Fábio Alexandre de Matos

Teorema 90 de Hilbert para o radical de Kaplansky e suas relações com o grupo de Galois do fecho quadrático

CAMPINAS
2014

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

FÁBIO ALEXANDRE DE MATOS

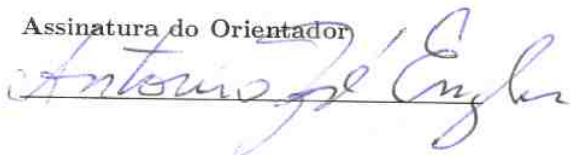
TEOREMA 90 DE HILBERT PARA O RADICAL DE KAPLANSKY E SUAS RELAÇÕES COM O GRUPO DE GALOIS DO FECHO QUADRÁTICO

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em matemática.

Orientador: Antonio José Engler

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO FÁBIO ALEXANDRE DE MATOS. E ORIENTADA PELO PROF. DR. ANTONIO JOSÉ ENGLER.

Assinatura do Orientador



CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

M428t

Matos, Fábio Alexandre de, 1976-
Teorema 90 de Hilbert para o radical de Kaplansky e suas relações com o grupo de Galois do fecho quadrático. / Fábio Alexandre de Matos. – Campinas, SP : [s.n.], 2014.

Orientador: Antonio José Engler.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Radical de Kaplansky. 2. Teoria de Galois. 3. Formas quadráticas. 4. Grupo de Brauer. I. Engler, Antonio José,1944-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Hilbert's Theorem 90 for the Kaplansky's radical and its relations with Galois group of quadratic closure
Palavras-chave em inglês:
Kaplansky's radical
Galois Theory
Quadratic forms
Brauer group
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Antonio José Engler [Orientador]
Dessislava Hristova Kochloukova
Paulo Roberto Brumatti
Pavel Zalesski
Ronie Peterson Dario
Data de defesa: 25-04-2014
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 25 de abril de 2014 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). PAULO ROBERTO BRUMATTI

Prof(a). Dr(a). PAVEL ZALESSKI

Prof(a). Dr(a). RONIE PETERSON DARIO

Resumo

Apresentaremos neste trabalho um estudo sobre a aritmética corpos de característica distinta de 2 com um número finito de classes de quadrados. Dividido em duas partes, começaremos com um estudo do radical de Kaplansky de um corpo F e seu comportamento em 2-extensões de F. Na segunda parte introduziremos um novo objeto, as bases distinguidas, e exploraremos suas propriedades obtendo uma generalização do Teorema 90 de Hilbert, versão para o radical de Kaplansky e propriedades cohomológicas de corpos que possuam base distinguida.

Abstract

We will present in this work a study about the arithmetic of fields of characteristic different from 2 with a finite number of square class. Divided in two parts, we will start with a study of the Kaplansky's radical of a field F and its behavior in 2-extensions of F. In the second part will introduce a new object, the distinguished bases, and we will explore its properties obtaining a generalization of Hilbert's Theorem 90 for the Kaplansky's radical and cohomological properties of fields that own distinguished basis.

Sumário

Dedico este trabalho aos meus pais Edson e Maria do Carmo.

Agradecimentos

Ao Prof. Antonio José Engler, pela orientação, ensinamentos e seriedade profissional com que conduziu este trabalho.

Agradeço, em especial, aos meus pais Edson e Maria do Carmo, por incentivarem meus estudos e em alguns momentos se sacrificarem para que eu tivesse a melhor formação profissional possível.

Aos meus irmãos Júlio, Daniela, Fernanda e Denise, pelo carinho e amizade.

À minha amada esposa Aline que, com seu amor e companheirismo, não me deixou desanimar no longo caminho percorrido até a realização deste trabalho.

A todos os professores que fizeram parte da minha vida acadêmica e sempre me incentivaram a prosseguir em meus estudos e a não desistir de meus objetivos.

A todos os funcionários do IMECC-Unicamp, pela gentileza e atenção prestados.

À FAPESP pela bolsa de estudos concedida (Processo 03/12126-7).

Também quero dizer que me sinto muito feliz de ter encontrado durante o período de doutorado grandes amigos, como o Júlio, Dudu e Guilherme.

Enfim, agradeço a todos que colaboraram de alguma forma para a realização deste trabalho.

Muito Obrigado!

Introdução

Antes de entrarmos na apresentação dos resultados principais da tese, vamos fixar algumas notações e definições que irão aparecer com maior frequencia. No decorrer do trabalho, todos os corpos considerados são de característica distinta de 2. Para um corpo F, usaremos sempre $F^\times$, $(F^\times)^2$ e $\sum F^2$ para denotar os grupos multiplicativos dos elementos não nulos de F, dos quadrados de $F^\times$ e das somas de quadrados não nulas. Ainda, todas as formas quadráticas serão consideradas na forma diagonal e uma forma quadrática q n-dimensional sobre F será denotada por $q = \langle a_1, \ldots, a_n \rangle_F$, e o conjunto de valores não nulos representados por q em F será indicado por $D_F(q)$. Denotaremos por $W(F)$ o anel de Witt do corpo F, isto é, o anel formado pelas classes de anisotropia das formas quadráticas. Para mais informações sobre o anel de Witt sugerimos [**L**]. Denotaremos ainda por IF o ideal fundamental de $W(F)$, que é gerado pelas formas quadráticas de dimensão par.

A álgebra de quatérnios sobre F gerado pelos símbolos a e b será denotada por $(a, b)_F$ e a parte de $2-$torção do grupo de Brauer será denotada por ${}_2Br(F)$. Usaremos $(a, b)_F$ tamém para representar, caso não haja ambiguidade, a classe de ${}_2Br(F)$ representada pela álgebra de quatérnios $(a, b)_F$.

A reunião de todas as extensões galoisianas de grau potência de 2 de F será denotada por $F(2)$ e o respectivo grupo de Galois, $Gal(F(2)/F)$, por $G_2(F)$. Finalmente, o n-ésimo grupo de cohomologia de $G_2(F)$ com coeficientes no corpo $\mathbb{F}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ será denotado simplesmente por $H^n(F)$. No Capítulo 1, o leitor encontrará resultados extraídos da literatura sobre sobre formas quadráticas, grupo de Brauer que utilizaremos com frequencia nos capítulos seguintes; O leitor que esteja familiarizado pode seguir diretamente para o capítulo 2.

Em 1969 no trabalho *Fröhlich's local quadratic forms*, Irving Kaplansky definiu um novo objeto para um corpo F, que chamou simplesmente de radical. O Radical de Kaplansky, como ficou conhecido na literatura, é definido a partir das 2-formas de Pfister. Mais especificamente, o Radical de Kaplansky é o conjunto, denotado usualmente por $R(F)$, dos elementos $x \in F^\times$ tais que a $2-$forma de Pfister $\langle 1, -x \rangle$ é universal, isto é, $D_F\langle 1, -x \rangle = F^\times$. Equivalentemente, temos que $R(F)$ é o conjunto dos elementos $x \in F^\times$ tais que $(x, y)_F \simeq M_2(F)$, para todo $y \in F^\times$. Segue diretamente da definição do radical de Kaplansky que $R(F)$ é um subgrupo do grupo multiplicativo $F^\times$ e $(F^\times)^2 \subseteq R(F) \subseteq F^\times$. Podemos dizer que o radical de Kaplansky se tornou peça central no desenvolvimento do nosso trabalho e o Capítulo 2 da tese é totalmente dedicado a ele. Este capítulo se divide em 3 partes, sendo a primeira delas dedicada somente ao estudo do radical de Kaplsnky e o comportamento do radical em extensões quadráticas $K = F(\sqrt{a})$, onde $a \in F^\times \setminus (F^\times)^2$.

Na segunda parte, apresentamos um estudo mais detalhado sobre o radical de Kaplansky e extensões quadráticas $K = F(\sqrt{a})$, onde $a \in R(F) \setminus (F^\times)^2$, que chamamos de extensões quadráticas radicais de F. Podemos destacar nesta parte do trabalho o **Teorema 2.2.4**, onde mostramos que o radical de Kaplansky de uma extensão quadrática $K = F(\sqrt{a})$ é determinado diretamente pelas classes de quadrados de F. Nesta parte do trabalho, tínhamos como objetivo mostrar uma versão do Teorema 90 de Hilbert para o radical de Kaplansky e extensões quadráticas radicais. Mais especificamente, tínhamos o objetivo de mostrar que para uma extensão radical $K = F(\sqrt{a})$, $N^{-1}_{K/F}R(F) = F^\times R(K)$. Demonstramos a validade deste teorema no Capítulo 3, com o uso das bases distinguidas(veja **Definição 3.2.1**).

Encerraremos o Capítulo 2 apresentando, em analogia ao fecho quadrático $F(2)$, um fecho para o radical de Kaplansky. Este fecho não é novidade na literatura, pois foi apresentado primeiramente por *Becher* em [**B**]. Denotando o fecho radical por F_{red}, nos dedicaremos a uma apresentação construtiva deste fecho, diferentemente da apresentação existencial de Becher. Nossa construção fornecerá informações mais precisas sobre este corpo e reunimos as propriedades principais sobre o fecho reduzido no **Teorema 2.3.13.** Com a validade do Teorema 90 de Hilbert citado acima, mostraremos no Capítulo 3 que a extensão F_{red}/F é galoisiana com grupo de Galois $Gal(F_{red}/F)$ livre, **Teorema 3.2.23**.

Antes de apresentarmos os capítulos restantes, é válido ressaltar que nosso foco, desde o início, era demonstrar que para um corpo F tal que $|_2Br(F)| = 2$, isto é, se F possui somente duas álgebras de quatérnios, a menos de isomorfismo, o grupo $Gal(F(2)/F)$ é isomorfo a um produto livre, na categoria dos pro-2 grupos, de um grupo de Demushkin por um grupo livre de posto finito. Para a definição de produto livre sugerimos [**RZ**].

Esperávamos com a construção do fecho reduzido F_{red} e o Teorema 90 de Hilbert teríamos os objetos necessários para a demonstração da conjectura inicial, mas infelizmente este objetivo não foi alcançado em geral. Apesar de não conseguirmos a demonstração no caso citado, com a introdução de novos objetos que descobrimos no decorrer dos estudos, conseguimos demonstrar que a decomposição vale para corpos bem específicos, a saber, **Teorema 4.1.18**. E dentre os corpos para os quais demonstramos valer a decomposição do grupo de Galois se inserem os corpos tais que $\dim_{\mathbb{F}_2} F^\times/R(F) = 1$, que são corpos formalmente reais com duas álgebras de quatérnios, a menos de isomorfismo.

Vamos voltar a falar da conjectura em geral, pois dela extraímos objetos interessantes. A expectativa de demonstrar que o grupo de Galois $Gal(F(2)/F)$, onde F é um corpo tal que $|_2Br(F)| = 2$, é decomponível em um produto livre da forma $\mathcal{L} * \mathcal{D}$ com $\mathcal{L}$ livre e $\mathcal{D}$ de Demushkin, vem dos seguintes fatos:

1. Se F é um corpo tal que $R(F) = F^\times$ e $F^\times/R(F)$ tem dimensão finita como $\mathbb{F}_2-$espaço vetorial, então $G_2(F)$ é livre de posto finito.

2. Se F é um corpo tal que $R(F) = (F^\times)^2$ e $F^\times/R(F)$ tem dimensão finita como $\mathbb{F}_2-$ espaço vetorial, então $G_2(F)$ é um grupo de Demushkin.

E nossa estratégia era a de construir duas extensões L e H satisfazendo a segunda afirmação do seguinte teorema devido a Neukirch:

Teorema *Sejam F um corpo qualquer e $\{H_j \subseteq F(2)\}$, $j \in J$, $2-$extensões de F. Denotando por G_j o grupo de galois $Gal(F(2)/H_j)$, são equivalentes:*

(i) $G_2(F) \simeq *_{j\in J} G_j$

(ii) $Res^i : H^i(G) \longrightarrow \bigoplus_{j\in J} H^i(G_j)$, *é um isomorfismo para* $i = 1$ *e monomorfismo para* $i = 2$, *onde* Res^i *e á função restrição.*

Com este objetivo paralizado, fizemos o caminho inverso utilizando o teorema acima. Isto é, assumimos ter um corpo F tal que o $G_2(F)$ possui uma decomposição em produto livre na categoria dos pro-2 grupos da forma

$$G_2(F) \simeq \mathcal{L} * \mathcal{D}_1 * \cdots * \mathcal{D}_t,$$

onde $\mathcal{D}_i$ é um grupo de Demushkin para todo $i = 1, \ldots, t$ e $\mathcal{L}$ é um grupo livre. Nesse caminho descobrimos a necessidade de o grupo quociente $F^\times/R(F)$ posssuir uma base, como $\mathbb{F}_2-$espaço vetorial, com boas propriedades. Mais especificamente, para que tal decomposição seja verdadeira é necessário, mas ainda não mostramos ser suficiente, que o $\mathbb{F}_2-$espaço vetorial $F^\times/R(F)$ possuia uma base $\{x_1, \ldots, x_n\}$, que, dentre outras propriedades, satisfaça $(F^\times : D_F\langle 1, -x_i\rangle) = 2$, para todo $i = 1, \ldots, n$. A esta base demos o nome de *Base Distinguida.*

Pensávamos agora que nosso objetivo não era de todo inoportuno, pois se F é um corpo tal que $|_2Br(F)| = 2$, então toda base de $F^\times/R(F)$ é uma base distinguida. Este fato é verdadeiro pois sabemos que para um elemento $x \in F^\times \setminus R(F)$, o conjunto das álgebras gerados por x, usualmente denotado por $Q_F(x)$, é isomorfo como $\mathbb{F}_2-$espaço vetorial a $F^\times/D_F\langle 1, -x\rangle$. Desta forma, como $Q_F(x)$ é um subgrupo de $_2Br(2)$, temos que $(F^\times : D_F\langle 1, -x\rangle) \leq 2$.

Continuando com a descrição do trabalho, no Capítulo 3, além de apresentarmos formalmente as bases distinguidas, faremos um estudo sobre extensões quadráticas radicais de um corpo F que possui base distinguida. Podemos destacar como resultados principais, os **Teoremas 3.2.23 e 3.2.27.** O primeiro deles é o Teorema 90 de Hilbert, já mencionado acima. Este resultado é uma das contribuições da tese, uma vez que generaliza as versões encontradas na literatura até então. Ainda, como consequência deste resultado, mostramos que o grupo de Galois $Gal(F_{ref}/F)$ é livre, assumindo que F é um corpo com base distinguida.

O segundo teorema que destacamos garante que se F possui base distinguida completa(veja **Definição 3.2.13**) então toda extensão quadrática $K = F(\sqrt{a})$ radical também possui base distinguida completa. Podemos ressaltar que, no caminho para encontrar estes resultados, obtivemos muitos resultados auxiliares que também são importantes e que motivaram a continuidade dos estudos.

No Capítulo 4, continuamos nossos estudos sobre a existência de bases distinguidas para extensões quadráticas, agora sem a restrição de radicalidade. E neste caminho chegamos a conclusões

importantes sobre a estrutura cohomológica dos corpos com base distinguida. O resultado mais importante que obtivemos neste capítulo é o **Teorema 4.1.20**, que garante que se F é um corpo com base distinguida completa cuja partição principal não possui subconjuntos unitários(veja Definição 1.2.4) então a dimensão cohomológica de F é igual a 2, isto é, $H^i(F)$ é nulo para todo $i \geq 3$. A parte final do capítulo é dedicado ao caso em que a base distinguida completa do corpo F admite partições unitárias. Nesta parte final demonstramos o **Teorema 4.1.15**, que entre outras afirmações, garante que F, neste caso, é formalmente real com tantas ordens quantas forem os subconjuntos unitários da partição principal.

Finalmente, dedicaremos o último capítulo da tese para o estudo das extensões quadráticas não radicais de corpos com base distinguida completa. Apresentaremos neste capítulo o Teorema 90 de Hilbert, versão radical de Kaplansky, para extensões quadráticas não radicais de corpos com base distinguida completa, **Teorema 5.1.8**. Ainda, mostraremos a existência de base distinguida para extensões quadráticas não radicais de corpos com base distinguida completa. Este último fato, juntamente com os resultados alcançados no Capítulo 3, garantem a existência de base distinguida para $2-$extensões finitas quaisquer de F.

Capítulo 1

Preliminares

Com o objetivo de dar completude ao trabalho, apresentaremos neste capítulo alguns resultados sobre a teoria algébrica das formas quadráticas, álgebra de quatérnios e o Teorema 90 de Hilbert, versão extraída da Teoria de cohomologia de grupos. Salientamos que estes resultados aparecem dispersos na literatura e para um estudo mais geral, sugerimos [**L**], [**M**] e [**R**]. Ainda, poderemos omitir algumas demonstrações, dando as devidas referências.

1.1 Resultados sobre formas quadráticas

Assumiremos, para o restante do trabalho, que o leitor esteja familiarizado com as notações e resultados gerais acerca das formas quadráticas sobre um corpo F. Entretanto, alguns resultados extraídos da literatura que foram importantes para o desenvolvimento serão apresentados.

Neste capítulo, as formas quadrática que desempenharão papel importante serão as $n-$forma de Pfister, que serão denotadas por $\langle\langle a_1, \ldots, a_n\rangle\rangle$.

Usaremos com frequência que se q é uma forma de Pfister, então $D_F(q)$ é subgrupo de $F^\times$, veja [**L**]. E estes grupos serão muito importantes para a desenvolvimento do trabalho.

Ainda, pela [**L**], IF é um ideal de $W(F)$ e é gerado, como grupo abeliano aditivo, pelas $1-$formas de Pfister. Além disso, para cada $n \in \mathbb{N}$ podemos considerar as potências do ideal fundamental, I^nF, que são geradas, aditivamente, pelas $n-$formas de Pfister. Desta forma, temos que $I^mF \subseteq I^nF$ se $m \geq n$, e usaremos os grupos quocientes $I^nF/I^{n+1}F$ para fazer a ligação entre a Teoria de formas quadráticas e a Cohomologia Galoisiana, que estabeleceremos mais adiante.

Apresentaremos, a seguir, resultados envolvendo $q-$formas de Pfister, os grupo de valores das $q-$forma de Pfister $D_F(q)$, e o ideal fundamental, IF, do anel de Witt do corpo F.

Lema 1.1.1. *Sejam F um corpo e $a, b \in F^\times$. Então $a \in D_F\langle 1, -b\rangle$ se, e somente se, $b \in D_F\langle 1, -a\rangle$.*

Demonstração. Pela simetria do resultado, vamos mostrar simplesmente que se $a \in D_F\langle 1, -b\rangle$, então $b \in D_F\langle 1, -a\rangle$. Vejamos, se $a \in D_F\langle 1, -b\rangle$, então existem $c, d \in F^\times$, não ambos nulos, tais

que $a = c^2 - bd^2$. Se $d = 0$, então $a \in (F^\times)^2$ e a 1-forma de pfister $\langle 1, -a\rangle$ é universal, o que implica que $b \in D_F\langle 1, -a\rangle$. Supondo então que $d \neq 0$ e multiplicando a igualdade por d^{-2}, teremos que $b = (cd^{-1})^2 - a(d^{-1})^2$, isto é, $b \in D_F\langle 1, -a\rangle$. □

Vamos relembrar, na definição a seguir, as operações do anel de Witt $W(F)$.

Definição 1.1.2. *Se $q_1 \simeq \langle a_1, \ldots, a_n\rangle$ e $q_2 \simeq \langle b_1, \ldots, b_m\rangle$, são duas formas quadráticas em $W(F)$, então*

1. *a soma de q_1 e q_2, usualmente denotada por $\perp$, é dado por*

$$q_1 \perp q_2 \simeq \langle a_1, \ldots, a_n, b_1, \ldots, b_m\rangle;$$

2. *a produto de q_1 e q_2, usualmente denotada por $\otimes$, é dado por*

$$q_1 \otimes q_2 \simeq \langle a_1b_1, \ldots, a_ib_j, \ldots, a_nb_m\rangle.$$

Note que $q_1 \perp q_2$ tem dimensão $n + m$ e $q_1 \oplus q_2$ tem dimensão nm.

Lema 1.1.3. *Seja φ uma $n-$forma de Pfister qualquer sobre um corpo F. Para $a, b \in F^\times$ temos que*

$$D_F(\varphi \otimes \langle 1, -a\rangle) \cap D_F(\varphi \otimes \langle 1, -b\rangle) = D_F(\varphi \otimes \langle 1, -a\rangle) \cap D_F(\varphi \otimes \langle 1, -ab\rangle)$$

Demonstração. Desde que as formas $\langle 1, -b\rangle$ e $\langle 1, -a^2b\rangle$ são isométricas, basta mostrar que

$$D_F(\varphi \otimes \langle 1, -a\rangle) \cap D_F(\varphi \otimes \langle 1, -b\rangle) \subseteq D_F(\varphi \otimes \langle 1, -a\rangle) \cap D_F(\varphi \otimes \langle 1, -ab\rangle).$$

Seja $x \in D_F(\varphi \otimes \langle 1, -a\rangle)$. Considerando que φ é uma $n-$forma de Pfister, então existem 2^n-uplas z_1, z_2, z_1', z_2' tais que $x = \varphi(z_1) - a\varphi(z_2) = \varphi(z_1') - b\varphi(z_2')$.

Agora, se $\varphi(z_2) = 0$ ou $\varphi(z_2') = 0$, então $x = \varphi(z_1)$ ou $x = \varphi z_1'$, mas em todo caso, temos que $x \in D_F(\varphi)$ e a inclusão está demonstrada, uma vez que $D_F(\varphi)$ é um subgrupo de $D_F(\varphi \otimes \langle 1, -a\rangle)$, $D_F(\varphi \otimes \langle 1, -b\rangle)$ e $D_F(\varphi \otimes \langle 1, -ab\rangle)$.

Assuma então que $\varphi(z_2) \neq 0$ e $\varphi(z_2') \neq 0$. Daí, temos que $a = \varphi(z_1)\varphi(z_2)^{-1} - x\varphi(z_2)^{-1}$ e $b = \varphi(z_1')\varphi(z_2')^{-1} - x\varphi(z_2')^{-1}$ e ambos estão em $D_F(\varphi \otimes \langle 1, -x\rangle)$. Desta maneira, temos que $ab \in D_F(\varphi \otimes \langle 1, -x\rangle)$, desde que $D_F(\varphi \otimes \langle 1, -x\rangle)$ é um subgrupo de $F^\times$. Logo, existem duas 2^n-uplas u, v tais que $ab = \varphi(u) - x\varphi(v)$.

Suponha que $\varphi(v) = 0$. Então $ab = \varphi(u)$ e, consequentemente, podemos escrever $a = \varphi(u)b^{-2}b$. Agora, $\varphi(\alpha) - a\varphi(\beta) = \varphi(\alpha) - bb^{-2}\varphi(u)\varphi(\beta) \in D_F(\varphi \otimes \langle 1, -b\rangle)$, onde α, β são duas 2^n-uplas quaisquer. Dái, $D_F(\varphi \otimes \langle 1, -a\rangle) \subseteq D_F(\varphi \otimes \langle 1, -b\rangle)$. Analogamente, como estamos assumindo $ab = \varphi(u)$, podemos escrever $b = \varphi(u)a^{-2}a$ e pelos mesmos argumentos, temos que $D_F(\varphi \otimes \langle 1, -b\rangle) \subseteq D_F(\varphi \otimes \langle 1, -a\rangle)$. Portanto, $D_F(\varphi \otimes \langle 1, -a\rangle) = D_F(\varphi \otimes \langle 1, -b\rangle)$. Usando o mesmo procedimento acima com ab e 1, teríamos que $D_F(\varphi \otimes \langle 1, -ab\rangle) = D_F(\varphi \otimes \langle 1, -1\rangle) = F^\times$. Concluímos assim que se $\varphi(v) = 0$, então a inclusão segue.

Suponha agora que $\varphi(v) \neq 0$. Então, $x = \varphi(u)\varphi(v)^{-1} - ab\varphi(v)^{-1} \in D_F(\varphi \otimes \langle 1, -ab\rangle)$ e a inclusão também é verdadeira.

□

Sabemos que toda extensão quadrática de um corpo F, $K = F(\sqrt{a})$, é galoisiana. Considerando o grupo de Galois $\mathrm{Gal}(K/F) = \{1, \sigma\}$, a aplicação $N : K \longrightarrow F$, dada por $N(x) = x\sigma(x)$ é chamada de função **norma** da extensão K/F.

Observe que se $x \in K^\times$, então $x = \alpha + \beta\sqrt{a}$, com $\alpha, \beta \in F$ não ambos nulos. Portanto,

$$N(x) = (\alpha + \beta\sqrt{a})(\alpha - \beta\sqrt{a}) = \alpha^2 - \beta^2 a \in D_F\langle 1, -a\rangle.$$

E reciprocamente, se dado $c \in D_F\langle 1, -a\rangle$, temos que existem $\alpha, \beta \in F$, não ambos nulos, tais que $c = \alpha^2 - \beta^2 a$. Tomando $x = \alpha + \beta\sqrt{a} \in K^\times$ segue que $N(x) = c$.

Portanto, temos que $N(K^\times) = D_F\langle 1, -a\rangle$.

Enunciaremos a seguir o Teorema 90 de Hilbert, que será utilizado no decorrer do trabalho.

Teorema 1.1.4 (Teorema 90 de Hilbert)**.** *Sejam $K = F(\sqrt{a})$, uma extensão quadrática de F, e $x \in K^\times$. Então $N(x) = 1$, se, e somente se, existe $y \in K$ tal que $x = \dfrac{y}{\sigma(y)}$, onde σ é o gerador de* $\mathrm{Gal}(K/F)$. *Em particular, $N(x) \in (F^\times)^2$ se, e somente se, $x \in F^\times(K^\times)^2$.*

Demonstração. [**La**] □

Sabemos que para um corpo F, $(F^\times)^2$ é subgrupo de $F^\times$. Desta forma, podemos definir a seguinte função, induzida pela inclusão,

$$r^* : \frac{F^\times}{(F^\times)^2} \longrightarrow \frac{K^\times}{(K^\times)^2},$$

dada por $r^*(c(F^\times)^2) = c(K^\times)^2$.

Ainda, como $N(K) \subseteq F^\times$, podemos também definir

$$\overline{N} : \frac{K^\times}{(K^\times)^2} \longrightarrow \frac{F^\times}{(F^\times)^2},$$

dada por $\overline{N}(z(K^\times)^2) = N(z)(F^\times)^2$. As aplicações r^* e $\overline{N}$ não homomorfismos de grupos.

Lema 1.1.5. *Considere $K = F(\sqrt{a})$, r^* e $\overline{N}$ como acima. Então*

$$1 \longrightarrow \{(F^\times)^2, a(F^\times)^2\} \longrightarrow \frac{F^\times}{(F^\times)^2} \xrightarrow{r^*} \frac{K^\times}{(K^\times)^2} \xrightarrow{\overline{N}} \frac{D_F\langle 1, -a\rangle}{(F^\times)^2} \longrightarrow 1,$$

é uma sequência exata de grupos e homomorfismos.

Demonstração. Note que se $x \in F^\times \cap (K^\times)^2$, então $x = (\alpha + \beta\sqrt{a})^2 = \alpha^2 + a\beta^2 + 2\alpha\beta\sqrt{a}$. Logo, temos que $2\alpha\beta = 0$ e assim, $x = \alpha^2 \in (F^\times)^2$ ou $x = a\beta^2 \in a(F^\times)^2$. E como $a \in (K^\times)^2$, temos que a sequência é exata em $\dfrac{F^\times}{(F^\times)^2}$. Além disso, $\overline{N}$ é sobrejetora, pois $D_F\langle 1, -a\rangle$ é a imagem da função norma.

Falta então mostrar que a sequência é exata em $\dfrac{\dot{K}}{(K^\times)^2}$. Note que $N(\alpha) = \alpha^2$ para todo $\alpha \in F$ e assim, a imagem de r^* está contida no núcleo de $\overline{N}$. Reciprocamente, seja $z \in K$ tal que $N(z) \in (F^\times)^2$, ou seja, $N(z) = \alpha^2$ para algum $\alpha \in F^\times$. Daí, temos que $N(z\alpha^{-1}) = 1$ e, pelo **Teorema 1.1.4**, existe $u \in K$ tal que $z\alpha^{-1} = \dfrac{u}{\sigma(u)}$, onde σ é o gerador de $Gal(K/F.)$ Assim,

$$\frac{z}{\alpha} = \frac{u}{\sigma(u)} = \frac{u^2}{u\sigma(u)} = \frac{u^2}{N(u)},$$

o que implica que

$$z = \frac{\alpha}{N(u)}u^2 \in \frac{\alpha}{N(u)}(K^\times)^2.$$

Portanto, z pertence à imagem da função r^*.

□

Sejam F e $K = F(\sqrt{a})$ como acima e para $y = b + c\sqrt{a} \neq 0 \in K$ defina o seguinte funcional linear

$$\begin{array}{rccc} s_y: & K & \longrightarrow & F \\ & \alpha + \beta\sqrt{a} & \longmapsto & \alpha c - \beta b. \end{array}$$

Vamos a seguir recordar alguns fatos envolvendo o transfer de Scharlau. Para o funcional definido acima, tomaremos as construções que podem ser encontradas em [**L**]. Ainda, usaremos a função transfer apresentada em [**CR**].

Proposição 1.1.6 (Cordes-Ramsey)**.** *Sejam $x, y \in K$ e considere o funcional linear s_y definido acima. Então $s_y^*\langle x\rangle = \gamma\langle 1, -N(xy)\rangle$, onde $\gamma \in D_F(s_y^*\langle x\rangle)$ e N denota a função norma da extensão K/F.*

Demonstração. Temos que $x = \alpha+\beta\sqrt{a}$ e $y = b+c\sqrt{a}$ e desta maneira, $xy = \alpha b+\beta ca+(\alpha c+\beta b)\sqrt{a}$. Além disso, a forma $\langle x\rangle_K$ tem por forma bilinear

$$\begin{array}{rccc} B_x: & K \times K & \longrightarrow & K \\ & (z, t) & \longmapsto & xzt. \end{array}$$

Tomando a base $\{1, \sqrt{a}\}$ de K sobre F, temos que a matriz da forma bilinear $s_y(B_x)$ será

$$\begin{pmatrix} s_y(x) & s_y(\sqrt{a}x) \\ s_y(\sqrt{a}x) & s_y(ax) \end{pmatrix} = \begin{pmatrix} \alpha c - \beta b & a\beta c - \alpha b \\ a\beta c - \alpha b & a(\alpha c - \beta b) \end{pmatrix},$$

que tem determinante $a(\alpha c - \beta b)^2 - (a\beta c - \alpha b)^2$.

Note que $a(\alpha c-\beta b)^2-(a\beta c-\alpha b)^2 = a(\alpha c+\beta b)^2-(a\beta c+\alpha b)^2$, pois desenvolvendo os quadrados teremos $2abc\alpha\beta-2abc\alpha\beta$ no primeiro e $-2abc\alpha\beta+2abc\alpha\beta$ no segundo caso, e ambos são iguais a 0. Logo o determinante da matriz é $a(\alpha c+\beta b)^2-(a\beta c+\alpha b)^2 = -((a\beta c+\alpha b)^2-a(\alpha c+\beta b)^2) = -N(xy)$. Por construção, temos que a dimensão de $s_y^*\langle x\rangle$ é 2. Agora, tomando $\gamma \in D_F(s_y^*\langle x\rangle)$, então $s_y^*\langle x\rangle \simeq \langle \gamma, -\gamma N(xy)\rangle$, e o resultado segue.

□

O resultado acima nos dá a imagem da função transfer para um elemento $y \in K$ qualquer. No próximo resultado, vamos fazer uma relação entre a função transfer s_y^* e a função transfer s_1^*, denotada simplesmente por s^*.

Corolário 1.1.7. *Sejam $K = F(\sqrt{a})$ uma extensão quadrática do corpo F, $s : K \to F$ o funcional liner satisfazendo $s(1) = 0$ e $s(\sqrt{a}) = 1$, e N a função norma da extensão K/F.*

Para o funcional linear s_y, temos que $s_y(kz) = s(z)$ para todo $z \in K$, onde $k = -y/N(y)$.

Ainda, para as respectivas funções transfer temos $s_y^* \circ \langle k\rangle = s^*$.

Demonstração. Sejam $z = u + v\sqrt{a}, y = b + c\sqrt{a} \in K$. Então $yz = (bu + acv) + (bv + cu)\sqrt{a}$ e

$$s_y(kz) = s_y\left(\left(\frac{-(bu+acv)}{N(y)}\right) + \left(\frac{-(bv+cu)}{N(y)}\right)\sqrt{a}\right) =$$

$$= c\left(\frac{-(bu+acv)}{N(y)}\right) - b\left(\frac{-(bv+cu)}{N(y)}\right) = \frac{-cbu - ac^2v + b^2v + bcu}{N(y)} =$$

$$= v\,\frac{b^2-ac^2}{N(y)} = v = s(u+v\sqrt{a}) = s(z),$$

ficando assim demonstrada a relação entre s_y e s, do que decorre $s_y^* \circ \langle k\rangle = s^*$. □

Corolário 1.1.8. *Mantendo as notações do **Corolário 1.1.7**, considere q uma forma quadrática sobre o corpo $K = F(\sqrt{a})$. Então $s_y^*(q)$ é isotrópica se, e somente se, existe $f \in F^\times$ tal que $fy \in D_K(q)$.*

Demonstração. Suponha que $s_y^*(q)$ seja isotrópica. Então existe $x \in D_K(q)$ tal que $s_y(x) = 0$. Mas isso implica que $x \in \ker s_y = yF$. Assim, temos que $x = fy$, para algum $f \in F$. Por outro lado, se existe $f \in F$ tal que $x = fy$, temos que $s_y(x) = 0$ e portanto, $s_y^*(q)$ é isotrópica. □

Este resultado finaliza o estudo da função transfer. Apresentaremos agora o **princípio da norma** que será uma de muitas aplicações das funções transfer.

