma pré-ordem T de F, suponhamos que $\mathcal{R}(T) = \bigcap_{t\in T} D\langle 1, -t\rangle \neq \dot{F}^2$ e que exista um anel de valorização A de F que seja T-henseliano, com corpo de resíduos k_A formalmente real e com $v_A(T) \neq 2\Gamma_A$.

Se denotarmos $R = (1 + \mathfrak{m}_A)\dot{F}^2$, então, pela Proposição 4.9, $R \cap T = \dot{F}^2$. Seja $d \in T$ tal que $v_A(d) \notin 2\Gamma_A$. De modo análogo ao que fizemos no Exemplo 3.7 da página 20 ou na demonstração do Corolário 3.14, item (3), podemos concluir que d é R-birígido. Mais ainda, como $d \in T$

$$D\langle 1, d\rangle \subset (R + dR) \cap T = (R \cup dR) \cap T = (R \cap T) \cup d(R \cap T) = \dot{F}^2 \cup d\dot{F}^2$$

o que mostra que d é rígido.

A seguir, mostraremos que $-d$ não é rígido. Primeiro, como $d \in T$, temos $\mathcal{R}(T) \subset D\langle 1, -d\rangle$. Supondo, por absurdo, que $-d$ fosse rígido, teríamos $\mathcal{R}(T) \subset D\langle 1, -d\rangle =$

$\dot{F}^2 \cup -d\dot{F}^2$. Se $\mathcal{R}(T) \cap -d\dot{F}^2 \neq \emptyset$, então $-d \in \mathcal{R}(T)$. Logo, $-d \in D\langle 1, -t\rangle$, para todo $t \in T$, isto é, $T \subset D\langle 1, d\rangle = \dot{F}^2 \cup d\dot{F}^2$, pois d é rígido. Como $\sum \dot{F}^2 \subset T \subset \dot{F}^2 \cup d\dot{F}^2$ e $\sum \dot{F}^2 \not\subset \dot{F}^2$, pois F não é pitagórico, teríamos $d\dot{F}^2 \cap \sum \dot{F}^2 \neq \emptyset$, ou seja, $d \in \sum \dot{F}^2$. Como k_A é formalmente real teríamos, pelo Lema 3.7, página 23, de [22], que $v_A(d) \in v_A(\sum \dot{F}^2) = 2\Gamma_A$, contrariando a escolha de d. Assim, $\mathcal{R}(T) \cap -d\dot{F}^2 = \emptyset$ e $\mathcal{R}(T) = \dot{F}^2$, contrariando nossa hipótese. Portanto, $-d$ não é rígido.

Para produzir um anel de valorização satisfazendo as condições impostas no Exemplo 5.29, podemos proceder da seguinte maneira. Primeiro, tomemos um corpo formalmente real L munido de um anel de valorização B tal que k_B é formalmente real e $\Gamma_B \neq 2\Gamma_B$. Fixemos uma pré-ordem S de L e consideremos o S-fecho L_S de L (veja a Definição 2.8). Tomemos então (F, A) como sendo uma S-henselização de (L, B) (veja a página 52) e $T = \dot{L}_S^2 \cap F$. Notemos que o T-fecho de F é igual ao S-fecho de L. De fato, F_T é pitagórico e $\dot{F}_T^2 \cap L = (\dot{F}_T^2 \cap F) \cap L = T \cap L = S$, logo $L_S \subseteq F_T$. Por outro lado, L_S é pitagórico e $\dot{L}_S^2 \cap F = T$ (por definição), logo $F_T \subseteq L_S$. Vale portanto a igualdade $L_S = F_T$ e o anel de valorização A é T-henseliano. Como a extensão $(L, B) \subset (F, A)$ é imediata, temos $k_A = k_B$ formalmente real e $\Gamma_A \neq 2\Gamma_A$, pois $\Gamma_A = \Gamma_B$.

5.5 O caso $d \in \sum \dot{F}^2$

No que segue usaremos, como de costume, a letra d para designar um elemento do corpo F que é rígido e não é birígido. No decorrer do trabalho, mantivemos a hipótese $d \notin \sum \dot{F}^2$. Essa hipótese é necessária para provarmos, usando o Lema 3.6, que T_d é pré-ordem (Proposição 3.17) e que d é T_d-birígido (Corolário 3.18). Portanto, é uma hipótese essencial para a construção do anel de valorização associado, feita no Capítulo 4, e para a conseqüente decomposição do anel de Witt obtida no Teorema 5.26.

Como vimos na página 28, se F não é pitagórico e $d \notin \sum \dot{F}^2$ então $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$. No que segue, **continuamos a admitir que F não é pitagórico e admitimos também que $\sum \dot{F}^2 \not\subset \dot{F}^2 \cup d\dot{F}^2$, mas passamos a assumir que $d \in \sum \dot{F}^2$.** Veremos a seguir que neste caso também há uma decomposição de $W(F)$ como no Teorema 5.26.

Primeiramente, se $d \in \sum \dot{F}^2$, temos $R_d = D\langle 1, -d\rangle \cap R_0 = R_0$, onde $R_0 = \bigcap_{s \in \sum \dot{F}^2} D\langle 1, -s\rangle$ como no item (3) da Proposição 3.19. Recordemos a notação, introduzida na página 39,

$$A_\pi(F) = \{x \in \sum \dot{F}^2 \mid x \text{ não é rígido}\}.$$

Lembremos ainda que, por um resultado de [13] citado nessa mesma página, $A_\pi(F)$ é um subgrupo de $\sum \dot{F}^2$.

Uma vez que $d \in \sum \dot{F}^2$ é rígido, temos $(\sum \dot{F}^2 : A_\pi(F)) \geq 2$. De acordo com [14], Teorema 2.8 e Proposição 3.2, se

$$(\sum \dot{F}^2 : A_\pi(F)) > 2$$
$$\text{ou} \tag{5.5.1}$$
$$(\sum \dot{F}^2 : A_\pi(F)) = 2 \quad \text{e} \quad (\sum \dot{F}^2 : \dot{F}^2) = 4,$$

existe um anel de valorização $\mathcal{O}$ de F com $1 + \mathfrak{m}_\mathcal{O} \subset R_0$ e corpo de resíduos $k_\mathcal{O}$ não formalmente real e com característica diferente de 2. Como nossas hipóteses implicam que $A_\pi(F) \neq \sum \dot{F}^2$ e $(\sum \dot{F}^2 : \dot{F}^2) > 2$, o Teorema 2.7 de [14] garante que

$$R_0 = (1 + \mathfrak{m}_\mathcal{O})\dot{F}^2.$$

A partir daqui, passaremos a supor que vale uma das condições de (5.5.1).

Notemos que vários resultados do Capítulo 3 continuam válidos. Por exemplo, todas as hipóteses do Corolário 3.14 continuam válidas. Logo, podemos afirmar que

(1) Para todo $t \in R_0 \smallsetminus \dot{F}^2$, $D\langle 1, -t\rangle$ é uma pré-ordem de F.

(2) d é R_0-birígido.

A presença de um elemento rígido d em $\sum \dot{F}^2$ tem conseqüências sobre a estrutura de $\sum \dot{F}^2$. Mais precisamente, pelo Lema 1.7 de [5], existe um elemento $w \in \sum \dot{F}^2$ tal que $\sum \dot{F}^2 = D\langle 1, w\rangle$. Assim, para todo $s \in \sum \dot{F}^2$ temos $s \in D\langle 1, w\rangle$, ou seja, $-w \in D\langle 1, -s\rangle$, para todo $s \in \sum \dot{F}^2$. Em outras palavras, $-w \in \bigcap_{s \in \sum \dot{F}^2} D\langle 1, -s\rangle = R_0$. Portanto, $-\sum \dot{F}^2 \cap R_0 \neq \emptyset$ e isso mostra que, ao contrário do que ocorre no caso em que d não é soma de quadrados, não existem ordens de F contendo R_0.

Como fizemos na página 52, podemos tomar uma 2-henselização $(H, \mathcal{O}')$ de $(F, \mathcal{O})$. Pela Proposição 5.24, temos $\dot{H}^2 \cap \dot{F} = R_0$, $\dot{H}/\dot{H}^2 \simeq S_0/\dot{F}^2$, onde $S_0 = \mathcal{R}(R_0) = \bigcap_{t \in R_0} D\langle 1, -t\rangle$. Em particular, o corpo H não é formalmente real. De fato, se Q fosse uma ordem de H, então $\dot{H}^2 \subset Q$, logo $R_0 = \dot{H}^2 \cap F \subset Q \cap F$, com $Q \cap F$ ordem de F. Como não existem ordens de F contendo R_0, H não pode ser formalmente real. Logo, o corpo de resíduos $k_\mathcal{O}$ também não pode ser formalmente real e $\overline{\sum \dot{F}^2} = \dot{k}_\mathcal{O}$.

Outra conseqüência de $\sum \dot{F}^2 = D\langle 1, -z\rangle$, com $z = -w \in R_d$ é que a pré-ordem $S_0 = \mathcal{R}(R_0) = \bigcap_{t \in R_0} D\langle 1, -t\rangle$ satisfaz $S_0 \subset D\langle 1, -z\rangle = \sum \dot{F}^2$. Logo $S_0 = \sum \dot{F}^2$. De acordo com o que observamos acima, $\overline{\mathcal{R}(R_0)} = \dot{k}_\mathcal{O}$.

No presente contexto, vale a seguinte reformulação da Proposição 5.4:

Proposição 5.30 *Seja F um corpo, $d \in \sum \dot{F}^2$ um elemento rígido de F tal que $\sum \dot{F}^2 \not\subset D_F\langle 1, d\rangle$ e $\mathcal{O}$ um anel de valorização tal que $R_0 = (1 + \mathfrak{m}_{\mathcal{O}})\dot{F}^2$, com corpo de resíduos $k_{\mathcal{O}}$ e grupo de valores $\Gamma_{\mathcal{O}}$. As seguintes afirmações são equivalentes:*

(1) $\dot{F}/\dot{F}^2 \simeq R_0/\dot{F}^2 \times \sum \dot{F}^2/\dot{F}^2$ *(produto direto de grupos abelianos).*

(2) $R_0 \cdot \sum \dot{F}^2 = \dot{F}$.

(3) $v_{\mathcal{O}}(\sum \dot{F}^2) = \Gamma_{\mathcal{O}}$.

Demonstração. Com as observações feitas nos parágrafos logo acima, as equivalências da Proposição têm as mesmas demonstrações daquelas da Proposição 5.4. Vale notar que a condição geral (5.0.1) pode ser reescrita, no nosso caso, como em (3) pois, como observamos acima, $\overline{\mathcal{R}(R_0)} = \overline{\sum \dot{F}^2} = \dot{k}_{\mathcal{O}}$ vale sempre. ■

A partir desse ponto vamos supor que valem as condições equivalentes da Proposição 5.30.

Pelo Teorema 5.23, existe uma 2-extensão pitagórica $K|F$, contendo o fecho pitagórico F_π de F, tal que $R_0/\dot{F}^2 \simeq \dot{K}/\dot{K}^2$ e $\dot{K}^2 \cap \dot{F} = S_0 = \sum \dot{F}^2$. Além disso, os espaços de ordens X_F e X_K são homeomorfos.

Dessa forma, obtemos um teorema análogo ao Teorema 5.26 para o caso $d \in \sum \dot{F}^2$, cuja demonstração é inteiramente similar. Vale ressaltar que, na presente situação, como H não é formalmente real, o único ideal primo de $W(H)$ é IH, logo $W(H)$ é um anel local (cf. [23], Corolário 7.8, página 280 ou [31], Teorema 7.9, página 58).