Teorema 1.1.9 (Princípio da Norma)**.** *Sejam F um corpo e $K = F(\sqrt{a})$ uma extensão quadrática de F. Denotando por N a função norma da extensão, então para $x \in K^\times$ e $c \in F^\times$ temos o seguinte:*

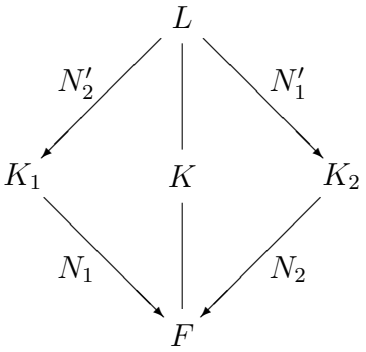
$$N(x) \in D_F\langle 1, -c\rangle \text{ se, e somente se } x \in F^\times D_K\langle 1, -c\rangle.$$

Demonstração. Note que $N(x) \in D_F\langle 1,-c\rangle$ é equivalente a $\langle 1,-c,-N(x),cN(x)\rangle_F$ ser isotrópica sobre F. Agora, pela **Proposição 1.1.6**, $s^*(\langle x\rangle \otimes \langle 1,-c\rangle_K) = s^*(\langle x\rangle) \perp -cs^*(\langle x\rangle) = \alpha\langle 1,-c,-N(x),cN(x)\rangle$, onde $\alpha \in F^\times$. Logo, $s^*(x \otimes \langle 1,-c\rangle_K)$ é isotrópica, que é equivalente a $F^\times \cap D_K(x \otimes \langle 1,-c\rangle_K) \neq \emptyset$ pelo **Corolário 1.1.8**, com $y = 1$. Desta forma, temos que $N(x) \in D_F\langle 1,-c\rangle$, se, e somente se, existe $\beta \in F^\times$ tal que $\beta \in D_K(x \otimes \langle 1,-c\rangle_K)$. Mas daí, $\beta = xy$, onde $y \in D_K\langle 1,-c\rangle$ e consequentemente, $x = \beta y^{-1} \in F^\times D_K\langle 1,-c\rangle$, pois $D_K\langle 1,-c\rangle$ é um subgrupo de $F^\times$.

□

Estudaremos os grupos de valores de 1−forma de Pfister sobre F e em extensões quadráticas de F.

Lema 1.1.10. *Sejam F um corpo e $a_1, a_2 \in (F^\times)^2$ tais que $a_1a_2 \neq (F^\times)^2$. Considere $K_i = F(\sqrt{a_i})$, $i = 1, 2$. Denote a extensão $F(\sqrt{a_1}, \sqrt{a_2})$ por L e tome $K = F(\sqrt{a_1a_2})$. Considere também $N_2' : L \longrightarrow K_1$, $N_1' : L \longrightarrow K_2$, $N_1 : K_1 \longrightarrow F$ e $N_2 : K_2 \longrightarrow F$, as funções norma correspondentes. Se existe $z_i \in K_i$ tais que $N_1(z_1) = N_2(z_2)$ então existem $z \in L$ e $c \in F$ tais que $N_2'(z) = cz_1$ e $N_1'(z) = cz_2$.*



Demonstração. Vamos escrever $G = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$ para o grupo $Gal(L/F)$, onde $\sigma_{1|_{K_2}} = id$ e $\sigma_{2|_{K_1}} = id$. Desta maneira, temos que $Gal(K_1/F) = \{1, \sigma_1\}$ e $Gal(K_2/F) = \{1, \sigma_2\}$. Note ainda que K é o corpo fixo por $\{1, \sigma_1\sigma_2\}$ e seja $N' : L \longrightarrow K$ a função norma correspondente. Então, usando as propriedades descritas acima, temos que

$$\begin{aligned} N'(z_1z_2^{-1}) &= (z_1z_2^{-1})\sigma_1\sigma_2(z_1z_2^{-1}) = (z_1z_2^{-1})\sigma_1(z_1)\sigma_2(z_2)^{-1} \\ &= (z_1\sigma_1(z_1))(z_2^{-1}\sigma_2(z_2)^{-1}) = N_1(z_1)N_2(z_2)^{-1} = 1. \end{aligned}$$

Pelo **Teorema 1.1.4**, temos que existe $u \in L$ tal que

$$\frac{z_1}{z_2} = \frac{u}{\sigma_1\sigma_2(u)}, \text{ ou seja, } uz_2 = z_1\sigma_1\sigma_2(u).$$

Seja $z = z_2 u \in L$ e observe que

$$\begin{aligned} z_2\sigma_2(z) &= z_2\sigma_2(z_2u) = z_2\sigma_2(z_1\sigma_1\sigma_2(u)) \\ &= z_2z_1\sigma_1(u) = z_1\sigma_1(z_2u) = z_1\sigma_1(z). \end{aligned}$$

Agora, seja $c = N_1'(z)z_2^{-1} \in K_2$. Então

$$c = \frac{z\sigma_1(z)}{z_2} = \frac{z\sigma_2(z)}{z_1} = \frac{N_2'(z)}{z_1} \in K_1.$$

Consequentemente, temos que $c \in K_1 \cap K_2 = F$ e além disso,

$$N_1'(z) = cz_2 \text{ e } N_2'(z) = cz_1.$$

□

Lema 1.1.11. *Seja $K = F(\sqrt{a})$, onde $a \in F^\times \smallsetminus (F^\times)^2$. Para qualquer $b \in F^\times$, temos*

$$D_K\langle 1, b\rangle \cap F^\times = D_F\langle 1, b\rangle D_F\langle 1, ab\rangle.$$

Demonstração. Note primeiramente que $D_K\langle 1, b\rangle = D_K\langle 1, ab\rangle$, pois $a \in (K^\times)^2$. Logo temos que $D_F\langle 1, b\rangle D_F\langle 1, ab\rangle \subseteq D_K\langle 1, b\rangle$, o que mostra uma inclusão. Para mostrar a outra inclusão, tome $x \in D_K\langle 1, b\rangle \cap F^\times$ e sejam $\alpha, \beta, \gamma, \delta \in F$ tais que $x = (\alpha + \beta\sqrt{a})^2 + b(\gamma + \delta\sqrt{a})^2 = \alpha^2 + \beta^2 a + \gamma^2 b + \delta^2 ab + 2(\alpha\beta + \gamma\delta b)\sqrt{a}$. Conseqüetemente, $\alpha\beta + \gamma\delta b = 0$ e

$$x = \alpha^2 + \beta^2 a + \gamma^2 b + \delta^2 ab. \quad (\dagger)$$

Vamos agora, separar em dois casos. O primeiro caso que analisaremos é quando $\beta = 0$ e então $\gamma = 0$ ou $\delta = 0$. Para $\gamma = 0$, temos que $x = \alpha^2 + \delta^2 ab \in D_F\langle 1, ab\rangle$. Agora, se $\delta = 0$, temos que $x = \alpha^2 + \gamma^2 b \in D_F\langle 1, b\rangle$. Portanto, para $\beta = 0$, temos que $x \in D_F\langle 1, b\rangle D_F\langle 1, ab\rangle$.

O segundo caso, $\beta \neq 0$, multiplicando (†) por β^2 e usando que $\alpha\beta = -\gamma\delta b$, temos que

$$\begin{aligned} x\beta^2 &= (\alpha\beta)^2 + \beta^2\beta^2 a + \gamma^2\beta^2 b + \delta^2\beta^2 ab \\ &= (-\gamma\delta b)^2 + \beta^2\beta^2 a + \gamma^2\beta^2 b + \delta^2\beta^2 ab \\ &= \gamma^2 b(\delta^2 b + \beta^2) + \beta^2 a(\beta^2 + \delta^2 b) \\ &= a(\beta^2 + (\gamma a^{-1})^2 ab)(\beta^2 + \delta^2 b), \end{aligned}$$

portanto, multiplicando ambos os lados por a^{-1}, temos

$$x(\beta a^{-1})^2 a = (\beta^2 + (\gamma a^{-1})^2 ab)(\beta^2 + \delta^2 b) \in D_F\langle 1, b\rangle D_F\langle 1, ab\rangle.$$

Agora, desde que $D_F\langle 1, b\rangle D_F\langle 1, ab\rangle$ é subgrupo de $F^\times$ que contém b, ab e $(F^\times)^2$ então contém também a. Logo, $x \in D_F\langle 1, b\rangle D_F\langle 1, ab\rangle$, mostrando a outra inclusão.

□

Corolário 1.1.12. *Considerando a situação como no* ***Lema 1.1.10****, temos que a seguinte sequência é exata*

$$1 \longrightarrow \{(F^\times)^2, a_2(F^\times)^2\} \xrightarrow{i} (D_F\langle 1,-a_1\rangle D_F\langle 1,-a_1a_2\rangle)/(F^\times)^2 \xrightarrow{j} D_{K_2}\langle 1,-a_1\rangle/({K_2}^\times)^2 \xrightarrow{\overline{N_2}} (D_F\langle 1,-a_1\rangle \cap D_F\langle 1,-a_2\rangle)/(F^\times)^2 \longrightarrow 1,$$

onde j é induzido pela inclusão $F \subset K_2$ e $\overline{N_2}$ por N_2.

Demonstração. Note que $a_2 \in D_F\langle 1,-a_1\rangle D_F\langle 1,-a_1a_2\rangle$ e $a_2 \notin (F^\times)^2$, assim i está bem definido e é injetivo. Além disso, pelo Lema anterior, temos que $D_F\langle 1,-a_1\rangle D_F\langle 1,-a_1a_2\rangle = D_{K_2}\langle 1,-a_1\rangle \cap F^\times$ e assim a inclusão $F \subset K_2$ induz a função j. Ainda, como visto na demonstração do **Lema 1.1.5**, $(K^\times)_2^2 \cap F = (F^\times)^2 \cup a_2(F^\times)^2$, isto é, o núcleo da função j é $\{(F^\times)^2, a_2(F^\times)^2\}$.

Observe que a imagem de j está contida no núcleo de $\overline{N_2}$.

Falta então mostrar que $(D_F\langle 1,-a_1\rangle \cap D_F\langle 1,-a_2\rangle)/(F^\times)^2$ é a imagem de $\overline{N_2}$ e que o núcleo de $\overline{N_2}$ está contido na imagem de j.

Observe, da notação do **Lema 1.1.10**, que $D_{K_2}\langle 1,-a_1\rangle$ é a imagem de N_1'. Assim, se $z \in D_{K_2}\langle 1,-a_1\rangle$ então existe $u \in L = K_2(\sqrt{a_1})$ tal que $N_1'(u) = z$. Portanto $N_2(z) = N_2(N_1'(u)) = N_1(N_2'(u)) \in (D_F\langle 1,-a_1\rangle \cap D_F\langle 1,-a_2\rangle)$ e N_2 induz $\overline{N_2}$.

Vamos agora mostrar a sobrejetividade de $\overline{N_2}$. Para $x \in (D_F\langle 1,-a_1\rangle \cap D_F\langle 1,-a_2\rangle)$, existem $z_1 \in K_1$ e $z_2 \in K_2$ tais que $N_1(z_1) = x$ e $N_2(z_2) = x$. Pelo **Lema 1.1.10**, existe $z \in L$ e $c \in F$ tais que $N_1'(z) = cz_2$ e $N_2'(z) = cz_1$. Desta maneira, $c^2x = N_2(cz) = N_2(N_1'(z))$. Ainda, $N_1'(z) \in D_{K_2}\langle 1,-a_1\rangle$ e daí, $x = c^{-2}N_2(N_1'(z)) \in N_2(D_{K_2}\langle 1,-a_1\rangle)$ e $\overline{N_2}$ é sobrejetiva.

Seja $x \in D_{K_2}\langle 1,-a_1\rangle$ tal que $N_2(x) \in (F^\times)^2$. Pelo **Teorema 1.1.4**, existe $u \in K_2$ tal que

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

onde $y = \sigma_2(x)$.

Daí, $yN_2(u)^{-1} = xu^{-2} \in F \cap D_{K_2}\langle 1,-a_1\rangle$ e pelo Lema anterior, segue que $yN_2(u)^{-1} \in D_F\langle 1,-a_1\rangle D_F\langle 1,-a_1a_2\rangle$ e assim,

$$x({K_2}^\times)^2 = yN_2(u)^{-1}({K_2}^\times)^2 = j(yN_2(u)^{-1}(F^\times)^2)$$

o que implica que o núcleo de $\overline{N_2}$ está contido na imagem de j. □

1.2 Álgebras de quatérnios

Apresentaremos nesta seção alguns resultados sobre as álgebras de quatérnios. Sugerimos Capítulo 3 de [**L**] como leitura complementar. Os resultados que apresentaremos serão utilizados com frequencia durante o trabalho e fixaremos algumas notações para facilitar a leitura.

Começaremos apresentando a definição formal de uma álgebra de quatérnios.

Para $a, b \in F^\times$, a **álgebra de quatérios** gerada por a e b, e denotada por $(a,b)_F$, é a $F-$álgebra de dimensão 4 com base $\{1, i, j, k, \}$, onde

$$i^2 = a,\ j^2 = b,\ ij = -ji = k.$$

Desta forma, os elementos i, j, k anticomutam. Ainda, podemos identificar o grupo multiplicativo $F^\times$ em $(a,b)_F$ como sendo o subespaço gerado por 1, isto é, $\{1 \cdot a \mid a \in F^\times\}$.

A seguir, um resultado que apresenta algumas propriedades das álgebras de quatérnios.

Proposição 1.2.1. *1.* $(a,b)_F \otimes K \simeq (a,b)_K$, *onde* K *é uma extensão de* F.

2. $(a,b)_F \simeq (ax^2, by^2)_F$, *onde* $a, b, x, y \in F^\times$.

3. $(-1,1)_F = 0 \in {}_2Br(F)$, *isto é, a representa a classe trivial do subgrupo* ${}_2Br(F)$ *de* $Br(F)$.

4. $(a,b)_F$ *é uma álgebra central simples, isto é, o centro de* $(a,b)_F$ *é o subespaço* $1 \cdot F$ *e não possui ideiais bilaterais não triviais.*

Demonstração. [**L**].

□

Vimos na seção anterior que as $1-$formas de Pfister sobre um corpo F estão ligadas diretamente a normas de extensões quadráticas de F. Estamos interessados em estabelecer uma conexão entre álgebras de quatérnios e $2-$formas de Pfister.

Desta maneira, poderemos estudar as propriedades de $(a,b)_F$ usando a forma quadrática associada.

Para cada $x = x_0 + x_1 i + x_2 j + x_3 k \in (a,b)_F$ definimos o **conjugado** de x por $\overline{x} = x_0 - x_1 i - x_2 j - x_3 k$. Note que $x \in F$ se, e somente se, $x = \overline{x}$. Considere agora as seguintes funções:

$$\begin{array}{rccc} \mathsf{tr}: & A \times A & \longrightarrow & F \\ & (x,y) & \longmapsto & \dfrac{x\overline{y} + y\overline{x}}{2} \end{array}$$

e

$$\begin{array}{rccc} N: & (a,b)_F & \longrightarrow & F \\ & x & \longmapsto & \mathsf{tr}(x,x) \end{array}$$

Note primeiramente que a função tr está bem definida, pois $\overline{\mathsf{tr}(x,y)} = \mathsf{tr}(x,y)$ e consequentemente $\mathsf{tr}(x,y) \in F$.

Ainda, tr é uma função bilinear e simétrica, definindo um produto interno sobre o espaço vetorial $(a,b)_F$. A forma quadrática associada à função será a função N, chamada também de norma.

Com relação ao produto interno tr, temos que a base $\{1, i, j, k\}$ é uma base ortogonal e portanto a forma quadrática N tem como representante a forma quadrática $\langle N(1), N(i), N(j), N(k)\rangle$. Note que $N(1) = 1$, $N(i) = -i^2 = -a$, $N(j) = -b$ e $N(k) = -k^2 = i^2j^2 = ab$.

Portanto, temos que a forma quadrática $\langle N(1), N(i), N(j), N(k)\rangle$ é justamente a $2-$forma de Pfister $\langle 1, -a, -b, ab\rangle = \langle 1, -a\rangle \otimes \langle 1, -b\rangle$.

No próximo teorema, agrupamos alguns resultados acerca das álgebras de quatérnios que usaremos mais adiante. As demonstrações podem ser encontradas em [L], dispersas entre as páginas 58 e 75.

Teorema 1.2.2. *Mantendo as notações acima, as seguintes afirmações são verdadeiras:*

1. *Para a álgebra de quatérnios $(a, b)_F$ são equivalentes:*
   - *(a)* $(a, b)_F$ *é um anel com divisão*
   - *(b)* $\langle a, b\rangle$ *é anisotrópica.*
   - *(c)* $\langle -a, -b, ab\rangle$ *é anisotrópica.*
   - *(d)* $a \notin D_F\langle 1, -b\rangle$.
   - *(e)* $1 \notin D_F\langle a, b\rangle$.
2. *Se $(a, b)_F$ não é anel com divisão, então $(a, b)_F \simeq M_2(F)$ e $\langle 1, -a, -b, ab\rangle \simeq \langle 1, -1, 1, -1\rangle$. Além disso, $a \in D_F\langle 1, -b\rangle$.*
3. *Dados $a, b, c, d \in F^\times$, são equivalentes:*
   - *(a)* $(a, b)_F \simeq (c, d)_F$.
   - *(b)* $\langle 1, -a, -b, ab\rangle \simeq \langle 1, -c, -d, cd\rangle$.
   - *(c) Existe $e \in F^\times$ tal que $(a, b)_F \simeq (a, e)_F$, $(c, d)_F \simeq (c, e)_F$ e $(ac, e)_F \simeq M_2(F)$.*
   - *(d)* $bD_F\langle 1, -a\rangle \cap dD_F\langle 1, -c\rangle \cap D_F\langle 1, -ac\rangle \neq \emptyset$.
4. *Dados $a, b, c \in F^\times$, valem:*
   - *(a)* $(a, b)_F \simeq (b, a)_F$.
   - *(b)* $(1, a)_F \simeq (a, -a)_F \simeq M_2(F)$.
   - *(c)* $(a, a)_F \simeq M_2(F)$ *se, e somente se,* $a \notin D_F\langle 1, 1\rangle$.
   - *(d)* $(a, b)_F \otimes_F (c, b)_F \simeq (ac, b)_F \otimes_F M_2(F)$.
     Em particular, $(a, b)_F \otimes_F (a, b)_F \simeq M_2(F) \otimes_F M_2(F) \simeq M_4(F)$.

A equivalência entre os ítems $3a$ e $3c$ do **Teorema 1.2.2** é chamada de propriedade *linkage*, que é uma das mais importantes propriedadas das álgebras de quatérnios.

1.2.1 Grupo de Brauer

Neste parágrafo, vamos apresentar o grupo de Brauer de um corpo F. Considere inicialmente $\mathcal{B}$ o conjunto $\{A \mid A$ é álgebra central simples sobre de dimensão finita$F\}$. Para $A, B \in \mathcal{B}$ dizemos que A e B são **Brauer equivalentes** se existem inteiros n, m tais que

$$A \otimes_F M_n(F) \simeq B \otimes_F M_m(F).$$

Esta relação é uma relação de equivalência e denotaremos por $\mathrm{Br}(F)$ o conjunto das classes de equivalência.

Sejam agora $[A], [C] \in \mathrm{Br}(F)$ e defina a seguinte operação binária

$$\begin{array}{rccc} + : & \mathrm{Br}(F) \times \mathrm{Br}(F) & \longrightarrow & \mathrm{Br}(F) \\ & ([A], [B]) & \longmapsto & [A \otimes_F B] \end{array}$$

Com esta operação, temos que $\mathrm{Br}(F)$ é um grupo comutativo com elemento neutro $0 = [M_n(F)]$. O grupo $\mathrm{Br}(F)$ é chamado de **grupo de Brauer** do corpo F. Por abuso de notação, poderemos escrever simplesmente A para representar a classe $[A]$ em $\mathrm{Br}(F)$.

Nosso interesse está no conjunto ${}_2Br(F) = \{A \in \mathrm{Br}(F);\ A \otimes_F A = 0 \in \mathrm{Br}(F)\}$, isto é, o conjunto das álgebras sobre F de ordem 2. Em vista do ítem *4.* parte (d) do **Teorema 1.2.2**, temos que as classes representadas por álgebras de quatérnios pertencem a ${}_2Br(F)$.

Pelas propriedades de álgebras centrais simples, temos que ${}_2Br(F)$ é um subgrupo de $\mathrm{Br}(F)$ e, pelo teorema de Merkurjev, que apresentaremos a seguir, ${}_2Br(F)$ é gerado aditivamente, pelas classes de álgebras de quatérnios.

Teorema 1.2.3 (Merkurjev)**.** *Mantendo as notações anteriores, temos que a aplicação*

$$\begin{array}{rccc} \varphi : & I^2F/I^3F & \longrightarrow & {}_2Br(F) \\ & \langle 1, -a, -b, ab\rangle + I^3F & \longmapsto & (a,b)_F \end{array}$$

se estende, por linearidade, a um isomorfismo de grupos.

Desta forma, se $A \in {}_2Br(F)$, então existe $n \in \mathbb{N}$ tal que

$$A \simeq (a_1, b_1)_F \oplus \cdots \oplus (a_n, b_n)_F \oplus M_n(F).$$

Para um corpo F, denotaremos por $Q_F(b)$ o conjunto das classes de álgebras de quatérnios sobre F geradas por b, isto é, $Q_F(b) = \{(a,b)_F \mid a \in F^\times\}$.

Proposição 1.2.4. *Sejam F um corpo e $b \notin (F^\times)^2$. Então temos um isomorfismo*

$$Q_F(b) \simeq F^\times / D_F\langle 1, -b\rangle.$$

Demonstração. Considere a seguinte aplicação $\varphi : F^\times/(F^\times)^2 \longrightarrow Q_F(b)$, dada por $\varphi(a(F^\times)^2) = (a,b)_F$. Note que φ é um homomorfismo sobrejetor. Pelo ítem *2.* do **Teorema 1.2.2**, temos que o núcleo de φ é o grupo $D_F\langle 1, -b\rangle$. Portanto, temos o resultado. □

O próximo resultado caracteriza as interseções $Q_F(b) \cap Q_F(c)$, onde $b, c \in F^\times$.

Proposição 1.2.5. *Para $a, b \in F^\times$ temos que*

$$Q_F(a) \cap Q_F(b) \simeq D_F\langle 1, -ab\rangle / D_F\langle 1, -a\rangle \cap D_F\langle 1, -b\rangle.$$

Demonstração. Vamos definir uma aplicação ϑ de $D_F\langle 1, -ab\rangle$ em $Q_F(a) \cap Q_F(b)$ de forma que seja homomorfismo sobrejetor com núcleo $D_F\langle 1, -a\rangle \cap D_F\langle 1, -b\rangle$.

Seja então $\vartheta : D_F\langle 1, -ab\rangle \longrightarrow Q_F(a)$, dada por $\vartheta(\alpha) = (a, \alpha)_F$. Como $\alpha \in D_F\langle 1, -ab\rangle$ temos pelo ítem *3* do **Teorema 1.2.2** que a classe de $(\alpha, ab)_F$ seja nula em ${}_2Br(F)$ e consequentemente $(a, \alpha)_F = (b, \alpha)_F$ como classes de ${}_2Br(F)$. Logo, segue que $\operatorname{Im}\vartheta \subseteq Q_F(a) \cap Q_F(b)$ e podemos considerar então $\vartheta : D_F\langle 1, -ab\rangle \longrightarrow Q_F(a) \cap Q_F(b)$. Usando novamente o ítem *3.* do **Teorema 1.2.2** temos que ϑ é um homomorfismo injetor com núcleo $D_F\langle 1, -a\rangle \cap D_F\langle 1, -b\rangle$.

Falta mostrar que ϑ é sobrejetiva, isto é, $\operatorname{Im}\vartheta = Q_F(a) \cap Q_F(b)$. Seja então $Q \in Q_F(a) \cap Q_F(b)$ e $x, y \in F^\times$ tais que $Q \simeq (x, a)_F \simeq (y, b)_F$. Pelo ítem *3.* parte *(c)* do **Teorema 1.2.2** existe $z \in F^\times$ tal que $(z, a)_F \simeq (x, a)_F$, $(z, b)_F \simeq (y, b)_F$ e $(z, ab)_F = 0 \in {}_2Br(F)$. Portanto $z \in D_F\langle 1, -ab\rangle$ e $\vartheta(z) = Q$, mostrando a sobrejetividade da aplicação ϑ.

□

1.3 Fecho quadrático e cohomologia galoisiana

Esta seção será destinada à apresentação formal do fecho quadrático de um corpo F e alguns resultados extraídos da Cohomologia Galoisiana, que usaremos no decorrer do trabalho.

Convém relembrar que F é um corpo *quadraticamente fechado* se $F^\times = (F^\times)^2$. Denotando por $\widetilde{F}$ o fecho algébrico de F, o corpo

$$F(2) = \bigcap_{E \subseteq \widetilde{F}} E,$$

onde E é quadraticamente fechado, possui as seguintes propriedades:

1. $F(2)$ é quadraticamente fechado e minimal para esta propriedade, isto é, se K é corpo quadraticamente fechado tal que $F \subseteq K \subseteq \widetilde{F}$, então $F(2) \subseteq K$.
2. $F(2)$ é uma extensão galoisiana de F.

O corpo $F(2)$ é chamado de **fecho quadrático** de F, e as propriedades que citamos sobre $F(2)$ seguem diretamente da definição.

Antes de darmos uma outra caracterização de $F(2)$, que será últil para explorarmos o grupo de Galois $Gal(F(2)/F)$, relembremos que $K \subseteq \widetilde{F}$ é uma $2-$extensão finita de F se K/F é galoisiana e $[K : F]$ é um potência de 2.

Teorema 1.3.1. *O fecho quadrático $F(2)$ é a união de todas as $2-$extensões finitas de F.*

Demonstração. [**L**].

□

Pelo Teorema acima, podemos chamar $F(2)$ de a **máxima $2-$extensão de F.**

Vale ressaltar também que se F não for quadraticamente fechado, então a extensão $F(2)/F$ só será finita se F for um corpo euclidiano. E neste caso, $F(2)$ será uma extensão quadrática de F. Mais espcificamente, $F(2) = F(\sqrt{-1})$, veja [**L**].

Finalmente, sobre o fecho quadrático, o grupo de Galois da extensão $F(2)/F$, que será denotado simplesmente por $G_2(F)$, será dado por:

$$G_2(F) = \varprojlim Gal(K/F),$$

onde K percorre todas as $2-$extensões finitas de K, como no **Teorema 1.3.1**.

Durante o nosso trabalho, alguns dos nossos resultados foram obtidos utilizando sequências exatas envolvendo grupos de cohomologia com coeficientes em $\mathbb{Z}/2\mathbb{Z}$. E a tradução destes resultados em Teoria de Formas Quadráticas foi obtida através da Teoria de Kummer e o Teorema de Merkurjev. Mais especificamente, o n-ésimo grupo de cohomologia $H^n(G_2(F); \mathbb{Z}/2\mathbb{Z})$, que denotaremos simplesmente por $H^n(F)$ tem a seguinte caracterização para $n = 1, 2$:

1. $H^1(F) \simeq F^\times/(F^\times)^2$.
2. $H^2(F) \simeq {}_2Br(F)$.

A definição formal dos grupos $H^n(G, A)$, onde G é um grupo pro-finito e A é um $G-$módulo discreto, que apresentaremos posteriormente, será utilizada na demonstração do Teorema 90 de Hilbert, versão para o radical de Kaplansky, **Teorema 3.2.22**.

Teorema 1.3.2 (Teorema 90 de Hilbert)**.** *Seja N/F uma extensão galoisiana de corpos e denote por G o grupo de Galois da extensão. Então $H^1(G, N^\times) = 1$.*

Demonstração. [**NSW**] □

Capítulo 2

Radical de Kaplansky e fecho reduzido

Este capítulo será dedicado ao estudo do radical de Kaplansky de um corpo F e o comportamento do radical de Kaplansky de Kaplansky de F em relação à suas 2-extensões finitas.

2.1 Radical de Kaplansky

Começaremos esta seção definindo o radical de Kaplansky. É válido ressaltar que este radical apareceu primeiramente em [**K**], onde Kaplansky estava interessado no estudo de corpos que possuem somente duas álgebras de quatérnios, a menos de isomorfismo.

Definição 2.1.1. *Seja F um corpo qualquer e, para cada $x \in F^\times$, considere o grupo de valores $D_F\langle 1, -x\rangle$ da 1-forma de Pfister $\langle 1, -x\rangle$. O* ***radical de Kaplansky*** *do corpo F é definido por*

$$R(F) = \bigcap_{x \in F^\times} D_F\langle 1, -x\rangle.$$

As seguintes propriedades seguem diretamente da definição do radical de Kaplansky.

(i) $R(F)$ é um subgrupo de $F^\times$.

(ii) Uma vez que $(F^\times)^2 \subseteq D_F\langle 1, -x\rangle$, para todo $x \in F^\times$ e $R(F) \subseteq D_F\langle 1, 1\rangle$ segue que $(F^\times)^2 \subseteq R(F) \subseteq D_F\langle 1, 1\rangle$, isto é, todo elemento de $R(F)$ é uma soma de no máximo dois quadrados.

Definição 2.1.2. *Dizemos que um corpo F tem* ***radical trivial*** *se $R(F) = (F^\times)^2$ ou $R(F) = F^\times$. No caso particular onde que $R(F) = (F^\times)^2$, chamaremos o corpo F simplesmente de* ***corpo com radical reduzido****.*

Lema 2.1.3. *Sejam F um corpo qualquer e $R(F)$ o radical de Kaplansky do corpo F. Então:*

1. *Para $x \in F^\times$, temos que $x \in R(F)$ se, e somente se, $D_F\langle 1, -x\rangle = F^\times$, isto é, se a $1-$forma de Pfister $\langle 1, -x\rangle$ for universal. Em particular, $Q_F(x) = 0$ para todo $x \in R(F)$. Relembremos aqui que $Q_F(x)$ denota o subgrupo de ${}_2Br(F)$ gerado por x.(Veja a* ***Proposição 1.2.4.****)*

2. $D_F\langle 1, a\rangle = D_{R(F)}\langle 1, a\rangle$, *para todo* $a \in F^\times$, *onde* $D_{R(F)}\langle 1, a\rangle = \{r_1 - r_2 a;\, r_i \in R(F)\}$.

3. *Para* $x, y \in R(F)$ *tal que* $x + y \neq 0$, *temos que* $x + y \in D_F\langle 1, 1\rangle$

Demonstração. Para o *1*, suponha seja $x \in R(F)$. Pela **Definição 2.1.1** temos que $x \in D_F\langle 1, -a\rangle$ para todo $a \in F^\times$ e pelo **Lema 1.1.1** segue que $a \in D_F\langle 1, -x\rangle$, para todo $a \in F^\times$. Por outro lado, se $D_F\langle 1, -x\rangle = F^\times$, então, novamente pelo **Lema 1.1.1**, temos que $x \in D_F\langle 1, -a\rangle$, para todo $a \in F^\times$, isto é, $x \in R(F)$ pela **Definição 2.1.1**.

Para *2.*, note que para todo $a \in F^\times$ temos que $D_F\langle 1, a\rangle \subseteq D_{R(F)}\langle 1, a\rangle$, pois $(F^\times)^2 \subseteq R(F)$. Agora, se $x \in D_{R(F)}\langle 1, a\rangle$ então existem $r_1, r_2 \in R(F)$ tais que $x = r_1 + r_2 a = r_1(1 + a r_2 r_1^{-1})$. Para mostrar que $x \in D_F\langle 1, a\rangle$, precisamos mostrar que $1 + a r_2 r_1^{-1} \in D_F\langle 1, a\rangle$, pois $D_F\langle 1, a\rangle$ é um grupo multiplicativo e $r_1 \in D_F\langle 1, a\rangle$. Usando o **Lema 1.1.3** temos que para qualquer $r \in R(F)$

$$D_F\langle 1, a\rangle \cap D_F\langle 1, ar\rangle = D_F\langle 1, ar\rangle \cap D_F\langle 1, -r\rangle = D_F\langle 1, ar\rangle,$$

pois $D_F\langle 1, -r\rangle = F^\times$ pelo ítem anterior. Portanto, temos que para todo $r \in R(F)$, $D_F\langle 1, ar\rangle \subseteq D_F\langle 1, a\rangle$ e consequentemente $1 + ar \in D_F\langle 1, a\rangle$ para todos $a, r \in F^\times$.

Para a terceira parte do lema, vamos assumir que $-1 \notin R(F)$, pois caso contrário $D_F\langle 1, 1\rangle = F^\times$ e a afirmação é verdadeira. Tome $x, y \in F^\times$ e escreva $x + y = y(1 + xy^{-1})$ e observe que $-xy^{-1} = 1 - (1 + xy^{-1}) \in D_F\langle 1, -(1 + xy^{-1})\rangle$ e também $xy^{-1} \in R(F) \subseteq D_F\langle 1, -(1 + xy^{-1})\rangle$, pois $x, y \in R(F)$. Como $D_F\langle 1, -(1 + xy^{-1})\rangle$ é um subgrupo de $F^\times$ temos que $-1 = xy^{-1}(xy^{-1})^{-1} \in D_F\langle 1, -(1 + xy^{-1})\rangle$. Agora, se $-1 \in D_F\langle 1, -(1 + xy^{-1})\rangle$, então $-1 = a^2 - b^2(1 + xy^{-1})$ e consequentemente, $(1 + xy^{-1}) = (ab^{-1})^2 + 1 \cdot (b^{-1})^2 \in D_F\langle 1, 1\rangle$. Portanto, temos que $x + y \in D_F\langle 1, 1\rangle$. □

Como conseqüencia imediata do ítem *2.* do lema anterior temos o seguinte resultado devido a Cordes.

Corolário 2.1.4 (Cordes)**.** *Seja* $\varphi = \langle 1, -b\rangle$ *uma* $1-$*forma de Pfister. Para todo* $r \in R(F)$ *temos que* $D_F\langle 1, -b\rangle = D_F\langle 1, -br\rangle$.

Demonstração. Note inicialmente que, pelo ítem *2* do lema anterior, $D_F\langle 1, -br\rangle = D_{R(F)}\langle 1, -br\rangle$. Como $D_{R(F)}\langle 1, -br\rangle = D_{R(F)}\langle 1, -b\rangle$ temos, usando novamente o ítem *2* do lema anterior, que $D_{R(F)}\langle 1, -br\rangle = D_F\langle 1, -b\rangle$. Portanto, $D_F\langle 1, -b\rangle = D_F\langle 1, -br\rangle$. □

Proposição 2.1.5. *Seja* F *um corpo tal que* $R(F) \neq F^\times$. *Então as seguintes condições são equivalentes:*

1. $R(F)$ *é aditivamente fechado, isto é,* $R(F) + R(F) = R(F)$.

2. $R(F) = D_F\langle 1, 1\rangle$.

3. *Existe* $a \in F^\times$ *tal que* $R(F) = D_F\langle 1, a\rangle$.

4. $R(F) = \sum F^2$ *e* F *é formalmente real.*

Demonstração. Assumindo *1.* e usando que $(F^\times)^2 \subseteq R(F)$, segue que $(F^\times)^2 + (F^\times)^2 \subseteq R(F)$. Logo, $D_F\langle 1,1\rangle \subseteq R(F)$ que mostra *2.*, pois $R(F) \subseteq D_F\langle 1,1\rangle$ por definição. Note que *2.* implica em *1.* pelo Lema **Lema 2.1.3**.

2. implica *3.*, basta tomar $a = 1$.

Agora suponha *3.*, isto é, suponha que existe $a \in F^\times$ tal que $R(F) = D_F\langle 1, a\rangle$. Neste caso, $a \in R(F)$ e usando o **Lema 2.1.3**, temos que

$$R(F) = D_F\langle 1,a\rangle = D_{R(F)}\langle 1,a\rangle = D_{R(F)}\langle 1,1\rangle = D_F\langle 1,1\rangle,$$

onde a úçtima igualdade vem do ítem *2.* do **Lema 2.1.3**.Portanto, temos *2.*

Vamos mostrar que *1.* implica em *4.* Seja $x = x_1^2 + \cdots x_n^2 \in \sum F^2$, vamos mostrar que $x \in R(F)$ por indução em n. Note que se $n = 1$, $x \in R(F)$ pois $(F^\times)^2 \subseteq R(F)$. Agora, suponha por hipótese de indução que $x_1^2 + \cdots x_{n-1}^2 \in R(F)$. Estamos assumindo que $R(F) \neq F^\times$ e então, $-1 \neq R(F)$ pois caso contrário, $R(F) = D_F\langle 1,1\rangle = F^\times$ por ***2***, o que seria uma contradição. Usando agora a equivalência entre *1.* e *2.*, segue que $x_1^2 + \cdots x_{n-1}^2 + x_n^2 \neq 0$ e consequentemente $x = x_1^2 + \cdots x_{n-1}^2 + x_n^2 \in R(F)$, novamente pelo **Lema 2.1.3**. Portanto, $R(F) = \sum F^2$ e como $-1 \notin R(F)$ temos que F é formalemente real.

Finalmente, *4.* implica em *1.* trivialmente.

□

Definição 2.1.6. *Sejam F e $K = F(\sqrt{a})$, onde $a \in F^\times \smallsetminus (F^\times)^2$, uma extensão quadrática de F. Dizemos que a extensão K/F é uma* ***extensão radical*** *se $a \in R(F) \smallsetminus (F^\times)^2$. Caso contrário, dizemos que a* ***extensão não radical.***

Lema 2.1.7. *Seja $K = F(\sqrt{a})$, onde $a \in F^\times \smallsetminus (F^\times)^2$, uma extensão quadrática qualquer de F. Então as seguintes afirmações são verdadeiras:*

(a) $R(F) \subseteq R(K)$.

(b) $R(K) \cap F^\times = \{x \in F^\times \mid D_F\langle 1,-x\rangle D_F\langle 1,-xa\rangle = F^\times \text{ e } D_F\langle 1,-a\rangle \subset D_F\langle 1,-x\rangle\}$.

(c) $N(x) \in R(F)$, *para todo* $x \in R(K)$, *isto é,* $N(R(K)) \subseteq R(F)$.

Demonstração. Seja $r \in R(F)$ e considere $a_2 = a$ e $a_1 = r$ no **Corolário 1.1.12**. Temos assim a seguite sequencia exata

$$1 \longrightarrow \{(F^\times)^2, a(F^\times)^2\} \longrightarrow \frac{F^\times}{(F^\times)^2} \xrightarrow{j} \frac{D_K\langle 1,-r\rangle}{(K^\times)^2} \xrightarrow{\overline{N}} \frac{D_F\langle 1,-a\rangle}{(F^\times)^2} \longrightarrow 1.$$

Então, $\overline{N} : \dfrac{D_K\langle 1,-r\rangle}{(K^\times)^2} \longrightarrow \dfrac{D_F\langle 1,-a\rangle}{(F^\times)^2}$ é sobrejetiva com núcleo $j(F^\times/(F^\times)^2)$. Note que a imagem da norma de $K = F(\sqrt{a})$ em $F^\times$ é exatamente $D_F\langle 1,-a\rangle$. Desta maneira, temos que $K^\times = D_K\langle 1,-r\rangle$, portanto $r \in R(K)$.

Dado $r \in R(F)$ temos que $r \in D_K\langle 1,y\rangle$ para todo $y \in F^\times$. Aplicando o **Corolario 1.1.12** para $a_2 = a$ e $a_1 = -y$, temos que $N(r) \in D_F\langle 1,y\rangle \cap D_F\langle 1,-a\rangle$. Desta maneira, temos que $N(r) \in R(F)$.

□

Corolário 2.1.8. *Sejam $K = F(\sqrt{a})$, onde $a \in R(F) \setminus (F^\times)^2$, uma extensão quadrática de F e $b \in F^\times$. Então $D_K\langle 1, -b\rangle \cap F^\times = D_F\langle 1, -b\rangle$. Ainda, para $a_1, \ldots, a_n \in R(F)$ considere $K_n = F(\sqrt{a_1}, \ldots, \sqrt{a_n})$. Então $D_{K_n}\langle 1, -b\rangle \cap F^\times = D_F\langle 1, -b\rangle$.*

Demonstração. Usando o **Lema 1.2.5**, temos que $D_K\langle 1, -b\rangle \cap F^\times = D_F\langle 1, -b\rangle D_F\langle 1, -ab\rangle$. E pelo **Corolário 2.1.4** $D_F\langle 1, -b\rangle = D_F\langle 1, -ab\rangle$, ou seja, $D_F\langle 1, -b\rangle D_F\langle 1, -ab\rangle = D_F\langle 1, -b\rangle$. Portanto, $D_K\langle 1, -b\rangle \cap F^\times = D_F\langle 1, -b\rangle$.

O próximo passo será demostrado por indução em n. Se $n = 1$, então temos exatamente o caso que acabamos de demonstrar. Para $n > 1$ e $a_1, \ldots, a_n \in R(F)$ como acima, existe uma cadeia de extensões quadráticas

$$K_0 = K = F(\sqrt{a}) \subseteq K_1 = K(\sqrt{a_1}) \subseteq \cdots \subseteq K_n = K_{n-1}(\sqrt{a_n}).$$

Vamos supor, por hipótese de indução que $D_{K_{n-1}}\langle 1, -b\rangle \cap F = D_F\langle 1, -b\rangle$. Agora, pelo caso anterior temos que $D_{K_n}\langle 1, -b\rangle \cap K_{n-1} = D_{K_{n-1}}\langle 1, -b\rangle$, uma vez que $a_n \in R(K_{n-1})$ pelo lema anterior.

Portanto,

$$D_{K_n}\langle 1, -b\rangle \cap F = (D_{K_n}\langle 1, -b\rangle \cap K_{n-1}) \cap F = D_{K_{n-1}}\langle 1, -b\rangle \cap F = D_F\langle 1, -b\rangle.$$

□

Corolário 2.1.9. *Seja $K = F(\sqrt{a})$, onde $a \in R(F) \setminus (F^\times)^2$. Então $R(K) \cap F^\times = R(F)$. Ainda, para $a_1, \ldots, a_n \in R(F)$ tome $K_n = F(\sqrt{a_1}, \ldots, \sqrt{a_n})$, então $R(K_n) \cap F^\times = R(F)$.*

Demonstração. Pelo lema anterior temos que

$$R(K) \cap F^\times = \{x \in F^\times \mid D_F\langle 1, -x\rangle D_F\langle 1, -xa\rangle = F^\times \text{ e } D_F\langle 1, -a\rangle \subset D_F\langle 1, -x\rangle\}.$$

Agora pelo *item 1.* do **Lema 2.1.3**, temos que $D_F\langle 1, -a\rangle = F^\times$ e consequentemente, $R(K) \cap F^\times = \{x \in F^\times \mid D_F\langle 1, -x\rangle = F^\times\}$. E usando novamente o *item 1.* do **Lema 2.1.3** podemos trocar a igualdade $D_F\langle 1, -x\rangle = F^\times\}$ por $x \in R(F)$ e o resultado fica demonstrado.

A segunda parte será demonstrada por indução em n. Se $n = 1$, então temos exatamente o caso que acabamos de demonstrar.

Para $n > 1$ e $a_1, \ldots, a_n \in R(F)$ como acima, existe uma cadeia de extensões quadráticas

$$K_0 = K = F(\sqrt{a}) \subseteq K_1 = K(\sqrt{a_1}) \subseteq \cdots \subseteq K_n = K_{n-1}(\sqrt{a_n}).$$

Vamos supor, por hipótese de indução que $R(K_{n-1}) \cap F^\times = R(F)$. Agora, pelo caso anterior temos que $R(K_n) \cap K_{n-1}^\times = R(K_{n-1})$, uma vez que $a_n \in R(K_{n-1})$ pelo lema anterior.

Portanto,

$$R(K_n) \cap F^\times = (R(K_n) \cap FK_{n-1}) \cap F^\times = R(K_{n-1}) \cap F^\times = R(F).$$

□

Vamos agora mostrar um lema mais geral que relaciona $R(F)$ e $R(M)$, onde M é uma extensão de F tal que $M \subseteq F(2)$, relembrando que $F(2)$ denota o fecho quadrático de F introduzido no capítulo anterior.

Lema 2.1.10. *Para toda 2-extensão M de F temos que $R(F) \subset R(M)$. Relembramos que M é uma 2-extensão de F se $F \subset M \subset F(2)$.*

Demonstração. Pela construção do fecho quarático, temos que $F(2) = \bigcup_{E \subseteq \bar{F}} E$, onde $\bar{F}$ é um fecho algébrico de F e E é uma 2-extensão finita.

Note primeiramente que para o caso em que $M = F(\sqrt{a})$ onde $a \in F^\times \setminus (F^\times)^2$ o resultado segue do **Lema 2.1.7**.

Para uma 2−extensão finita $R(F) \subseteq R(E)$ segue por indução sobre o grau $[E : F]$, pois E pode ser obtido de F por uma cadeia finita de extensões quadráticas $F_0 = F \subseteq F_1 \subseteq \cdots \subseteq F_n = E$.

Vamos agora ao caso geral. Sejam $r \in R(F)$ e $y \in M$, vamos mostrar que $y \in D_M\langle 1, -r\rangle$. Desde que $M \subset F(2) = \bigcup_{E \subseteq \bar{F}} E$, então $y \in E$ para algum E. Portanto, como $R(F) \subseteq R(E)$, $D_E\langle 1, -r\rangle = E^\times$ e assim $y \in D_E\langle 1, -r\rangle \subseteq D_M\langle 1, -r\rangle$. □

2.2 Extensões radicais

Nesta seção abordaremos somente resultados envolvendo extensões radicais de F, isto é, extensões $K = F(\sqrt{a})$, onde $a \in R(F) \setminus (F^\times)^2$. Já apresentamos alguns resultados envolvendo extensões radicias, a saber os **Corolários 2.1.8** e **2.1.9**. Voltaremos a tratar do Radical de Kaplansky e extensões radicais no estudo de corpos com base ditinguida, veja **Definição 3.2.1**, e demonstraremos o Teorema 90 de Hilbert para o radical de Kaplansky em uma versão mais geral, **Teorema 3.2.18**.

Antes de prosseguirmos, vamos relembrar a caracterização dos grupos de cohomologia $H^n(F)$, já apresentada no **Capítulo 1.**

(1) $H^1(F) \simeq \dfrac{F^\times}{(F^\times)^2}$.

(2) $H^2(F) \simeq {}_2Br(F)$.

Uma vez identificado $H^1(F)$ com o grupo de classes de quadrados $\dfrac{F^\times}{(F^\times)^2}$, temos que para dois homomorfimos $\chi_a, \chi_b \in H^1(F)$, o produto *cup* $\chi_a \cup \chi_b$ será identificado com a classe $(a, b)_F$ em $H^2(F) \simeq {}_2Br(F)$.

O próximo resultado apresenta a ordem do grupo $H^2(K) \simeq {}_2Br(K)$, onde $K = F(\sqrt{a})$ é uma extensão radical.

Lema 2.2.1. *Sejam F corpo qualquer e $K = F(\sqrt{a})$ uma extensão radical de F. Então $|{}_2Br(K)| = |{}_2Br(F)|^2$. Além disso a função restrição, $Res : {}_2Br(F) \to {}_2Br(K)$ dada por $Res((a, b)_F) \mapsto (a, b)_F \otimes_F K$, é injetora.*

Demonstração. Considere a seguinte exata longa e [**A**].

$$\cdots \to H^1(F) \to H^1(K) \to H^1(F) \overset{\chi_a \cup \_}{\to} H^2(F) \to H^2(K) \to H^2(F) \overset{\chi_a \cup \_}{\to} H^3(F) \to \cdots .$$

Desde que $a \in R(F)$, temos que a aplicação $\chi_a \cup \_$ é nula. Assim, produzimos a seguinte sequencia exata curta

$$0 \longrightarrow H^2(F) \longrightarrow H^2(K) \longrightarrow H^2(F) \longrightarrow 0.$$

E usando as observações acima, obtemos:

$$0 \longrightarrow {}_2Br(F) \longrightarrow {}_2Br(K) \longrightarrow {}_2Br(F) \longrightarrow 0.$$

Portanto, temos que $|{}_2Br(K)| = |{}_2Br(F)|^2$.

□

Proposição 2.2.2. *Sejam F um corpo e $K = F(\sqrt{a})$ uma extensão radical de F. Então*

$$(K : D_K\langle 1, -b\rangle) = (F : D_F\langle 1, -b\rangle)^2,$$

para todo $b \in F^\times \smallsetminus (F^\times)^2$.

Demonstração. De início, considere a seguinte aplicação

$$\varphi : F^\times/(F^\times)^2 \longrightarrow F^\times/D_F\langle 1, -b\rangle.$$

O núcleo dessa aplicação é $D_F\langle 1, -b\rangle/(F^\times)^2$ e portanto pelo primeiro teorema do isomorfismo temos:

$$(F^\times/(F^\times)^2)/(D_F\langle 1, -b\rangle/(F^\times)^2) \simeq F^\times/D_F\langle 1, -b\rangle.$$

Além disso, usando o primeiro e o segundo teorema do isomorfismo para grupos, temos

$$\begin{aligned}(F^\times D_K\langle 1, -b\rangle/(K^\times)^2)/(D_K\langle 1, -b\rangle/(K^\times)^2) &\simeq F^\times D_K\langle 1, -b\rangle/D_K\langle 1, -b\rangle \\ &\simeq F^\times/(F \cap D_K\langle 1, -b\rangle) \simeq F^\times/D_F\langle 1, -b\rangle.\end{aligned}$$

Portanto,

$$|(F^\times D_K\langle 1, -b\rangle/(K^\times)^2)/(D_K\langle 1, -b\rangle/(K^\times)^2| = |F^\times/D_F\langle 1, -b\rangle|) \quad (\dagger).$$

Ainda, usando a sequencia exata do **Lema 1.1.5** e observando que $D_F\langle 1, -a\rangle = F^\times$ e $N^{-1}(D_F\langle 1, -b\rangle/(F^\times)^2) = (F^\times D_K\langle 1, -b\rangle/(K^\times)^2)$, temos que

$$|(K/(K^\times)^2)/F^\times D_K\langle 1, -b\rangle/(K^\times)^2| = |(F^\times/(F^\times)^2)/(D_F\langle 1, -b\rangle/(F^\times)^2)| = |F^\times/D_F\langle 1, -b\rangle| \quad (\ddagger).$$

Assim, de (†) e (‡), obtemos que

$$|(K/(K^\times)^2)/(D_K\langle 1, -b\rangle/(K^\times)^2| = |F^\times/D_F\langle 1, -b\rangle|^2.$$

Novamente pelo primeiro teorema do isomorfismo, temos que

$$(K : D_K\langle 1, -b\rangle) = (F : D_F\langle 1, -b\rangle)^2.$$

□

Lema 2.2.3. *Sejam $K = F(\sqrt{a})$ uma extensão radical, $x \in K^\times$ tal $N(x) \in R(F)$ e $Gal(K/F) = \{1, \sigma\}$ o grupo de Galois da extensão K/F. Então valem:*

1. *$D_K\langle 1, -x\rangle = D_K\langle 1, -\sigma(x)\rangle$, $Q_K(x) = Q_K(\sigma(x))$ e para todo $y \in K^\times$ vale $(x, y)_K \cong (x, \sigma(y))_K$. Consequentemente $D_K\langle 1, -x\rangle^\sigma = D_K\langle 1, -x\rangle$ e $Q_K(x) = Q_K(x)^\sigma$.*

2. *Para $y \in K^\times$ temos que $N(y) \in D_F\langle 1, -x\rangle$ se e somente se $y \in F^\times D_K\langle 1, -x\rangle$. Consequentemente, $N^{-1}(D_K\langle 1, -x\rangle \cap F^\times) = F^\times D_K\langle 1, -x\rangle$.*

3. *$D_K\langle 1, -x\rangle \cap F^\times = N(D_K\langle 1, -x\rangle) = N(F^\times D_K\langle 1, -x\rangle)$.*

Demonstração. 1. Como $\sigma(x) = x(N(x)x^{-2})$ e $N(x)x^{-2} \in R(K)$, pelo **Corolário 2.1.4** temos que $D_F\langle 1, -\sigma(x)\rangle = D_F\langle 1, -x\rangle$. A igualdade $\sigma(x) = x(N(x)x^{-2})$ mostra também $(x, y)_K \cong (\sigma(x), y)_K$.

Agora, pela **Proposição 1.2.5** temos que $Q_K(x) \cap Q_K(\sigma(x)) \cong D_F\langle 1, -N(x)\rangle / D_F\langle 1, x\rangle \cap D_F\langle 1, -\sigma(x)\rangle = K^\times / D_F\langle 1, -N(x)\rangle \cong Q_K(x)$. Logo $Q_K(x) = Q_K(x) \cap Q_K(\sigma(x))$ e por simetria $Q_K(\sigma(x)) = Q_K(x) \cap Q_K(\sigma(x))$, também. Logo $Q_K(x) = Q_K(\sigma(x))$.

2. Numa direção a equivalência é trivial. De fato, se $y = az$, com $a \in F^\times$ e $z \in D_K\langle 1, -x\rangle$, então $N(y) = a^2N(z)$. Pelo item anterior, $D_K\langle 1, -x\rangle$ é invariante por σ e portanto $N(z) = z\sigma(z) \in D_K\langle 1, -x\rangle$, já que $D_K\langle 1, -x\rangle$ é multiplicativamente fechado. Concluímos então que $N(y) \in D_K\langle 1, -x\rangle$, como afirmado.

Na outra direção observemos primeiro que se $N(y) \in (F^\times)^2$, então pelo Teorema 90 de Hilbert, **Teorema 1.1.4**, $y \in F^\times(K^\times)^2$ e portanto o resultado vale. Vamos então assumir que $N(y) \in D_K\langle 1, -x\rangle$ e $N(y) \notin (F^\times)^2$.

Temos agora que $\sigma(y) = y(N(y)y^{-2})$. Como $N(y)y^{-2} \in D_K\langle 1, -x\rangle$ temos que $(x, \sigma(y))_K \cong (x, y)_K$. Logo pelo item *1.* temos $(x, y)_K \cong (\sigma(x), \sigma(y))_K \cong (x, y)_K^\sigma$, pois $(x, y)_K$ é invariante por automorfismos de $Gal(K/F)$. Vamos agora lançar mão de [**KMRT**]. Na notação desse livro $N_{K|F}$ corresponde a função correstrição da cohomologia. Mas independente disso, no item (a) da proposição que acabamos de citar, encontramos $N_{K|F}((x, y)_K) \otimes_F K \cong (x, y)_K \otimes_K (x, y)_K^\sigma$. Mas então $N_{K|F}(x, y)_K \otimes_F K$ é trivial.

No nosso caso, $K = F(\sqrt{a})$ com $a \in R(F)$, a inclusão ${}_2Br(F) \hookrightarrow {}_2Br(K)$ é injetiva. Ainda, se A é uma álgebra central simples sobre F, A, vale que $A_F \otimes_F K \simeq A_K$. Logo, no caso radical, A_K é trivial se e somente se A_F é trivial. Concluímos assim que $N_{K|F}(x, y)_K$ é trivial. Por [**KMRT**] temos que $(x, y)_K$ admite uma involução de segunda espécie. Nesse caso [**KMRT**] implica que existem b, $c \in F^\times$ tais que $(b, c)_K \cong (b, c)_F \otimes_F K \cong (x, y)_K$. Obtemos então a isometria das forma quadráticas $\langle 1, -b, -c, bc\rangle_K \simeq \langle 1, -x, -y, xy\rangle_K$, onde o índice K indica a extensão da forma sobre F para uma forma sobre K.

Vamos agora lançar mão das duas formas de transfer estudadas na **Proposição 1.1.6** e no **Corolário 1.1.7**. Por [**L**] temos que $s^*(\langle 1, -b, -c, bc\rangle_K) = 0 \in W(F)$ e como $\langle 1, -b, -c, bc\rangle_K \simeq \langle 1, -x, -y, xy\rangle_K$ vamos obter $s^*(\langle 1, -x, -y, xy\rangle) = 0 \in W(F)$.

Pelo **Corolário 1.1.7**, $s_y^* \circ \langle k\rangle(\langle 1, -x, -y, xy\rangle) = s_y^*(\langle k\rangle\langle 1, -x, -y, xy\rangle) = 0 \in W(F)$.

Observe agora que $-y \in D_K\langle 1, -x, -y, xy\rangle$ e também $N(y) \in D_K\langle 1, -x\rangle \subset D_K\langle 1, -x, -y, xy\rangle$. Logo $\langle k\rangle\langle 1, -x, -y, xy\rangle \simeq \langle 1, -x, -y, xy\rangle$, do que resulta $y_y^*(\langle 1, -x, -y, xy\rangle) = 0 \in W(F)$. Vamos agora fazer o cálculo direto

$$s_y^*(\langle 1,-x,-y,xy\rangle) = s_y^*(\langle 1,-x\rangle) - s_y^*(\langle y\rangle) - s_y^*(\langle xy\rangle) \in W(F).$$

Pela **Proposição 1.1.6** exite $\alpha \in F^\times$ tal que $s_y^*(\langle y\rangle) = \langle\alpha\rangle\langle 1,-N(y^2)\rangle = 0 \in W(F)$. Por outro lado, existe $\beta \in F^\times$ tal que $s_y^*(\langle xy\rangle) = \langle\beta\rangle\langle 1,-N(xy^2)\rangle \in W(F)$. Observe agora que como $N(x) \in R(F)$ temos para todo $\beta \in F^\times$ que $\langle\beta\rangle\langle 1,-N(x)\rangle \simeq \langle 1,-N(x)\rangle$.

Juntando tudo vamos obter

$$0 = s_y^*(\langle 1,-x,-y,xy\rangle) = s_y^*(\langle 1,-x\rangle) - \langle 1,-N(x)\rangle \in W(F).$$

Ou então

$$s_y^*(\langle 1,-x\rangle) = \langle 1,-N(x)\rangle \in W(F). \qquad (\dagger)$$

Como $N(y) \notin (F^\times)^2$, por hipótese, $\langle 1,-N(x)\rangle$ é anisotrópica. Por outro lado sabemos que $s_y^*(\langle 1,-x\rangle)$ tem dimensão 4. Portanto a igualdade $(\dagger)$ significa que a parte anisotrópica de $s_y^*(\langle 1,-x\rangle)$ tem dimensão 2, já que é isométrica a $\langle 1,-N(x)\rangle$. Logo $s_y^*(\langle 1,-x\rangle)$ é isotrópica. Mas isso implica, pelo **Corolário 1.1.8**, que $y \in F^\times D_K\langle 1,-x\rangle$, conforme queríamos.

3. Pelo item anterior vale que $D_K\langle 1,-x\rangle \cap F^\times = N(F^\times D_K\langle 1,-x\rangle)$. Também é claro que $N(D_K\langle 1,-x\rangle) \subset D_K\langle 1,-x\rangle \cap F^\times$, pois por *1.*, $D_K\langle 1,-x\rangle$ é invariante por σ. Resta então mostrar que se $c \in D_K\langle 1,-x\rangle \cap F^\times$, então $c \in N(D_K\langle 1,-x\rangle)$. Como N é sobrejetiva, existe $z \in K^\times$ tal que $N(z) = c$. Pelo item *2.*, existem $b \in F^\times$ e $y \in D_K\langle 1,-x\rangle$ tais que $z = by$. Logo $c = N(by) = b^2N(y)$. Por outro lado, existe também $u \in K^\times$ tal que $N(u) = b$. Vemos agora que $z_1 = u^2y \in D_K\langle 1,-x\rangle$ e $N(u^2y) = c^2N(y) = c$. Portanto $c \in N(D_K\langle 1,-x\rangle)$, como queríamos. □

Podemos agora, a partir do resultado anterior, caracterizar melhor $R(K)$, onde $K = F(\sqrt{a})$ é uma extensão radical do corpo F.

Teorema 2.2.4. *Mantendo as notações acima, temos que* $R(K) = \bigcap_{c\in F^\times} D_K\langle 1,-c\rangle$.

Demonstração. Para simplificar a notação, vamos escrever simplesmente R_o para denotar a intersecção $\bigcap_{c\in F^\times} D_K\langle 1,-c\rangle$.

Como $x \in D_K\langle 1,-c\rangle$, para todo $c \in F^\times$ temos pelo **Lema 1.1.1** que $F^\times \subset D_K\langle 1,-x\rangle$. Mas então para todo $z \in K^\times$ temos $N(z) \in D_K\langle 1,-x\rangle$. Dessa forma, pelo **Lemma 2.2.3** ítem *2.*, temos $z \in F^\times D_K\langle 1,-x\rangle = D_K\langle 1,-x\rangle$, já que $D_K\langle 1,-x\rangle$ é multiplicativamente fechado. Mas então $K^\times \subset D_K\langle 1,-x\rangle$, resultando em $x \in R(K)$. Portanto $R_o \subset R(K)$, demonstrando a igualdade.

□

2.3 Fecho reduzido

Nesta seção, apresentaremos o segundo resultado citado no início do Capítulo. Para tanto, inicaremos definindo formalmente o fecho reduzido para um corpo F de característica distinta de 2.

Definição 2.3.1. *Seja F um corpo qualquer e considere*

$$\mathcal{R} = \{F \subset M \subset F(2) \mid R(M) = (M^\times)^2\}.$$

O conjunto $\mathcal{R}$ assim definido é composto de todas as $2-$extensões de F que possuam radical reduzido.

Considere agora

$$F_{red} = \bigcap_{M \in \mathcal{R}} M.$$

*Como $F_{red} \subseteq M$, para toda extensão $M \in \mathcal{R}$, segue que $R(F_{red}) \subseteq R(M)$, para todo $M \in \mathcal{R}$, pelo **Lema 2.1.10**. Logo, $R(F_{red}) = (F^\times)^2_{red}$, isto é, F_{red} é um corpo com radical reduzido e chamaremos de **fecho reduzido** de F.*

Observação 2.3.2. *Definido desta maneira o fecho reduzido nos apresenta poucas propriedades que nos possibilitem estudar sua estrutura. Antes de apresentar F_{red} de uma maneira construtiva, apresentaremos algumas de suas propriedades que seguem diretamente da definição e dos resutados anteriores.*

(1) $R(F_{red}) = (F^\times)^2_{red}$.

(2) Se E é corpo tal que $R(E) = (E^\times)^2$ e $F \subseteq E$, então $F_{red} \subseteq E$.

Considere primeiramente, $\mathcal{K} = \{K_t = F(\sqrt{r_1}, \ldots \sqrt{r_t}),$ onde $r_i \in R(F)\}$, ordenado por inclusão.

Lema 2.3.3. *O conjunto $\mathcal{K}$ é indutivo, isto é, dados $K_{t_1}, K_{t_2} \in \mathcal{K}$ temos que $K_{t_1}, K_{t_2} \subseteq K_t$, para algum $K_t \in \mathcal{K}$.*

Demonstração. Note que $K_{t_1} = F(\sqrt{r_{11}}, \ldots \sqrt{r_{1t}})$ e $K_{t_2} = F(\sqrt{r_{21}}, \ldots \sqrt{r_{2t}})$ e considerando

$$K_t = F(\sqrt{r_{11}}, \ldots, \sqrt{r_{1t}}, \sqrt{r_{21}}, \ldots, \sqrt{r_{2t}}),$$

temos que $K_{t_1}, K_{t_2} \subseteq K_t$ e $K_t \in \mathcal{K}$.

□

Vamos considerar a seguir a seguinte construção.

Seja $L_1 = F(\{\sqrt{r} \mid r \in R(F)\})$, subcorpo de $F(2)$ gerado por F e $\{\sqrt{r} \mid r \in R(F)\}$, ou seja, $L_1 = \bigcap E$, onde $F \subseteq E \subseteq F(2)$ e $\{\sqrt{r} \mid r \in R(F)\} \subset E$.

Lema 2.3.4. *Para o corpo L_1 e conjunto $\mathcal{K}$ definidos acima valem:*

(a) $L_1 = \bigcup_t K_t$.

(b) Para todo $K_t \in \mathcal{K}$, temos que $R(K_t) \cap F^\times = R(F)$.

(c) $(L_1{}^{\times})^2 \cap F^{\times} = R(F)$ *e para todo* K_t *temos que* $(L_1{}^{\times})^2 \cap K_t = R(K_t)$.

Demonstração. (a) Note que $\bigcup_t K_t \subset L_1$, por construção de L_1. Seja $z \in L_1$, então existem $\{r_i\}_{i\in I}$, $r_i \in R(F)$ tais que $z \in F(\{\sqrt{r_i} \mid i \in I\}$. Denote por α_i o elemento $\sqrt{r_i}$. Assim, temos que $z = \sum_{s=1}^{m} \beta_s \prod_{i\in I} \alpha_i^{s_i}$, onde $s_i \in \{0,1\}$ e $s_i = 0$ a menos de um número finito J_s. Considere $J = \bigcup_s J_s$. Daí, temos que $z \in F(\{\sqrt{r_j} \mid j \in J\} = K_J \in \mathcal{K}$.

(b) Vamos mostrar por indução. O caso $K = F(\sqrt{r})$, $r \in R(F)$ foi mostrado no **Corolário 2.1.9**. Suponha verdadeira a afirmação para toda extensão com t geradores e considere $K_{t+1} \in \mathcal{K}$. Então $K_{t+1} = F(\sqrt{r_1}, \ldots \sqrt{r_{t+1}})$, com $r_i \in R(F)$. Assim, temos que $F(\sqrt{r_1}) \subset F(\sqrt{r_1}, \ldots \sqrt{r_{t+1}})$. Por hipótese de indução, temos que $R(F(\sqrt{r_1}, \ldots \sqrt{r_{t+1}})) \cap F(\sqrt{r_1}) = R(F(\sqrt{r_1}))$. Assim, temos que $R(F(\sqrt{r_1}, \ldots \sqrt{r_{t+1}})) \cap F^{\times} = (R(F(\sqrt{r_1}, \ldots \sqrt{r_{t+1}})) \cap F(\sqrt{r_1})) \cap F^{\times} = R(F(\sqrt{r_1})) \cap F^{\times} = R(F)$.

(c) Seja $r \in R(F)$, então $r \in (L_1{}^{\times})^2$ por definição de L_1. Reciprocamente, seja $r \in (L_1{}^{\times})^2 \cap F^{\times}$. Assim, $r = \beta^2$, para algum $\beta \in L_1{}^{\times}$. Por (a), temos que $\beta \in K_t$, para algum $K_t \in \mathcal{K}$. Logo, $r = \beta^2 \in (K_t{}^{\times})^2 \subset R(K_t)$. Portanto, temos que $r \in R(K_t) \cap F^{\times} = R(F)$, por (b).