Teorema 5.31 *Seja F um corpo com um elemento rígido $d \in \sum \dot{F}^2$. Suponhamos que vale uma das condições de* (5.5.1) *e consideremos $\mathcal{O}$ o anel de valorização de F tal que $R_0 = (1+\mathfrak{m}_{\mathcal{O}})\dot{F}^2$. Suponha que vale uma das condições equivalentes da Proposição* 5.30*. Então, as extensões $H|F$ e $K|F$ dadas acima são tais que*

$$W(F) \simeq W(H) \times W(K),$$

sendo o isomorfismo induzido pelas inclusões $F \subset H$ e $F \subset K$. Mais ainda, $W(H) \simeq W(k_{\mathcal{O}})[G]$ é um anel de grupo local com $k_{\mathcal{O}}$ corpo de resíduos de $\mathcal{O}$, $G \simeq \Gamma_{\mathcal{O}}/2\Gamma_{\mathcal{O}}$ e $W(K)$ é um anel de Witt livre de torção.

Demonstração. Veja a demonstração do Teorema 5.26. ■

Apêndice A

Breve resumo sobre a teoria de Galois infinita

Resumimos abaixo algumas informações essenciais sobre a teoria de Galois no caso em que as extensões têm grau infinito. O material exposto neste apêndice pode ser encontrado com maior detalhe por exemplo no Capítulo I de [30], em [35], Capítulo 3 ou ainda [29], Capítulo VII.

O teorema fundamental da teoria de Galois, no caso finito, estabelece uma correspondência bijetiva entre os subcorpos de uma extensão galoisiana *finita* $K|F$ (isto é, os subcorpos de K que contêm F) e os subgrupos do grupo de Galois $G(K|F)$, dada da seguinte maneira: se $\mathcal{G} = \{H \,|\, H \text{ é subgrupo de } G\}$ e $\mathcal{K} = \{L \,|\, L \text{ é corpo, } F \subset L \subset K\}$, definimos $\Phi : \mathcal{G} \to \mathcal{K}$ dada por $\Phi(H) = \{x \in K \,|\, \sigma(x) = x, \forall \sigma \in H\} = K^H$ e $\Psi : \mathcal{K} \to \mathcal{G}$, dada por $\Psi(L) = \{\sigma \in G \,|\, \sigma(x) = x, \forall x \in L\} = G(K|L)$. Então $\Psi = \Phi^{-1}$.

Por outro lado, se $K|F$ é uma extensão *infinita*, essa correspondência pode deixar de ser bijetiva, como mostra o exemplo a seguir.

Exemplo. [30], p.3 Sejam $p \neq q \neq 2$ números primos. Seja $F = \mathbb{F}_p$ e

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots$$

tal que F_i é a única extensão de F de grau $[F_i : F] = q^i$. Definimos

$$N = \bigcup_{i=1}^{\infty} F_i.$$

Temos, então, $F_i = \{x \in N \,|\, x^{p^{q^i}} - x = 0\}$. Seja $G = G(N|F)$.

Se $\varphi : N \to N$ é o automorfismo de Frobenius, dado por $\varphi(x) = x^p$, e $H = \{\varphi^n \mid n \in \mathbb{Z}\}$, vamos provar que $\Phi(H) = \Phi(G)$ e $H \neq G$, o que mostra que Φ não é injetiva.

Primeiramente, dado $x \in N$ tal que $\sigma(x) = x$, para todo $\sigma \in H$, temos, em particular, que $\varphi(x) = x$, ou seja, $x^p = x$. Logo, $x \in F$, o que mostra que $\Phi(H) = F = \Phi(G)$.

Para mostrar que $H \neq G$, devemos construir um F-automorfismo σ de N que não pertença a H. Para cada $i = 1, 2, \ldots$, seja $k_i = 1 + q + \cdots + q^{i-1}$. Consideremos o F-automorfismo φ^{k_i} de N. Uma vez que $\varphi^{k_{i+1}}|_{F_i} = \varphi^{k_i}|_{F_i}$, podemos definir um F-automorfismo $\sigma : N \to N$, dado por $\sigma(x) = \varphi^{k_i}(x)$, se $x \in F_i$. Supondo $\sigma \in H$, teríamos $\sigma = \varphi^n$ e $\sigma|_{F_i} = \varphi^n|_{F_i} = \varphi^{k_i}|_{F_i}$, o que implicaria $n \equiv k_i (\mod q^i)$, para cada i, pois $G(F_i|F)$ é um grupo cíclico gerado por $\varphi|_{F_i}$. Multiplicando essa congruência por $q - 1$, obteríamos

$$(q-1)n \equiv -1 (\mod q^i)$$

para cada i, o que é impossível, se $q \neq 2$. Portanto, $\sigma \in G \setminus H$.

No exemplo acima, apesar de $\sigma \in G \setminus H$, podemos obter "aproximações" de σ pelos homomorfismos $\varphi^{k_i} \in H$, pois $\sigma|_{F_i} = \varphi^{k_i}|_{F_i}$ e as subextensões $F \subset F_i \subset N$ tornam-se maiores, conforme i cresce. Isso nos leva à idéia de introduzir uma topologia em G de tal modo que $\sigma = \lim \varphi^{k_i}$. Assim σ, embora não pertença a H, pertenceria ao fecho de H, relativo à essa topologia, o que sugere uma correspondência bijetiva entre os subcorpos de $K|F$ e os subgrupos *fechados* de G. Essa é a topologia de Krull, que introduziremos a seguir.

Uma extensão $K|F$ (finita ou infinita) é dita *galoisiana* se, para cada polinômio irredutível $f \in F[X]$, o número de raízes distintas de f em K é 0 ou igual ao grau de f. Se $K|F$ é uma extensão galoisiana e $G = G(K|F)$, então

$$S = \{G(K|L) \,:\, L|F \text{ é extensão normal finita e } F \subset L \subset K\} \tag{A.0.1}$$

é uma base de abertos do elemento $1 \in G$. A topologia definida por S é chamada *topologia de Krull* de G.

Se $K|F$ é uma extensão galoisiana finita, então a topologia de Krull de $G(K|F)$ é a topologia discreta.

Se $\sigma, \tau \in G(K|F)$, então $\tau \in \sigma G(K|L)$ se, e somente se, $\sigma^{-1}\tau \in G(K|L)$, isto é, se, e somente se, $\sigma|_L = \tau|_L$. Logo, dois elementos de $G(K|F)$ estão "próximos" se, e somente se, coincidem em um subcorpo grande $F \subset L \subset K$, onde $L|F$ é extensão finita.

Um *grupo topológico* é um espaço topológico que tem uma estrutura de grupo tal que a aplicação $(x, y) \mapsto xy^{-1}$ de $G \times G$ (com a topologia produto) para G é contínua.

Um grupo topológico G é dito *profinito* quando é Hausdorff[1], compacto[2] e totalmente desconexo[3].

É possível mostrar que todo grupo de Galois munido da topologia de Krull é Hausdorff, compacto e totalmente desconexo, logo é um grupo profinito. Reciprocamente, cada grupo profinito pode ser representado como grupo de Galois de alguma extensão de corpos.

A seguir, daremos uma caracterização importante de um grupo profinito em termos de um "limite projetivo" (cf. [29], página 122). Todo grupo profinito $G = G(K|F)$ (onde $K|F$ é uma extensão, possivelmente infinita) é limite projetivo de um sistema projetivo (sobre um conjunto dirigido) de grupos finitos, isto é,

$$G = \varprojlim G_L \tag{A.0.2}$$

Onde $G_L = G(L|F) \simeq G(K|F)/G(K|L)$ é um grupo finito (pois $L|F$ é extensão finita) para todo L.

De especial interesse para nós são os 2-*grupos profinitos*, também chamados *grupos pro*-2. Estes grupos são exatamente os grupos de Galois das 2-extensões $K|F$ (veja a definição na página 2). Os 2-grupos profinitos ocorrem naturalmente como grupos de Galois dos fechos pitagóricos $F_T|F$ (veja a Proposição 2.9). Convém mencionar que, para cada "classe" $\mathcal{C}$ de grupos finitos, podemos definir grupos pro-$\mathcal{C}$, mas não precisaremos de tal generalização aqui (para detalhes, o leitor interessado deve consultar [35], página 19).

Notemos que, por (A.0.2), se G é um p-grupo profinito, então $G = \varprojlim G_L$, onde $G_L = G(L|F)$ é um p-grupo (finito). Logo, $G = G(K|F)$, onde $K = \varinjlim L_i$, $L_i|F$ extensão finita, $K \subset F(p)$. Supondo que, dados $i, j \in I$, existe $k \in I$ tal que $L_i \cup L_j \subset L_k$, o limite injetivo $\varinjlim$ coincide com a reunião $\bigcup_{i\in I} L_i$.

Exemplos. (1) O grupo de Prüfer $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$, onde, dados $m, n \in \mathbb{Z}$, com $n|m$, definimos $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ como a projeção natural. Se $\mathbb{F}_p$ é o corpo finito com p elementos e $\overline{\mathbb{F}}_p$ é o seu fecho algébrico, então $G_{\mathbb{F}_p} = G(\overline{\mathbb{F}_p}|\mathbb{F}_p) = \varprojlim G(K_m|\mathbb{F}_p) = \varprojlim \mathbb{Z}/m\mathbb{Z} = \hat{\mathbb{Z}}$

[1]Um espaço topológico E é Hausdorff se, dados $x, y \in E$, com $x \neq y$, existem vizinhanças abertas $U \ni x$ e $V \ni y$ tais que $U \cap V = \emptyset$.

[2]Um espaço topológico Hausdorff E é compacto, quando toda cobertura aberta de E possui uma subcobertura finita.

[3]Um espaço topológico E é totalmente desconexo, quando, dado $x \in E$ a componente conexa de E que contém x é $\{x\}$.

(K_m é a extensão de grau m de $\mathbb{F}_p$).

(2) Se p é um número primo e $m, n \in \mathbb{N}$, com $m \leq n$, definimos $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ como sendo a projeção natural. Logo, existe o limite $\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$, o grupo aditivo dos inteiros p-ádicos.

Os grupos $\hat{\mathbb{Z}}$ e $\mathbb{Z}_p$ dos exemplos (1) e (2) acima são limites projetivos de grupos cíclicos. Tais grupos são ditos *pró-cíclicos*. Um grupo pró-cíclico G é topologicamente gerado por um único elemento $\sigma \in G$. Isso significa que G é o fecho de $\{\sigma^n \mid n \in \mathbb{Z}\}$.

A seguir, enunciaremos o Teorema Fundamental da Teoria de Galois, para extensões galoisianas (finitas ou) infinitas.

Teorema A.1 ([35], Teorema 3.2.1, p.49) *Seja $K|F$ uma extensão galoisiana (finita ou infinita). Então as aplicações*

$$\Psi : L \longmapsto G(K|L)$$

$$\Phi : H \longmapsto K^H$$

estabelecem uma correspondência biunívoca entre as subextensões $L|F$ de $K|F$ e os subgrupos fechados *de $G(K|F)$. Os subgrupos abertos de $G(K|F)$ correspondem exatamente às subextensões finitas de $K|F$.*

Apêndice B

Corpos Ordenados e Estudo de Pré-ordens

Neste parágrafo estudamos alguns fatos básicos sobre os corpos ordenados. O material a seguir é bem conhecido e pode ser encontrado em diversos livros. Mesmo assim, resolvemos incluí-lo por uma questão de conveniência para o leitor. As referências sobre o assunto que seguimos ao redigir as linhas seguintes foram os livros, [21], [22] e [27].

Notação: a seguir, usaremos livremente os símbolos $\dot{F} = F^{\times}$ para denotar o grupo multiplicativo $F \smallsetminus \{0\}$.

Uma *ordem* em um corpo F é um subconjunto $P \subseteq \dot{F}$ tal que:

(i) $P \neq \dot{F}$

(ii) $P + P \subset P$

(iii) $PP \subset P$

(iv) $P \cup (-P) = \dot{F}$

Um corpo F, munido de uma ordem P (notação: (F, P)), é dito *corpo ordenado*.