□

Considere agora a cadeia de corpos $F = L_0 \subset L_1 \subset \cdots \subset L_n \subset \cdots F(2)$ onde para todo $i = 0, 1, 2, \ldots$ temos

$$L_{i+1} = L_i(\{\sqrt{r} \mid r \in R(L_i)\}).$$

Corolário 2.3.5. *Dados* $i > j \geq 0$, *temos que* $(L_i{}^{\times})^2 \cap L_j{}^{\times} = R(L_j)$ *e para todo* $i \geq 1$, $(L_i{}^{\times})^2 \cap F^{\times} = R(F)$. *Ainda, para* $L = \bigcup_{i\geq 0} L_i$, *temos que* $(L^{\times})^2 \cap F = R(F)$.

Demonstração. Para a demonstração deste resultado, note que L_{i+1} é obtido de L_i com a mesma construção de L_1 a partir de F no lema anterior. Desta forma, o resultado segue novamente por indução em i. □

Lema 2.3.6. *Seja* $\mathcal{K}$ *conjuto das extensões consideradas no* ***Lema 2.3.3****. Então para* $K_t \in \mathcal{K}$ *e* $a \in K_t$, $D_{L_1}\langle 1, a\rangle = \bigcup D_{K_{t'}}\langle 1, a\rangle$, *para* $K_t \subset K_{t'} \in \mathcal{K}$.

Demonstração. Seja $x \in D_{L_1}\langle 1, a\rangle$, então $x = x_1^2 + x_2^2 a$, com $x_1, x_2 \in L_1{}^{\times}$. Desde que $L_1 = \bigcup_t K_t$, segue que $x_1, x_2 \in K_s{}^{\times}$, para algum s. Pelo **Lema 2.3.3**, temos que existe n tal que $K_t, K_s \subseteq K_n$. Logo, $a, x_1, x_2 \in K_n$, ou seja, $x \in D_{K_n}\langle 1, a\rangle$ o que implica que $D_{L_1}\langle 1, a\rangle \subset \bigcup D_{K_{t'}}\langle 1, a\rangle$. A outra inclusão segue diretamente do fato que $K_{t'} \subset L_1$, para todo t'. □

Corolário 2.3.7. *Com as notações anteriores, temos:*

(a) Para $i > j \geq 0$ *e* $a \in L_j$, $D_{L_i}\langle 1, a\rangle \cap L_j{}^{\times} = D_{L_j}\langle 1, a\rangle$.

(b) Para todo $j \geq 0$ *e* $a \in L_j$, $D_L\langle 1, a\rangle \cap L_j{}^{\times} = D_{L_j}\langle 1, a\rangle$. *Em particular,* $D_L\langle 1, a\rangle \cap F^{\times} = D_F\langle 1, a\rangle$, *para todo* $a \in F^{\times}$.

Demonstração. (a) Considere a cadeia de corpos

$$L_j \subseteq L_{j+1} \subseteq \cdots \subseteq L_i.$$

Desde que L_{j+1} foi construído a partir de L_j analogamente à construção de L_1 a partir de F, podemos supor então que $L_j = F$ e $L_{j+1} = L_1$ e mostraremos que $D_{L_1}\langle 1, a\rangle \cap F = D_F\langle 1, a\rangle$. Seja $y \in D_{L_1}\langle 1, a\rangle \cap F$ Pelo lema anterior, $y \in D_{K_t}\langle 1, a\rangle \cap F$, para algum t. Mas K_t/F é extensão finita e $K_t \subseteq F_{red}$. Desta maneira, temos que K_t é uma $2-$extensão finita e então pelo **Corolário 2.1.8**, $D_{K_t}\langle 1, a\rangle \cap F = D_F\langle 1, a\rangle$, mostrando que $y \in D_F\langle 1, a\rangle$. Logo, $D_{L_1}\langle 1, a\rangle \cap F \subseteq D_F\langle 1, a\rangle$ e a outra inclusão é clara.

Portanto, por recorrência, temos que

$D_{L_i}\langle 1, a\rangle \cap L_j = (D_{L_i}\langle 1, a\rangle \cap L_{i-1}) \cap L_j = \cdots = D_{L_{j+1}}\langle 1, a\rangle \cap L_j = D_{L_j}\langle 1, a\rangle$.

(b) Seja $y \in D_L\langle 1, a\rangle \cap L_j$, então existem i e $y_1, y_2 \in L_i$ tais que $y = y_1^2 + ay_2^2 \in L_i$, por construção de L. Agora, se $i \leq j$, temos que $L_i \subseteq L_j$ e portanto $y \in D_{L_j}\langle 1, a\rangle$. Se $i > j$, então o resultado segue pelo ítem (a). A última afirmação é clara, desde que $F = L_0$. □

Corolário 2.3.8. *Para L construído no **Corolário 2.3.5**, temos que $R(L) = (L^\times)^2$.*

Demonstração. $R(L) = (L^\times)^2$ segue da construção de L e do **Corolário 2.3.5**. □

Note que pelo Corolário anterior, temos que $R(L) = (L^\times)^2$ e portando, por definição de F_{red}, $F_{red} \subseteq L$.

Vamos mostrar a outra inclusão.

Proposição 2.3.9. *Qualquer que seja corpo M tal que $F \subseteq M \subseteq L$ e $R(M) = (M^\times)^2$, temos que $L \subseteq M$.*

Demonstração. Se M é um corpo tal que $F \subseteq M \subseteq L$ e $R(M) = (M^\times)^2$, então voltando à construção do corpo L, temos que $L_1 \subseteq M$, uma vez que $L_1 = F(\{\sqrt{r} \mid r \in R(F)\})$ e $R(F) \subseteq R(M) = (M^\times)^2$.

E desta maneira, considere novamente a cadeia de corpos $F = L_0 \subset L_1 \subset \cdots \subset L_n \subset \cdots$ onde para todo $i = 1, 2, \ldots$ temos

$$L_{i+1} = L_i(\{\sqrt{r} \mid r \in R(L_i)\}),$$

temos que $L_j \subseteq M$, para todo j. Portanto,

$$L = \bigcup_{j \geq 0} L_j \subseteq M.$$

□

Corolário 2.3.10. *Para L e F_{red} como acima, temos que $L = F_{red}$.*

Demonstração. Observe que pela **Proposição 2.3.9** temos que $L \subseteq F_{red}$.

E por definição de F_{red}, temos que $F_{red} \subseteq L$, completando a demonstração.

□

Proposição 2.3.11. *Para toda extensão intermediária $F \subset E \subset M \subset F_{red}$ as seguintes afirmações valem:*

(a) Para todo $a \in E^\times$, $D_M\langle 1, a\rangle \cap E = D_E\langle 1, a\rangle$.

(b) $(M^\times)^2 \cap E = R(E)$.

Demonstração. Basta notar que pela construção do F_{red}, temos que $E_{red} = F_{red}$ para $F \subset E$, pelo **Lema 2.3.4**(c) e o **Corolário 2.3.7**.

□

Proposição 2.3.12. *Seja $\sigma : E \longrightarrow K$ isomorfismo de corpos, então $R(K) = \sigma(R(E))$.*

Demonstração. Se $x \in R(E)$, então $D_E\langle 1, -x\rangle = E^\times$. Tome $z \in K$ e desde que σ é isomorfismo, existe $y \in E$ tal que $z = \sigma(y)$. Mas $y = {y_1}^2 - x{y_2}^2$ e assim, $z = \sigma(y) = \sigma(y_1)^2 - \sigma(x)\sigma(y_2)^2 \in D_K\langle 1, -\sigma(x)\rangle$, ou seja, $\sigma(x) \in R(K)$. Para a outra inclusão basta notar que $E = \sigma^{-1}(K)$. □

Pelo resultado anterior, temos que se E é reduzido, ou seja, $R(E) = (E^\times)^2$, então todo conjugado de E é também reduzido. Usaremos este fato nos próximos resultados.

Teorema 2.3.13. *Seja F corpo e considere F_{red}. Então valem as seguintes propriedades:*

(a) $R(F_{red}) = (F^\times)^2_{red}$ e para toda extensão M de F tal que $R(M) = (M^\times)^2$ temos $F_{red} \subset M$.

(b) Para toda extensão intermediária $F \subset E \subset F_{red}$ temos que $F_{red} = E_{red}$.

(c) F_{red} é extensão normal de F e $(F^\times)^2_{red} \cap F^\times = R(F)$.

(d) Para todo $a \in F^\times$ temos que $D_{F_{red}}\langle 1, a\rangle \cap F^\times = D_F\langle 1, a\rangle$.

(e) Sejam $a, b \in F^\times$. Então $(a, b)_F \otimes_F F_{red} = 0 \in {}_2Br(F_{red})$, se e somente se, $(a, b)_F = 0 \in {}_2Br(F)$.

Demonstração. Para a demonstração do teorema, resta demonstrar somente que F_{red} é extensão normal e o item (e).

Por construção, temos que

$$F_{red} = \bigcap_{M \in \mathcal{R}} M$$

onde $\mathcal{R} = \{M \mid F \subseteq M \subseteq F(2) \text{ e } R(M) = (M^\times)^2\}$.

Usando a **Proposição 2.3.12**, temos que $\sigma(M) \in \mathcal{R}$ para todos $M \in \mathcal{R}$ e $\sigma \in G_2(F)$. Portanto, temos que

$$F_{red} = \bigcap_{\sigma \in G_2(F)} \sigma(M),$$

ou seja, F_{red} é invariante por automorfismos. Assim F_{red} é normal.

(e) Se $(a, b)_{F_{red}} = 0 \in {}_2Br(F_{red})$, então $a \in D_{F_{red}}\langle 1, -b\rangle$. Assim, $a \in D_{F_{red}}\langle 1, -b\rangle \cap F^\times = D_F\langle 1, -b\rangle$, ou seja, $(a, b)_F = 0 \in {}_2Br(F)$.

□

Capítulo 3

Bases distinguidas - parte I

Este capítulo é totalmente dedicado ao estudo de corpos com base distinguida(veja **Definição 3.2.1**) e extensões radicais destes corpos. O conceito de base distinguida apareceu no trabalho após a demonstração dos **Teoremas 3.2.23 e 3.2.18**. Como já havíamos determinado o comportamento do radical sobre as extensões quadráticas, procuramos uma maneira de entender o comportamento das álgebras de quatérnios sobre extensões finitas de corpos com $\dim_{\mathbb{F}_2} {}_2Br(F)$ finita. Este é um conceito novo na teoria de corpos que tivemos que introduzir para podermos lidar com 2-extensões gerais. No caso de anéis de Witt abstratos, Marshal introduziu um conceito parecido em [M], mas não trabalhou suas propriedades.

O principal objetivo deste capítulo é mostrar que as propriedades de base distinguida completa(veja **Definição 3.2.13**) se transferem para toda extensão finita K/F, onde $F \subseteq K \subseteq F_{red}$.
O caso não radical será deixado para o capítulo seguinte.

Durante este Capítulo e nos seguintes, usaremos sempre expressões como "base," "linearmente independente," ou "conjunto de geradores" considerando espaços vetoriais sobre $\mathbb{F}_2$.

3.1 Motivação

Mandendo as notações anteriores, assumiremos nesta primeira seção que temos um corpo F com grupo de Galois $G_2(F)$ decomponível em um produto livre da forma

$$G_2(F) \simeq \mathcal{L} * \mathcal{D}_1 * \cdots * \mathcal{D}_t, \tag{3.1.1}$$

onde $\mathcal{D}_1, \ldots, \mathcal{D}_t$ são grupos de Demushkin e $\mathcal{L}$ é um grupo livre.
Por [**NSW**], temos que $\mathcal{D}$ é um grupo de Demushkin se:

1. $\dim_{\mathbb{F}_2} H^1(\mathcal{D}) < \infty$.
2. $\dim_{\mathbb{F}_2} H^2(\mathcal{D}) = 1$.

3. O produto cup $H^1(\mathcal{D}) \times H^1(\mathcal{D}) \longrightarrow H^2(D)$ é não degenerado.

Relembramos que $H^n(\mathcal{D})$ denota o n-ésimo grupo de Cohomologia de $\mathcal{D}$ com coeficientes em $\mathbb{Z}/2\mathbb{Z}$.

Sobre os grupos de Cohomologia dos grupos livres, temos, pelo [**RZ**] que $H^n(\mathcal{L}) = 0$ para todo $n \geq 2$, isto é, a dimensão cohomológica de $\mathcal{L}$ é 1.

Corpos K com $G_2(K)$ livre ou de Demushkin são bem conhecidos. Podemos ver por exemplo em [**Se**] e [**Se**]. Desta maneira, podemos garantir que as parcelas da decomposição (3.0) são realizáveis, e o próximo teorema, garantirá que o produto livre de tais grupos é realizável.

Teorema 3.1.1 (Jacob-Ware)**.** *Sejam $G_1, \dots G_n$ pro-2 grupos realizáveis como $G_2(F_i)$ para convenientes corpos F_i. Então $G = G_1 * \cdots * G_n$ também é realizável, isto é, existe corpo F tal que $G \simeq G_2(F)$.*

Demonstração. **Teorema 3.6** de [**JW**].

□

Dada a apresentação do corpo F e das parcelas da decomposição do grupo de Galois $G_2(F)$, vamos agora ao estudo da estrutura do corpo F. Do isomorfismo de 3.1.1, segue que $\mathcal{L}, \mathcal{D}_1, \dots, \mathcal{D}_t$ são subgrupos fechados de $G_2(F)$, e para cada $i = 1, \dots, t$, considere $H_i = Fix(\mathcal{D}_i)$ e $E = Fix(\mathcal{L})$, isto é, os subcorpos de $F(2)$ fixos pelos subgrupos fechados $\mathcal{D}_1, \dots, \mathcal{D}_t, \mathcal{L}$. Consequentemente, temos que $H_1, \dots, H_t, E$ são $2-$extensões de F, isto é, são extensões de F contidas no fecho quadrático $F(2)$.

E desta maneira, temos o seguinte:

$$G_2(F) \simeq G_2(E) * G_2(H_1) * \cdots * G_2(H_t). \quad (3.1)$$

Lema 3.1.2. *Usando as propriedades sobre grupos de Demushkin e grupos livres, juntamente com o isomorfismo (3.0), temos o seguinte:*

1. *para todo $i = 1, \dots, t$, $\dim_{\mathbb{F}_2} {}_2Br(H_i) = 1$ e $R(H_i) = (H^\times)_i^2$. Além disso, para todo $a \in H_i^\times \setminus (H^\times)_i^2$ temos que $(H_i^\times : D_{H_i}\langle 1, -a\rangle) = 2$ e ${}_2Br(H_i) = Q_{H_i}(a)$.*
2. *${}_2Br(E) = 0$ e consequentemente $R(E) = E^\times$.*

Demonstração. Note que para todo $i = 1, \dots, t$, $Gal(F(2)/H_i)$ é um grupo de Demushkin e obtemos, pela teoria de Kummer, que $\dim_{\mathbb{F}_2} {}_2Br(H_i) = \dim_{\mathbb{F}_2} H^2(F(2)/H_i) = 1$. Vamos mostrar agora que $R(H_i) = (H^\times)_i^2$. Suponha que exista $a \in H_i^\times \setminus (H^\times)_i^2$ tal que $a \in R(H_i)$. Desta maneira, temos pelo Lema 2.1.3 que $(a, b)_{H_i} \simeq M_2(H_i)$ para todo $b \in H_i^\times$, isto é, $\chi_a \cup \chi_b = 0$, contradizendo o fato de o produto *cup*

$$H^1(Gal(F(2)/H_i)) \times H^1(Gal(F(2)/H_i)) \longrightarrow H^2(Gal(F(2)/H_i))$$

ser não degenerado. Portanto, temos que $R(H_i) = (H^\times)_i^2$.

Para finalizar a demonstração do ítem *1.*, note para todo $a \in H_i^\times \setminus (H^\times)_i^2$, temos que

$$0 < \dim_{\mathbb{F}_2} Q_{H_i}(a) \leq \dim_{\mathbb{F}_2} {}_2Br(H_i) = 1,$$

o que implica que $\dim_{\mathbb{F}_2} Q_{H_i}(a) \leq \dim_{\mathbb{F}_2} {}_2Br(H_i) = 1$. Agora, pela **Proposição 1.2.4**, $Q_{H_i}(a) \simeq H_i^\times / D_{H_i}\langle 1, -a\rangle$, para todo $a \in H_i^\times$ e $i = 1, \ldots, t$. Consequentemente, $(H_i^\times : D_{H_i}\langle 1, -a\rangle) = 2$ e $\dim_{\mathbb{F}_2} Q_{H_i}(a) = 1$, mostrando também que $Q_{H_i}(a) = {}_2Br(H_i)$.

Para a segunda afirmação, note que o fato de $Gal(F(2)/E)$ ser um grupo livre implica que ${}_2Br(E) \simeq H^2(E) = H^2(Gal(F(2)/E) = 0$. Daí, se $x \in E^\times \setminus (E^\times)^2$, então $(x, b)_E = 0$ para todo $b \in E^\times$. E novamente pelo **Lema 2.1.3**, temos que $x \in R(E)$.

□

Observação 3.1.3. *Vamos aqui considerar, para todo $i = 1, \ldots, t$, $H_i^\times/(H^\times)_i^2$, como $\mathbb{F}_2-$espaço vetorial. Observe que se $B_i = \{h_{i1}, \ldots, h_{ii_t}\}$ induz uma base de $H_i^\times/(H^\times)_i^2$, então pelo ítem 1. do lema anterior, temos que:*

1. $(H_i^\times : D_{H_i}\langle 1, -h_{ij}\rangle) = 2$, *para todo* $j = 1, \ldots i_t$.
2. ${}_2Br(H_i) = Q_{H_i}(h_{ij})$, *para todo* $j = 1, \ldots i_t$.

Para continuarmos, vamos apresentar um resultado que usaremos para determinar a estrutura de $F^\times/(F^\times)^2$.

Teorema 3.1.4 (Neukirch)**.** *Sejam F um corpo qualquer e $\{H_j \subseteq F(2)\}$, $j \in J$, $2-$extensões de F. Denotando por G_j o grupo de galois $Gal(F(2)/H_j)$, são equivalentes:*

(i) $G_2(F) \simeq *_{j\in J} G_j$

(ii) $Res^i : H^i(G) \longrightarrow \bigoplus_{j\in J} H^i(G_j)$, *é um isomorfismo para $i = 1$ e monomorfismo para $i = 2$, onde Res^i e a função restrição.*

Demonstração. A demonstração pode ser encontrada em [**NSW**].

□

No nosso caso, onde estamos assumindo verdadeira a afirmação (i) do teorema acima, podemos concluir que vale o seguinte:

Corolário 3.1.5. *Para os corpos F, H_i, $i = 1, \ldots, t$, e E, valem:*

1. $F^\times/(F^\times)^2 \simeq H_1^\times/(H^\times)_1^2 \oplus \cdots \oplus H_t^\times/(H^\times)_t^2 \oplus E^\times/(E^\times)^2$
2. $\bigcap_{i=1}^{t} (D_{H_i}\langle 1, -a\rangle \cap F^\times) \subseteq D_F\langle 1, -a\rangle$, *para todo* $a \in F^\times/(F^\times)^2$.

3. $R(F)/(F^\times)^2 \simeq E^\times/(E^\times)^2$.

Demonstração. A afirmação *1.* segue do teorema acima, pois para cada $i = 1, \ldots, t$ valem os seguintes isomorfismos $H^1(Gal(F(2)/H_i)) \simeq {H_i}^\times/(H^\times)_i^2$ e $H^1(Gal(F(2)/E)) \simeq E^\times/(E^\times)^2$.

Para a afirmação *2.*, note inicialmente que pela afirmação *(ii)* do teorema anterior, a aplicação $Res^2 : H^2(G) \longrightarrow H^2(Gal(F(2)/H_1)) \oplus \cdots \oplus H^2(Gal(F(2)/H_t))$ é injetiva, pois $H^2(Gal(F(2)/E))$ é trivial.

Para todo $a \in F^\times/(F^\times)^2$, por *1.* do **Teorema 1.2.2**, temos a álgebra de quatérnios $(a,b)_F \in {}_2Br(F)$ é trivial se, e somente se, $b \in D_F\langle 1, -a\rangle$. Tomando-se agora $a, b \in F^\times$ a injetividade do parágrafo anterior implica que se a álgebra de quatérnios $(a,b)_F \otimes H_j \simeq (a,b)_{H_j}$ for trivial em ${}_2Br(H_j)$, para todo $j = 1, \ldots, t$, então $(a,b)_F$ é trivial em ${}_2Br(F)$. Em outras palavras, dado qualquer que seja $a \in F^\times$, temos que se $b \in F^\times$ pertence a interseção $\bigcap_{j=1}^{t} D_{H_j}\langle 1, -a\rangle$, então $b \in D_F\langle 1, -a\rangle$. Concluimos assim que $\bigcap_{j=1}^{t}(D_{H_j}\langle 1, -a\rangle \cap F) \subseteq D_F\langle 1, -a\rangle$ para todo $a \in F^\times/(F^\times)^2$.

Para o último ítem, vamos denotar o isomorfismo do ítem *1.* por φ e mostrar que a restrição de φ a $R(F)/(F^\times)^2$ é o ismorfismo desejado. Para $x \in R(F) \setminus (F^\times)^2$, temos pelo **Lema 2.1.10** que $x \in R(H_i)$, para todo $i = 1, \ldots, t$. Se $\varphi(x) = (h_1, \ldots, h_t, e)$, onde $h_i \in H_i^\times/(H^\times)_i^2$, para todo $i = 1, \ldots, t$ e $e \in E^\times/(E^\times)^2$, então, $\varphi(x) = (1, \ldots, 1, e)$, pois $R(H_i) = (H^\times)_i^2$ e φ é induzido pela inclusão. Note que se $x \neq 1 \in F^\times/(F^\times)^2$, então $x \neq 1 \in E^\times/(E^\times)^2$, mostrando a injetivdade.

Vamos agora mostrar a sobrejetividade da função φ. Para toda classe $e \in E^\times/(E^\times)^2$, considere

$$(1, \ldots, 1, e) \in H_1^\times/(H^\times)_1^2 \oplus \cdots \oplus H_t^\times/(H^\times)_t^2 \oplus E^\times/(E^\times)^2.$$

Desta forma, por φ ser um isomorfismo, existe $x \in F^\times/(F^\times)^2$ tal que $\varphi(x) = (1, \ldots, 1, e)$. Para garantir que $x \in R(F)$, vamos usar a injetividade da restrição

$$Res^2 : H^2(G) \longrightarrow H^2(Gal(F(2)/H_1)) \oplus \cdots \oplus H^2(Gal(F(2)/H_t)).$$

Suponha que $x \notin R(F)$. Então $Q_F(x) \neq 0$ e consequentemente, existe pelo menos um índice i tal que $Q_{H_i}(x) \neq 0$. Portanto, $x \notin R(H_i)$ e consequentemente, $\varphi(x) = (\ldots, h_i, \ldots)$, onde $h_i \neq 1 \in H_i^\times/(H^\times)_i^2$, contrariando a escolha de x.

□

Usaremos agora os argumentos semelhantes aos usados na demonstração do ítem *3.* do corolário anterior para construir uma base para $F^\times/R(F)$, considerado como $\mathbb{F}_2$ espaço vetorial.

Pelos ítens *1.* e *3.* do corolário anterior, temos que

$$F^\times/R(F) \simeq H_1^\times/(H^\times)_1^2 \oplus \cdots \oplus H_t^\times/(H^\times)_t^2.$$

Para cada $i = 1, \ldots, t$, considere $B_i = \{h_{i1}, \ldots, h_{it_i}\}$ uma base de $H_i^\times/(H^\times)_i^2$ como na Observação 3.1.3.

Agora, usando o isomorfismo φ, existem $\{x_{i1}, \ldots, x_{it_i}\} \subseteq F^\times/R(F)$, tais que

$$\varphi(x_{ij}) = (1, \ldots, 1, h_{ij}, 1, \ldots, 1),$$

para $j = 1, \ldots, t_i$, onde h_{ij} está na i-ésima posição. Denote por C_i o conjunto $\{x_{i1}, \ldots, x_{it_i}\}$. Para facilitar a notação, usaremos que $\varphi(x_{ij}) = h_{ij}$ ao invés de escrever $(1, \ldots, 1, h_{ij}, 1, \ldots, 1)$.

Teorema 3.1.6. *Considere para cada $i = 1, \ldots, t$, o conjunto C_i como acima. Então o conjunto $C = \bigcup_{i=1}^{t} C_i$ possui as seguintes propriedades:*

1. $(F^\times : D_F\langle 1, -c\rangle) = 2$, *para todo $c \in C$ e consequentemente, $Q_F(c)$ tem ordem* 2.
2. *Denotando por F_i o subespaço de $F^\times/R(F)$ gerado por C_i, temos que $F_i \simeq H_i^\times/(H^\times)_i^2$, para todo $i = 1, \ldots, t$. Além disso, todo $x \in F^\times \setminus R(F)$ pode ser decomposto em um produto da forma $x = x_{\lambda_1} \cdots x_{\lambda_r}$, onde $x_{\lambda_j} \in F_{\lambda_j}$ e $Q_F(x) = Q_F(x_{\lambda_1}) \oplus \cdots \oplus Q_F(x_{\lambda_r})$.*
3. *C é uma base de $F^\times/R(F)$.*

Demonstração. 1. Seja $c \in C$, então $c \in C_i$, para algum i. Pelas propriedades dos conjuntos C_i, temos que$\varphi(c) \in R(H_j)$, para todo $j \neq i$ e consequentemente, $Q_F(c) \otimes H_j = 0$, se $j \neq i$, onde $Q_F(c) = \{(x, c)_F \otimes H_j \mid x \in F^\times\}$.

Agora, como Res^2 é injetiva, temos que $0 < \dim_{\mathbb{F}_2} Q_F(c) \leq \dim_{\mathbb{F}_2} Q_F(c) \otimes H_i = 1$. Portando, $Q_F(c)$ tem ordem 2 e $(F^\times : D_F\langle 1, -c\rangle) = 2$, pela **Proposição 1.2.4**.

2. Vamos primeiramente mostrar que o conjunto C_i é linearmente independente visto como subconjuntos das classes de $F^\times/R(F)$, para todo $i = 1, \ldots, t$. Para tanto, suponha que $x = x_{i1}^{\alpha_1} \cdots x_{it_i}^{\alpha_{t_i}} \in R(F)$, onde $\alpha_j \in \{0, 1\}$. Então, usando o fato que $R(H_i) = (H^\times)_i^2$ e que φ é um isomorfismo, segue que $\varphi(x) \doteq h_{i1}^{\alpha_1} \cdots h_{it_i}^{\alpha_{t_i}} \in R(H_i) = (H^\times)_i^2$. Agora, como $B_i = \{h_{i1}, \ldots, h_{it_i}\}$ é linearmente independente, temos que $\alpha_j = 0$, para $j = 1, \ldots, t_i$ e consequentemente, $C_i = \{x_{i1}, \ldots, x_{it_i}\}$ é linearmente independente. Agora, denotando por F_i o subespaço de $F^\times/R(F)$ gerado por C_i, temos que $\dim_{\mathbb{F}_2} F_i = \dim_{\mathbb{F}_2} H_i^\times/(H^\times)_i^2 = t_i$. Podemos concluir então que $F_i \simeq H_i^\times/(H^\times)_i^2$, pelo isomorfismo induzido por φ, pois $\varphi(F_i) \subseteq H_i^\times/(H^\times)_i^2$, para todo $i = 1, \ldots, t$. E desta forma,

$$F^\times/R(F) \simeq F_1 \oplus \cdots \oplus F_t.$$

Considere agora $x \in F^\times \setminus R(F)$. Pelo isomorfismo acima, $x = x_{\lambda_1} \cdots x_{\lambda_r}$, onde $x_{\lambda_j} \neq 1 \in F_{\lambda_j}$, para todo $j = 1, \ldots, t$. Além disso, note que para cada x_{λ_j}, temos que $Q_F(x_{\lambda_j}) \neq 0$, pois $x_{\lambda_j} \notin R(F)$ e $Q_F(x_{\lambda_j}) \oplus H_i = 0$ para $i \neq \lambda_j$. Finalmente, uma vez que $\varphi(x_{\lambda_j}) = 1 \in H_i$, para $i \neq \lambda_j$, temos que

$$\dim_{\mathbb{F}_2} Res^2(Q_F(x)) = r.$$

Por outro lado, Res^2 é injetiva e daí $\dim_{\mathbb{F}_2} Q_F(x) = r$. Portanto, temos que

$$Q_F(x) = Q_F(x_{\lambda_1}) \oplus \cdots \oplus Q_F(x_{\lambda_r}),$$

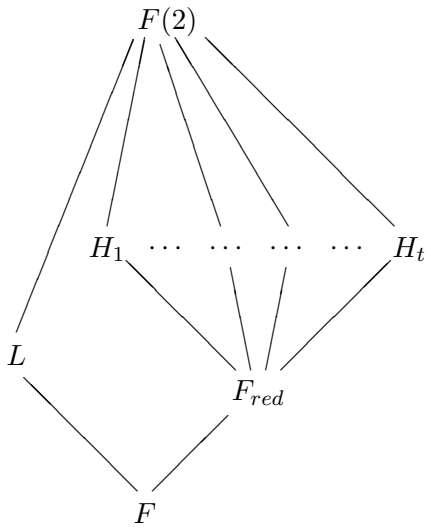
pois $Q_F(x_{\lambda_i}) \cap Q_F(x_{\lambda_j}) = 0$, se $\lambda_i \neq \lambda_j$ e $\dim_{\mathbb{F}_2} Q_F(x) = \dim_{\mathbb{F}_2} Q_F(x_{\lambda_1}) + \ldots \dim_{\mathbb{F}_2} Q_F(x_{\lambda_{\lambda_r}})$.

3. Para mostrar que C é uma base, precisamos somente mostrar que C é linearmente independente, pois vimos no parágrafo anterior que $F^\times/R(F)$ é gerado por C como $\mathbb{F}_2-$espaço vetorial. Mas note que

$$\dim_{\mathbb{F}_2} F^\times/R(F) = \sum_{i=1}^{t} \dim_{\mathbb{F}_2} F_i = \sum_{i=1}^{t} \#C_i = \#C.$$

Portanto, C deve ser linearmente independete, pois caso contrário, $\dim_{\mathbb{F}_2} F^\times/R(F)$ seria menor que $\#C$, uma contradição. □

A seguir um diagrama ilustrativo dos corpos envolvidos.



No início desta seção, assumimos que F é um corpo cujo grupo de Galois $G_2(F)$ é decomponível da forma

$$G_2(F) \simeq \mathcal{L} * \mathcal{D}_1 * \cdots * \mathcal{D}_t, \tag{3.1.2}$$

onde $\mathcal{D}_1, \ldots, \mathcal{D}_t$ são grupos de Demushkin e $\mathcal{L}$ é um grupo livre.

O **Teorema 3.1.6** nos diz que:

1. o espaço vetorial $F^\times/R(F)$ possui uma base C tal que $(F^\times : D_F\langle 1, -c\rangle) = 2$, para todo $c \in C$.

2. A base C é a união de t subconjuntos linearmente independentes, onde $t = \dim_{\mathbb{F}_2} {}_2Br(F)$.

3. Toda álgebra de quatérnios $(x, y)_F$ pode ser decomposta em ${}_2Br(F)$ da forma

$$(x, y)_F \simeq (x_{\lambda_1}, y_{\lambda_1})_F \oplus \cdots \oplus (x_{\lambda_t}, y_{\lambda_t})_F,$$

onde $x_{\lambda_j}, y_{\lambda_j} \in C_{\lambda_j}$.

Podemos obter resultados semelhantes se trocarmos os grupos de Demushkin por grupos de ordem 2 na decomposição abaixo do grupo $G_2(F)$.

$$G_2(F) \simeq \mathcal{L} * \mathcal{D}_1 * \cdots * \mathcal{D}_t. \tag{3.1.3}$$

Como preparação vamos recordar os pontos que nos interessam sobre corpos formalmente reais, que também serão usados na parte final do trabalho.

Vamos relembrar a seguir a definição de corpo formalmente real e ordem.

Definição 3.1.7. *1. Dizemos que F é um corpo **formalmente real** se $-1 \notin \sum F^2$.*

*2. Dizemos que $P \subseteq F^\times$ é um **cone positivo de uma ordem** do corpo F se possui as seguintes prorpiedades:*

(a) $P + P \subseteq P$

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

(c) $P \cup (-P) = F^\times$

Lema 3.1.8. *Para um corpo F as seguintes afirmações são equivalentes:*

1. $-1 \notin \sum F^2$, isto é, F é formalmente real.

2. Para todo $n \in \mathbb{N}$ a $n-$forma quadrática $\langle 1, \ldots, 1\rangle$ á anisotrópica, isto é, $0 \notin D_F(\langle 1, \ldots, 1\rangle)$.

Reuniremos no próximo resultado algumas propriedades envolvento corpos formalmente reais e ordens.

Proposição 3.1.9. *Sejam F um corpo e P um cone positivo de uma ordem de F. Então as seguintes propriedades são verdadeiras:*

1. F é formalmente real e, consequentemente, a característica de F é 0.

2. $(F^\times)^2 \subseteq P$.

3. $-1 \notin P$ e $P \cap (-P) = \{0\}$.

4. $P^\times$ é um subgrupo de índice 2 de $F^\times$.

5. Se P' é um cone positivo e $P' \subseteq P$, então $P' = P$.

Demonstração. [**L**].

□

Vamos assumir agora que F é um corpo cujo grupo de Galois $G_2(F)$ é decomponível na forma

$$G_2(F) \simeq \mathcal{L} * \mathcal{D}_1 * \cdots \mathcal{D}_n * \mathcal{G}_{n+1} * \cdots * \mathcal{G}_t,$$

onde $\mathcal{D}_j$, $j = 1, \ldots, n$ é um grupo de Demushkin e $\mathcal{G}_j \simeq \mathbb{Z}/2\mathbb{Z}$ para $j = n+1, \ldots, t$. Note que estamos apenas trocando algumas das parcelas de Demushkin por grupos de ordem 2.

Desta maneira, temos que os corpos H_j, tais que $Gal(F(2)/H_j) = \mathcal{G}_j$, $j = n+1, \ldots, t$ satisfazem:

1. $H_j^\times/(H_j{}^\times)^2$ é de ordem 2.
2. H_j é um corpo formalmente real e euclidiano.

Desta maneira, temos que os conjuntos C_j, associados às 2−extensões H_j, $j = n+1, \ldots, t$ são unitários. Denotaremos por J o conjunto de índices $n+1, \ldots, t$.

Teorema 3.1.10. *Seja F corpo tal que $G_2(F) \simeq \mathcal{L}*\mathcal{D}_1*\cdots\mathcal{D}_n*\mathcal{G}_{n+1}*\cdots*\mathcal{G}_t$, onde $\mathcal{D}_j$, $j = 1, \ldots, n$ é um grupo de Demushkin e $\mathcal{G}_j \simeq \mathbb{Z}/2\mathbb{Z}$ para $j = n+1, \ldots, t$. Então valem:*

1. *F é um corpo formalmente real.*
2. *Os grupos $D_F\langle 1, -x_j\rangle$, $j = n+1, \ldots, t$, são ordens para o corpo F.*

Demonstração. 1. Para $j = n, \ldots, t$, temos que H_j é um corpo formalmente real. Como $F \subseteq H_j$, segue que F é um corpo formalmente real, mostrando a afirmação *1.*

O ítem *2.* será demonstrado em alguns passos. Para tanto, considere os subespaços F_j, gerados pelos conjuntos C_j, com $j \in J = \{n+1, \ldots, t\}$.

• $\dim_{\mathbb{F}_2} F^\times/D_F\langle 1, -x_j\rangle = 1$, segue das propriedades dos conjuntos C_j.

• $-1 \notin D_F\langle 1, -x_j\rangle$.

Em H_j temos $(-1,-1)_{H_j} \neq 0$, pois H_j é formalmente real. Seja $x_j \in F_j$ tal que $\varphi(x_j) = (1, ..., -1, ...1,)$, onde o -1 está na j-ésima posição. Logo $Res^2((x_j, x_j)_F) = (0, ..., (-1,-1)_{H_j}, ...0)$. Assim, temos que $x_j \notin D_F\langle 1, -x_j\rangle$. Agora, caso $-1 \in D_F\langle 1, -x_j\rangle$ teríamos $x_j = (-1)\cdot(-x_j) \in D_F\langle 1, -x_j\rangle$, pois $D_F\langle 1, -x_j\rangle$ é grupo multiplicativo e $-x_j \in D_F\langle 1, -x_j\rangle$. Portanto, temos que $-1 \notin D_F\langle 1, -x_j\rangle$.

• $F^\times = D_F\langle 1, -x_j\rangle \cup -D_F\langle 1, -x_j\rangle$.

Seja $x \in F^\times$ e suponha que $x \notin D_F\langle 1, -x_j\rangle$. Como $F^\times/D_F\langle 1, -x_j\rangle$ é de ordem 2, temos que $x = x_j r$, para algum $r \in D_F\langle 1, -x_j\rangle$. Como $-1 \notin D_F\langle 1, -x_j\rangle$, temos que $-1 = x_j a$, onde $a \in D_F\langle 1, -x_j\rangle$. Portanto, $-x = x_j^2 ar \in D_F\langle 1, -x_i\rangle$, como queríamos.

• Para finalizar a demonstração de que $D_F\langle 1, -x_j\rangle$ é uma ordem, precisamos mostrar que $D_F\langle 1, -x_j\rangle$ é aditivamente fechado.

Vamos mostrar que $D_F\langle 1, -x_j\rangle = D_F\langle 1, -x_j, -x_j, 1\rangle \subseteq F^\times$.

Como $D_F\langle 1, -x_j\rangle \subset D_F\langle 1, -x_j, -x_j, 1\rangle$ e $F^\times/D_F\langle 1, -x_j\rangle$ tem ordem 2, basta verificar que $D_F\langle 1, -x_j, -x_j, 1\rangle \neq F^\times$.

Se $x_j \in D_F\langle 1, -x_j, -x_j, 1\rangle$, então $\langle 1, -x_j\rangle \otimes \langle 1, -x_j\rangle \otimes \langle 1, -x_j\rangle$ seria isotrópica, e portanto hiperbólica, pois é uma forma de Pfister. Mas então $\langle 1, -x_j\rangle \otimes \langle 1, -x_j\rangle \otimes \langle 1, -x_j\rangle = 0 \in W(F)$.

Como $\langle 1, -x_j\rangle \otimes \langle 1, -x_j\rangle \otimes \langle 1, -x_j\rangle = 3\langle 1, -x_j\rangle$ teremos que a classe de $\langle 1, -x_j\rangle$ em $W(F)$ seria um elemento de torção. Nesse caso, por [**L**] x_j é uma soma de quadrados em F. Mas isso é impossível pois nesse caso, como H_j é euclidiano, temos $x_j \in (H_j^\times)^2$ contra escolha de x_j.

□

3.2 Bases distinguidas

Definição 3.2.1. *Sejam F um corpo e $\{a_1, \dots a_n\} \subset F^\times$ um conjunto não vazio tal que:*

(i) $\{a_1R(F), \dots, a_nR(F)\}$ é uma base de $F^\times/R(F)$;

(ii) Para todo $1 \leq j \leq n$, $(F^\times : D_F\langle 1, -a_j\rangle) = 2$.

Chamamos um conjunto $\{a_1, \dots a_n\}$ com as propriedades acima de ***base distinguida*** de F.

Nossa expectativa era demonstrar que reciprocamente o grupo de Galois $G_2(F)$ de um corpo com base distinguida admitiria uma decomposição em produto livre na categoria dos pro-2 grupos como as que foram consideradas no parágrafo anterior. Contudo, depois de muito tempo e muitas páginas escritas ainda não chegamos a demonstrar o resultado no caso geral. Isso é o projeto que temos para um futuro imediato. Entretanto, como veremos nas páginas seguintes, o estudo de corpos com base distinguida mostrou-se produtivo e obtivemos vários resultados importantes, em particular o *Teorema 90 de Hilbert* para o Radical de Kaplansky e a validade da decomposição para alguns corpos formalmente reais.

Vamos iniciar o estudo de corpos com base distinguida, apresentando um resultado técnico que será bastante útil neste trabalho.

Lema 3.2.2. *Dado um corpo F, quaisquer que sejam $x_1, \dots, x_r \in F^\times$ temos a igualdade abaixo*

$$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_r\rangle = D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_{r-1}\rangle \cap D_F\langle 1, -x_1 \cdots x_r\rangle.$$

Em particular,

1. *se $\{x_1R(F), \dots, x_rR(F)\}$ é uma base de $F^\times/R(F)$, então $R(F) = \bigcap_{j=1}^{r} D_F\langle 1, -x_j\rangle$.*
2. *Se $x_1 \cdots x_r \in (F^\times)^2$, então $D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_r\rangle = D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_{r-1}\rangle$.*
3. *$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_r\rangle \subset D_F\langle 1, -x_1 \cdots x_r\rangle$.*

Demonstração. Mostraremos a igualdade por indução sobre r. No caso $r = 2$, para $x \in D_F\langle 1, -x_1\rangle \cap D_F\langle 1, -x_2\rangle$ temos que x_1, $x_2 \in D_F\langle 1, -x\rangle$, pelo **Lema 1.1.1**. Logo $x_1x_2 \in D_F\langle 1, -x\rangle$ e consequentemente $x \in D_F\langle 1, -x_1x_2\rangle$, mostrando assim a inclusão $D_F\langle 1, -x_1\rangle \cap D_F\langle 1, -x_2\rangle \subset D_F\langle 1, -x_1\rangle \cap D_F\langle 1, -x_1x_2\rangle$. Tomando $b = x_1x_2$ e usando a inclusão anterior temos que $D_F\langle 1, -x_1\rangle \cap D_F\langle 1, -b\rangle \subset D_F\langle 1, -x_1\rangle \cap D_F\langle 1, -x_1b\rangle$, que mostra a inclusão na outra direção e portanto a igualdade no caso $r = 2$.

Vamos assumir que a igualdade vale para $r = k$ e tomemos $x_1, \ldots, x_k, x_{k+1} \in F^\times$. Temos então por hipótese de indução que $D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_k\rangle = D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_{k-1}\rangle \cap D_F\langle 1, -x_1 \cdots x_k\rangle$. Logo

$$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_k\rangle \cap D_F\langle 1, -x_{k+1}\rangle =$$

$$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_{k-1}\rangle \cap D_F\langle 1, -x_1 \cdots x_k\rangle \cap D_F\langle 1, -x_{k+1}\rangle. \qquad (\dagger)$$

Aplicando-se o caso $r = 2$ nos dois últimos grupos do segundo membro da igualdade obtemos $D_F\langle 1, -x_1 \cdots x_k\rangle \cap D_F\langle 1, -x_{k+1}\rangle = D_F\langle 1, -x_1 \cdots x_k\rangle \cap D_F\langle 1, -x_1 \cdots x_k x_{k+1}\rangle$ e substituindo-se esta igualdade em (†) vamos obter

$$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_k\rangle \cap D_F\langle 1, -x_{k+1}\rangle =$$

$$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_{k-1}\rangle \cap D_F\langle 1, -x_1 \cdots x_k\rangle \cap D_F\langle 1, -x_1 \cdots x_k x_{k+1}\rangle.$$

Agora, usando novamente a hipótese de indução voltamos para

$$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_k\rangle \cap D_F\langle 1, -x_{k+1}\rangle =$$

$$D_F\langle 1, -x_1\rangle \cap \cdots \cap D_F\langle 1, -x_k\rangle \cap D_F\langle 1, -x_1 \cdots x_k x_{k+1}\rangle,$$

ficando assim demonstrada a primeira parte do lema.

(1) Seja $x = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} \in F^\times$, com $\varepsilon_1, \ldots, \varepsilon_r \in \{0, 1\}$. Pela primeira parte do lema obtemos a igualdade

$$D_F\langle 1, -x_1^{\varepsilon_1}\rangle \cap \cdots \cap D_F\langle 1, -x_{r-1}^{\varepsilon_{r-1}}\rangle \cap D_F\langle 1, -x\rangle = D_F\langle 1, -x_1^{\varepsilon_1}\rangle \cap \cdots \cap D_F\langle 1, -x_r^{\varepsilon_r}\rangle.$$

Consequentemente

$$\bigcap_{j=1}^{r} D_F\langle 1, -x_j\rangle \subset \bigcap_{x \in F^\times} D_F\langle 1, -x\rangle = R(F),$$

e como $R(F) \subseteq \bigcap_{j=1}^{r} D_F\langle 1, -x_j\rangle$ concluimos que $R(F) = \bigcap_{j=1}^{r} D_F\langle 1, -x_j\rangle$.

(2) É imediato, pois nesse caso $D_F\langle 1, -x_1 \cdots x_r\rangle = F^\times$. Também (3) é consequência imediata da primeira parte do lema. □

Proposição 3.2.3. *Sejam F um corpo e $\{a_1, \ldots a_n\} \subset F^\times$ uma base distinguida de F. Então as seguintes afirmações valem:*

1. $F^\times/R(F) \cong \prod_{j=1}^{n} F^\times/D_F\langle 1, -a_j\rangle$.
2. *Para todo subconjunto $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$ e para todo $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_m\}$ vale*
$$\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) D_F\langle 1, -a_j\rangle = F^\times.$$

Demonstração. 1. Note que pelo lema anterior temos que $R(F) = \bigcap_{j=1}^{n} D_F\langle 1, -a_j\rangle$ e então a projeção natural $F^\times \to \prod_{j=1}^{n} F^\times/D_F\langle 1, -a_j\rangle$ induz o homomorfismo $F^\times/R(F) \to \prod_{j=1}^{n} F^\times/D_F\langle 1, -a_j\rangle$ que será injetivo. Devido às condições da **Definição 3.2.1** os $\mathbb{F}_2$-espaços vetoriais tem a mesma dimensão e portanto são isomorfos.

2. Devido à condição (ii) da **Definição 3.2.1** basta demonstrarmos que qualquer que seja $j \in \{1, \ldots, n\} \smallsetminus \{i_1, \ldots, i_m\}$ temos $\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) \not\subset D_F\langle 1, -a_j\rangle$. Note porém que caso ocorresse $\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) \subset D_F\langle 1, -a_j\rangle$ obteríamos $R(F) = \bigcap_{\substack{1\le i\le n\\ i\neq j}} D_F\langle 1, -a_i\rangle$. Mas nesse caso teríamos homomorfismo injetivo $F^\times/R(F) \to \prod_{\substack{1\le i\le n\\ i\neq j}} F^\times/D_F\langle 1, -a_i\rangle$ induzido pela projeção natural. Mas isso implicaria $\dim_{\mathbb{F}_2}(F^\times/R(F)) \le n-1$, contradizendo o fato de $\{a_1R(F), \ldots, a_nR(F)\}$ ser uma base de $F^\times/R(F)$. □

Proposição 3.2.4. *Sejam F um corpo, $a_1, \ldots, a_n \in F^\times$, $e \in F^\times \smallsetminus (F^\times)^2$, e $K = F(\sqrt{e})$. Denotemos também por σ o gerador de $Gal(K/F)$ e assumimos que $|F^\times/R(F)| < \infty$.*

Consideremos as seguintes afirmações:

1. *Para todo subconjunto $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$ e para todo $j \in \{1, \ldots, n\} \smallsetminus \{i_1, \ldots, i_m\}$*
$$\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) D_F\langle 1, -a_j\rangle = F^\times.$$

2. *A projeção natural induz um isomorfismo*
$$F^\times/\left(\bigcap_{i=1}^{n} D_F\langle 1, -a_i\rangle\right) \cong \prod_{i=1}^{n} F^\times/D_F\langle 1, -a_i\rangle$$

3. *Para todo $I \subset \{1, \ldots, n\}$, não vazio, a projeção natural induz um isomorfismo*
$$F^\times/\left(\bigcap_{i\in I} D_F\langle 1, -a_i\rangle\right) \cong \prod_{i\in I} F^\times/D_F\langle 1, -a_i\rangle$$

4. *Considerando-se $a_1, \ldots, a_n \in K^\times$ e um subconjunto $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$, então*
$$\left(\bigcap_{t=1}^{m} F^\times D_K\langle 1, -a_{i_t}\rangle\right) = F^\times\left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right).$$

5. *Considerando-se $a_1, \ldots, a_n \in K^\times$ e um subconjunto $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$, então*
$$(F^\times)^2 N_{K|F}\left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right) = \left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) \cap \text{Im } N_{K/F}.$$

Convém observar que $\text{Im } N_{K/F} = D_F\langle 1, -e\rangle$.

6. *Considerando-se* $a_1, \ldots, a_n \in K^\times$ *e assumindo-se adicionalmente que*

$$\text{Im } N = \left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle \cap \text{Im } N\right)(D_F\langle 1, -a_j\rangle \cap \text{Im } N)$$

temos para todo subconjunto $\{ i_1, \ldots, i_m\} \subset \{ 1, \ldots, n \}$ *e todo* $j \in \{ 1, \ldots, n \} \smallsetminus \{ i_1, \ldots, i_m\}$

$$\left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right) D_K\langle 1, -a_j\rangle = K^\times.$$

7. *Com a mesma hipótese adicional do item anterior temos para todo* $I \subset \{ 1, \ldots, n \}$*, não vazio, que a projeção natural induz um isomorfismo*

$$K^\times / \left(\bigcap_{i\in I} D_K\langle 1, -a_i\rangle\right) \cong \prod_{i\in I} K^\times / D_K\langle 1, -a_i\rangle.$$

Nessas condições valem as seguintes afirmações: (1) implica (3); (3) implica (2); (1) implica (4); (4) implica (5). Temos também que (1) e (5) com a hipótese adicional implicam (6). Finalmente (6) implica (7) e assim (1) implica todas as outras afirmações menos (6) e (7) que dependem da hipótese adicional.

Demonstração. (1) $\Longrightarrow$ (3) Considere $I = \{ i_1, \ldots, i_k \}$ e note que a aplicação

$$F^\times / \left(\bigcap_{i\in I} D_F\langle 1, -a_i\rangle\right) \to \prod_{i\in I} F^\times / D_F\langle 1, -a_i\rangle$$

que associa a $x \in F^\times$ a k-upla $(xD_F\langle 1, -a_{i_1}\rangle, \ldots, xD_F\langle 1, -a_{i_k}\rangle)$ é um homomorfismo injetivo. Logo, para termos o isomorfismo só resta demonstrar que para $x_{i_1}, \ldots, x_{i_k} \in F^\times$ existe $y \in F^\times$ tal que $y^{-1}x_{i_t} \in D_F\langle 1, -a_{i_t}\rangle$, para todo $t = 1, \ldots, s$. Vamos verificar recursivamente sobre o número k de elementos de I, isto é, que para todo $I = \{ i_1, \ldots, i_k \}$, com $1 \leq k \leq n$, e toda k-upla $x_{i_1}, \ldots, x_{i_k}$ existe y tal que $y^{-1}x_{i_t} \in D_F\langle 1, -a_i\rangle$, para todo $t = 1, \ldots, k$.

Para $k = 1$, basta tomar $y = x_1$. Suponha, indutivamente, que para todo $k = 1, \ldots, m < n$ a afirmação está demonstrada e tome uma $(m+1)$-upla $x_{i_1}, \ldots, x_{i_m}, x_{i_{m+1}}$. Por hipótese de indução exite z tal que $z^{-1}x_{i_t} \in D_F\langle 1, -a_{i_t}\rangle$, para todo $t = 1, \ldots, m$. Por outro lado, usando (1) temos a igualdade

$$\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) D_F\langle 1, -a_{i_{m+1}}\rangle = F^\times,$$

e consequentemente existem u, $b \in \bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle$ e v, $c \in D_F\langle 1, -a_{i_{m+1}}\rangle$ tais que $z = uv$ e $x_{i_{m+1}} = bc$. Tomando $y = vb$ segue que

$$\begin{aligned} &y^{-1}x_{i_t} = z^{-1}b^{-1}ux_{i_t} = z^{-1}x_{i_t}(b^{-1}u) \in D_F\langle 1, -a_{i_t}\rangle, \quad \text{para todo } t = 1, \ldots, m \\ &\text{e } y^{-1}x_{i_{m+1}} = v^{-1}c \in D_F\langle 1, -a_{i_{m+1}}\rangle \end{aligned}$$

mostrando que $y^{-1}x_{i_t} \in D_F\langle 1, -a_{i_t}\rangle$, para todo $t = 1, \ldots, m+1$ como queríamos.

(3) $\Longrightarrow$ (2) Fazendo-se $k = n$ em (3) obtemos (2).

(1) $\Longrightarrow$ (4) Note que a inclusão $F^\times \left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right) \subset \left(\bigcap_{i=1}^{m} F^\times D_K\langle 1, -a_{i_t}\rangle\right)$ é claramente verdadeira. Vamos mostrar que a inclusão inversa também vale recursivamente, isto é, para todo $1 \leq k \leq n$ e todo $x \in \left(\bigcap_{t=1}^{k} F^\times D_K\langle 1, -a_{i_t}\rangle\right)$ mostraremos que existem $a \in F^\times$ e $y \in \left(\bigcap_{t=1}^{k} D_K\langle 1, -a_{i_t}\rangle\right)$ tais que $x = ay$.

Para $k = 1$ o resultado é direto. Suponha indutivamente que para todo $k = 1, \ldots, m < n$ a inclusão está demonstrada e tome $x \in \left(\bigcap_{t=1}^{m+1} F^\times D_K\langle 1, -a_{i_t}\rangle\right)$.

Por hipótese de indução existem $a \in F^\times$ e $y \in \left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right)$ tais que $x = ay$, e como $x \in F^\times D_K\langle 1, -a_{i_{m+1}}\rangle$, existem $b \in F^\times$ e $z \in D_K\langle 1, -a_{i_{m+1}}\rangle$ satisfazendo $x = bz$.

Por outro lado, como por (1) vale a igualdade

$$\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) D_F\langle 1, -a_{i_{m+1}}\rangle = F^\times,$$

existem $y_1,\, z_1 \in \bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle$ e $a_1,\, b_1 \in D_F\langle 1, -a_{i_{m+1}}\rangle$ tais que $a = a_1y_1$ e $b = b_1z_1$. Juntando as informações temos que $a_1y_1y = x = b_1z_1z$ e consequentemente

$$u = y_1yz_1^{-1} = a_1^{-1}b_1z \in \bigcap_{t=1}^{m+1} D_K\langle 1, -a_{i_t}\rangle.$$

Tomando em seguida $c = a_1z_1 \in F^\times$ podemos concluir que

$$x = cu \in F^\times \left(\bigcap_{t=1}^{m+1} D_K\langle 1, -a_{i_t}\rangle\right),$$

com queríamos. Logo, para $k = m + 1$ obtemos a que a inclusão inversa vale, completando a demonstração da igualdade.

(4) $\Longrightarrow$ (5) Denotaremos $N_{K|F}$ simplesmente por N. Pelo Princípio da Norma, **Teorema 1.1.9**,

$$N^{-1}\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) = \bigcap_{t=1}^{m} N^{-1}(D_F\langle 1, -a_{i_t}\rangle) = \bigcap_{t=1}^{m} F^\times D_K\langle 1, -a_{i_t}\rangle = F^\times \bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle,$$

onde a última igualdade decorre do item (4) anterior.

Logo

$$\left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) \cap \mathrm{Im}N = N\left(F^\times \bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right) = (F^\times)^2 N\left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right),$$

conforme afirmado.

(1), (5) e a hipótese adicional $\Longrightarrow$ (6) Para $z \in K^\times$, pela hipótese adicional temos que

$$N(z) \in \text{Im } N = \left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle \cap \text{Im } N\right)\left(D_F\langle 1, -a_j\rangle \cap \text{Im } N\right).$$

Pelo item (5) temos

$$(F^\times)^2 N\left(D_K\langle 1, -a_j\rangle\right) = D_F\langle 1, -a_j\rangle \cap \text{Im } N \quad \text{e}$$
$$(F^\times)^2 N\left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right) = \left(\bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle\right) \cap \text{Im } N.$$

Garantimos que existem $x_1 \in \bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle$, $x_2 \in D_K\langle 1, -a_j\rangle$ e $x_3 \in F^\times$ tais que $N(z) = x_3^2 N(x_1)N(x_2) = x_3^2 N(x_1x_2)$. Desta maniera, utilizando o **Teorema 1.1.4**, podemos garantir a existência de $u \in K^\times$ tal que $z = u(\sigma(u))^{-1}x_1x_2x_3^2 = N(u)(\sigma(u)^{-2})x_1x_2x_3^2$. Uma vez que vale (1) para o corpo F, temos que $N(u) = c_1c_2$ com $c_1 \in \bigcap_{t=1}^{m} D_F\langle 1, -a_{i_t}\rangle$ e $c_2 \in D_F\langle 1, -a_j\rangle$. Portanto, temos que

$$z = (c_1x_1)(c_2x_2\sigma(u)^{-2})x_3^2 \in \left(\bigcap_{t=1}^{m} D_K\langle 1, -a_{i_t}\rangle\right) D_K\langle 1, -a_j\rangle,$$

demonstrando (6).

(6) $\Longrightarrow$ (7) Como no caso do corpo F em (3), temos que a projeção natural induz homomorfismo injetivo

$$K^\times / \left(\bigcap_{i\in I} D_K\langle 1, -a_i\rangle\right) \to \prod_{i\in I} K^\times / D_K\langle 1, -a_i\rangle,$$

restando mostrar então a sobrejetividade.

Demonstraremos a sobrejetividade por indução sobre o número de elementos de $I = \{i_1, \ldots, i_k\}$. Se $k = 1$ então o resultado é claramente verdadeiro. Suponhamos que vale para todo I com $k < n$ elementos e seja I com $k + 1$ elementos. Fixe $j \in I$ e considere $J = \{i \in I \mid i \neq j\}$. Logo $I = J \cup \{\, j \,\}$.

Sejam agora $x_i \in K^\times$ para todo $i \in I$. Por hipótese de indução existe $y \in K^\times$ tal que $x_iy^{-1} \in D_K\langle 1, -a_i\rangle$, para todo $i \in J$.

Usando (6), temos que existem $u \in \bigcap_{i\in J} D_K\langle 1, -a_i\rangle$ e $v \in D_K\langle 1, -a_j\rangle$ tais que $x_j = uv$. Aplicando o mesmo argumento para y temos que existem $c \in \bigcap_{i\in J} D_K\langle 1, -a_i\rangle$ e $d \in D_K\langle 1, -a_j\rangle$ tais que $y = cd$. Para $x = du \in K^\times$, temos que

$$\begin{array}{l} x^{-1}x_i = d^{-1}u^{-1}c^{-1}cx_i = y^{-1}x_i(u^{-1}c) \in D_K\langle 1, -a_i\rangle \quad \text{para todo } i \neq j, \\ \text{e } x^{-1}x_j = d^{-1}u^{-1}uv = d^{-1}v \in D_F\langle 1, -a_j\rangle \end{array},$$

que mostra que $x^{-1}x_i \in D_K\langle 1, -a_i\rangle$, para todo $i \in I$, e consequentemente a sobrejetividade para I.

□

Corolário 3.2.5. *Sejam um corpo F e $a_1, \ldots, a_r \in F^\times$ tais que $\{ a_1R(F), \ldots, a_rR(F)\}$ é uma base de $F^\times/R(F)$ que satisfaz o item (1) da* ***Proposição 3.2.4****. Para $K = F(\sqrt{e})$, onde $e \in F^\times \setminus (F^\times)^2$ e*

$$R_o = \bigcap_{i=1}^{r} D_K\langle 1, -a_i\rangle,$$

tem-se que $(F^\times)^2 N(R_o) = R(F)$ e $N^{-1}(R(F)) = F^\times R_o$.

Demonstração. Pelo item (5) da **Proposição 3.2.4** temos que

$$(F^\times)^2 N(R_o) = \left(\bigcap_{i=1}^{r} D_F\langle 1, -a_i\rangle\right) \cap \text{Im } N.$$

Como, pelo item (2) do **Lemma 3.2.2** temos

$$R(F) = \bigcap_{i=1}^{r} D_F\langle 1, -a_i\rangle$$

e $R(F) \subset \text{Im } N = D_F\langle 1, -e\rangle$ a igualdade fica demonstrada.

Por outro lado, pelo pelo Princípio da Norma, **Teorema 1.1.9**, juntamente com item (4) da **Proposição 3.2.4** obtemos a segunda igualdade. □

Definição 3.2.6. *Seja $\{ a_1, \ldots, a_n \}$ uma base distinguida de F e sejam $b_1, \ldots, b_n \in F^\times$. Dizemos que $\{ b_1, \ldots, b_n \}$ é uma base dual de $\{ a_1, \ldots, a_n \}$ em F se para todo $1 \leq j \leq n$ tivermos $b_i \in D_F\langle 1, -a_j\rangle$, para todo $i \neq j$ e o conjunto $\{ b_1R(F), \ldots, b_{j-1}R(F), b_{j+1}R(F), \ldots, b_nR(F) \}$ for uma base de $D_F\langle 1, -a_j\rangle/R(F)$.*

Proposição 3.2.7. *Seja $\{ a_1, \ldots, a_n \}$ uma base distinguida de F. Então:*

1. *Existe base dual $\{ b_1, \ldots, b_n \}$ de $\{ a_1, \ldots, a_n \}$ em F.*
2. *Se $\{ b_1, \ldots, b_n \}$ é uma base dual de $\{ a_1, \ldots, a_n \}$ em F então $\{ b_1, \ldots, b_n \}$ também é uma base distinguida de F e $\{ a_1, \ldots, a_n \}$ é uma base dual de $\{ b_1, \ldots, b_n \}$ em F.*
3. *Para todo subconjunto $\{ i_1, \ldots, i_m\} \subset \{ 1, \ldots, n \}$ temos que $\{ b_jR(F) \mid j \notin \{ i_1, \ldots, i_m\} \}$ é uma base de $\left(D_F\langle 1, -a_{i_1}\rangle \cap D_F\langle 1, -a_{i_2}\rangle \cap \cdots \cap D_F\langle 1, -a_{i_m}\rangle\right)/R(F)$.*

Demonstração. Para cada $1 \leq j \leq n$ seja

$$S_j = \bigcap_{\substack{1 \leq i \leq n \\ i \neq j}} D_F\langle 1, -a_i\rangle.$$

Pelo item (2) da **Proposição 3.2.3** temos $S_jD_F\langle 1, -a_j\rangle = F^\times$. Pela construção de S_j e pelo **Lema 3.2.2** temos que $S_j \cap D_F\langle 1, -a_j\rangle = R(F)$. Portanto $(S_j : R(F)) = 2$. Seja $b_j \in S_j \setminus D_F\langle 1, -a_j\rangle$. Logo $S_j = R(F) \cup b_jR(F)$.

Vamos mostrar que $\{ b_1, \ldots, b_n \}$ é uma base dual de $\{ a_1, \ldots, a_n \}$ em F e é uma base distinguida de F. Além disso, $\{ a_1, \ldots, a_n \}$ é uma base dual de $\{ b_1, \ldots, b_n \}$ em F.

Observe que $b_j \in D_F\langle 1, -a_i\rangle$, para todo $i \neq j$, mas $b_j \notin D_F\langle 1, -a_j\rangle$. Logo $a_i \in D_F\langle 1, -b_j\rangle$, para todo $i \neq j$, mas $a_j \notin D_F\langle 1, -b_j\rangle$. Podemos então concluir que $D_F\langle 1, -b_j\rangle \neq F^\times$ e que $\dim_{\mathbb{F}_2}(D_F\langle 1, -b_j\rangle / R(F)) \geq n-1$. Concluímos então que:

• $(F^\times : D_F\langle 1, -b_j\rangle) = 2$, que é a condição (ii) da **Definição 3.2.1** para $\{ b_1, \ldots, b_n \}$ ser uma base distinguida de F, e que

• $\{ a_1R(F), \ldots, a_{j-1}R(F), a_{j+1}R(F), \ldots, a_nR(F) \}$ é uma base de $D_F\langle 1, -b_j\rangle / R(F)$, que é parte da condição para que $\{ a_1, \ldots, a_n \}$ seja uma base dual de $\{ b_1, \ldots, b_n \}$ em F, faltando mostrar ainda que $\{ b_1R(F), \ldots, b_nR(F)\}$ é uma base de $F^\times/R(F)$.

Note agora que pela construção dos conjuntos S_j temos que fixado um a_t, $S_j \subset D_F\langle 1, -a_t\rangle$ para todo $j \neq t$. Logo

• $b_j \in D_F\langle 1, -a_t\rangle$ para todo $j \neq t$ e consequentemente, caso o conjunto $\{ b_1R(F), \ldots, b_nR(F) \}$ seja uma base de $F^\times/R(F)$, podemos concluir que $\{ b_1R(F), \ldots, b_{j-1}R(F), b_{j+1}R(F), \ldots, b_nR(F) \}$ é uma base de $D_F\langle 1, -a_j\rangle / R(F)$. Isto é, uma vez demonstrado que $\{ b_1R(F), \ldots, b_nR(F)\}$ é uma base distinguida de $F^\times/R(F)$, então $\{ b_1, \ldots, b_n \}$ é uma base dual de $\{ a_1, \ldots, a_n \}$ em F.

• Por outro lado $b_t \notin D_F\langle 1, -a_t\rangle$, pela construção de b_t.

Vamos mostrar que $\{ b_1R(F), \ldots, b_nR(F) \}$ é uma base de $F^\times/R(F)$, isto é, a condição (i) da **Definição 3.2.1**. Suponha que $z = b_1^{\varepsilon_1} \cdots b_n^{\varepsilon_n}$ com $\varepsilon_1, \ldots, \varepsilon_r \in \{ 0, 1 \}$ é tal que $z \in R(F)$ e que existe $1 \leq j \leq n$ com $\varepsilon_j \neq 0$. Daí, temos que $z \in D_F\langle 1, -a_t\rangle$, para todo $t = 1, \ldots, n$, pois $z \in R(F)$ Como $z \in D_F\langle 1, -a_j\rangle$ e também $b_1 \ldots, b_{j-1}, b_{j+1}, \ldots, b_n \in D_F\langle 1, -a_j\rangle$, obtemos que $b_j \in D_F\langle 1, -a_j\rangle$, uma contradição. Logo $\varepsilon_j = 0$, para todo $j = 1, \ldots, n$, e assim $\{ b_1R(F), \ldots, b_nR(F) \}$ é um conjunto linearmente independente em $F^\times/R(F)$.

Portanto, temos que esse conjunto é uma base de $F^\times/R(F)$, completando a demonstração de que $\{ b_1, \ldots, b_n \}$ é uma base distinguida de F.

O último e o penúltimo pontos que foram destacados completam a demonstração dos itens *1.* e *2.*.