Observações:

(1) $\dot{F}^2 \subseteq P$. De fato, se $x \in \dot{F}$, então $x \in P$ ou $-x \in P$. Assim, $x^2 = xx = (-x)(-x) \in P$ (pelo item (iii)). Portanto, $\dot{F}^2 \subseteq P$. Pelo item (ii), vemos ainda

que $\sum \dot{F}^2 \subset P$, onde $\sum \dot{F}^2$ é o conjunto formado por todas as somas finitas não nulas de quadrados em F, isto é:

$$\sum \dot{F}^2 = \{\sum_{i=1}^{n} x_i^2 \neq 0 \,|\, n \in \mathbb{N}, x_i \in F\} \tag{B.0.1}$$

Denotamos ainda $\sum F^2 = \sum \dot{F}^2 \cup \{0\}$.

(2) O item (i) é equivalente a $-1 \notin P$. De fato, é claro que $-1 \notin P$ implica que $P \neq F$. Para a outra implicação, se $-1 \in P$, então, para todo $x \in \dot{F}$, podemos escrever $x = (\frac{x+1}{2})^2 + (-1)(\frac{x-1}{2})^2 \in F^2 + (-1)F^2 \subseteq P + PP \subseteq P$. Logo, $-1 \in P$ o que implica que $F \subseteq P$, isto é, $F = P$.

(3) $P \cap (-P) = \emptyset$. De fato, se existisse $x \in P \cap (-P)$, então $x \in P$ e $-x \in P$. Logo, $-1 = -xx^{-1} = -x\frac{x}{x^2} \in P$, o que não ocorre.

(4) Uma ordem P é um subgrupo de índice 2 em $\dot{F}$. Isto fica claro a partir de (iii) e (iv) e do seguinte fato: se $x \in P$, então $x^{-1} = x(\frac{1}{x})^2 \in P \cdot \dot{F}^2 \subset P$.

Vamos denotar o conjunto das ordens de um corpo F por X_F . Podemos introduzir uma topologia nesse conjunto, tomando como subbase de abertos a família dos *conjuntos de Harrison* :

$$H(x) := \{P \in X_F \,|\, x \in P\}, \text{ onde } x \in \dot{F}.$$

É possível mostrar que, com essa topologia, X_F torna-se um espaço *booleano* , ou seja, um espaço compacto, Hausdorff, e totalmente desconexo (cf. [23], Teorema 6.3, página 271).

Observação: Se $K|F$ é uma extensão de corpos, então $\rho : X_K \to X_F$ dada por $P \mapsto P \cap F$ é uma aplicação contínua. De fato, para cada $x \in \dot{F}$, $\rho^{-1}(H_F(x)) = H_K(x)$, onde o subescrito indica o corpo respectivo.

Dada uma ordem $P \in X_F$, escrevemos $x >_P y$ se $x - y \in P$. Dessa maneira, podemos falar em elementos positivos (aqueles em P) e em elementos negativos (aqueles em $-P$). Quando a ordem for clara do contexto, podemos escrever a desigualdade $>_P$ simplesmente como $>$.

Vamos introduzir, agora, um dos conceitos centrais no que se segue:

Definição B.1 *Uma* pré-ordem *em um corpo F é um subconjunto $T \subseteq \dot{F}$ tal que*

(i) $T \neq \dot{F}$

(ii) $\dot{F}^2 \subseteq T$

(iii) $T + T \subseteq T$

(iv) $TT \subseteq T$

De modo similar ao que foi feito na observação (1), podemos mostrar que a condição $T \neq \dot{F}$ pode ser substituida por $-1 \notin T$. Se $x \in T$, então $x^{-1} = (x^{-1})^2 x \in (\dot{F})^2 T \subseteq T$. Assim, T é um subgrupo de $\dot{F}$. O número $[\dot{F} : T] \leq \infty$ é chamado *índice* da pré-ordem T. Note que uma pré-ordem T é uma ordem se, e somente se, tem índice 2. De fato, pela observação (4) acima, toda ordem tem índice 2. Por outro lado, se T é uma pré-ordem e $[\dot{F} : T] = 2$, então existe $x \in \dot{F}$ tal que $\dot{F} = T \cup xT$. Como $-1 \in \dot{F}$ e $-1 \notin T$, temos $-1 \in xT$, o que implica $-1 = xt, t \in T$. Assim, $x = -t^{-1}$, donde $xT = -t^{-1}T = -T$.

Definição B.2 *Um corpo é dito* formalmente real *se, e somente se,* $-1 \notin \sum \dot{F}^2$.

Pela Definição B.1, um corpo é formalmente real se, e somente se, $\sum \dot{F}^2$ é uma pré-ordem de F. Neste caso, $\sum \dot{F}^2$ está contida em qualquer pré-ordem T, logo é a menor pré-ordem de F. $\sum \dot{F}^2$ é chamada *pré-ordem fraca* de F.

Dados uma pré-ordem T de F e um elemento $a \in F$, denotamos

$$T[a] = T + aT = \{t + at' \neq 0 \,|\, t, t' \in T \cup \{0\}\} \tag{B.0.2}$$

As propriedades (ii)-(iv) da definição B.1 valem para $T[a]$. De fato, $\dot{F}^2 \subset T \subset T[a]$, o que prova (ii). Se $x, y \in T[a]$, então $x = t + at'$, $y = u + au'$, com $t, t', u, u' \in T$, logo, $x + y = (t + u) + a(t' + u') \in T + aT = T[a]$, o que prova (iii). O produto $xy = (tu + a^2 t'u') + a(tu' + t'u) \in T + aT = T[a]$, provando (iv). Assim, para que $T[a]$ seja uma pré-ordem, é necessário e suficiente que $-1 \notin T[a]$. O Lema a seguir, fornece um critério, envolvendo a, para que $T[a]$ seja uma pré-ordem.

Lema B.3 ([22], Lema 1.2, p.2) *Seja $T \subset F$ uma pré-ordem e $a \in \dot{F}$. Então $T[a]$ é uma pré-ordem se, e somente se, $a \notin -T$.*

Corolário B.4 ([22], Corolário 1.3, p.2) *Uma pré-ordem $T \subset \dot{F}$ é maximal (em relação à inclusão) se, e somente se, T é uma ordem.*

Corolário B.5 ([22], Corolário 1.4, p.3) *Qualquer pré-ordem $T \subset F$ está contida em pelo menos uma ordem de F.*

Teorema B.6 (Artin-Schreier, [22], Teorema 1.5, p.3) *Um corpo é formalmente real se, e somente se, admite uma ordem.*

Se F é um corpo de característica prima car $(F) = p > 0$, então $1+1+\cdots+1+1 = 0$ para um número $n > 1$ finito de parcelas. Daí, $-1 = 1^2+\cdots+1^2 \in \sum \dot{F}^2$ e, assim, F não é formalmente real. Portanto, todo corpo ordenado tem, necessariamente, característica igual a zero.

Notação: Dada uma pré-ordem T de F, denotamos

$$X/T = \{P \in X_F | T \subseteq P\}.$$

Pelo Corolário B.5, sabemos que $X/T \neq \emptyset$. Mencionamos ainda que X/T é um subespaço do espaço de ordens X_F, com a topologia induzida pela topologia de Harrison em X_F, ou seja, $H_T(x) = \{P \in X/T \,|\, x \in P\}$, para cada $x \in \dot{F}$.

Teorema B.7 (Artin, [22], Teorema 1.6, p.3) *Para toda pré-ordem $T \subset F$, temos* $T = \bigcap_{P \in X/T} P$.

Seja $K|F$ uma extensão de corpos, $P \in X_F$ e $Q \in X_K$. Uma ordem qualquer de K projeta-se sobre uma ordem de F do seguinte modo: $Q \cap F \in X_F$. No entanto, como veremos adiante, nem sempre um ordem de F "sobe" para K. Dizemos que Q é uma *extensão* de P, ou que P prolonga-se a Q, quando $P = Q \cap F$. De modo análogo, se T é uma pré-ordem de F e S é uma pré-ordem de K, dizemos que S *estende* T se $T = S \cap F$.

Os três lemas a seguir nos dão critérios para decidir quando uma ordem de F se estende para K. O Lema B.8 refere-se a extensões arbitrárias e vamos usá-lo na demonstração do Lema B.9, que dá um critério simples para o caso de extensões quadráticas, e do Lema B.10, que mostra que, no caso das extensões de grau ímpar, todas as ordens se estendem.

Lema B.8 ([27], Lema 1.2.1, p.13) *Se $K|F$ é uma extensão de corpos e P é uma ordem de F, então P estende-se a K se, e somente se*

$$T_K(P) = \{\sum_{i=1}^{n} t_i {\beta_i}^2 \,|\, n \in \mathbb{N}, t_i \in P \ e \ \beta_i \in K, \forall i\}$$

é uma pré-ordem de K.

Observação: $T_K(P)$ é uma pré-ordem de K que estende P.

Lema B.9 ([27], Teorema 1.2.3, p.13) *Uma ordem P de F estende-se ao corpo $F(\sqrt{a})$ $(a \in F)$ se, e somente se, $a \in P$.*

Como conseqüência direta do Lema B.9 acima, temos: se $a \in \sum \dot{F}^2 \setminus \dot{F}^2$, então todas as ordens de F se estendem para $F(\sqrt{a})$. Por outro lado, se $a \in -\sum \dot{F}^2$, então nenhuma ordem de F se estende para $K = F(\sqrt{a})$ (em particular, K não é formalmente real neste caso).

Lema B.10 ([27], Teorema 1.2.4, p.13) *Se $K|F$ é uma extensão finita de grau ímpar, então toda ordem de F se estende para uma ordem de K. Em particular, K é formalmente real.*

Exibimos, a seguir, alguns exemplos de corpos ordenados.

(1) O corpo $\mathbb{R}$ dos números reais é um corpo ordenado, possuindo uma única ordem: $\sum \mathbb{R}^2 = \mathbb{R}^2$.
(2) O corpo $\mathbb{Q}$ dos números racionais é um corpo ordenado, também com uma única ordem, a saber, $\sum \mathbb{Q}^2$. Observe, porém, que $\sum \mathbb{Q}^2 \neq \mathbb{Q}^2$, pois, por exemplo, $\sqrt{2} \notin \mathbb{Q}$, ou seja, $1^2 + 1^2 = 2 \notin \mathbb{Q}^2$, enquanto $1^2 + 1^2 \in \sum \mathbb{Q}^2$.

(3) O corpo $\mathbb{Q}(\sqrt{2})$ tem exatamente duas ordens, uma onde $\sqrt{2}$ é positivo e outra onde $\sqrt{2}$ é negativo. Observe que $\mathbb{Q}(\sqrt{2})$ pode ser imerso em $\mathbb{R}$ (por homomorfismos que preservam ordem) de duas maneiras: a primeira, levando $\sqrt{2}$ nele mesmo (identidade) e a outra levando $\sqrt{2}$ em $-\sqrt{2}$. Estes homomorfismos são exatamente os elementos do grupo de Galois $G(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$. Em geral, se K e $K(\sqrt{a})$ são corpos ordenados, cada ordem de K estende-se a duas ordens de $K(\sqrt{a})$, uma na qual $\sqrt{a}$ é positiva e outra na qual $\sqrt{a}$ é negativa.

(4) Fixado um corpo ordenado (F_0, P_0), considere o corpo de funções racionais $F = F_0(t)$. Podemos construir algumas ordens em F extendendo a ordem P_0, da maneira seguinte: **(a)** Considere um polinômio $f \in F_0[t]$ positivo se o coeficiente líder de f for positivo. Uma fração $\frac{f}{g} \in F(t)$ é positiva se e somente se f e g têm o mesmo sinal. Obtemos assim uma ordem P_1 em F estendendo a ordem P_0 dada em F_0 (isto é, $P_1 \cap F_0 = P_0$). A ordem total induzida em $F_0[t]$ coincide com a ordem lexicográfica. Para todo $a \in F_0$

temos $t - a \in P_1$, de modo que t é um elemento "infinitamente grande" em relação aos elementos de F_0. Denotamos $F_0 < t$ para resumir a seguinte informação: $a < t, \forall a \in F_0$. Se aplicarmos o F_0-automorfismo de F que leva t em $-t$, obteremos a ordem P_2 "conjugada" de P_1 em F onde t é negativo, menor que qualquer elemento de F_0, isto é $t < F_0$ (uma espécie de "$-\infty$"). **(b)** Considere um polinômio $f \in F_0[t]$ positivo, se o coeficiente de menor grau de f for positivo e uma fração $\frac{f}{g} \in F_0(t)$ positiva se e somente se f e g têm o mesmo sinal. De modo similar ao que fizemos em (a), obtemos uma ordem P_3 em $F_0(t)$ tal que $0 < t < F_0$ (t em um "infinitesimal" positivo). O F_0-automorfismo de F que leva t em $-t$ tranforma a ordem P_3 em sua "conjugada" P_4, onde t faz agora o papel de "infinitesimal" negativo, isto é, $-F_0 < t < 0$.

Um corpo F é dito *real fechado* se F é formalmente real e se nenhuma extensão algébrica de F é formalmente real. A seguir, exibimos duas caracterizações (clássicas) de um corpo real fechado.

Teorema B.11 (Artin-Schreier, 1926, [27], Teorema 1.2.10, p.14) *As seguintes afirmações são equivalentes:*

(1) *F é real fechado.*

(2) *F^2 é uma ordem de F e todo polinômio $p(X) \in F[X]$ de grau ímpar tem uma raiz em F.*

(3) *$F \neq F(\sqrt{-1})$ e $F(\sqrt{-1})$ é algebricamente fechado.*

O Teorema B.11 acima garante que o corpo $\mathbb{R}$ dos números reais é real fechado. Podemos usar, por exemplo, a condição (2), pois $\mathbb{R}^2$ é uma ordem em $\mathbb{R}$ e todo polinômio de grau ímpar $p(X) \in \mathbb{R}[X]$ tem uma raiz em $\mathbb{R}$ (isso é uma conseqüência, por exemplo, do teorema de Bolzano). Veja que, pela condição (3) do Teorema, $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$ é algebricamente fechado. Isso fornece uma demonstração do "Teorema Fundamental da Álgebra".

Definição B.12 *Dado um par (F, P), onde F é um corpo formalmente real e P é uma ordem de F, uma extensão $\Delta \supset F$ é chamada* fecho real *de F (relativo à ordem P) se satisfaz:*

(1) *Δ é real fechado.*

(2) $\Delta|F$ *é extensão algébrica (não necessariamente finita).*

(3) $P = \Delta^2 \cap F$.

Um corpo E é dito *euclidiano* se é formalmente real e $|\dot{E}/\dot{E}^2| = 2$. Um corpo euclidiano tem uma única ordem, a saber E^2. Exemplos imediatos de corpos euclidianos são os corpos reais fechados. O resultado a seguir fornece várias caracterizações dos corpos euclidianos:

Teorema B.13 ([21], Teorema 10.1, p.89) *Para um corpo formalmente real E, as seguintes afirmações são equivalentes:*

(1) E *é euclidiano.*

(2) E *é pitagórico*[1] *com uma única ordem.*

(3) $K = E(\sqrt{-1})$ *é quadraticamente fechado, i.e.,* $K^2 = K$.

(4) E *tem uma extensão finita que é quadraticamente fechada.*

(5) *Nenhuma extensão quadrática de* E *é formalmente real.*

Na página 1, definimos o fecho quadrático de F, denotado por $F(2)$, como o menor corpo quadraticamente fechado que contém F. A seguir, iremos estabelecer uma correspondência biunívoca entre as involuções do grupo de Galois $G(F(2)|F)$ (veja a definição na página 4) e os corpos euclidianos E tais que $F \subset E \subset F(2)$.

Lema B.14 *Se* $\sigma \in G(F(2)|F)$ *é uma involução, então* $-1 \notin E_\sigma^2$.

Demonstração. Suponhamos que $-1 \in E_\sigma^2$. Então, para todo $x \in E_\sigma$, teríamos $x = (\frac{x+1}{2})^2 + (-1)(\frac{x-1}{2})^2 \in E_\sigma^2 + E_\sigma^2$. Logo $E_\sigma = E_\sigma^2 + E_\sigma^2$.

Se $1 + c^2 \in E_\sigma^2$, para todo $c \in E_\sigma$, então $E_\sigma = E_\sigma^2 + E_\sigma^2 = E_\sigma^2$ e logo $E_\sigma = E_\sigma^2$, o que é uma contradição pois, como σ é uma involução, $F \subset E_\sigma \subsetneq F(2)$ e $F(2)$ é o menor corpo quadraticamente fechado contendo F.

Suponha, agora, que $1 + c^2 \notin E_\sigma^2$. Tomemos $a = \frac{1}{1+c^2}$ e consideremos as extensões de corpos $E_\sigma \subset E_\sigma(\sqrt{a}) \subset E_\sigma(\sqrt{1+\sqrt{a}})$. De $[F(2) : E_\sigma] = 2$ e $E_\sigma(\sqrt{1+\sqrt{a}}) \subset F(2)$ temos, necessariamente, $1 + \sqrt{a} = (x + y\sqrt{a})^2$ com $x, y \in E_\sigma$. Assim, $x^2 + y^2 a = 1$ e $2xy = 1$. Resolvendo este par de equações para x, obtemos $x^2 = \frac{1 \pm \sqrt{1-a}}{2}$ e assim $1 - a = (2x^2 - 1)^2$, o que implica, substituindo a por $\frac{1}{1+c^2}$, que $1 + c^2 = \frac{c^2}{(2x^2-1)^2} \in E_\sigma^2$. Entretanto, isto contradiz a hipótese. Concluímos, então, que $-1 \notin E_\sigma^2$. ■

[1] Para a definição de corpo pitagórico, veja a página 4.

Proposição B.15 *Seja F um corpo formalmente real. Dado um F-automorfismo $\sigma \in G(F(2)|F)$, temos: σ é uma involução se, e somente se, $F(2) = E_\sigma(\sqrt{-1})$ e E_σ^2 é uma ordem de E_σ. Em particular, E_σ é euclidiano.*

Demonstração. (Somente se) Primeiramente, uma vez que $F(2)|E_\sigma$ é uma extensão quadrática, temos que $|G(F(2)|E_\sigma)| = |\{1, \sigma\}| = 2$. Logo, $F(2) = E_\sigma(\sqrt{y})$, para algum $y \in E_\sigma$. Como $F(2)$ é quadraticamente fechado, -1 é um quadrado em $E_\sigma\left(\sqrt{y}\right) = F\left(2\right)$. Assim, $-1 = \left(\alpha + \beta\sqrt{y}\right)^2$, onde $\alpha, \beta \in E_\sigma$. Logo, $-1 = \alpha^2 + \beta^2 y + 2\alpha\beta\sqrt{y}$. Esta última igualdade pode ser reescrita como $-1 = \alpha^2 + \beta^2 y$ e $\alpha\beta = 0$. Se $\beta = 0$, então $\alpha^2 = -1$, com $\alpha \in E_\sigma$. Mas isso é impossível, pelo Lema B.14. Assim, $\alpha = 0$ e $\beta^2 y = -1$, o que implica que $y = -\beta^{-2}$. Portanto, $F\left(2\right) = E_\sigma\left(\sqrt{y}\right) = E_\sigma\left(\sqrt{-\beta^{-2}}\right) = E_\sigma\left(\sqrt{-1}\right)$.

Devemos mostrar agora que E_σ^2 é uma ordem de E_σ. As únicas partes não triviais que precisamos verificar são $E_\sigma^2 + E_\sigma^2 \subset E_\sigma^2$ e $E_\sigma^2 \cup -E_\sigma^2 = E_\sigma$. De $E_\sigma\left(\sqrt{-1}\right)^2 = E_\sigma\left(\sqrt{-1}\right)$ temos que, para $u, v \in E_\sigma$ arbitrários, existem $x, y \in E_\sigma$ tais que $\left(x + y\sqrt{-1}\right)^2 = u + v\sqrt{-1}$ (ou seja, todo elemento $E_\sigma\left(\sqrt{-1}\right)$ tem uma raíz quadrada). Assim, temos $x^2 - y^2 = u$ e $2xy = v$. Podemos eliminar y das últimas duas igualdades para obtermos $4x^4 - 4ux^2 - v^2 = 0$ e, resolvendo essa equação na indeterminada x, obtemos $x^2 = \frac{u \pm \sqrt{u^2+v^2}}{2}$. Logo $\pm\sqrt{u^2 + v^2} = 2x^2 - u \in E_\sigma$. Isso mostra que $u^2 + v^2 \in E_\sigma^2$ quaisquer que sejam $u, v \in E_\sigma$. Portanto, $E_\sigma^2 + E_\sigma^2 \subset E_\sigma^2$.

Finalmente, dado $x \in E_\sigma \setminus E_\sigma^2$ devemos mostrar que $x \in -E_\sigma^2$. Temos $\sqrt{x} \in F\left(2\right)$ (de fato, $x \in E_\sigma \subset F\left(2\right)$ e $F\left(2\right)^2 = F\left(2\right)$). Assim, $E_\sigma \subsetneq E_\sigma\left(\sqrt{x}\right) \subseteq F\left(2\right)$ e $[F\left(2\right) : E_\sigma] = 2$, o que implica $E_\sigma\left(\sqrt{x}\right) = F\left(2\right) = E_\sigma\left(\sqrt{-1}\right)$. Assim, $\sqrt{x} \in E_\sigma\left(\sqrt{-1}\right)$. Logo, existem $u, v \in E_\sigma$ tais que $\sqrt{x} = u + v\sqrt{-1}$, ou seja, $x = u^2 - v^2 + 2uv\sqrt{-1}$. Temos, então $u^2 - v^2 = x$ e $uv = 0$. Se $v = 0$, então $x = u^2 \in E_\sigma^2$, o que contradiz a hipótese. Portanto, $u = 0$ e $x = -v^2 \in -E_\sigma^2$.

(Se) Seja $E \supset F$ um corpo tendo E^2 como ordem (e, portanto, formalmente real) e tal que $F(2) = E(\sqrt{-1})$. Temos $|G(F(2)|E)| = |G(E(\sqrt{-1})|E)| = [E(\sqrt{-1}) : E] \leq 2$. Se $[E(\sqrt{-1}) : E] = 1$, então $\sqrt{-1} \in E$, logo $-1 \in E^2$. Mas, por hipótese, E é formalmente real e, assim, temos necessariamente $[E(\sqrt{-1}) : E] = 2$, o que implica $|G(F(2)|E)| = 2$. Conseqüentemente, $G(F(2)|E) = \{1, \sigma\}$ para alguma involução σ. Portanto, $E = E_\sigma$.

Dado $\sigma \in G(F(2)|F)$, uma vez que E_σ é formalmente real e $E_\sigma(\sqrt{-1})$ é quadraticamente fechado, o Teorema B.13 nos diz que E_σ é euclidiano. ■

Dada uma ordem P em F, um fecho euclidiano (veja a página 9) de (F, P) não é único. De fato, se $x \in P$, a ordem P tem duas extensões a $P(\sqrt{x})$ e cada uma fornece

fechos euclidianos de (F, P). Apesar de não termos unicidade, quaisquer dois fechos euclidianos de (F, P) são conjugados, no sentido da proposição abaixo.