3. Devido a definição de base dual temos que $b_j \in D_F\langle 1, -a_{i_t}\rangle$ para todo $j \notin \{ i_1, \ldots, i_m \}$ e todo $t \in \{ 1, \ldots, m \}$. Temos então o conjunto $\{ b_jR(F) \mid j \notin \{ i_1, \ldots, i_m \} \}$ que é linearmente independente contido em $\left(D_F\langle 1, -a_{i_1}\rangle \cap D_F\langle 1, -a_{i_2}\rangle \cap \cdots \cap D_F\langle 1, -a_{i_m}\rangle\right)/R(F)$. Pelo item (3) da **Proposição 3.2.4** o $\mathbb{F}_2$-espaço vetorial $F^\times / \bigcap_{t=1}^m D_F\langle 1, -a_{i_t}\rangle$ tem dimensão m. Uma vez que $\dim_{\mathbb{F}_2} F^\times/R(F) = n$, temo que $\left(D_F\langle 1, -a_{i_1}\rangle \cap D_F\langle 1, -a_{i_t}\rangle D_F\langle 1, -a_{i_2}\rangle \cap \cdots \cap D_F\langle 1, -a_{i_m}\rangle\right)/R(F)$ tem dimensão $n-m$, que é o número de elementos do conjunto $\{ b_jR(F) \mid j \notin \{ i_1, \ldots, i_m \} \}$. Logo esse conjunto é uma base, conforme afirmado. □

Vamos a seguir introduzir alguns novos elementos com os quais poderemos ter uma visão mais clara dos subgrupos de ${}_2\mathrm{Br}(F)$, para um corpo F que tenha base distinguida. Recordemos antes que dado $d \in F^\times$ seja o subgrupo de ${}_2\mathrm{Br}(F)$, $Q_F(d) = \{ (d, x)_F \mid x \in F^\times \}$. Pela **Proposição 1.2.4** temos que cong $Q_F(d) \simeq F^\times/D_F\langle 1, -d\rangle$.

Definição 3.2.8. *Seja $\{ a_1, \ldots, a_n \}$ uma base distinguida de um corpo F. Consideremos a partição*

$$\{ 1, \ldots, n \} = \bigcup_{\lambda=1}^{m} I_\lambda \quad \textit{onde} \quad i, j \in I_\lambda \Longleftrightarrow Q_F(a_i) = Q_F(a_j).$$

Chamaremos tal partição de ***partição principal em*** F.
Ainda, para $1 \leq \lambda \leq m$ *introduzimos dois novos objetos, a saber:*

1. $F_\lambda = \langle \{ a_i \mid i \in I_\lambda \} \rangle R(F)$ *o subgrupo de* $F^\times$ *gerado por* $\{ a_i \mid i \in I_\lambda \}$ *e* $R(F)$.
2. $Q_F(\lambda) = Q_F(a_i)$, *para* $i \in I_\lambda$.

Observação 3.2.9. *Observe que a relação que aparece na partição principal é claramente uma relação de equivalência.*
Ainda, na definição de $Q_F(\lambda)$ *não importa o índice escolhido em* I_λ.

Lema 3.2.10. *Seja* F *um corpo e sejam* $x, y \in F^\times$ *tais que* $D_F\langle 1, -x\rangle = D_F\langle 1, -y\rangle$ *e* $Q_F(x) = Q_F(y)$. *Então* $xy \in R(F)$.

Demonstração. Temos que

$$Q_F(x) = Q_F(x) \cap Q_F(y) \cong D_F\langle 1, -xy\rangle / (D_F\langle 1, -x\rangle \cap D_F\langle 1, -y\rangle) = D_F\langle 1, -xy\rangle / D_F\langle 1, -x\rangle,$$

pela **Proposição 1.2.5**. Por outro lado, temos que $Q_F(x) \cong F^\times / D_F\langle 1, -x\rangle$, pela **Proposição 1.2.4**. Logo $F^\times = D_F\langle 1, -xy\rangle$ e $xy \in R(F)$. □

Teorema 3.2.11. *Tomemos um corpo* F *com base distinguida* $\{ a_1, \ldots, a_n \}$, *partição principal* I_λ, $1 \leq \lambda \leq m$, *e os subgrupos* F_λ *e* $Q_F(\lambda)$ *definidos acima. Então*

1. *para todo* $a \in F_\lambda \smallsetminus R(F)$ *temos que* $Q_F(a) = Q_F(\lambda)$. *Consequentemente para todo* $a \in F_\lambda \smallsetminus R(F)$, *temos que* $(F^\times : D_F\langle 1, -a\rangle) = 2$.
2. *dados* $x, y \in F^\times$ *tais que* $|Q_F(x)| = 2 = |Q_F(y)|$ *e* $Q_F(x) \neq Q_F(y)$, *temos que* $x \in D_F\langle 1, -y\rangle$ *(e igualmente* $y \in D_F\langle 1, -x\rangle$*). Consequentemente,*
   (a) *para* $1 \leq \gamma \neq \lambda \leq m$, *dados* $x \in F_\gamma$ *e* $y \in F_\lambda$ *temos que* $y \in D_F\langle 1, -x\rangle$. *Em particular,* $a_i \in D_F\langle 1, -x\rangle$ *para todo* $i \notin I_\gamma$, *e consequentemente* $F_\lambda \subseteq D_F\langle 1, -x\rangle$ *para todo* $\gamma \neq \lambda$.
   (b) *Para todo* $a \in F^\times$ *tal que* $|Q_F(a)| = 2$, *existe e é único* $1 \leq \lambda \leq m$ *tal que* $a \in F_\lambda$.
3. *Fixado* $1 \leq \gamma \leq m$, *temos que*
$$F_\gamma = \bigcap_{\substack{i \in I_\lambda \\ \lambda \neq \gamma}} D_F\langle 1, -a_i\rangle.$$
4. *Dados* $1 \leq \lambda_1, \ldots, \lambda_s \leq m$ *distintos e* $\lambda \notin \{ \lambda_1, \ldots, \lambda_s \}$, *então* $F_\lambda \cap (F_{\lambda_1} \oplus \cdots \oplus F_{\lambda_s}) = R(F)$, *onde a operação de composição é a multiplicação. Consequentemente*
$$F^\times / R(F) \cong F_1/R(F) \oplus \cdots \oplus F_m/R(F).$$
5. *Toda base distinguida de* F *induz a mesma partição* $Q_1, \ldots, Q_m$ *em* ${}_2\mathrm{Br}(F)$. *Isto é dada* $\{ e_1, \ldots, e_n \}$ *uma outra base distinguida de* F, *a partição induzida por essa base apenas permuta os elementos dos conjuntos* $\{ Q_F(1), \ldots, Q_F(m) \}$, *e* $\{ F_1, \ldots, F_m \}$.

Demonstração. 1. Seja $a = \prod_{i\in I_\lambda} a_i^{\varepsilon_i} \in F_\lambda \smallsetminus R(F)$, onde $\varepsilon_i \in \{\,0,1\,\}$, para todo $i \in I_\lambda$. Dado $d \in F^\times$, temos que

$$(d,a)_F \simeq \sum_{i\in I_\lambda} (d,a_i)_F^{\varepsilon_i} \in Q_F(\lambda),$$

porque $(d,a_i)_F \in Q_F(\lambda)$, para todo $i \in I_\lambda$. Como $a \notin R(F)$, temos $Q_F(a) = Q_F(\lambda)$, já não é um subgrupo trivial. Logo $|Q_F(a)| = 2$ implicando a segunda parte do item.

2. Suponhamos por absurdo que $x \notin D_F\langle 1,-y\rangle$. Nesse caso $(x,y)_F \neq 0 \in {}_2\mathrm{Br}(F)$. Mas $(x,y)_F \in Q_F(x)$, e igualmente, $(x,y)_F \in Q_F(y)$. Resulta disso a contradição $Q_F(x) = Q_F(y)$.

2.(a) Decorre imediatamente do item 1. e do que acabamos de provar, pois $Q_F(x) = Q_F(\lambda) \neq Q_F(\gamma) = Q_F(y)$.

2.(b) Dado $a \in F^\times$ nas condições do item 2.(b) se $Q_F(a) \neq Q_F(\lambda)$ para todo $1 \leq \lambda \leq m$, então pelo item 2. demonstrado, temos para todo $1 \leq \lambda \leq m$ e todo $i \in I_\lambda$, $a_i \in D_F\langle 1,-a\rangle$. Mas isso implica que $F^\times \subset D_F\langle 1,-a\rangle$, contradizendo a hipótese de que $|Q_F(a)| = 2$. Logo existe $1 \leq \lambda \leq m$ tal que $Q_F(a) = Q_F(\lambda)$.

Concluímos então que para todo $1 \leq \gamma \leq m$, com $\gamma \neq \lambda$, temos que $Q_F(a) \neq Q_F(\gamma)$. Logo, pelo item 2., $a_i \in D_F\langle 1,-a\rangle$, para todo $i \in I_\gamma$ com $\gamma \neq \lambda$.

Vamos em seguida escrever $a = a_1^{\varepsilon_1}\cdots a_n^{\varepsilon_n}$, com $\varepsilon_1,\ldots,\varepsilon_n \in \{\,0,\,1\,\}$. Tomando-se $d = a_1^{\mu_1}\cdots a_n^{\mu_n}$, onde $\mu_i = 0$ para todo $i \in I_\lambda$ e $\mu_i = \varepsilon_i$ para todo $i \in I_\gamma$ com $\gamma \neq \lambda$, resulta pela observação anterior que $d \in D_F\langle 1,-a\rangle$. Analogamente se $c = a_1^{\nu_1}\cdots a_n^{\nu_n}$, onde $\nu_i = \varepsilon_i$ para todo $i \in I_\lambda$ e $\nu_i = 0$ para todo $i \in I_\gamma$ com $\gamma \neq \lambda$, vamos obter $c \in F_\lambda$ satisfazendo $cd = a$, como queríamos.

4. É imediato pois $\bigcup_{\lambda=1}^m \{a_i R(F) \mid i \in I_\lambda\,\}$ é uma base de $F^\times/R(F)$.

5. Seja $\{\,1,\ldots,n\,\} = \bigcup_{\gamma=1}^s J_\gamma$, $\Gamma = \{\,1,\ldots,s\,\}$, e $F_\gamma^{'}$ gerado módulo $R(F)$ por $\{e_j \mid j \in J_\gamma\,\}$ com $\gamma \in \Gamma$, a partição associada a base $\{\,e_1,\ldots,e_n\,\}$. Decorre do item 2(b) anterior que para todo $1 \leq i \leq n$ existe um único $1 \leq \lambda \leq m$ tal que $e_i \in F_\lambda$ e portanto $Q_F(e_i) = Q_F(\lambda)$. Seja $1 \leq \gamma \leq s$ tal que $i \in J_\gamma$. Para todo $j \in J_\gamma$ temos que $Q_F(e_j) = Q_F(e_i) = Q_F(\lambda)$. Logo $e_j \in F_\lambda$ para todo $j \in J_\gamma$ e assim $F_\gamma^{'} \subset F_\lambda$.

Por simetria, já que temos duas bases distinguidas, existe um único $\delta \in \Gamma$ tal que $F_\lambda \subset F_\delta^{'}$. Logo $F_\lambda^{'} \subset F_\delta^{'}$, implicando $\delta = \gamma$ (se $\delta \neq \gamma$, $F_\gamma^{'} \cap F_\delta^{'} = R(F)$). Dessa forma $F_\gamma^{'} = F_\lambda$ e temos uma correspondência injetiva $\Gamma \to \Lambda$ dada por $\gamma \mapsto \lambda$ tal que $F_\gamma^{'} = F_\lambda$. Assim $s \leq m$ e novamente por simetria vamos concluir que $m \leq s$, i.e., $s = m$ e a aplicação acima é uma bijeção.

Concluímos assim que uma troca de bases distinguidas apenas produz uma permutação nos conjuntos $\{\,Q_F(1),\ldots,Q_F(m)\,\}$, $\{\,F_1,\ldots,F_m\,\}$.

□

Observação 3.2.12. *Com as hipóteses e notações do* ***Teorema 3.2.11*** *vemos que dado $c \in F^\times$ temos uma representação $c = \prod_{i\in I} c_i$, onde $I \subset \Lambda$, $c_i \in F_i$, e $c_i \notin R(F)$, para todo $i \in I$.*

Relembramos que Λ representa o conjunto de índices na partição principal. Mais ainda, pelo item (4) desse teorema essa representação é única. Isto é, caso $c = \prod_{j\in J} c'_j$, com $J \subset \Lambda$ e $c'_j \in F_j$ para todo $j \in J$, então $J = I$ e $c'_i \in c_i R(F)$, para todo $i \in I = J$.

Definição 3.2.13. *Sejam $\{ a_1, \ldots, a_n \}$ uma base distinguida de um corpo F e $\{ 1, \ldots, n \} = \bigcup_{\lambda=1}^{m} I_\lambda$ sua partição principal. Dizemos que $\{ a_1, \ldots, a_n \}$ é* ***completa*** *$|{}_2\mathrm{Br}(F)| = 2^m$.*

Teorema 3.2.14. *Sejam F um corpo com base distinguida $\{ a_1, \ldots, a_n \}$ e base dual $\{ b_1, \ldots, b_n \}$, partição principal I_λ, $1 \leq \lambda \leq m$ e os subgrupos F_λ e $Q_F(\lambda)$ como na* ***Definição 3.2.8****.*

Se a base $\{ a_1, \ldots, a_n \}$ é ***completa****, então para todo subconjunto $J \subset \{ 1, \ldots, m \}$ e $k \in \{ 1, \ldots, m \} \smallsetminus J$ temos $Q_F(k) \cap \left(\sum_{j\in J} Q_F(j) \right) = \{ 0 \}$. Concluimos assim que para todo subconjunto $J \subset \{ 1, \ldots, m \}$ temos que*

$$\sum_{j\in J} Q_F(j) = \bigoplus Q_F(j) \text{ e em particular } {}_2\mathrm{Br}(F) = Q_F(1) \oplus \cdots \oplus Q_F(m).$$

Mais ainda, seja $J \subset \{ 1, \ldots, m \}$ um subconjunto não vazio com t elementos e tomemos $c_j \in F_j / R(F)$, para cada $j \in J$. Para

$$c = \prod_{j\in J} c_j \text{ temos que } D_F\langle 1, -c \rangle = \bigcap_{j\in J} D_F\langle 1, -c_j \rangle,\ Q_F(c) = \bigoplus_{j\in J} Q_F(j),$$

e $(F^\times : D_F\langle 1, -c \rangle) = 2^t$.

Demonstração. Observemos inicialmente que dados $x, y \in F^\times$ se escrevermos $x = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} u$ e $y = b_1^{\eta_1} \cdots b_n^{\eta_n} v$, com $\varepsilon_1, \ldots, \varepsilon_n, \eta_1, \ldots, \eta_n \in \{ 0, 1 \}$ e $u, v \in R(F)$, temos que em ${}_2Br(F)$

$$(x, y)_F = \sum_{1\leq i,j\leq n} (a_i, b_j)_F^{\varepsilon_i \eta_j} = \sum_{1\leq k\leq n} (a_k, b_k)_F^{\varepsilon_k \eta_k} \in \sum_{\lambda=1}^{m} Q_F(\lambda),$$

pois pelo ítem 2. do **Teorema 3.2.11** $(a_k, b_j)_F = 0$, para todo $j \neq k$. Note que se $k, k' \in I_\lambda$ temos $(a_k, b_k)_F \simeq (a_{k'}, b_{k'})_F$, isto é, a soma acima pode ser nula mesmo com $\varepsilon_k, \eta_k \neq 0$. Usando o Teorema de Merkurjev, que garante que todo elemento de ${}_2\mathrm{Br}(F)$ é uma soma de classes de álgebras de quatérnios, podemos concluir que

$${}_2\mathrm{Br}(F) = \sum_{\lambda=1}^{m} Q_F(\lambda)$$

Suponhamos agora que exista $k \in \{ 1, \ldots, m \} \smallsetminus J$, para algum $J \subset \{ 1, \ldots, m \}$ tal que $Q_F(k) \subset \sum_{j\in J} Q_F(j)$. Logo

$$\sum_{\lambda=1}^{m} Q_F(\lambda) = \sum_{\substack{1\leq\lambda\leq m \\ \lambda\neq k}} Q_F(\lambda).$$

Por outro lado, como os grupos envolvidos são todos abelianos, temos que

$$\left| \sum_{\substack{1\leq\lambda\leq m\\ \lambda\neq k}} Q_F(\lambda) \right| \leq \prod_{\substack{1\leq\lambda\leq m\\ \lambda\neq k}} |Q_F(\lambda)| < 2^m.$$

Mas isso contradiz a hipótese de que $|_2\mathrm{Br}(F)| = 2^m$, pois a base é completa.. Logo, para todo subconjunto $J \subset \{\,1,\ldots,m\,\}$ e $k \in \{\,1,\ldots,m\,\} \smallsetminus J$ temos $Q_F(k) \cap \left(\sum_{j\in J} Q_F(j)\right) = \{\,0\,\}$, que completa a demonstração da primeira afirmação do teorema.

A segunda afirmação decorre da primeira pois dado $J \subset \{\,1,\ldots,m\,\}$ e tomando $J_k = \{\,j \in J \mid j \neq k\,\}$, temos

$$Q_F(k) \cap \left(\sum_{\substack{j\in J\\ j\neq k}} Q_F(j) \right) = \{\,0\,\},$$

para todo $k \in J$, que é a condição para que a soma de subgrupos $\sum_{j\in J} Q_F(j)$ seja uma soma direta.

Finalmente, por 1. do **Teorema 3.2.11** temos que $Q_F(c_j) = Q_F(j)$, para cada $j \in J$ e consequentemente $(c,x)_F \simeq \sum_{j\in J}(c_j,x)_F \in \bigoplus_{j\in J} Q_F(j)$, para todo $x \in F^\times$. Logo $Q_F(c) \subset \bigoplus_{j\in J} Q_F(j)$.

Para verificarmos a outra inclusão observemos que para cada $j \in J$ temos que $a_{i(j)} \notin D_F\langle 1,-c_j\rangle$ para algum $i(j) \in \{\,1,\ldots,n\,\}$, pois $\{\,a_1R(F),\ldots,a_nR(F)\,\}$ é uma base de $F^\times/R(F)$ e pelo ítem 1. do **Teorema 3.2.11** temos que $(F^\times : D_F\langle 1,-c_j\rangle) = 2$. Daí, podemos concluir que $(c_j,a_{i(j)})_F \neq 0 \in {}_2Br(F)$ implicando que $Q_F(j) = Q_F(c_j) = Q_F(a_{i(j)})$, uma vez que $2 = |Q_F(c_j)| = |Q_F(a_{i(j)})|$. Portanto $a_{i(j)} \in F_j$, pois a última igualdade significa que $i(j) \in I_j$, conforme a definição de partição principal.

Por outro lado, pelo item 2. (a) do **Teorema 3.2.11**, temos que $a_{i(j)} \in D_F\langle 1,-c_s\rangle$, para todo $s \in J$ e $s \neq j$ $(i(j) \notin I_s)$. Logo $(c_s,a_{i(j)})_F = 0 \in {}_2Br(F)$ para todo $s \in J$ e $s \neq j$ e $(c_j,a_{i(j)})_F \simeq (c,a_{i(j)})_F$, implicando em $Q_F(c_j) \subset Q_F(c)$ para todo $j \in J$, que mostra a inclusão contrária conforme desejado.

A igualdade $Q_F(c) = \bigoplus_{j\in J} Q_F(j)$ acarreta em $(F^\times : D_F\langle 1,-c\rangle) = |Q_F(c)| = 2^t$. Para terminar a demonstração do teorema verificaremos por indução sobre $t = |J|$ que

$$D_F\langle 1,-c\rangle = \bigcap_{j\in J} D_F\langle 1,-c_j\rangle.$$

Para $t = 2$ e $J = \{\,\lambda,\gamma\,\}$ sabemos que $Q_F(c_\lambda) \cap Q_F(c_\gamma) = \{\,0\,\}$. Pela **Proposição 1.2.5** temos o isomorfismo de grupos $Q_F(c_\lambda) \cap Q_F(c_\gamma) \cong D_F\langle 1,-c_\lambda c_\gamma\rangle/(D_F\langle 1,-c_\lambda\rangle \cap D_F\langle 1,-c_\gamma\rangle)$ Logo $D_F\langle 1,-c_\lambda c_\gamma\rangle = D_F\langle 1,-c_\lambda\rangle \cap D_F\langle 1,-c_\gamma\rangle$ como queríamos.

Suponhamos que seja verdadeira para todo $k < t$. Fixemos $i \in J$ e sejam $J' = J \smallsetminus \{\,i\,\}$ e $c' = \prod_{j\in J'} c_j$. Por hipótese de indução temos que

$$D_F\langle 1,-c'\rangle = \bigcap_{j\in J'} D_F\langle 1,-c_j\rangle.$$

Por outro lado, conforme demonstrado acima temos que

$$(F^\times : D_F\langle 1, -c'\rangle) = 2^{t-1} \qquad \text{e} \qquad Q_F(c') = \bigoplus_{j\in J'} Q_F(j).$$

Ainda, $Q_F(c_i) \cap \bigoplus_{j\in J'} Q_F(j) = \{\,0\,\}$, pois $i \notin J'$. Portanto $Q_F(c') \cap Q_F(c_i) = \{\,0\,\}$ implicando que $D_F\langle 1, -c'\rangle \cap D_F\langle 1, -c_i\rangle = D_F\langle 1, -c'c_i\rangle$. Como $c = c'c_i$ decorre da hipótese de indução que

$$D_F\langle 1, -c\rangle = \bigcap_{j\in J} D_F\langle 1, -c_j\rangle,$$

conforme afirmado. □

Observação: Tomando-se $J \subset \{\,1, \ldots, m\,\}$ com $t \neq 0$ elementos e duas famílias c_j, $c_j^{'} \in F_j$, para cada $j \in J$, se definirmos

$$c = \prod_{j\in J} c_j \;\text{ e }\; c^{'} = \prod_{j\in J} c_j^{'}$$

vamos obter pelo **Teorema 3.2.14** acima que $Q_F(c) = Q_F(c^{'})$. Valerá também

$$D_F\langle 1, -c\rangle = \bigcap_{j\in J} D_F\langle 1, -c_j\rangle \qquad D_F\langle 1, -c^{'}\rangle = \bigcap_{j\in J} D_F\langle 1, -c_j^{'}\rangle,$$

mas não podemos dizer que $D_F\langle 1, -c\rangle = D_F\langle 1, -c^{'}\rangle$ e assim concluir que $c^{-1}c^{'} \in R(F)$, pelo **Lema 3.2.10**.

Teorema 3.2.15. *Sejam F um corpo, $e \in F^\times \smallsetminus (F^\times)^2$ e $K = F(\sqrt{e})$. Considere também σ o gerador de $Gal(K/F)$ e também* $\mathrm{Res} : {}_2\mathrm{Br}(F) \to {}_2\mathrm{Br}(K)$ *a função restrição.*

Dados x, $y \in K^\times$, se $(x, y)_K \in$ Im Res, então existe $c \in F^\times$ tal que $(x, y)_K \cong (x, c)_K$. Isto é, dados x, $y \in K^\times$ se existem a, $b \in F^\times$ tais que $(x, y)_K \cong (a, b)_K$, então existe $c \in F^\times$ tal que $(x, y)_K \cong (x, c)_K$.

Demonstração. Do isomorfismo entre álgebras $(x, y)_K \cong (a, b)_K$ obtemos a isometria entre formas quadráticas:

$$\langle 1, -x, -y, xy\rangle \simeq \langle 1, -a, -b, ab\rangle. \qquad (\dagger)$$

Vamos usar duas funções transfer de Scharlau, como no **Corolário 1.1.7**, s^* e s_y, onde $y = \alpha + \beta\sqrt{e}$. Pelo **Corolário 1.1.7** temos que $y_y^* \circ < k >= s_*$, onde $k = -y/N(y)$.

Da isometria em (†) temos que $s^*(\langle 1, -x, -y, xy\rangle) = 0 \in W(F)$. Logo $s_y^*(\langle k\rangle\langle 1, -x, -y, xy\rangle) = 0 \in W(F)$. Mas $-y \in D_K\langle 1, -x, -y, xy\rangle$, e como $D_K\langle 1, -x, -y, xy\rangle = D_K\langle 1, -a, -b, ab\rangle$ vamos ter que $\sigma\,(D_K\langle 1, -x, -y, xy\rangle) = D_K\langle 1, -x, -y, xy\rangle$. Portanto $\sigma(-y) \in D_K\langle 1, -x, -y, xy\rangle$ e assim $N(y) = (-y)\sigma(-y) \in D_K\langle 1, -x, -y, xy\rangle$, também. Finalmente $k \in D_K\langle 1, -x, -y, xy\rangle$. Podemos então concluir que $\langle k\rangle\langle 1, -x, -y, xy\rangle \simeq \langle 1, -x, -y, xy\rangle$. Portanto $s_y^*(\langle 1, -x, -y, xy\rangle) = 0 \in W(F)$. Temos então que

$$0 = s_y^*(\langle 1, -x\rangle) - s_y^*(\langle y\rangle) + s_y^*(\langle xy\rangle) \in W(F).$$

Fazendo-se os cálculos obtemos $s_y^*\langle y\rangle = \langle\gamma\rangle\langle 1, -N(y^2)\rangle = 0 \in W(F)$ e $s_y^*\langle xy\rangle = \langle\delta\rangle\langle 1, -N(xy^2)\rangle = \langle\delta\rangle\langle 1, -N(x)\rangle \in W(F)$, para apropriados γ, $\delta \in F^\times$. E desta maneira podemos concluir que $s_y^*(\langle 1, -x\rangle) = \langle\delta\rangle\langle 1, -N(x)\rangle \in W(F)$. Como $s_y^*(\langle 1, -x\rangle)$ tem dimensão 4, essa última igualdade mostra que $s_y^*(\langle 1, -x\rangle)$ é isotrópica em $W(F)$. Como consequência obtemos que $y \in F^\times D_K\langle 1, -x\rangle$. Sejam $c \in F^\times$ e $z \in D_K\langle 1, -x\rangle$ tais que $y = cz$. Substituindo-se esse valor de y na álgebra obtemos $(x, y)_K \cong (x, cz)_K \cong (x, c)_K$, como queríamos. □

Vamos a seguir usar o resultado anterior para determinar a parte fixa de um subgrupo $Q_K(z)$, onde $z \in K = F(\sqrt{e})$.

Lema 3.2.16. *Sejam F um corpo tal que* $\mathrm{Cor} : H^2(K) \to H^2(F)$ *é sobrejetiva onde $K = F(\sqrt{a})$ com $a \in F^\times \smallsetminus (F^\times)^2$. Denotemos $G = \mathrm{Gal}(K; F)$, o grupo de Galois da extensão, e seja σ o gerador de G. Então*

$$\mathrm{Im\ Res} = \mathrm{kernel\ Cor} = (\sigma - 1)H^2(K) \subset H^2(F)^G,$$

para $\mathrm{Res} : H^2(F) \to H^2(K)$. *Recordando que $H^2(F) \cong {}_2\mathrm{Br}(F)$, temos para o homomorfismo $\chi_a \cup \_ : H^1(F) \to H^2(F)$ que* $\mathrm{Im}\ \chi_a \cup \_ = Q_F(a)$ *que*

$$\mathrm{kernel\ Res} = \mathrm{Im}\ \chi_a \cup \_ = Q_F(a) \cong H^2(K)^G/(\sigma - 1)H^2(K).$$

Conclusão $\mathrm{Cor}({}_2\mathrm{Br}(K)) = {}_2\mathrm{Br}(F)$ *e* $\mathrm{Cor}({}_2\mathrm{Br}(K)^G) = Q_F(a)$.

Observemos que $\mathrm{Im\ Res} = H^2(K)^G$ *se e somente se $a \in R(F)$ e nesse caso* Res *é injetiva pois $Q_F(a) = \{0\}$.*

Demonstração. A igualdade kernel Cor = Im Res decorre da sequência exata de Arason, [**A**]. Já a igualdade kernel Cor $= (\sigma - 1)H^2(K)$ é o Corolário da Proposição 2 de [**LLMS**]. Aplicando-se agora [**LLMS**], para $p = 2$, obtemos $(\sigma - 1)H^2(K) \subset H^2(K)^G$. Finalmente, decorre da ação de G sobre $H^2(K)$ que Im Res $\subset H^2(K)^G$. Juntando-se tudo, concluímos a primeira afirmação do teorema.

A igualdade kernel Res = Im $\chi_a \cup \_$ decorre de [**A**]. O isomorfismo $Q_F(a) \cong H^2(K)^G/(\sigma - 1)H^2(K)$ é consequência direta de [**LLMS**].

Para a última afirmação do teorema observemos que $Q_F(a) = 0$ se e somente se $a \in R(F)$. A segunda afirmação implica que $H^2(K)^G \subset$ kernel Cor se e somente se $Q_F(a) = 0$. Juntando-se esses dois fatos com a primeira conclusão obtemos o resultado. □

Teorema 3.2.17. *Sejam F um corpo, $e \in F^\times \smallsetminus (F^\times)^2$ e $K = F(\sqrt{e})$. Considere também σ o gerador de $Gal(K/F)$ e assuma que* $\mathrm{Cor} : H^2(K) \to H^2(F)$ *é sobrejetiva.*

Para cada $z \in K^\times$ consideremos o homomorfismo

$$\theta : K^\times \longrightarrow Q_K(z) \subset {}_2\mathrm{Br}(K)$$

dado por $\theta(x) = (x, z)_K$ que induz isomorfismo

$$\overline{\theta} : K^\times/D_K\langle 1, -z\rangle \to Q_K(z).$$

1. *A restrição de θ a $D_K\langle 1, -N(z)\rangle \cap F^\times$ induz isomorfismo*

$$D_K\langle 1, -N(z)\rangle \cap F^\times/(D_K\langle 1, -z\rangle \cap F) \longrightarrow Q_K(z) \cap {}_2\mathrm{Br}(K)^G. \qquad (*)$$

2. *$Q_K(z) \cap {}_2\mathrm{Br}(K)^G = \{0\}$ implica $Q_K(z) \cap Q_K(\sigma(z)) = \{0\}$.*

Demonstração. (1) Para $a \in D_F\langle 1, -N(z)\rangle$ temos que $(a, N(z))_F = 0 \in {}_2\mathrm{Br}(F)$. Decorre de $\mathrm{Cor}((a,z)_K) = (a, N(z))_F$ que $(a,z)_K \in \ker(\mathrm{Cor}) = \mathrm{Im}\,\mathrm{Res}$, conforme **Teorema 3.2.16**.

Vemos então que a restrição de θ a $D_F\langle 1, -N(z)\rangle$ tem imagem dentro de $Q_K(z) \cap \mathrm{Im}\,\mathrm{Res}$. Como o núcleo dessa restrição será $D_K\langle 1, -z\rangle \cap F$ obtemos injetividade para a flecha $(*)$.

Seja agora $y \in K^\times$ tal que $(y,z)_K \in \mathrm{Im}\,\mathrm{Res}$. Teremos então $(y,z)_K \cong (a,b)_K$, para apropriados $a, b \in F^\times$. Logo, pelo **Teorema 3.2.15** existe $c \in F^\times$ tal que $(y,z)_K \cong (c,z)_K$. Pelo **Teorema 3.2.16** temos que $0 = \mathrm{Cor}((c,z)_K) \simeq (c, N(z))_K$. Mas então $c \in D_F\langle 1, -N(z)\rangle$ e como $\theta(c) = (c,z)_K \simeq (y,z)_K$ obtemos a sobrejetividade, completando a demonstração.

(2) Sejam $x, y \in K$ tais que $(x,z)_K \cong (y, \sigma(z))_K \in Q_K(z) \cap Q_K(\sigma(z))$. Pelo **Teorema 1.2.2**, existe $u \in K$ tal que $\cong (x,z)_K$ e $(u, \sigma(z))_K \cong (y, \sigma(z))_K$. Mas $(u,z)_K \cong (u, \sigma(z))_K$ (♣) implica $(u, N(z))_K = 0 \in {}_2\mathrm{Br}(K)$. Resulta então que $u \in D_K\langle 1, -N(z)\rangle$. Logo, pelo Princípio da Norma, **Teorema 1.1.9**, $N(u) \in D_F\langle 1, -N(z)\rangle$.

Por outro lado, a hipótese $Q_K(z) \cap {}_2\mathrm{Br}(K)^G = \{0\}$ implica $Q_K(z) \cap \mathrm{Im}\,\mathrm{Res} = \{0\}$. Logo, o item (1), aplicado a $\sigma(z)$, implica que $D_F\langle 1, -N(z)\rangle = D_K\langle 1, -\sigma(z)\rangle \cap F^\times$ (Claro que o item (1) deve valer tando para z como para $\sigma(z)$.). Logo $u\sigma(u) = N(u) \in D_K\langle 1, -\sigma(z)\rangle$ e portanto $(u, \sigma(z))_K \cong (\sigma(u), \sigma(z))_K$ (♠).

Juntando (♣) com (♠) vamos obter $(u,z)_K \cong (\sigma(u), \sigma z)_K \cong (u,z)_K^\sigma$. Logo

$$(x,z)_K \simeq (u,z)_K^\sigma \in Q_K(z) \cap {}_2\mathrm{Br}(K)^G = \{0\}$$

o que nos permite concluir que $Q_K(z) \cap Q_K(\sigma(z)) = \{0\}$, como queríamos. □

3.2.1 Teorema 90 de Hilbert para extensões radicais

Como mencionado no **Capítulo 2**, vamos demonstrar o Teorema 90 de Hilbert, versão radical de Kaplansky, para extensões quadráticas radicais de corpos com base distinguida.