Proposição B.16 *Se E_1 e E_2 são extensões euclidianas de F, e σ_1, σ_2 são as involuções relacionadas com E_1 e E_2, respectivamente, as seguintes condições são equivalentes:*

(a) $E_1^2 \cap F = E_2^2 \cap F$

(b) $E_2 = g(E_1)$, *para algum* $g \in G(F(2)|F)$

(c) $\sigma_2 = g\sigma_1 g^{-1}$, *para algum* $g \in G(F(2)|F)$

Demonstração.(a)⇒(b): Seja Δ_i o fecho real de E_i $(i = 1, 2)$. Como cada E_i é euclidiano, E_i^2 é a única ordem de E_i e $E_i^2 = \Delta_i^2 \cap E_i$. Logo, $\Delta_1^2 \cap F = E_1^2 \cap F = E_2^2 \cap F = \Delta_2^2 \cap F$. Assim, Δ_1 e Δ_2 são fechos reais de F em relação a uma mesma ordem e, portanto, são F-isomorfos [2]. Uma vez que $F(2)|F$ é uma extensão normal e $E_i = F(2) \cap \Delta_i$ $(i = 1, 2)$, o F-isomorfismo $\sigma : \Delta_1 \to \Delta_2$ induz um F-isomorfismo $g : E_1 \to E_2$.

(b)⇒(a): Suponha que exista $g \in G(F(2)|F)$ tal que $g(E_1) = E_2$. Seja $x \in E_1^2 \cap F$. De $x \in E_1^2$ vem $x = y^2$, com $y \in E_1$. Assim, $g(x) = g(y^2) = g(y)^2 \in E_2^2$ e, como $g \in G(F(2)|F)$ e $x \in F$, temos $x = g(x) \in E_2^2 \cap F$. Logo, $E_1^2 \cap F \subseteq E_2^2 \cap F$. A outra inclusão é similar.

(b)⇒(c): Se $x \in E_1$ (i.e., $\sigma_1(x) = x$) e $g(E_1) = E_2$, temos $g(x) \in E_2$ (i.e., $\sigma_2 g(x) = g(x)$). Assim, $g(x) = \sigma_2 g(x) = \sigma_2 g \sigma_1(x)$, $\forall x \in E_1$. A partir desse fato, concluímos que $g = \sigma_2 g \sigma_1$, o que implica $1 = \sigma_2 g \sigma_1 g^{-1}$ e, assim, $\sigma_2 = \sigma_2^{-1} = g\sigma_1 g^{-1}$ (note que $\sigma_2^2 = 1$ implica que $\sigma_2^{-1} = \sigma_2$).

(c)⇒(b): $g(E_1) = \{g(x) \mid \sigma_1(x) = x\}$. De $g(x) = g\sigma_1(x) = \sigma_2 g(x)$ vem $\sigma_2(g(x)) = g(x)$ e logo $g(x) \in E_2, \forall x \in E_1$. Assim $g(E_1) \subseteq E_2$. Por outro lado, se $x \in E_2$ então $g^{-1}(E_2) = \{g^{-1}(x) \mid \sigma_2(x) = x\}$. Agora, $g^{-1}(x) = g^{-1}\sigma_2(x) = \sigma_1 g^{-1}(x)$ implica que $g^{-1}(x) \in E_1, \forall x \in E_2$, e, portanto, $g^{-1}(E_2) \subseteq E_1$, o que implica $E_2 \subseteq g(E_1)$. Juntando as duas inclusões, podemos concluir que $g(E_1) = E_2$. ■

Finalizamos este apêndice apresentando um Teorema clássico devido a R. Baer (1929) e W. Krull (1931) que fornece um critério para identificar ordens compatíveis com uma dada valorização em um corpo F. Mais precisamente, fixada uma valorização

[2]Para uma prova deste fato, veja, por exemplo, [27] Teorema 1.3.14, página 21

$(A, v_A, \mathfrak{m}_A, k_A, \ldots)$ de F com corpo de resíduos k_A formalmente real, o Teorema B.17 abaixo mostra como construir o conjunto

$$X_F^A = \{P \in X_F \mid 1 + \mathfrak{m}_A \subset P\}$$

das ordens de F compatíveis com A. Por conveniência, denotaremos o grupo de valores Γ_A multiplicativamente.

Teorema B.17 (Baer-Krull, [22], Teorema 3.10, p.24) *Sejam $(A, v_A, \mathfrak{m}_A, k_A, \ldots)$ e γ fixadas como acima. Toda ordem $P \in X_F^A$ dá origem a uma ordem $\overline{P}$ em k_A e a um homomorfismo $\chi_P : \Gamma_A/\Gamma_A^2 \to \{\pm 1\}$. Por outro lado, dada uma ordem P_0 de k_A e um homomorfismo $\chi : \Gamma_A/\Gamma_A^2 \to \{\pm 1\}$, existe uma única ordem $P \in X_F^A$ tal que $\overline{P} = P_0$ e $\chi_P = \chi$. Assim, existe uma correspondência biunívoca*

$$X_F^A \leftrightarrow X_k \times (\Gamma_A/\Gamma_A^2)^*$$

onde X_k denota o conjunto das ordens de $k = k_A$ e $(\Gamma_A/\Gamma_A^2)^* = Hom(\Gamma_A/\Gamma_A^2, \{\pm 1\})$.

Observação B.18 *Com as notações estabelecidas acima, se $|\Gamma_A/\Gamma_A^2| = n < \infty$ e $|X_k| = m < \infty$, então $|X_F^A| = mn$. Reciprocamente, se $|X_F^A| < \infty$, então $|\Gamma_A/\Gamma_A^2| < \infty$, $|X_k| < \infty$ e $|X_F^A| = |X_k| \cdot |\Gamma_A/\Gamma_A^2|$.*

Observação B.19 *Se T é uma pré-ordem de F e $X_T^A = \{P \in X/T \mid 1 + \mathfrak{m}_A \subset P\}$ é um conjunto finito, então $|X_T^A| = |X/\overline{T}| \cdot |\Gamma_A/\Gamma_A^2|$, onde $X/\overline{T}$ é o conjunto das ordens de k_A que contêm $\overline{T}$.*

Apêndice C

Formas Quadráticas

Nesta seção, expomos a teoria básica das formas quadráticas. Como fizemos nos apêndices anteriores, omitimos as demonstrações dos resultados mais conhecidos. Embora as referências para esse assunto sejam, geralmente, os livros de T.Y. Lam [23] e W. Scharlau [31], preferimos adotar como guia para esta seção, o livro de A. Pfister [26]. O que se segue é praticamente uma livre tradução dos parágrafos 1.1 e 2.1 desse livro, pelo menos até os exemplos da página 129. Na parte final, onde exibimos os rudimentos da teoria dos anéis de Witt abstratos, a referência é o livro de Marshall [24].

Dado um corpo F e um número natural n, uma *forma quadrática* de dimensão n sobre F é um polinômio homogêneo de grau 2 em n variáveis com coeficientes em F. Sua forma geral é:

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \in F[x_1, \ldots, x_n]. \tag{C.0.1}$$

Podemos escrever a forma f em notação matricial da maneira seguinte: seja x a matriz coluna com entradas $x_1, \ldots, x_n$ e x^t a transposta de x (portanto, uma matriz linha). Seja $A = (a_{ij})$ a matriz $n \times n$ com coeficientes em F, cujas entradas são os coeficientes de f. Então:

$$f(x) = x^t A x \tag{C.0.2}$$

Duas formas quadráticas f e g de dimensão n sobre F são ditas *equivalentes* se existe uma transformação linear não singular T tal que $g(x) = f(Tx)$. É imediato que a relação definida acima é uma relação de equivalência. Denotamos: $f \simeq g$.

Como car $F \neq 2$, podemos substituir os coeficientes a_{ij} por $\frac{a_{ij}+a_{ji}}{2}$ sem alterar a

forma quadrática. A vantagem dessa troca é que a matriz resultante é *simétrica*. Além disso, se A é simétrica, a matriz congruente $B = T^tAT$ também é simétrica. Logo, se $f \simeq g$ e $f(x) = x^tAx$, então $g(x) = (Tx)^tA(Tx) = x^t(T^tAT)x = x^tBx$, onde B é simétrica.

Novamente, se car $F \neq 2$, podemos associar a cada forma quadrática $f = x^tAx$ (com $A^t = A$, i.e., A simétrica), uma aplicação

$$b_f(x, y) = \frac{1}{2}\left(f(x + y) - f(x) - f(y)\right) = x^tAy = y^tAx \tag{C.0.3}$$

onde x e y são *vetores* (ou seja, matrizes coluna) independentes e de mesma dimensão (isto é, com o mesmo número de linhas). Chamamos b_f de *forma bilinear simétrica associada a* f. A verificação de que b_f é de fato bilinear e simétrica é automática.

Reciprocamente, dada uma forma bilinear simétrica $b(x, y) = x^tAy$, com $A^t = A$, o polinômio $f(x) := b(x, x)$ é uma forma quadrática. Essa associação mostra que as teorias das formas bilineares das formas quadráticas (com um número finito de variáveis) coincidem sobre um corpo de característica diferente de 2.

Note que as duas construções acima não valem se car $F = 2$. Em particular, neste caso as teorias de formas bilineares simétricas e de formas quadráticas são distintas. A partir deste ponto, vamos nos concentrar no caso em que car $F \neq 2$, que é o de maior interesse para nós.

Toda forma quadrática f de dimensão n induz uma aplicação $Q_f : V \to F$, onde $V = F^n$ é o espaço vetorial formado pelas matrizes coluna $n \times 1$ v com entradas em F. Q_f é definida de maneira natural como $Q_f(v) := f(v)$ e é denominada *aplicação quadrática*. Toda aplicação quadrática satisfaz $Q_f(av) = a^2Q_f(v)$, onde $a \in F$ e $v \in V$ são arbitrários.

Podemos definir uma aplicação bilinear simétrica $B_f : V \times V \to F$ dada por $B_f(v, w) := \frac{1}{2}\left(Q_f(v + w) - Q_f(v) - Q_f(w)\right)$, onde $(v, w) \in V \times V$ é arbitrário.

Se $f(x) = x^tAx$, onde $A = (a_{ij})$ e $\{e_1, \ldots, e_n\}$ é a base canônica de V sobre F, então $a_{ij} = B_f(e_i, e_j)$.

A discussão acima nos leva naturalmente a definir, para um F-espaço vetorial arbitrário V, de dimensão finita n, uma *aplicação quadrática* como sendo $Q : V \to F$, satisfazendo as seguintes condições:

(1) $Q(av) = a^2Q(v)$, para todo $a \in F$ e todo $v \in V$.

(2) A aplicação $B : V \times V \to F$ dada por

$$B(v, w) = \frac{1}{2}\left(Q(v + w) - Q(v) - Q(w)\right)$$

é bilinear sobre F.

O par (V, Q) é chamado *espaço quadrático* sobre F. Dois espaços quadráticos (V, Q) e (V', Q') de dimensão n sobre F são ditos *isométricos* se existe um isomorfismo F-linear $T : V \to V'$ tal que

$$Q(v) = Q'(Tv)$$

para todo $v \in V$. Denotamos: $(V, Q) \simeq (V', Q')$.

Proposição C.1 ([26], Proposição 1.6, p.3) *Existe uma correspondência biunívoca entre as classes de equivalência de formas quadráticas de dimensão n sobre F e as classes de isometria dos espaços quadráticos de dimensão n sobre F.*

A proposição acima nos permite considerar formas quadráticas de um ponto de vista "geométrico" (ou seja, livre de coordenadas). No que se segue, identificaremos uma forma quadrática f e sua forma bilinear associada b_f com a aplicação quadrática Q_f e com a aplicação bilinear B_f, respectivamente.

Dados dois espaços quadráticos (V_1, f_1) e (V_2, f_2) sobre F, de dimensões n_1 e n_2, respectivamente, podemos construir um espaço de dimensão $n = n_1 + n_2$, pondo:

$$V = V_1 \oplus V_2,$$

$$f(v) = f(v_1) + f(v_2),$$

onde $v_i \in V_i$, $i = 1, 2$ e $v = v_1 + v_2 \in V$. O espaço (V, f) é chamado *soma ortogonal* de (V_1, f_1) e (V_2, f_2). Denotamos: $f = f_1 \perp f_2$. Se a forma f_i tem matriz associada A_i $(i = 1, 2)$, então f tem matriz associada

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

De modo análogo, podemos definir a soma ortogonal de um número finito de espaços quadráticos e, a menos de equivalência, essa soma depende apenas das classes de equivalência das parcelas, e não da ordem da soma.

Por outro lado, se (V, f) é um espaço quadrático, $V = V_1 \oplus \cdots \oplus V_m$, onde cada V_i $(i = 1, \ldots, m)$ é subespaço de V e $b_f(v_i, v_j) = 0$, para $v_i \in V_i$, $v_j \in V_j$ e $i \neq j$, então $f = f_1 \perp \ldots \perp f_m$, onde $f_i = f|_{V_i}$ para cada $i \in \{1, \ldots, m\}$.

Mostraremos, a seguir, que toda forma quadrática (sobre um corpo F com car $F \neq 2$) pode ser "diagonalizada".

Teorema C.2 ([26], Teorema 1.8, p.4) *Todo espaço quadrático (V, f) é isométrico a uma soma ortogonal de espaços de dimensão* 1.

Observação: No Teorema C.2 acima, a forma f é equivalente à forma $g = \sum_{i=1}^{n} a_i x_i^2$, onde $a_i = f(v_i)$. Escrevemos a forma g como $\langle a_1, \ldots, a_n \rangle$, $a_i \in \dot{F}$.

Seja A uma matriz simétrica e (V, f), onde $f(v) = v^t A v$, o espaço quadrático correspondente. O subespaço $V^{\perp} = \{w \in V | b_f(w, v) = 0, \text{ para todo } v \in V\}$ é chamado *radical* de V e denotado por rad V . Dizemos que (V, f) é *regular* se rad $V = 0$. As afirmações a seguir são imediatas:

(1) rad $V = \{w \in V | w^t A v = 0, \text{ para todo } v \in V\} = \{w \in V | w^t A = 0\}$.

(2) rad $V = 0$ se, e somente se, $\det A \neq 0$.

(3) O radical é invariante por isometria. Logo, a propriedade de um espaço ser regular também é invariante por isometria.

(4) Se f não é regular, então $f \simeq \langle a_1, \ldots, a_n \rangle$, onde algum $a_i = 0$.

A afirmação (4) implica que uma forma não regular depende, de fato, de $n - 1$ variáveis. Como n pode ser qualquer número natural, podemos considerar apenas as formas quadráticas que são regulares. É o que faremos de agora em diante.

Se f é uma forma de dimensão n sobre F e $a \in F$, dizemos que f *representa* a, se existe $v \in F^n$, $v \neq 0$, tal que $f(v) = a$. O conjunto de todos os elementos de F representados por f é $\tilde{D}(f) = \{f(v) | 0 \neq v \in V\}$. Denotamos, ainda $D(f) = \tilde{D}(f) \setminus \{0\}$. Dizemos que a forma f é *universal* se $D(f) = \dot{F}$. Dizemos que f é *isotrópica* sobre F se $0 \in \tilde{D}(f)$. Caso contrário, f é dita *anisotrópica* sobre F.

Exemplo. Consideremos a forma $f = \langle 1, 1 \rangle$ (i.e., $f(x) = x_1^2 + x_2^2$, onde $x^t = (x_1, x_2)$) sobre os corpos $\mathbb{R}$ e $\mathbb{C}$. Como $a_1^2 + a_2^2 > 0$, quaisquer que sejam $a_1, a_2 \in \mathbb{R}$, a forma f não representa 0 nem -1 sobre $\mathbb{R}$. No entanto, f representa 0 e -1 sobre $\mathbb{C}$. De fato,

$0 = 1^2 + i^2$ e $-1 = 0^2 + i^2$. Isso mostra que as noções definidas acima dependem do corpo sobre o qual tomamos a forma, e não apenas da forma em si.

Uma forma regular $f = \langle a \rangle$ de dimensão 1 nunca é isotrópica. Para formas de dimensão 2, temos a seguinte

Proposição C.3 ([26], Proposição 1.11, p.5) *A menos de equivalência, existe apenas uma forma quadrática regular isotrópica, de dimensão 2, a saber $f(x) = 2x_1x_2$. Temos:*

$$f \simeq \langle a, -a \rangle$$

para algum $a \in \dot{F}$. Em particular, f é universal.

A classe de equivalência de uma forma quadrática regular isotrópica de dimensão 2 sobre F é denotada por $H \simeq \langle 1, -1 \rangle$ e chamada de *plano hiperbólico*.

A proposição seguinte é uma generalização de C.3.

Proposição C.4 ([26], Proposição 1.12, p.5) *Seja (V, φ) um espaço quadrático regular e isotrópico sobre um corpo F, com $dimV = n \geq 2$. Então $V = U \oplus W$, onde $U \simeq H$ (o plano hiperbólico), $dimW = n - 2$ e $\varphi \simeq \langle 1, -1 \rangle \perp \psi$, com $\psi = \varphi|_W$.*

Teorema C.5 (Teorema do Cancelamento, [26], Teorema 1.1, p.19) *Sejam f, g e h formas quadráticas sobre F tais que*

$$f \perp g \simeq f \perp h. \tag{C.0.4}$$

Então $g \simeq h$.

A partir deste ponto, estaremos interessados em trabalhar com classes de equivalência de formas quadráticas sobre F. Isso nos permite supor que todas as formas são regulares e diagonais, e é o que faremos. Usaremos, a seguir, a notação $rf \simeq \underbrace{f \perp \ldots \perp f}_{r \text{ vezes}}$. Se $f = \langle a_1, \ldots, a_n \rangle$ e $g = \langle b_1, \ldots, b_m \rangle$, o *produto tensorial* de f e g é dado por $f \otimes g = \langle \ldots, a_i b_j, \ldots \rangle$ onde $i = 1, \ldots, n$ e $j = 1, \ldots, m$.

Para $f \simeq \langle a_1, \ldots, a_m \rangle$, com $a_i \in \dot{F}$, definimos o *determinante* de f como

$$\det f = \left(\prod_{i=1}^{m} a_i \right) \cdot \dot{F}^2 \in \dot{F}/\dot{F}^2. \tag{C.0.5}$$

Definimos o *discriminante* de f como sendo

$$d(f) = (-1)^{\frac{m(m-1)}{2}} \det f. \tag{C.0.6}$$

Teorema C.6 (Teorema da Decomposição, [26], Teorema 1.2, p.22) *Toda forma quadrática regular f sobre o corpo F tem uma decomposição ortogonal*

$$f \simeq i \cdot \langle 1, -1 \rangle \perp f_0$$

onde $i \geq 0$ é um número inteiro e f_0 é anisotrópica. O número i (chamado de índice de Witt) é univocamente determinado por f e f_0 é única a menos de equivalência.

Sejam f e g formas quadráticas e f_0 e g_0 suas respectivas partes anisotrópicas, como no Teorema C.6. Dizemos que f e g são *similares* ou *Witt-equivalentes* se $f_0 \simeq g_0$. Denotamos: $f \sim g$. Em outras palavras, $f \sim g$ se, e somente se, existem inteiros não negativos r e s tais que

$$f \simeq r \cdot \langle 1, -1 \rangle \perp f_0, \quad g \simeq s \cdot \langle 1, -1 \rangle \perp g_0$$

e $f_0 \simeq g_0$. É uma operação de rotina checar que $\sim$ é uma relação de equivalência. Denotamos a classe de equivalência de uma forma f por $\tilde{f}$ e por $W(F)$ o conjunto das classes $\tilde{f}$, onde f é uma forma quadrática regular de dimensão finita $n \geq 0$ sobre F. Consideramos a forma vazia $f = 0$ de dimensão zero como regular e anisotrópica.

Teorema C.7 (Witt, [26], Proposição 1.9, p.23) *As operações $\perp$ e $\otimes$ podem ser naturalmente definidas em $W(F)$. Usando $\perp$ como adição e $\otimes$ como multiplicação, o conjunto $W(F)$ ganha estrutura de anel comutativo com unidade. $W(F)$ é chamado* anel de Witt *de F. Se a multiplicação é ignorada, $W(F)$ é chamado* grupo de Witt *de F.*

Exemplos:

(1) Se F é um corpo com car $F \neq 2$, quadraticamente fechado (veja, por exemplo, o item 3 do Teorema B.13), então as únicas formas anisotrópicas sobre F são 0 e $\langle 1 \rangle$. Portanto, $W(F) = \mathbb{Z}/2\mathbb{Z}$.

Por definição, $F = F^2$. Logo, $\langle x \rangle = \langle 1 \rangle \in W(F)$, ou seja, existe apenas uma forma de dimensão 1. Uma forma $\langle x, y \rangle$ de dimensão 2 é isotrópica, pois $-\frac{x}{y} \in \dot{F} = \dot{F}^2$ implica que $y\dot{F}^2 = -x\dot{F}^2$ e, daí, $\langle x, y \rangle = \langle x, -x \rangle$. Portanto, as únicas formas anisotrópicas sobre F são 0 e $\langle 1 \rangle$. Pela definição de $W(F)$, toda forma $f \in W(F)$ é representada por uma forma anisotrópica sobre F, única a menos de equivalência. Logo, $|W(F)| = 2$ e $W(F) \simeq \mathbb{Z}/2\mathbb{Z}$, como anéis.

(2) Se F é um corpo real fechado (veja a definição na página 119), então as únicas formas anisotrópicas sobre F são 0, $n\langle 1\rangle$ e $n\langle -1\rangle$. Logo, $W(F) = \mathbb{Z}$.

Em um corpo real fechado F, temos $F = F^2 \cup -F^2$. Assim, uma forma quadrática $f = \langle a_1, \ldots, a_n\rangle$ pode ser escrita como $f = (r \cdot \langle 1\rangle) \perp (s \cdot \langle -1\rangle)$, onde $r, s \in \mathbb{Z}$, $r, s \geq 0$ e $r + s = n$. Se $r > 0$ e $s > 0$, então f é isotrópica (pois $f \simeq \langle 1, -1\rangle \perp g$). Por outro lado, se $s = 0$, então $f = n\langle 1\rangle$ é anisotrópica, pois $x_1^2 + \cdots + x_n^2 = 0$, com $x_i \in F$ implica $x_i = 0$, para todo i. O mesmo argumento vale para o caso em que $r = 0$. Isso mostra que $W(F) = \mathbb{Z}$ como conjuntos, e é claro que as estruturas de anel em ambos coincidem.

(3) Seja $F = \mathbb{F}_p$ o corpo finito com p elementos, onde p é um número primo ímpar. Temos:

(a) $\dot{F}/\dot{F}^2$ tem exatamente dois elementos, a saber, $\dot{F}^2$ e $\epsilon\dot{F}^2$, onde $\epsilon \in \dot{F} \setminus \dot{F}^2$.

O homomorfismo de grupos $\varphi : \dot{F} \to \dot{F}$ dado por $x \mapsto x^2$ tem núcleo $\{\pm 1\}$. Logo, pelo teorema dos homomorfismos, sua imagem $\dot{F}^2$ tem $\frac{p-1}{2}$ elementos.

(b) ϵ é a soma de dois quadrados em F.

Os subconjuntos F^2 e $\epsilon - F^2$ têm $\frac{p+1}{2}$ elementos. Logo, sua interseção não é vazia, ou seja, existem $a, b \in F$ tais que $a^2 = \epsilon - b^2$.

(c) Toda forma quadrática binária (isto é, de dimensão 2) sobre F é universal. Logo, $|W(F)| = 4$.