Apresentaremos inicialmente a versão aritmética para um extensão $K = F(\sqrt{r})$, onde $r \in F^\times \setminus R(F)$. Algumas versões dete resultado podem ser encontradas na literatura, citamos especialemente as versões dos trabalhos dos trabalhos [**CR**] e [**KN**].

1. Em [**CR**], Cordes e Ramsey mostraram a validade somente no caso em que F é um corpo com duas álgebras de quatérnios, a menos de isomorfismo, isto é, $\dim_{\mathbb{F}_2} {}_2Br(F) = 1$.

2. A versão apresentada em [**KN**] vale somente se F é tal que o índice de $R(F)$ em $F^\times$ é 2.

Mas podemos observar que nos casos acima, os corpos F são corpos com base distinguida como já visto no decorrer do trabalho. E então, o resultado que apresenteremos a seguir engloba os resultados já existentes.

Teorema 3.2.18 (Teorema 90 de Hilbert)**.** *Se F é corpo com base distinguida e K uma extensão radical de F, então $N^{-1}(R(F)) = F^{\times}R(K)$.*

Demonstração. Considere $\{a_1, \ldots, a_n\}$ uma base distinguida de F. Pelo **Teorema 2.2.4** temos que

$$R(K) = \bigcap_{c \in F^{\times}} D_K\langle 1, -c\rangle.$$

Denotando por $\{a_1, \ldots, a_n\}$ a base ditinguida de F temos que $R(K) = \bigcap_{i=1}^{n} D_K\langle 1, -a_i\rangle$. Portanto, o resultado segue diretamente do **Colorolário 2.2.4.** □

Vejamos uma primeira consequência do Teorema 90 de Hilbert.

Corolário 3.2.19. *Se K é uma extensão quadrática radical de um corpo F com base distinguida, então*

$$\dim_{\mathbb{F}_2} K^{\times}/R(K) = 2\dim_{\mathbb{F}_2} F^{\times}/R(F).$$

Demonstração. Considere a seguinte sequência exata, extraída da demonstração do teorema acima

$$1 \to N^{-1}(R(F))/R(K) \to K^{\times}/R(K) \to F^{\times}/R(F) \to 1.$$

Pelo teorema acima $N^{-1}(R(F)) = F^{\times}R(K)$ e portanto a $N^{-1}(R(F))/R(K) = F^{\times}R(K)/R(K)$. Mas, pelo Teorema do Isomorfismo, $F^{\times}R(K)/R(K) \cong F^{\times}/(F^{\times} \cap R(K))$ e usando o **Corolário 2.1.9** concluimos que $N^{-1}(R(F))/R(K) \simeq F^{\times}/R(F)$. Portanto, a sequência acima e equivalente a

$$1 \to F^{\times}/R(F) \to K^{\times}/R(K) \to F^{\times}/R(F) \to 1$$

e o resultado segue. □

O próximo resultado que apresentaremos é a versão clássica do Teorema 90 de Hilbert, para o radical de Kaplansky. E para a demonstração precisamos da construção dos grupos de cohomologia, $H^n(F)$.

Seja G um grupo pro-finito. Dizemos que A é um *$G-$módulo discreto*, ou simplesmente um $G-$módulo, se A é um grupo e existe uma aplicação contínua

$$\varphi : G \times A \longrightarrow A$$

satisgazendo:

(i) $\varphi(\sigma\tau, a) = \sigma\varphi(\tau, a)$;

(ii) $\varphi(\sigma, a + b) = \varphi(\sigma, a) + \varphi(\sigma, b)$;

(iii) $\varphi(1_G, a) = a$,

para todos $\sigma, \tau \in G$ e $a \in A$. Denotaremos $\varphi(\sigma, a)$ simplesmente por σ_a.

Exemplo 3.2.20.

(1) Seja G um grupo pro-finito qualquer e A um grupo abeliano. Defina a ação $\sigma_a = a$ para todos $a \in A$ e $\sigma \in G$. Então A é um $G-$módulo, chamado de módulo trivial e a ação é chamada de ação trivial.

(2) Seja N/F uma extensão galoisiana de corpos e seja $G = Gal(N/F)$, o grupo de galois da extensão. Se definirmos para $\sigma \in G$ e $x \in L$ a ação $\sigma_x = \sigma(x)$, temos os seguintes exemplos de $G-$módulos:

   (a) $N^\times$, o grupo multiplicativo do corpo N,

   (b) $(N^\times)^2$, as classes de quadrados de N,

   (c) $R(N)$, o radical de Kaplansky do corpo N.

Sejam A e B $G-$módulos discretos. Um $G-$homomorfismo $\phi : A \longrightarrow B$, é um homomorfismo de grupos abelianos tal que

$$\phi(\sigma_a) = \sigma_{\phi(a)},$$

para todo $a \in A$. Denotaremos por $Mod(G)$ a classe dos $G-$modulos e $G-$homorfismos.

Considere agora G um grupo pro-finito e denote por G^q o produto cartesiano de q cópias de G. Para $A \in Mod(G)$, defina

$$\bar{C}^q(G, A) = \{x : G^q \longrightarrow A \setminus x \text{ contínuo}\},$$

chamado grupo das cadeias não homegêneas.

Para os seguintes homomorfismos

$$\bar{\delta}_{q+1} : \bar{C}^q(G, A) \longrightarrow \bar{C}^{q+1}(G, A),$$

dado por:

$$\begin{aligned}(\bar{\delta}_{q+1}x)(\sigma_1, \sigma_2, \ldots, \sigma_{q+1}) = \quad & \sigma_1 x(\sigma_2, \ldots, \sigma_{q+1}) + \sum_{i=1}^{q}(-1)^i x(\sigma_1, \sigma_2, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{q+1}) \\ & +(-1)^{q+1}x(\sigma_1, \sigma_2, \ldots, \sigma_q).\end{aligned}$$

temos o seguinte complexo de co-cadeias:

$$0 \longrightarrow \bar{C}^0(G, A) \xrightarrow{\bar{\delta}_1} \bar{C}^1(G, A) \xrightarrow{\bar{\delta}_2} \bar{C}^2(G, A) \longrightarrow \cdots$$

Por definição temos que o $q-$ésimo grupo de cohomologia de G com coeficientes em A é o grupo quociente

$$H^q(G, A) = \bar{Z}^q(G, A)/\bar{B}^q(G, A),$$

onde $\bar{Z}^q(G, A) = \ker \bar{\delta}_{q+1}$, que é chamado de *grupo dos co-ciclos* e $\bar{B}^q(G, A) = \operatorname{Im} \bar{\delta}_q$, é chamado *grupo dos co-bordos.*

Para maiores detalhes indicamos [**NSW**].

Observação 3.2.21. *Sejam N/F uma extensão galoisisana de F e $G = Gal(N/F)$ o grupo de Galois da extensão N/F. Sabemos que*

$$G = \varprojlim_{L/F} Gal(L/F),$$

onde L/F percorre todas as subextensões normais e finitas de N/F. Além disso, os grupos quocientes $Gal(N/L)$ formam uma base para a topologia de G, contendo a identidade.

Seja agora $A \in Mod(G)$ e denote por $A_L = A^{Gal(N/L)}$, o subgrupo fixo por $Gal(N/L)$, onde L/F é uma subextensão finita de N/F. Daí, temos que

$$A = \varinjlim_{L/F} A_L.$$

Consequentemente, temos que

$$H^q(G, A) \cong \varinjlim_{L/F} H^q(Gal(L/F), A_L).$$

Teorema 3.2.22 (Teorema 90 de Hilbert)**.** *Sejam F e $K = F(\sqrt{a})$, onde $a \in R(F)$. Então $H^1(Gal(K/F), R(K)) = 1$.*

Demonstração. Seja $x \in \bar{Z}^1(Gal(K/F), R(K))$. Como $R(K)$ é subgrupo de $K^\times$, temos que x pode ser considerado um co-ciclo com coeficientes em $K^\times$. Pelo **Teorema 1.3.2** existe $y \in K^\times$ tal que

$$x(\sigma) = \sigma(y)y^{-1}.$$

Daí, segue que

$$x(\sigma)y^2 = \sigma(y)y = N_{K/F}(y) \in R(K) \cap F = R(F).$$

Pelo **Teorema 3.2.18**, $y \in F^\times R(K)$, ou seja, existem $c \in F^\times$ e $z \in R(K)$ tais que $y = cz$. Temos, então, que para todo $\sigma \in Gal(K/F)$, $x(\sigma) = \sigma(y)y^{-1} = \sigma(cz)(cz)^{-1} = \sigma(z)z^{-1,}$ pois $c \in F^\times$.

Portanto, $x \in \bar{B}^1(Gal(K/F), R(K))$ e $H^1(Gal(K/F), R(K)) = 1$. □

Como consequência do teorema acima, mostraremos que se F é um corpo com base distinguida, então o grupo de Galois $Gal(F_{red}/F)$ é um pro-2-grupo livre.

Teorema 3.2.23. *Sejam F corpo com base distinguida e F_{red}, o fecho reduzido do corpo F. Então:*

1. $H^1(Gal(F_{red}/F), (F^\times)^2_{red}) = 1$
2. $G = Gal(F_{red}/F)$ *é um pro-2-grupo livre.*

Demonstração. 1. Pela observação feita antes do **Teorema 3.2.22**, temos que

$$H^1(Gal(F_{red}/F), (F^\times)^2_{red})) \cong \varinjlim_{L/F} H^1(Gal(L/F), ((F^\times)^2_{red})^{Gal(L/F)}),$$

onde L/F percorre todas as subextensões normais e finitas de F_{red}/F.

Ainda, como $((F^\times)^2_{red})^{Gal(L/F)} = (F^\times)^2_{red} \cap L = R(L)$, temos que

$$H^1(Gal(F_{red}/F), (F^\times)^2_{red})) \cong \varinjlim_{L/F} H^1(Gal(L/F), R(L)).$$

Logo, é suficiente mostrar que $H^1(Gal(L/F), R(L)) = 1$ para toda extensão galoisiana finita L/F, com $F \subseteq L \subseteq F_{red}$. A demonstração desse fato será feita por indução sobre n, oden $[L : F] = 2^n$. Se $n = 1$, o resultado segue do **Teorema 3.2.22**.

Suponha então $n > 1$. Como o grupo de Galois é um 2-grupo e é resóluvel por radicais, existe uma cadeia de corpos

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = L,$$

onde $F_{i+1} = F_i(\sqrt{a_i})$, $a_i \in R(F_i)$. Considerando $K = F_{n-1}$, G o grupo $Gal(L/F)$ e H o subgrupo $Gal(L/K)$, temos as seguintes propriedades de G e H(são consequencia da resolubilidade por radicais).

(1) $Gal(L/K) \triangleleft Gal(L/F)$;

(2) $Gal(K/F) \cong G/H$.

(3) $[K : F] = 2^{n-1}$

(4) $[L : K] = 2$.

Considere agora a sequência exata dos cinco termos, ver por exemplo [**NSW**], página 64.

$1 \longrightarrow H^1(G/H, R(L)^H) \longrightarrow H^1(G, R(L)) \longrightarrow H^1(H, R(L))^{G/H} \longrightarrow$

$\longrightarrow H^2(G/H, R(L)^H) \longrightarrow H^2(G, R(L))$.

Observe agora que $R(L)^{G/H} = R(L) \cap K = R(K)$, pois a $F \subseteq K \subseteq F_{red}$. Além disso, temos que $Gal(K/F) = G/H$. Daí, a sequência exata se escreve da forma:

$1 \longrightarrow H^1(Gal(K/F), R(K)) \longrightarrow H^1(G, R(L)) \longrightarrow H^1(H, R(L))^{Gal(K/F)} \longrightarrow \cdots$.

Mas, pelo **Teorema 3.2.22**, $H^1(H, R(L)) = 1$ e $H^1(Gal(K/F), R(K)) = 1$ por hipótese de indução. Portanto, temos que $H^1(G, R(L)) = 1$ e consequentemente, $H^1(Gal(F_{red}/F), (F^\times)^2_{red}) = 1$.

Vamos agora apresentar a demostração da segunda parte do teorema.

2. Considere inicialmente a seguinte sequência de $G-$módulos:

$$1 \longrightarrow \{1, -1\} \longrightarrow F^\times_{red} \longrightarrow (F^\times)^2_{red} \longrightarrow 1.$$

Usando [**NSW**], temos a seguinte sequência exata longa:

$$1 \longrightarrow \{1,-1\}^G \longrightarrow (F^\times_{red})^G \longrightarrow ((F^\times)^2_{red})^G \longrightarrow H^1(G,\{1,-1\}) \longrightarrow H^1(G,F^\times_{red}) \longrightarrow$$
$$\longrightarrow H^1(G,(F^\times)^2_{red}) \longrightarrow H^2(G,\{1,-1\}) \longrightarrow H^2(G,F^\times_{red}) \longrightarrow H^2(G,(F^\times)^2_{red}) \longrightarrow \cdots$$

Usando o **Teoremas 1.3.2** e o ítem (e) do **Teorema 2.3.13** temos que $H^2(G,F^\times_{red}) = 1$ e pela primeira parte $H^1(G,(F^\times)^2_{red}) = 1$. Logo, pela sequência exata acima segue que $H^2(G,\{1,-1\}) = 1$.

Agora, pela [**NSW**], temos que $cd(G) = 1$, onde $cd(G)$ denota dimensão cohomológica de G. Portanto temos que G é um pró-2-grupo livre pela [**NSW**].

□

3.2.2 Base distinguida para extensões radicais

Nesta seção vamos mostrar a existência de base distinguida completas para 2-extensões de um corpo F com base distinguida completa. Para o caso de uma extensão quadrática $K = F(\sqrt{e})$, onde $e \in R(F)$, vamos apresentar explicitamente a construção. Nesse caso, pelo **Lema 3.2.16**, temos que Res é injetiva e Im $Res = H^2(K)^G$. Podemos então considerar ${}_2\mathrm{Br}(F) \subset {}_2\mathrm{Br}(K)$.

Começaremos com um resultado que mostra que a condição $e \in R(F)$ é bastante restritiva.

Teorema 3.2.24. *Sejam F um corpo, $e \in F^\times \smallsetminus R(F)$ e $K = F(\sqrt{e})$. Conside ainda σ o gerador de $G = Gal(K;F)$ e $Res : {}_2\mathrm{Br}(F) \to {}_2\mathrm{Br}(K)$ a restrição. Para todo $u \in K^\times \smallsetminus R(K)$, $Q_K(u) \not\subset {}_2\mathrm{Br}(K)^G$.*

Demonstração. Suponhamos por absurdo que existisse $u \in K^\times$ com $Q_K(u) \subset {}_2\mathrm{Br}(K)^G$. Nesse caso, pelo **Teorema 3.2.17** temos que $(D_F\langle 1,-N(u)\rangle : F^\times \cap D_K\langle 1,-u\rangle) = |Q_K(u)| = (K^\times : D_K\langle 1,-u\rangle)$. Observemos agora que

$$(K^\times : D_K\langle 1,-u\rangle) \geq (F^\times D_K\langle 1,-u\rangle : D_K\langle 1,-u\rangle) = (F^\times : F^\times \cap D_K\langle 1,-u\rangle) \geq$$
$$\geq (D_F\langle 1,-N(u)\rangle : F^\times \cap D_K\langle 1,-u\rangle).$$

Juntando a igualdade inicial com as desigualdades concluimos que $(F^\times : F^\times \cap D_K\langle 1,-u\rangle) = (D_F\langle 1,-N(u)\rangle : F^\times \cap D_K\langle 1,-u\rangle)$ e consequentemente $F^\times = D_F\langle 1,-N(u)\rangle$, isto é, $N(u) \in R(F)$. Pelo **Teorema 3.2.18** obtemos $u = cz$ com $c \in F^\times$ e $z \in R(K)$. Como por hipótese $u \notin R(K)$ temos que $D_K\langle 1,-u\rangle = D_K\langle 1,-c\rangle$. Usando agora a outra ponta das desigualdades obtemos também que $(K^\times : D_K\langle 1,-u\rangle) = (F^\times D_K\langle 1,-u\rangle : D_K\langle 1,-u\rangle)$, implicando que $K^\times = F^\times D_K\langle 1,-u\rangle = F^\times D_K\langle 1,-c\rangle$.

Logo $(K^\times : D_K\langle 1,-c\rangle) = (F^\times : D_F\langle 1,-c\rangle)$, pois $F^\times \cap D_K\langle 1,-c\rangle = D_F\langle 1,-c\rangle$. Portanto temos um absurdo, pois sabemos que $(K^\times : D_K\langle 1,-c\rangle) = (F^\times : D_F\langle 1,-c\rangle)^2$ uma vez que K é uma extensão radical de F, pela **Proposição 2.2.2**.

□

Corolário 3.2.25. *Sejam $F \subset E \subset F_{red}$ uma extensão intermediária qualquer e $\mathrm{res}_{E|F} : {}_2\mathrm{Br}(F) \to {}_2\mathrm{Br}(E)$ a restrição. Então:*

1. *$\mathrm{res}_{E|F}$ é injetiva e podemos considerar ${}_2\mathrm{Br}(F) \subset {}_2\mathrm{Br}(E)$.*
2. *Caso E seja uma extensão galoisiana de F, então ${}_2\mathrm{Br}(E)^{G(K;F)} = {}_2\mathrm{Br}(F)$.*

Proposição 3.2.26. *Conservamos a notação e os objetos introduzidos no **Teorem 3.2.11**. Seja $K = F(\sqrt{r})$, com $r \in R(F) \setminus (F^\times)^2$. Dados c, $d \in F_\lambda$, para algum $1 \leq \lambda \leq m$, tais que $cd \notin R(F)$, temos que $Q_K(c) = Q_K(d)$.*

*Recordemos que para todo $c \in F_\lambda$, para algum $1 \leq \lambda \leq m$, $|Q_K(c)| = 4$, pela **Proposição 2.2.2***

Demonstração. Como c, $d \in F_\lambda$ e $cd \notin R(F)$ temos pelo **Lema 3.2.10** que $D_F\langle 1, -c\rangle \neq D_F\langle 1, -d\rangle$. Daí, como $(F^\times : D_F\langle 1, -c\rangle) = 2$ segue que $D_F\langle 1, -c\rangle D_F\langle 1, -d\rangle = F^\times$. Como $Im\ N = F^\times$, então $D_K\langle 1, -c\rangle D_K\langle 1, -d\rangle = K^\times$ pelo item (6) da **Proposição 3.2.4**. Sabemos pela **Proposição 2.2.2** que $(K^\times : D_K\langle 1, -c\rangle) = 4$. Portanto,

$$(D_K\langle 1, -d\rangle : D_K\langle 1, -c\rangle \cap D_K\langle 1, -d\rangle) = (K^\times : D_K\langle 1, -c\rangle) = 4.$$

Como também temos que $(K^\times : D_K\langle 1, -d\rangle) = 4$ obtemos

$$(K^\times : D_K\langle 1, -c\rangle \cap D_K\langle 1, -d\rangle) = 16.$$

Note agora que o fato de $cd \in F_\lambda$ implica em $(F^\times : D_F\langle 1, -cd\rangle) = |Q_F(cd)| = 2$ e consequentemente $(K^\times : D_K\langle 1, -cd\rangle) = 4$. Temos que $D_K\langle 1, -c\rangle \cap D_K\langle 1, -d\rangle \subset D_K\langle 1, -cd\rangle$ e assim $(D_K\langle 1, -cd\rangle : D_K\langle 1, -c\rangle \cap D_K\langle 1, -d\rangle) = 4$. Esta última igualdade implica que $|Q_K(c) \cap Q_K(d)| = 4$. Portanto $Q_K(c) = Q_K(d)$, pois $|Q_K(c)| = 4 = |Q_K(d)|$. □

Teorema 3.2.27. *Sejam $r \in R(F) \setminus (F^\times)^2$ e $K = F(\sqrt{r})$. Denotemos por σ o gerador de $G = Gal(K;F)$ e por $N = N_{K|F}$, a norma da extensão.*

1. *Se F possui uma base distinguida, então K também possui. Mais precisamente, dada uma base distinguida de F $\{a_1, \ldots, a_n\}$ existem $z_1, \ldots, z_n \in K^\times$ tais que:*
   (a) *$N(z_i) = a_i$, para todo $i = 1, \ldots, n$.*
   (b) *Para todo $i = 1, \ldots, n$ temos que $D_K\langle 1, -z_i\rangle \cap F = D_F\langle 1, -a_i\rangle$.*
   (c) *$D_K\langle 1, -z_i\rangle \cap D_K\langle 1, -\sigma(z_i)\rangle = D_K\langle 1, -a_i\rangle$.*
   (d) *$\{z_1, \ldots, z_n, \sigma(z_1), \ldots, \sigma(z_n)\}$ é uma base distinguida de K.*
2. *Se $\{a_1, \ldots, a_n\}$ é uma base distinguida completa de F então $\{z_1, \ldots, z_n, \sigma(z_1), \ldots, \sigma(z_n)\}$ é uma base distinguida completa de K (conforme **Definição 3.2.13**).*

Demonstração. 1. Considere inicialmente $\{ c_1, \ldots, c_n \}$ uma base dual de $\{ a_1, \ldots, a_n \}$ em F, conforme visto na **Proposição 3.2.7**. Desta forma, para cada $i = 1, \ldots, n$ temos que $D_F\langle 1, -a_i\rangle / R(F)$ é gerado por $\{ c_1 \ldots, c_{i-1}, c_{i+1}, \ldots, c_n \}$. Usando novamente a **Proposição 3.2.7** temos que $a_i \in D_F\langle 1, -c_j\rangle$, para todo $j \neq i$. Logo, se $z_i \in K$ é tal que $N(z_i) = a_i$, então pelo Princípio da Norma

$$z_i \in \bigcap_{j\neq i} F^\times D_K\langle 1, -c_j\rangle = F^\times \left(\bigcap_{j\neq i} D_K\langle 1, -c_j\rangle \right),$$

onde a igualdade vale pelo item 4. da **Proposição 3.2.4**, pois conforme o item 2. da **Proposição 3.2.3** uma base distinguida de F satisfaz a hipótese da **Proposição 3.2.4**. Portanto existem $x_i \in F^\times$ e $y_i \in \bigcap_{j\neq i} D_K\langle 1, -c_j\rangle$ tais que $z_i = x_i y_i$, consequentemente $x_i^{-1} z_i = y_i \in D_K\langle 1, -c_j\rangle$, para todo $j \neq i$ e $c_j \in D_K\langle 1, -x_i^{-1} z_i\rangle \cap F^\times$ para todo $j \neq i$.

Obtemos então que $\dim_{\mathbb{F}_2} \left(D_K\langle 1, -x_i^{-1} z_i\rangle \cap F^\times \right) / R(F) \geq n-1$ e como $c_i \notin D_K\langle 1, -x_i^{-1} z_i\rangle$ podemos concluir que $\dim_{\mathbb{F}_2} \left(D_K\langle 1, -x_i^{-1} z_i\rangle \cap F^\times \right) / R(F) = n-1$, pois $R(F) \subset D_K\langle 1, -x_i^{-1} z_i\rangle \cap F^\times$. Novamente pelo Princípio da Norma $D_K\langle 1, -x_i^{-1} z_i\rangle \cap F^\times \subset D_F\langle 1, -N(x_i^{-1} z_i)\rangle = D_F\langle 1, -x_i^{-2} a_i\rangle = D_K\langle 1, -a_i\rangle$.

Agora, como $\dim_{\mathbb{F}_2} \left(D_K\langle 1, -a_i\rangle / R(F) \right) = n - 1$, podemos concluir que $D_K\langle 1, -x_i^{-1} z_i\rangle \cap F^\times = D_K\langle 1, -a_i\rangle$.

Note que que podemos trocar $\{ a_1, \ldots, a_n \}$ por $\{ x_1^{-2} a_1, \ldots, x_n^{-2} a_n \}$ em F e $z_1, \ldots, z_n \in K$ por $x_1^{-1} z_1, \ldots, x_n^{-1} z_n$ que as propriedades se mantem. Logo podemos assumir sem perda de generalidade que $D_K\langle 1, -z_i\rangle \cap F^\times = D_K\langle 1, -a_i\rangle$. Dessa forma os elementos $z_1, \ldots, z_n \in K$ têm as propriedades (a) e (b) requeridas.

Vamos agora ao ítem (c). Note que o ítem (b) juntamente com o item 1. do **Teorema 3.2.17** nos garante que $Q_K(z_i) \cap ({}_2\mathrm{Br}(K))^{G(K;F)} = \{ 0 \}$, para todo $i = 1, \ldots, n$. Logo, usando o ítem 2. do **Teorema 3.2.17**, temos que $Q_K(z_i) \cap Q_K(\sigma(z_i)) = \{ 0 \}$, para todo $i = 1, \ldots, n$. Sabemos, pela **Proposição 1.2.5**, que $Q_K(z_i) \cap Q_K(\sigma(z_i)) \cong D_K\langle 1, -N(z_i)\rangle / (D_K\langle 1, -z_i\rangle \cap D_K\langle 1, -\sigma(z_i)\rangle)$ e consequentemente podemos concluir que $D_K\langle 1, -N(z_i)\rangle = D_K\langle 1, -z_i\rangle \cap D_K\langle 1, -\sigma(z_i)\rangle$, para todo $i = 1, \ldots, n$, mostrando (c).

Para o ítem (d) note inicialmente que $\{ z_1 R(K), \ldots, z_n R(K),\ \sigma(z_1) R(K), \ldots, \sigma(z_n) R(K) \}$ é uma base de $K/R(K)$. De fato, suponha que existam $\varepsilon_1, \ldots, \varepsilon_n, \eta_1, \ldots, \eta_n \in \{ 0, 1 \}$ tais que

$$z = \prod_{j=1}^{n} z_j^{\varepsilon_j} \prod_{j=1}^{n} \sigma(z_j)^{\eta_j} \in R(K)$$

e defina

$$J_1 = \{ j_t \mid \varepsilon_{j_t} = 1 \ \text{ e } \ \eta_{j_t} = 0 \};\ J_2 = \{ j_t \mid \varepsilon_{j_t} = 0 \ \text{ e } \ \eta_{j_t} = 1 \};\ J_3 = \{ j_t \mid \varepsilon_{j_t} = \eta_{j_t} \}.$$

Como $z \in R(K)$, pelo Princípio da Norma, **Teorema 1.1.9**, temos que $N(z) \in R(F)$. E o cálculo da norma de z produz a seguinte equação:

$$\left(\prod_{j\in J_1} a_j \right) \left(\prod_{j\in J_2} a_j \right) \left(\prod_{j\in J_3} a_j^{\varepsilon_j} \right)^2 \in R(F).$$

Como $J_1 \cap J_2 = \emptyset$, $J_1 \cap J_3 = \emptyset$, $J_2 \cap J_3 = \emptyset$ vamos obter um absurdo se $J_1 \neq \emptyset$ ou $J_2 \neq \emptyset$, pois por hipótese o conjunto $\{a_1, \ldots, a_n\}$ é linearmente independente módulo $R(F)$. Logo $J_1 = J_2 = \emptyset$ e $J_3 = \{1, \ldots, n\}$. Portanto temos que

$$z = \prod_{j=1}^{n} z_j^{\varepsilon_j} \sigma(z_j)^{\varepsilon_j} = \prod_{j=1}^{n} a_j^{\varepsilon_j} \in R(F)$$

e assim $z \in R(K) \cap F$, pois $a_j \in F^\times$, para $j = 1, \ldots, n$. Agora, pelo **Corolário 2.1.9**, temos que $R(K) \cap F = R(F)$ e como $\{a_1, \ldots, a_n\}$ uma base distinguida de F, segue que $\varepsilon_j = 0$, para todo $j = 1, \ldots, n$.

Portanto, temos que o conjunto $\{z_1 R(K), \ldots, z_n R(K), \sigma(z_1)R(K), \ldots, \sigma(z_n)R(K)\}$ é linearmente independente módulo $R(K)$ e consequentemente uma base de $K^\times/R(K)$, pois a dimensão de $K^\times/R(K)$ é $2n$ pelo **Corolário 3.2.19**.

Para completar a demonstração de que $\{z_1, \ldots, z_n, \sigma(z_1), \ldots, \sigma(z_n)\}$ é uma base distinguida falta mostra que $(K^\times : D_K\langle 1, -z_i\rangle) = (K^\times : D_K\langle 1, -\sigma(z_i)\rangle) = 2$ para todo $i = 1, \ldots, n$.

Vamos separar esse cáculo em alguns passos:

(i) Por construção temos que $c_i \notin D_F\langle 1, -a_i\rangle$ e daí $0 \neq (c_i, a_i)_F \in Q_F(c_i) \cap Q_F(a_i)$ e como $|Q_F(c_i)| = 2 = |Q_F(a_i)|$ concluímos que $Q_F(c_i) = Q_F(a_i)$. Portanto existe $1 \leq \lambda \leq m$ tal que c_i, $a_i \in F_\lambda$ e pela **Proposição 3.2.26**, $Q_K(c_i) = Q_K(a_i)$.

(ii) Pelo **Lema 3.2.2** temos que $R(F) = \bigcap_{i=1}^{n} D_F\langle 1, -c_i\rangle$ e usando o **Teorema 2.2.4** temos que $R(K) = \bigcap_{i=1}^{n} D_K\langle 1, -c_i\rangle$. Sabemos ainda que para todo $i = 1, \ldots, n$, $z_i \in \bigcap_{j \neq i} D_K\langle 1, -c_j\rangle$. Como $D_K\langle 1, -c_i\rangle \neq K^\times$, temos que $z_i \notin D_K\langle 1, -c_i\rangle$ do que resulta $0 \neq (z_i, c_i)_K \in Q_K(z_i) \cap Q_K(c_i)$. Portanto $|Q_K(z_i) \cap Q_K(c_i)| \geq 2$ e devido ao passo (ii) concluimos que $|Q_K(z_i) \cap Q_K(a_i)| \geq 2$ e Consequentemente, pela **Proposição 1.2.5**, $(D_K\langle 1, -z_i a_i\rangle : D_K\langle 1, -z_i\rangle \cap D_K\langle 1, -a_i\rangle) \geq 2$ para todo $i = 1, \ldots, n$.

(iii) Devido ao item (c), $D_K\langle 1, -z_i\rangle \cap D_K\langle 1, -a_i\rangle = D_K\langle 1, -a_i\rangle$ que junto com a última desigualdade significa que $(D_K\langle 1, -z_i a_i\rangle : D_K\langle 1, -a_i\rangle) \geq 2$. Agora, pelo item (a) temos que $z_i a_i = \sigma(z_i) z_i^2$ e assim $D_K\langle 1, -z_i a_i\rangle = D_K\langle 1, -\sigma(z_i)\rangle$. Obtemos destas observações que $(D_K\langle 1, -\sigma(z_i)\rangle : D_K\langle 1, -a_i\rangle) \geq 2$.

Finalmente, como vimos no passo (ii) que $c_i \notin D_K\langle 1, -z_i\rangle$ e igualmente $c_i \notin D_K\langle 1, -\sigma(z_i)\rangle$. Daí, $(K^\times : D_K\langle 1, -\sigma(z_i)\rangle) \geq 2$. Mas, pela **Proposição 2.2.2**, $(K^\times : D_K\langle 1, -a_i\rangle) = 4$ e portando, usando a desigualdade do passo (ii), temos que $(K^\times : D_K\langle 1, -\sigma(z_i)\rangle) = 2$, para todo $i = 1, \ldots, n$. Analogamente, mostra-se que $(K^\times : D_K\langle 1, -z_i\rangle) = 2$, para todo $i = 1, \ldots, n$, completando a demonstração do item (d).

2. Suponha que $\{a_1, \ldots, a_n\}$ seja uma base distinguida completa de F e vamos verificar que $\{z_1, \ldots, z_n, \sigma(z_1), \ldots, \sigma(z_n)\}$ é uma base distinguida completa de K. Note primeiramente que para todo $1 \leq k \leq n$ temos que $Q_K(z_k) \neq Q_K(\sigma(z_k))$. De fato, caso contrário teríamos que $\sigma(Q_K(z_k)) = Q_K(\sigma(z_k)) = Q_K(z_k)$, e como $Q_K(z_k)$ tem ordem 2, necessariamente a ação de $G(K; F)$ sobre $Q_K(z_k)$ seria trivial. Logo, como vimos no primeiro parágrafo desta subseção, $Q_K(z_k) \subset {}_2\mathrm{Br}(F)$, o que contradiz o **Teorema 3.2.24.** Portanto $Q_K(z_k) \neq Q_K(\sigma(z_k))$ e seguindo

os passos da demonstração do do caso $t = 2$ do **Teorema 3.2.14**(página 49) podemos concluir que $Q_K(a_k) = Q_K(z_k) \otimes Q_K(\sigma(z_k))$, para todo $1 \leq k \leq n$.

Conforme observado na **Proposição 3.2.26**, $|Q_K(a_k)| = 4$, para todo $k = 1, \ldots, n$. Logo $Q_K(a_k)$ tem exatamente três subgrupos próprios e todos de ordem 2, a saber $Q_K(z_k)$, $Q_K(\sigma(z_k))$, e $Q_K(a_k) \cap {}_2\mathrm{Br}(K)^{G(K;F)}$. A natureza desse último subgrupo decorre do item 1. do **Teorema 3.2.17** aplicado a $z = a_k$.