Toda forma binária anisotrópica sobre $\mathbb{F}_p$ é um múltiplo escalar de $f_0 = \langle 1, -\epsilon\rangle$. Devemos mostrar que f_0 é universal, ou seja, representa 1 e ϵ. Isso é conseqüência de $1 = 1 \cdot 1^2 - \epsilon \cdot 0^2$, $\epsilon = (\frac{\epsilon}{b})^2 - \epsilon(\frac{a}{b})^2$ ($ab \neq 0$, pois ϵ não é um quadrado). Se g é uma forma de dimensão ≥ 3, então $g \simeq \langle a, b, c\rangle$ e, se $\langle a, b\rangle$ não é isotrópica, é universal, isto é, $c \in D\langle a, b\rangle$ e, daí, g é isotrópica. Logo, os elementos de $W(F)$ são representados pelas formas anisotrópicas 0, $1 = \langle 1\rangle$, $\langle \epsilon\rangle$ e f_0.

(d) Como um grupo, $W(F) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{se } p \equiv 1(\mod 4) \\ \mathbb{Z}/4\mathbb{Z} & \text{se } p \equiv 3(\mod 4) \end{cases}$

O símbolo de Legendre $(\frac{-1}{p})$ é ± 1 de acordo com $p \equiv \pm 1(\mod 4)$. No primeiro caso, $\langle 1, 1\rangle \sim \langle 1, -1\rangle \sim 0$. Logo, $\langle 1\rangle$ tem ordem 2 no grupo $W(F)$. No segundo caso, $2 \cdot \langle 1\rangle = \langle 1, 1\rangle \not\sim 0$, mas $4 \cdot \langle 1\rangle \sim 0$, pois $|W(F)| = 4$.

Observação. A partir deste ponto, quando não houver perigo de confusão, iremos identificar uma forma f com sua imagem $\tilde{f}$ em $W(F)$, escrevendo simplesmente $f \in W(F)$ e operando com f como um elemento do anel de Witt.

Lema C.8 *Dado $x \in \dot{F}$, o conjunto $D\langle 1, x\rangle = \{y \in \dot{F} \,|\, y = a^2 + b^2x\}$ é um subgrupo de $\dot{F}$.*

Demonstração. Primeiramente, é claro que $\dot{F}^2 \subset D\langle 1, x\rangle$ e, dados $x, y \in \dot{F}$, $xy^2 \in D\langle 1, x\rangle$ (ou seja, $x\dot{F}^2 \subset D\langle 1, x\rangle$). Se $y \in D\langle 1, x\rangle$, então $y^{-1} = yy^{-2} \in D\langle 1, x\rangle$. Tomemos $y, z \in D\langle 1, x\rangle$. Vamos mostrar que $yz \in D\langle 1, x\rangle$. De fato, se $y = a^2 + b^2x$ e $z = c^2 + d^2x$, onde $a, b, c, d \in F$, então $yz = (ac - bdx)^2 + (ad + bc)^2x \in D\langle 1, x\rangle$. Isso mostra que $D\langle 1, x\rangle$ é subgrupo de $\dot{F}$, como queríamos. ■

A prova do Lema C.8 acima obscurece um fato relevante que explicitaremos agora. Se $x \in -\dot{F}^2$, então $\langle 1, x\rangle \simeq \langle 1, -1\rangle$ é universal, isto é, $D\langle 1, x\rangle = \dot{F}$ é um grupo. Caso $x \notin -\dot{F}^2$, podemos considerar a extensão de corpos $K|F$, onde $K = F(\sqrt{-x})$. Temos, então, definida uma *norma* $N_{K|F} : K \to F$ dada por $N_{K|F}(a+b\sqrt{-x}) = (a+b\sqrt{-x})\cdot(a-b\sqrt{-x})$, onde $a, b \in F$. Logo, $D\langle 1, x\rangle = N_{K|F}(K)$ e o lema acima é conseqüência direta da multiplicatividade da norma $N_{K|F}$.

O subconjunto de $W(F)$, formado pelas classes de formas de dimensão par:

$$IF = \{\tilde{f} \in W(F) \,|\, \dim f \in 2\mathbb{Z}\}$$

é um ideal de $W(F)$, que denominamos *ideal fundamental* de $W(F)$.

O homomorfismo $\dim_2 : W(F) \to \mathbb{Z}/2\mathbb{Z}$, induzido por $\dim : W(F) \to \mathbb{Z}$, tem núcleo IF e é sobrejetivo. Logo, temos o isomorfismo de anéis $W(F)/IF \simeq \mathbb{Z}/2\mathbb{Z}$, o que mostra que IF é um ideal maximal de $W(F)$.

Mencionamos, ainda, que IF é gerado, como grupo abeliano, pelas formas $\langle 1, x\rangle$, onde $x \in \dot{F}$. De fato, o grupo IF é gerado pelas formas binárias $\langle a, b\rangle$ e podemos escrever $\langle a, b\rangle = \langle 1, a\rangle - \langle 1, -b\rangle$, onde a igualdade significa que estamos identificando as formas com suas classes de equivalência em $W(F)$. O ideal $I^2F = (IF)^2$ é gerado pelas formas do tipo $\langle 1, x\rangle \otimes \langle 1, y\rangle$ onde $x, y \in \dot{F}$. Em geral, a n-ésima potência I^nF do ideal IF é gerada pelas *formas de Pfister* $\langle\langle x_1, \ldots, x_n\rangle\rangle := \langle 1, x_1\rangle \otimes \cdots \otimes \langle 1, x_n\rangle$, onde $x_1, \ldots, x_n \in \dot{F}$. Convém mencionar que os elementos de $\dot{F}$ representados por uma

forma de Pfister formam um subgrupo de $\dot{F}$. Para uma demonstração desse fato, veja [23], Teorema 1.8, página 319. O Lema **??** abaixo nos dá uma informação sobre a soma de classes em I^2F/I^3F.

A Proposição C.9 abaixo é usada várias vezes no texto, sobretudo no Capítulo 3. O item (2) desta Proposição é importante, pois permite simplificações nos cálculos com elementos rígidos (veja, por exemplo, as demonstrações dos Lemas 3.1 e 3.2, da Proposição 3.4 e do Corolário 3.14). Mencionamos que há uma versão mais forte do item (2) abaixo (cf. [5], Lema 1.1).

Proposição C.9 *Se $a, b \in \dot{F}$, então*

(1) *$a \in D\langle 1, -b\rangle$ se, e somente se, $b \in D\langle 1, -a\rangle$.*

(2) *$D\langle 1, a\rangle \cap D\langle 1, b\rangle = D\langle 1, a\rangle \cap D\langle 1, -ab\rangle$.*

Demonstração. (1) $a \in D\langle 1, -b\rangle$ se, e somente se, $a = x^2 - by^2$, onde $x, y \in F$. Rearranjando os termos dessa última igualdade, obtemos: $b = (xy^{-1})^2 - a(y^{-1})^2 \in D\langle 1, -a\rangle$.

(2) Para mostrar a igualdade acima, é suficiente, por simetria, verificar a validade de $D\langle 1, a\rangle \cap D\langle 1, b\rangle \subset D\langle 1, -ab\rangle$. Tomemos, então, $x \in D\langle 1, a\rangle \cap D\langle 1, b\rangle$. Faremos uso do item (1) acima várias vezes. Temos: $x \in D\langle 1, a\rangle$ se, e somente se, $-a \in D\langle 1, -x\rangle$ e $x \in D\langle 1, b\rangle$ se, e somente se, $-b \in D\langle 1, -x\rangle$. Como $D\langle 1, -x\rangle$ é um grupo, $ab = (-a)(-b) \in D\langle 1, -x\rangle$, ou seja, $x \in D\langle 1, -ab\rangle$. ■

Proposição C.10 *Se f e g são formas arbitrárias sobre um corpo F, então*

$$D(f \perp g) = \bigcup \{D\langle x, y\rangle \,|x \in D(f) \text{ e } y \in D(g)\}$$

Demonstração. A inclusão "$\supseteq$" é imediata. Vamos provar a outra inclusão. Para tal, tomemos as diagonalizações $f = \langle a_1, \ldots, a_m\rangle$, $g = \langle a_{m+1}, \ldots, a_n\rangle$. Se $z \in D(f \perp g) = D\langle a_1, \ldots, a_n\rangle$, então $z = \sum_{i=1}^{m} a_i\alpha_i^2 + \sum_{i=m+1}^{n} a_i\alpha_i^2 \in D\langle x, y\rangle$, onde $x = \sum_{i=1}^{m} a_i\alpha_i^2 \in D(f)$ e $y = \sum_{i=m+1}^{n} a_i\alpha_i^2 \in D(g)$, como queríamos demonstrar. ■

Anéis de Witt abstratos

Anéis de Witt abstratos foram introduzidos no início dos anos 70 por Knebusch, Rosenberg e Ware em [19]. A motivação inicial para o estudo de tais anéis é a possibilidade de dar um tratamento unificado aos anéis de Witt definidos sobre corpos (com característica diferente de 2) ou sobre anéis semi-locais onde 2 é uma unidade. Em [19], muitos dos teoremas já conhecidos para anéis de Witt sobre corpos foram demonstrados nesse contexto mais geral, usando técnicas da teoria abstrata de anéis.

Em [18], Kleinstein e Rosenberg definiram classes de anéis de Witt abstratos: "sucintos", "representacionais" e "fortemente representacionais", sendo cada classe mais restritiva que a anterior. Mesmo a classe dos anéis de Witt fortemente representacionais ainda inclui os anéis de Witt definidos sobre anéis semi-locais onde 2 é unidade. Por outro lado, a introdução de axiomas adicionais permite a obtenção de um número maior de resultados.

Em seu livro [24], Marshall estuda a classe dos anéis de Witt abstratos fortemente representacionais. Por uma questão de simplicidade e como não há perigo de confusão, Marshall chama apenas de anéis de Witt abstratos aqueles que são fortemente representacionais. É o que faremos também aqui, já que seguiremos [24].

Um *anel de Witt abstrato* é um anel comutativo com unidade R munido de um subgrupo G_R do grupo multiplicativo R^* que tem expoente 2 e contém $-1 \in R$. Os elementos do grupo G_R são denominados *formas unidimensionais*. Assumimos ainda que:

(W1) R é aditivamente gerado por G_R.

Uma vez que $-1 \in G_R$ isso é equivalente a supor que todo elemento de R é da forma $r = a_1 + \cdots + a_n$, onde $a_1, \ldots, a_n \in G_R$ e $n \geq 1$. Denotamos por I_R o ideal de R gerado por elementos $r \in R$ da forma $r = a + b$, com $a, b \in G_R$, que denominamos *ideal fundamental* de R. Se $k \geq 1$, consideremos a seguinte propriedade "de Arason-Pfister":

AP(k): se $r = a_1 + \cdots + a_n \in I_R^k$, com $n < 2^k$ e $a_1, \ldots, a_n \in G_R$, então $r = 0$.

Seguindo a definição dada em [24], assumimos que

(W2) AP(1) e AP(2) valem em R.

Finalmente, assumimos que vale o seguinte:

(W3) Se $a_, \ldots, a_n, b_1, \ldots, b_n \in G_R$ são tais que $a_1 + \cdots + a_n = b_1 + \cdots + b_n$ e $n \geq 3$, então existem $a, b, c_3, \ldots, c_n \in G_R$ tais que $a_2 + \cdots + a_n = a + c_3 + \cdots + c_n$, $a_1 + a = b_1 + b$ (e, portanto, $b_2 + \cdots + b_n = b + c_3 + \cdots + c_n$).

O exemplo canônico de anel de Witt abstrato é o anel de Witt $W(F)$ de um corpo F. O grupo das classes de quadrados $G = \dot{F}/\dot{F}^2$ é um 2-grupo abeliano elementar. Os elementos $x \in G$ correspondem às (classes de) formas unidimensionais $\langle x \rangle \in W(F)$ e, por esta identificação, $-1 = (-1)\dot{F}^2 \in G$ corresponde à forma $-1 = \langle -1 \rangle$. Como $W(F)$ é aditivamente gerado pelas formas unidimensionais, o grupo G gera $W(F)$, logo vale (W1).

Para o anel de Witt $W(F)$, a propriedade de Arason-Pfister AP(k) vale para todo $k \geq 1$. Esse é um resultado importante da teoria dos anéis de Witt sobre corpos, descoberto por Arason e Pfister (daí o nome da propriedade anterior). Uma demonstração pode ser encontrada em [23], Teorema 5.1, página 352 ou em [31], Teorema 5.6, página 156. Em particular vale (W2) para o anel de Witt de um corpo. Mencionamos que uma conseqüência imediata da validade de AP(k), para todo $k \geq 1$ é que vale a propriedade de interseção de Krull para $W(F)$:

$$\bigcap_{n=0}^{\infty} I^n F = 0.$$

Finalmente, a propriedade (W3) é uma conseqüência do Teorema C.5 (cf. [24], Teorema 1.13, p. 16) e pode ser vista como uma *descrição indutiva da relação de isometria*.

A seguir iremos descrever um anel de Witt abstrato R como um quociente do anel de grupo $\mathbb{Z}[G_R]$. Por (W1), existe um homomorfismo sobrejetivo de anéis $\phi : \mathbb{Z}[G_R] \to R$. Se $[a]$ denota o elemento de $a \in G_R$ visto como elemento de $\mathbb{Z}[G_R]$, temos $\phi([a]) = a$, para todo $a \in G_R$. Assim, existe uma seqüência exata

$$0 \to J_R \to \mathbb{Z}[G_R] \xrightarrow{\phi} R \to 0 \tag{C.0.7}$$

onde J_R é o núcleo de ϕ. Logo, $R \simeq \mathbb{Z}[G_R]/J_R$.

De acordo com [24] , Teorema 4.3, página 66, o ideal J_R é gerado pelos elementos $[1] + [-1]$ e $([1] - [a])([1] - [b])$, onde $a, b \in G_R$ são tais que $(1 - a)(1 - b) = 0 \in R$.

Um morfismo de anéis de Witt abstratos $\varphi : R \to S$ é um homomorfismo de anéis que associa formas unidimensionais de R a formas unidimensionais de S, isto é, tal que

$\varphi(G_R) \subseteq G_S$. A composição de morfismos é claramente um morfismo e o homomorfismo id : $R \to R$ faz o papel de morfismo identidade. Os anéis de Witt abstratos formam assim uma categoria.

Dizemos que dois corpos são *quadraticamente equivalentes* quando seus anéis de Witt são isomorfos na categoria dos anéis de Witt. À luz do resultado de Arason e Pfister citado acima e da Proposição 4.6, página 70, de [24], para que dois corpos sejam quadraticamente equivalentes é suficiente que seus anéis de Witt sejam isomorfos na categoria dos anéis.

Dizemos que um anel de Witt abstrato R é *realizado* como anel de Witt de um corpo, quando existe um corpo F tal que R é isomorfo a $W(F)$ na categoria dos anéis de Witt.

A categoria dos anéis de Witt abstratos admite um produto que é exatamente aquele exibido no início do Capítulo 5 (cf. [24], Proposição 5.7, página 99). Admite também uma extensão por grupos de expoente 2 dada da seguinte maneira: se S é um anel de Witt abstrato e Δ é um grupo de expoente 2, seja $R = S[\Delta]$ e $G_R = G_S \times \Delta \subseteq R$. Então (R, G_R) é um anel de Witt abstrato (cf. [24], Proposição 5.16, página 111).

Se S é realizado como anel de Witt de um corpo F e Δ é um grupo de ordem 2, então R é realizado pelo corpo $K = F((t))$ das séries de potências formais sobre F. Isto é conseqüência de um resultado devido a Springer (cf. [22], página 37). Por outro lado, M. Kula demonstrou em [20], Teorema 3.3 que, se R e S são realizados como anéis de Witt sobre corpos, então $R \times S$ também é realizado como anel de Witt sobre um corpo.

A seguir, iremos considerar anéis de Witt abstratos R tais que $|G_R| < \infty$. Para maiores detalhes, remetemos o leitor ao livro [24]. Se $|G_R| = 1$, então existe (a menos de isomorfismo) apenas um anel de Witt R realizado como $W(\mathbb{C}) \simeq \mathbb{Z}/2\mathbb{Z}$ (cf. Exemplo (1), p.129). Se $|G_R| = 2$ temos (a menos de isomorfismo) três possibilidades, $W(\mathbb{R}) \simeq \mathbb{Z}$ (cf. Exemplo (2), p.130), $W(\mathbb{F}_q) \simeq \mathbb{Z}/4\mathbb{Z}$, onde $q \equiv 3 \mod 4$ ou $W(\mathbb{F}_q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, onde $q \equiv 1 \mod 4$ (cf. Exemplo (3), p.130). Denotamos esses anéis de Witt por $\mathbb{L}_1$, $\mathbb{L}_{1,0}$ e $\mathbb{L}_{1,1}$, respectivamente.

Se $p \neq 2$ é um número primo e $\mathbb{Q}_p$ é o corpo dos números p-ádicos, denotamos:

$$W(\mathbb{Q}_p) = \begin{cases} \mathbb{L}_{2,0} & \text{se} \quad p \equiv 1 \mod 4 \\ \mathbb{L}_{2,1} & \text{se} \quad p \equiv 3 \mod 4 \end{cases}.$$

Se $k \geq 2$ e F é uma extensão do corpo $\mathbb{Q}_2$ dos números 2-ádicos, denotamos:

$$W(F) = \mathbb{L}_{2k-1}, \quad \text{se} \quad [F : \mathbb{Q}_2] = 2k - 3.$$

No caso em que $[F : \mathbb{Q}_2] = 2k - 2$, temos:

$$W(F) = \begin{cases} \mathbb{L}_{2k,0} & \text{se} \quad \sqrt{-1} \in F \\ \mathbb{L}_{2k,1} & \text{se} \quad \sqrt{-1} \notin F \end{cases} .$$

Na realidade, os anéis

$$\mathbb{L}_{1,0},\ \mathbb{L}_{1,1},\ \mathbb{L}_{2k,0},\ \mathbb{L}_{2k,1},\ \mathbb{L}_{2k-1},\ k \geq 1 \tag{C.0.8}$$

podem ser definidos abstratamente, usando a noção de "estrutura quaterniônica", e demonstra-se que os mesmos são realizados como anéis de Witt dos corpos acima (cf. [24], capítulo 5, seções 3 e 9).

Um anel de Witt é dito de *tipo elementar* se pode ser obtido a partir dos anéis de Witt de (C.0.8) usando-se as operações de produto direto e formação de anel de grupo (na categoria dos anéis de Witt abstratos). Podemos, enunciar a

Conjectura de Tipo Elementar (Marshall, [24], p.123): se R é um anel de Witt abstrato com $|G_R| < \infty$, então R é de tipo elementar.

Finalizamos observando que a conjectura acima foi demonstrada no caso em que R é *reduzido*, ou seja, quando R admite apenas elementos nilpotentes triviais (cf. [24], Corolário 6.25, p. 165). No caso em que R é realizado como anel de Witt $W(K)$ de um corpo K, isso corresponde a afirmarmos que K é pitagórico.

Referências Bibliográficas

[1] Arason, J.K., Elman, R. and Jacob, B., *Rigid elements, valuations, and realization of Witt rings*, J. Algebra **110** (1987), 449-467.

[2] Berman, L. *Quadratic forms and power series fields*, Pac. J. Math., **89**, No.2 (1980), 257-268.

[3] Berman, L., Cordes, C., Ware, R., *Quadratic Forms, Rigid Elements, and Formal Power Series Fields*, Journal of Algebra **66** (1980), 123-133.

[4] Bos, R., *Quadratic Forms, Orderings and Abstract Witt Rings*, PhD Thesis, Ultrecht (1984).

[5] Bos, R., *A structure theorem for abstract Witt rings containing rigid elements*, Indag. Math., **92** (1989), 125-140.

[6] Bredikhin, S.V., Ershov, Yu. L. and Kal'nei, V.E., *Fields with two linear orderings*, Math. Notes (1970) 319-325.

[7] Bröcker, L., *Characterization of fans and Hereditary Pythagorean Fields*, Math. Z., **151** (1976), 149-163.

[8] Cordes, C.M. and Ramsey, Jr., J.R., *Quadratic forms over fields with* $u = q/2 < +\infty$, Fundamenta Mathematicae, **XCIX** (1978), 1-10.

[9] Efrat, I., *On fields with finite Brauer groups*, Pac. J. Math. **177** (1977), 33-46.

[10] Efrat, I., *Free product decomposition of Galois groups over pythagorean fields*, Communications in Algebra, **21** (1993), 4495-4511.

[11] Endler, O., *Valuation Theory*, Springer-verlag, (1972).

[12] Engler, A.J., *Totally Real Rigid Elements and Galois Theory*, Can.J.Math, **50**(6), (1998), 1189-1208.

[13] Engler, A.J., *Witt-Grothendieck Rings and π-henselianity*, Matemática Contemporânea, **16**, (1999), 31-44.

[14] Engler, A.J., *π-henselianity: a new approach*, Matemática Contemporânea, **16** (1999), 31-44.

[15] Engler, A.J., Normas, elementos rígidos, valorizações e radicais, notas não publicadas, (2004).

[16] Engler, A.J., Prestel, A., *Valued Fields*, Springer-Verlag, (2005).

[17] Griffin, M.P., *The pythagorean closure of fields*, Math. Scand., **38** (1976), 177-191.

[18] Kleinstein, I., Rosenberg, A., *Succint and representational Witt rings*, Pac. J. Math., **86**, (1980), 99-137.

[19] Knebusch, M., Rosenberg A., Ware, R., *Structure of Witt rings and quotients of abelian group rings*, Amer. J. Math. **94**, (1972) 119-155.

[20] Kula, M., *Fields with prescribed quadratic form schemes*, Math. Zeit., **167** (1979), 201-212.

[21] Lam, T.Y., *The Theory of Ordered Fields*, Ring Theory and Algebra III (B. McDonald, editor), Lecture Notes in Pure and Applied Math., **55**, Dekker, New York, (1980).

[22] Lam, T.Y., *Orderings, Valuations and Quadratic Forms*, **52** AMS, (1983).

[23] Lam, T.Y., *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics, **67**, American Mathematical Society, Providence, Rhode Island, (2005).

[24] Marshall, M., *Abstract Witt Rings*, Queen's Papers in Pure and Applied Math., **57**, Queen's University, Kingston, Ontario, Canada, (1980).

[25] Marshall, M., *The Witt ring of a space of orderings*, Trans. Amer. Math. Soc., **258** (1980), 505-521.

[26] Pfister, A., *Quadratic Forms with Applications to Algebraic Geometry and Topology*, London Mathematical Society Lecture Note Series, **217**, (1995).

[27] Prestel, A., C. N. Delzell, *Positive Polinomials - From Hilbert's 17th Problem to Real Algebra*, Monographs in Mathematics, Springer-Verlag, (2001).

[28] Ribenboim, P., *Théorie des Valuations*, Les Presses de l'Université de montréal, (1964).

[29] Ribenboim, P., *L'Arithmétique des Corps*, Hermann Paris (1972).

[30] Ribes, L., *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Applied Math., **24**, Queen's University, Kingston, Ontario, Canada, (1970).

[31] Scharlau, W., *Quadratic and Hermitian Forms*, A Series of Comprehensive Studies in Mathematics, **270**, Springer-Verlag (1985).

[32] Szymiczek, K., *Quadratic forms over fields*, Dissertationes Math. **152** (1977).

[33] Ware, R., *Quadratic forms and profinite* 2*-groups*, Journal of Algebra, **58**, (1979), 227-237.

[34] Ware, R., *Valuation Rings and Rigid elements in Fields*, Can. J. Math., **33**, (1981), 1338-1355.

[35] Wilson, J.S., *Profinite Groups*, London Mathematical Society Monographs, new series, **19**, (1998).

Índice Remissivo