Seja $\{\, 1, \ldots, n \,\} = \bigcup_{\lambda=1}^{m} I_\lambda$ a partição principal da base distinguida $\{a_1, \ldots, a_n\}$ de F. Para cada $1 \leq \lambda \leq m$ dados $i, j \in I_\lambda$ temos pela **Proposição 3.2.26** que $Q_K(a_i) = Q_K(a_j)$. Logo, pelo que vimos no parágrafo anterior vamos ter

$$Q_K(z_i) \otimes Q_K(\sigma(z_i)) = Q_K(z_j) \otimes Q_K(\sigma(z_j)).$$

Concluímos então dos três últimos parágrafos que

$$Q_K(z_i) = Q_K(z_j) \quad \text{ou} \quad Q_K(z_i) = Q_K(\sigma(z_j))$$

Dessa forma, fixado I_λ, com $1 \leq \lambda \leq m$, podemos assumir que para todo par $i, j \in I_\lambda$ temos $Q_K(z_i) = Q_K(z_j)$. De fato, basta escolher $\{\, z_i \mid i \in I_\lambda\}$ como sendo exatamente os elementos para os quais os $Q_K(z_i)$ são iguais e denotar por $\sigma(z_i)$ os seus conjugados por σ. Desta maneira teremos que os grupos $Q_K(\sigma(z_i))$ são todos iguais para $i \in I_\lambda$. Reciprocamente, se $Q_K(z_i) = Q_K(z_j)$ então $\mathrm{Cor}(Q_K(z_i)) = \mathrm{Cor}(Q_K(z_j))$, isto é, $Q_F(a_i) = Q_F(a_j)$ e consequentemente $i, j \in I_\lambda$ para algum $1 \leq \lambda \leq m$. Portanto, temos que $Q_K(z_i) = Q_K(z_j)$ se e somente se $i, j \in I_\lambda$, para algum $1 \leq \lambda \leq m$.

Vamos agora reescrever a base $\{\, z_1, \ldots, z_n, \sigma(z_1), \ldots, \sigma(z_n) \,\}$. Para todo $1 \leq j \leq 2n$ considere

$$x_j = \begin{cases} z_j & \text{para todo } 1 \leq j \leq n \\ \sigma(z_{n-j}) & \text{para todo } n < j \leq 2n \end{cases}$$

Antes de definirmos a partição principal para a base distinguida $\{x_1, \ldots, x_{2n}\}$ de K, vamos fazer uma observação. Pelo exposto acima e pela definição dos elementos x_i, temos que se $Q_K(x_i) = Q_K(x_j)$ então necessariamente temos que $1 \leq i, j \leq n$ ou $n < i, j \leq 2n$. Defina então a seguinte partição

$$\{\, 1, \ldots, 2n \,\} = \bigcup_{\kappa=1}^{2m} J_\kappa, \text{ onde}$$

$$J_\kappa = \begin{cases} I_\kappa & \text{para todo } 1 \leq \kappa \leq m \\ n + I_{(\kappa-m)} := \{n + i_{(\kappa-m)} \mid i_{(\kappa-m)} \in I_{(\kappa-m)}\} & \text{para todo } m < \kappa \leq 2m \end{cases}$$

Portanto temos que a partição definida acima é principal pois $Q_K(x_i) = Q_K(x_j)$ se, e somente se $i, j \in J_\kappa$ para algum $1 \leq \kappa \leq 2m$.

Finalmente, da maneira como foi definida, temos que a base $\{x_1, \ldots, x_n\}$ será completa se $\{\, a_1, \ldots, a_n \,\}$ for completa pois $|{}_2\mathrm{Br}(K)| = |{}_2\mathrm{Br}(F)|^2$, pelo **Lema 2.2.1.** □

Corolário 3.2.28. *Seja $F \subset E \subset F_{red}$ uma extensão intermediária finita. Se F tem base distinguida completa, então E também tem.*

Demonstração. Seja $[E : F] = 2^k$. Vamos demonstrar o corolário por indução sobre k. O caso $k = 1$ corresponde ao **Teorema 3.2.27**. Assumindo-se que o resultado vale para k seja E tal que $[E : F] = 2^{k+1}$. Como estamos dentro de uma 2-extensão galoisiana, existe $F \subset K \subset E$ tal que $[E : K] = 2$. Como $[K : F] = 2^k$, pela hipótese de indução K tem uma base distinguida completa. Finalmente, pelo **Teorema 3.2.27** essa base distinguida completa de K dá origem a uma base distinguida completa de E. □

Capítulo 4

Bases distinguidas - parte II
Dimensão cohomológica

No capítulo anterior apresentamos as bases distinguidas, um objeto novo que deparamos durante nossos estudos. No contexto em que trabalhamos, as bases distinguidas nos oferecem uma nova visão sobre os corpos com um número finito de álgebras de quatérnios.

Vimos, nos resultados anteriores que as propriedades de base distinguida se transferem diretamente às extensões quadráticas radicais. Para o caso das extensões não radicais precisamos de resuldos mais gerais, que apresentaremos separadamente neste Capítulo.

No decorrer do estudo sobre a existência de bases distinguidas para extensões quadráticas quaisquer, chegamos a conclusões importantes sobre a estrutura Cohomológica destes corpos, que apresentaremos no final da primeira parte do Capítulo.

4.1 Resultados gerais

Nesta seção vamos apresentar resultados mais gerais, alguns são generalizações de resultados que aparecem no capítulo anterior e serão apresentados aqui com o objetivo de aplicá-los ao caso não radical também. Trataremos aqui do estudo das propriedades cohomológicas de corpos com base distinguida.

Conforme colocado na **Observação 3.2.12**, cada elemento $c \neq 0$ de um corpo com base distinguida tem uma decomposição única módulo $R(F)$ na forma $c = c_1 \cdots c_r$ com $c_i \in F_{\lambda_i}$ para algum λ_i correspondente a partição principal.

Nosso próximo resultado vai refinar os resultados obtidos no **Teorema 3.2.11** para tratarmos de extensões quadráticas não radicais.

Teorema 4.1.1. *Seja F um corpo com base distinguida $\{ a_1, \ldots, a_n \}$, partição principal I_λ, $1 \leq \lambda \leq m$ e os subgrupos F_λ e $Q_F(\lambda)$ definidos anteriormente.*
Denotemos por $\Lambda = \{ 1, \ldots, m \}$ e seja $c = \prod_{i \in I} c_i \in F^\times$, onde $I \subset \Lambda$, $c_i \in F_i$, e $c_i \notin R(F)$, para todo $i \in I$.

1. *Dado $e \in F_\gamma$, com $e \notin R(F)$, temos que*

$$D_F\langle 1, -c\rangle \subset D_F\langle 1, -e\rangle$$

se e somente se $\gamma \in I$, e também $e \in c_\gamma R(F)$.
Consequentemente $D_F\langle 1, -c_i\rangle$, com $i \in I$, são os únicos subgrupos da forma $D_F\langle 1, -y\rangle$, com índice 2 em $F^\times$, que contém $D_F\langle 1, -c\rangle$.

2. *Dado $d = \prod_{j\in J} d_j \in F^\times$, onde $J \subset \Lambda$, $d_j \in F_j$, e $d_j \notin R(F)$, para todo $j \in J$, $D_F\langle 1, -c\rangle \subset D_F\langle 1, -d\rangle$ se e somente se $J \subset I$ e ainda $d_j \in c_j R(F)$ para todo $j \in J$.*
*Consequentemente, $D_F\langle 1, -d\rangle = D_F\langle 1, -c\rangle$ se e somente se $dc \in R(F)$. (Vale aqui ressaltar que esta propriedade foi demonstrada por Cordes, em [**C**], para corpos com duas álgebras de quatérnios, mas vale para corpos com base distinguida.)*

3. *Dado $d = \prod_{j\in J} d_j \in F^\times$, onde $J \subset \Lambda$ e $d_j \in F_j$ para todo $j \in J$, seja $C_2 = \{\, \beta \in I \cap J \mid c_\beta \in d_\beta R(F)\,\}$, o conjunto de elementos "comuns" nas representações de c e d. Então*

$$\dim_{\mathbb{F}_2}(F^\times / \left(D_F\langle 1 - c\rangle D_F\langle 1, -d\rangle\right)) = \#C_2 \text{ e}$$

$$D_F\langle 1, -c\rangle D_F\langle 1, -d\rangle = \bigcap_{\lambda\in C_2} D_F\langle 1, -c_\lambda\rangle = D_F\langle 1, -z\rangle,$$

onde $z = \prod_{\lambda\in C_2} c_\lambda$. Consequentemente, no caso de não haver fator comum ($C_2 = \emptyset$), temos

$$D_F\langle 1 - c\rangle D_F\langle 1, -d\rangle = F^\times.$$

4. *Tomando-se $K = F(\sqrt{c})$ temos que*

$$R(K) \cap F = \langle c_i R(F), i \in I\rangle$$

o subgrupo de $F^\times$ gerado pelo conjunto $\{\, c_i \mid i \in I\,\}$ e $R(F)$. Mais ainda,

$$\dim_{\mathbb{F}_2}(R(K) \cap F)/R(F) = \#I.$$

Demonstração. (1) Observemos inicialmente que pelo item 2(b) do **Teorema 3.2.11** sabemos que existe $\gamma \in \Lambda$ tal que $e \in F_\gamma$. Se $\gamma \notin J$, então $F_\gamma \subset D_F\langle 1, -c_j\rangle$, para todo $j \in J$, pelo item 2(a) desse teorema. Por outro lado, pelo **Teorema 3.2.14**, temos que

$$\bigcap_{j\in J} D_F\langle 1, -c_j\rangle = D_F\langle 1, -c\rangle.$$

Juntando-se os dois fatos obtemos $F_\gamma \subset D_F\langle 1, -c\rangle \subset D_F\langle 1, -e\rangle$. Como $e \in F_\gamma$, essa última inclusão contradiz o item 2(a) do Teorema 3.2.11. Portanto $\gamma \in J$.

Seja agora $c_o = ec_\gamma \in F_\gamma$. Temos que $ec = c_o \prod_{\substack{i\in I\\ i\neq\gamma}} c_i$ é a decomposição de ec. Suponhamos que $c_o \notin R(F)$ e seja $d = ec$. Temos que

$$D_F\langle 1-d\rangle = D_F\langle 1,-c_o\rangle \cap \left(\bigcap_{\substack{i\in I\\ i\neq\gamma}} D_F\langle 1,-c_i\rangle\right),$$

pelo mesmo **Teorema 3.2.14**.

Como $D_F\langle 1,-c\rangle \subset D_F\langle 1,-e\rangle$ e também $D_F\langle 1,-c\rangle \subset D_F\langle 1,-c_\gamma\rangle$, usando o **Lema 1.1.3**, temos que

$$D_F\langle 1,-c\rangle \subset D_F\langle 1,-c_\gamma\rangle \cap D_F\langle 1,-e\rangle = D_F\langle 1,-c_\gamma\rangle \cap D_F\langle 1,-c_o\rangle.$$

Portanto $D_F\langle 1,-c\rangle \subset D_F\langle 1,-c_o\rangle$. Por outro lado

$$D_F\langle 1,-c\rangle \subset \bigcap_{\substack{i\in I\\ i\neq\gamma}} D_F\langle 1,-c_i\rangle,$$

implicando

$$D_F\langle 1,-c\rangle \subset D_F\langle 1,-c_o\rangle \cap \left(\bigcap_{\substack{i\in I\\ i\neq\gamma}} D_F\langle 1,-c_i\rangle\right) = D_F\langle 1,-d\rangle.$$

Mas isso implica que $D_F\langle 1,-c\rangle = D_F\langle 1,-d\rangle$, pois, $\dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-c\rangle = \#I = \dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-d\rangle$ pelo **Teorema 3.2.14**.

Por outro lado, por esse mesmo resultado temos que

$$Q_F(c) = \bigoplus_{i\in I} Q_F(i) = Q_F(d),$$

pois $Q_F(c_o) = Q_F(\gamma)$. Logo, pelo **Lema 3.2.10**, temos que $cd \in R(F)$. Mas isso produz uma contradição, pois devido a construção de d temos que $cd = ec^2 \notin R(F)$.

(2) Esse item é consequência do item (1) pois $D_F\langle 1,-d\rangle \subset D_F\langle 1,-d_j\rangle$ para todo $j \in J$.

(3) Sem perda de generalidade vamos assumir, simplificadamente, que $d_\beta = c_\beta$, para todo $\beta \in C_2$. Escrevemos então $y = \left(\prod_{\beta\in C_2} c_\beta\right)\left(\prod_{j\notin C_2} d_j\right)$.

Pelo **Teorema 3.2.14** temos que $\dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-d\rangle = \#J$, $\dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-c\rangle = \#I$,

$$D_F\langle 1,-d\rangle = \left(\bigcap_{\beta\in C_2} D_F\langle 1,-c_\beta\rangle\right) \cap \left(\bigcap_{j\notin C_2} D_F\langle 1,-d_j\rangle\right) \quad \text{e} \quad D_F\langle 1,-c\rangle = \bigcap_{i\in I} D_F\langle 1,-c_i\rangle.$$

Logo

$$D_F\langle 1,-d\rangle \cap D_F\langle 1,-c\rangle = \left(\bigcap_{\beta\in C_2} D_F\langle 1,-c_\beta\rangle\right) \cap \left(\bigcap_{j\notin C_2} D_F\langle 1,-d_j\rangle\right) \cap \left(\bigcap_{i\notin C_2} D_F\langle 1,-c_i\rangle\right).$$

Resultando então **Teorema 3.2.14** que

$$\dim_{\mathbb{F}_2} F^\times/(D_F\langle 1,-d\rangle \cap D_F\langle 1,-c\rangle) = \#I + \#J - \#C_2.$$

Pelo Teorema do Isomorfismo temos que

$$D_F\langle 1,-d\rangle D_F\langle 1,-c\rangle/D_F\langle 1,-d\rangle \simeq D_F\langle 1,-c\rangle/(D_F\langle 1,-d\rangle \cap D_F\langle 1,-c\rangle).$$

Logo

$$\dim_{\mathbb{F}_2} D_F\langle 1,-d\rangle D_F\langle 1,-c\rangle/D_F\langle 1,-d\rangle =$$
$$= \dim_{\mathbb{F}_2} F^\times/(D_F\langle 1,-d\rangle \cap D_F\langle 1,-c\rangle) - \dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-c\rangle = \#J - \#C_2$$

e

$$\dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-d\rangle D_F\langle 1,-c\rangle =$$
$$= \dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-d\rangle - \dim_{\mathbb{F}_2} D_F\langle 1,-d\rangle D_F\langle 1,-c\rangle/D_F\langle 1,-d\rangle = \#C_2,$$

como afirmado.

Para a segunda igualdade como $z = \prod_{\lambda\in C_2} c_\lambda$ é o produto dos termos comuns, então pelo item (2) temos $D_F\langle 1,-c\rangle$, $D_F\langle 1,-d\rangle \subset D_F\langle 1,-z\rangle$. Logo $D_F\langle 1,-c\rangle D_F\langle 1,-d\rangle \subset D_F\langle 1,-z\rangle$. Pelo **Teorema 3.2.14** temos que $\dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-z\rangle = \#C_2$. Logo

Como $\dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-z\rangle = \dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-c\rangle D_F\langle 1,-d\rangle$ resultando na igualdade. Finalmente, pelo **Teorema 3.2.14**, $D_F\langle 1,-z\rangle$ é igual a interseção dos grupos de seus fatores.

Para a demonstração do ítem (4), vamos apresentar um lema auxiliar. Para tanto, recordemos que, pelo **Lema 2.1.7**, $d \in R(K)\cap F$ se e somente se $D_F\langle 1,-d\rangle D_F\langle 1,-dc\rangle = F^\times$ e $D_F\langle 1,-c\rangle \subset D_F\langle 1,-d\rangle$, onde K é uma extensão quadrática de F. No caso em que F tenha uma base distinguida a segunda condição pode ser simplificada:

Lema 4.1.2. *Assumido-se as hipóteses e notações do* ***Teorema 4.1.1*** *temos para c, $d \in F^\times$ que $D_F\langle 1,-c\rangle \subset D_F\langle 1,-d\rangle$ implica em $D_F\langle 1,-d\rangle D_F\langle 1,-cd\rangle = F^\times$. Logo, para $K = F(\sqrt{c})$ temos que $d \in R(K)\cap F$ se e somente se $D_F\langle 1,-c\rangle \subset D_F\langle 1,-d\rangle$.*

Demonstração. Consideremos c e d como no **Teorema 4.1.1**. Caso $D_F\langle 1,-c\rangle \subset D_F\langle 1,-d\rangle$, temos pelo item (2) do **Teorema 4.1.1** $J \subset I$ e $d_j \in c_j R(F)$, para todo $j \in J$. Isto é, $C_2 = J$ e todos os termos de d são comuns. Portanto $cd = \prod_{i\notin J} c_i d^2$. Resulta disso que d e cd não tem fatores em comum e assim $D_F\langle 1,-d\rangle D_F\langle 1,-cd\rangle = F^\times$, pelo item (3) do **Teorema 4.1.1.** □

Voltando à demonstração do teorema.

(4) Usaremos aqui o lema anterior.

Pelo **Lema 4.1.2**, $d \in R(K)\cap F$ se e somente se $D_F\langle 1,-c\rangle \subset D_F\langle 1,-d\rangle$. Por outro lado, pelo item (2), já demonstrado, a condição $D_F\langle 1,-c\rangle \subset D_F\langle 1,-d\rangle$ é equivalente a $d \in \langle c_i R(F), i \in I\rangle$. □

Introduziremos na observação a seguir uma nova notação que será bastante usada no decorrer do trabalho.

Observação 4.1.3. *Seja F um corpo com base distinguida $\{ a_1, \ldots, a_n \}$, partição principal I_λ, $1 \leq \lambda \leq m$ e os subgrupos F_λ e $Q_F(\lambda)$ como na* ***Definição 3.2.8****. Continuamos denotando $\Lambda = \{ 1, \ldots, m \}$.*

Dados $c = \prod_{i \in I} c_i$ e $d = \prod_{j \in J} d_j$ em $F^\times$, onde I, $J \subset \Lambda$ e $c_i \in F_i \smallsetminus R(F)$, para todo $i \in I$, e $d_j \in F_j \smallsetminus R(F)$, para todo $j \in J$, respectivamente, sejam

$$I_1 = I \smallsetminus (I \cap J),\ J_1 = J \smallsetminus (I \cap J),\ C_1 = \{ \alpha \in I \cap J \mid c_\alpha \notin d_\alpha R(F) \},\ C_2 = \{ \beta \in I \cap J \mid c_\beta \in d_\beta R(F) \}.$$

Observe que $C_1 \cup C_2 = I \cap J$, $J_1 \cap I_1 = \emptyset$, $J_1 \cap C_1 = \emptyset$, $I_1 \cap C_1 = \emptyset$, $C_1 \cap C_2 = \emptyset$, etc.

Veremos a seguir uma combinação do item (3) do **Teorema 4.1.1** com o item (5) da **Poposição 3.2.4**, apresentada no **Capítulo 3**.

Proposição 4.1.4. *Considere as condições da* ***Observação 4.1.3*** *acima. Sejam c, $d \in F^\times \smallsetminus (F^\times)^2$, com decomposições como descritas na* ***Observação 4.1.3****, e seja $K = F(\sqrt{c})$. Então*

$$\dim_{\mathbb{F}_2} K^\times / D_K\langle 1, -d \rangle = 2\#J_1 + \#C_1.$$

Demonstração. Pelo **Lema 1.1.11**, $D_K\langle 1, -d \rangle \cap F = D_F\langle 1, -d \rangle D_F\langle 1, -cd \rangle$ será conveniente encontrar a decomposição de cd em fatores dos F_λ.

$$cd = \left(\prod_{j \in J_1} d_j \right) \left(\prod_{i \in I_1} c_i \right) \left(\prod_{\alpha \in C_1} d_\alpha c_\alpha \right).$$

Vemos que os termos correspondentes a $\beta \in C_2$ podem ser descartados, pois $d_\beta c_\beta \in R(F)$, para todo β.

Concluímos então que J_1 é o conjunto dos termos "comuns" a d e cd e portanto, pelo item (3) do **Teorema 4.1.1** temos

$$D_F\langle 1, -d \rangle D_F\langle 1, -cd \rangle = \bigcap_{j \in J_1} D_F\langle 1, -d_j \rangle = D_F\langle 1, -d^{(o)} \rangle,$$

onde $d^{(o)} = \prod_{j \in J_1} d_j$. Sabemos também que $\dim_{\mathbb{F}_2} F^\times / D_F\langle 1, -d^{(o)} \rangle = \#J_1$.

Pelo **Corolário 1.1.12**, a seguinte sequência é exata

$$\begin{aligned} 1 \to \{ (F^\times)^2, c(F^\times)^2 \} \to D_F\langle 1, -d^{(o)} \rangle / (F^\times)^2 \xrightarrow{j} D_K\langle 1, -d \rangle / (K^\times)^2 \\ \xrightarrow{\overline{N}} \left(D_F\langle 1, -d \rangle \cap D_F\langle 1, -c \rangle \right) / (F^\times)^2 \to 1, \end{aligned} \tag{4.1.1}$$

onde j é induzida pela inclusão $F \subset K$ e $\overline{N}$ pela norma $N_{K|F}$.

Vamos inicialmente determinar $\dim_{\mathbb{F}_2} \left(D_F\langle 1, -d \rangle \cap D_F\langle 1, -c \rangle \right) / (F^\times)^2$. Para isso recordemos que, pela **Proposição 1.2.5**, $Q_F(c) \cap Q_F(d) \simeq D_F\langle 1, -cd \rangle / (D_F\langle 1, -c \rangle \cap D_F\langle 1, -d \rangle)$. Conforme **Teorema 3.2.14**

$$Q_F(c) = \bigoplus_{i\in I} Q_F(i) \quad \text{e} \quad Q_F(d) = \bigoplus_{j\in J} Q_F(j).$$

Logo

$$Q_F(c) \cap Q_F(d) = \bigoplus_{\lambda\in I\cap J} Q_F(\lambda),$$

resultado em $\dim_{\mathbb{F}_2}\ (Q_F(c) \cap Q_F(d)) = \#(I \cap J) = \#C_1 + \#C_2$. Assim

$$\dim_{\mathbb{F}_2}\ D_F\langle 1, -cd\rangle/(D_F\langle 1, -c\rangle \cap D_F\langle 1, -d\rangle) = \#C_1 + \#C_2.$$

Como

$$\begin{aligned}\dim_{\mathbb{F}_2}\ F^\times/(D_F\langle 1, -c\rangle \cap D_F\langle 1, -d\rangle) = \ & \dim_{\mathbb{F}_2}\ F^\times/D_F\langle 1, -cd\rangle + \\ & \dim_{\mathbb{F}_2}\ D_F\langle 1, -cd\rangle/(D_F\langle 1, -c\rangle \cap D_F\langle 1, -d\rangle)\end{aligned}$$

a decomposição de cd descrita acima juntamente com o **Teorema 3.2.14**, nos dizem que $\dim_{\mathbb{F}_2}\ F^\times/D_F\langle 1, -cd\rangle = \#J_1 + \#I_1 + \#C_1$. Juntando os dois últimos cálculos obtemos

$$\dim_{\mathbb{F}_2}\ F^\times/(D_F\langle 1, -c\rangle \cap D_F\langle 1, -d\rangle) = \#J_1 + \#I_1 + 2\#C_1 + \#C_2. \tag{4.1.2}$$

Devido a sequência exata (4.1.1) acima, temos que

$$\dim_{\mathbb{F}_2}\ D_K\langle 1, -d\rangle/(K^\times)^2 = \dim_{\mathbb{F}_2}\ D_F\langle 1, -d^{(o)}\rangle/(F^\times)^2 - 1 + \dim_{\mathbb{F}_2}\ (D_F\langle 1, -c\rangle \cap D_F\langle 1, -d\rangle)/(F^\times)^2.$$

Como $\dim_{\mathbb{F}_2}\ (D_F\langle 1, -c\rangle \cap D_F\langle 1, -d\rangle)/(F^\times)^2 = \dim_{\mathbb{F}_2}\ F^\times/(F^\times)^2 - \dim_{\mathbb{F}_2}\ F^\times/(D_F\langle 1, -c\rangle \cap D_F\langle 1, -d\rangle)$ vamos concluir que

$$\begin{aligned}\dim_{\mathbb{F}_2}\ D_K\langle 1, -d\rangle/(K^\times)^2 \ = \ & \dim_{\mathbb{F}_2}\ D_F\langle 1, -d^{(o)}\rangle/(F^\times)^2 - 1 + \\ & \dim_{\mathbb{F}_2}\ F^\times/(F^\times)^2 - (\#J_1 + \#I_1 + 2\#C_1 + \#C_2),\end{aligned} \tag{4.1.3}$$

devido a equação (4.1.2).

Por outro lado, $\dim_{\mathbb{F}_2}\ D_F\langle 1, -d^{(o)}\rangle/(F^\times)^2 = \dim_{\mathbb{F}_2}\ F^\times/(F^\times)^2 - \dim_{\mathbb{F}_2}\ F^\times/D_F\langle 1, -d^{(o)}\rangle$, e sabemos pelo **Teorema 3.2.14** que $\dim_{\mathbb{F}_2}\ F^\times/D_F\langle 1, -d^{(o)}\rangle = \#J_1$. Substituindo-se esses valores na equação (4.1.3) obtemos

$$\dim_{\mathbb{F}_2}\ D_K\langle 1, -d\rangle/(K^\times)^2 = 2\dim_{\mathbb{F}_2}\ F^\times/(F^\times)^2 - 1 - 2\#J_1 - \#I_1 - 2\#C_1 - \#C_2. \tag{4.1.4}$$

Calculando-se as dimensões por outro caminho vamos obter

$$\dim_{\mathbb{F}_2}\ D_K\langle 1, -d\rangle/(K^\times)^2 = \dim_{\mathbb{F}_2}\ K^\times/(K^\times)^2 - \dim_{\mathbb{F}_2}\ K^\times/D_K\langle 1, -d\rangle.$$

Recordemos a seguir a sequência exata

$$1 \to \{\ (F^\times)^2, c(F^\times)^2\ \} \to F^\times/(F^\times)^2 \to K^\times/(K^\times)^2 \xrightarrow{\overline{N}} D_F\langle 1, -c\rangle/(F^\times)^2 \to 1,$$

onde $\overline{N}$ é induzido pela norma. Essa sequência permite substituir $\dim_{\mathbb{F}_2} K^\times/(K^\times)^2$ na equação acima para obter

$$\dim_{\mathbb{F}_2} D_K\langle 1,-d\rangle/(K^\times)^2 = \dim_{\mathbb{F}_2} F^\times/(F^\times)^2 - 1 + \dim_{\mathbb{F}_2} D_F\langle 1,-c\rangle/(F^\times)^2 - \dim_{\mathbb{F}_2} K^\times/D_K\langle 1,-d\rangle. \tag{4.1.5}$$

Temos ainda que $\dim_{\mathbb{F}_2} D_F\langle 1,-c\rangle/(F^\times)^2 = \dim_{\mathbb{F}_2} F^\times/(F^\times)^2 - \dim_{\mathbb{F}_2} F^\times/D_K\langle 1,-c\rangle$; de onde, pelo **Teorema 3.2.14**, obtemos $\dim_{\mathbb{F}_2} D_F\langle 1,-c\rangle/(F^\times)^2 = \dim_{\mathbb{F}_2} F^\times/(F^\times)^2 - \#I_1 - \#C_1 - \#C_2$. Substituindo-se esse último valor na igualdade (4.1.5) obtemos

$$\dim_{\mathbb{F}_2} D_K\langle 1,-d\rangle/(K^\times)^2 = 2\dim_{\mathbb{F}_2} F^\times/(F^\times)^2 - 1 - \#I_1 - \#C_1 - \#C_2 - \dim_{\mathbb{F}_2} K^\times/D_K\langle 1,-d\rangle. \tag{4.1.6}$$

Finalmente, comparando-se as equações (4.1.4) com (4.1.6) obtemos

$$\dim_{\mathbb{F}_2} K^\times/D_K\langle 1,-d\rangle = 2\#J_1 + \#C_1,$$

conforme afirmado. □

Proposição 4.1.5. *Seja $K = F(\sqrt{c})$, onde $c \in F^\times \smallsetminus (F^\times)^2$ possui decomposição $c = \prod_{i\in I} c_i$, com $I \subseteq \Lambda$ e $c_i \in F^\times \smallsetminus R(F)$ para todo $i \in I$. Considere também $d \in F_\lambda \smallsetminus R(F)$, para algum $\lambda \in \Lambda$. Então:*

1. $$(K^\times : D_K\langle 1,-d\rangle) = \begin{cases} 1 & \text{se } \lambda \in I \text{ e } d \in c_\lambda R(F) \\ 2 & \text{se } \lambda \in I \text{ e } d \notin c_\lambda R(F) \\ 4 & \text{se } \lambda \notin I. \end{cases}$$

2. *Consequentemente*
$$|Q_K(d)| = \begin{cases} 2 & \text{se } \lambda \in I \text{ e } d \notin c_\lambda R(F) \\ 4 & \text{se } \lambda \notin I. \end{cases}$$

3. $$\begin{cases} F^\times \subset D_K\langle 1,-d\rangle & \text{se } \lambda \in I \\ D_K\langle 1,-d\rangle \cap F = D_F\langle 1,-c\rangle & \text{se } \lambda \notin I. \end{cases}$$

4. *Para todo $e \in F_\lambda \smallsetminus R(F)$ e caso $\lambda \in I$, assumimos e, $d \notin c_\lambda R(F)$, temos que $Q_K(d) = Q_K(e)$.*

Demonstração. (1) Para o primeiro caso temos que $d \in R(K)\cap F$, pelo item (4) do **Teorema 4.1.1**. Logo $D_K\langle 1,-d\rangle = K^\times$, como afirmado.

Usando-se a notação da **Observação 4.1.3** temos no caso $\lambda \in I$ e $d \notin c_\lambda R(F)$ temos $J_1 = \emptyset = C_2$ e $C_1 = \{\lambda\}$. Portanto $\dim_{\mathbb{F}_2} K^\times/D_K\langle 1,-d\rangle = 1$, como afirmado.

O último caso também decorre diretamente do **Teorema 4.1.4** pois $J_1 = \{\lambda\}$ e $C_1 = \emptyset = C_2$.

(2) é equivalente ao item (1).

(3) Caso $\lambda \in I$ e $d \in c_\lambda R(F)$ já vimos que $D_K\langle 1,-d\rangle = K^\times$ e portanto $F \subset D_K\langle 1,-d\rangle$ trivialmente.

Recordemos que $D_K\langle 1,-d\rangle \cap F = D_F\langle 1,-d\rangle D_F\langle 1,-cd\rangle$ e pelo item (3) do **Teorema 4.1.1** temos $\dim_{\mathbb{F}_2} F^\times/D_F\langle 1,-d\rangle D_F\langle 1,-cd\rangle =$ número dos temos "comuns" nas fatorações de d e cd. No caso $\lambda \in I$ e $d \notin c_\lambda R(F)$ não há fator em comum entre $d \in F_\lambda$ e cd. De fato cd terá como fator em F_λ o produto dc_λ. Portanto $D_F\langle 1,-d\rangle D_F\langle 1,-cd\rangle = F^\times$ e assim $F^\times \subset D_F\langle 1,-d\rangle$, como afirmado.

Para $\lambda \notin I$ teremos que d é o fator de cd em F_λ. Logo há um fator em comum entre d e cd, a saber d. Nesse caso, ainda pelo ítem (3) do **Teorema 4.1.1**, $D_F\langle 1,-d\rangle D_F\langle 1,-cd\rangle = D_F\langle 1,-d\rangle$, completando a demonstração deste item.

Para a demonstração do último ítem, precisamos de um Lema auxiliar.

Lema 4.1.6. *Sejam $c = \prod_{i\in I} c_i$, com $c_i \in F_i \smallsetminus R(F)$ para todo $i \in I$, e $K = F(\sqrt{c})$. Denotemos por N a norma $N_{K|F}$ e por σ o gerador de $G(K;F)$.*

Sejam também $d, e \in F_\lambda$ tais que $de \notin R(F)$ e se $\lambda \in I$, então $d, e \notin c_\lambda R(F)$. Nessas condições temos que

$$D_F\langle 1,-c\rangle = (D_F\langle 1,-d\rangle \cap D_F\langle 1,-c\rangle)(D_F\langle 1,-e\rangle \cap D_F\langle 1,-c\rangle);$$
$$D_K\langle 1,-d\rangle D_K\langle 1,-e\rangle = K^\times.$$

Demonstração. Pelo item (2) do **Teorema 4.1.1**, $D_F\langle 1,-c\rangle \not\subset D_F\langle 1,-d\rangle, D_F\langle 1,-e\rangle$. Logo $D_F\langle 1,-c\rangle D_F\langle 1,-d\rangle = F^\times$ e $D_F\langle 1,-c\rangle D_F\langle 1,-e\rangle = F^\times$ Portanto $2 = (F^\times : D_F\langle 1,-d\rangle) = (D_F\langle 1,-c\rangle : D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle)$ e, analogamente, $(D_F\langle 1,-c\rangle : D_F\langle 1,-c\rangle \cap D_F\langle 1,-e\rangle) = 2$.

Para completarmos a demonstração, **afirmamos** que os subgrupos $D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle$ e $D_F\langle 1,-c\rangle \cap D_F\langle 1,-e\rangle$ de $F^\times$ são não comparáveis.

E desta forma temos que $D_F\langle 1,-c\rangle = (D_F\langle 1,-d\rangle \cap D_F\langle 1,-c\rangle)(D_F\langle 1,-e\rangle \cap D_F\langle 1,-c\rangle)$, como queríamos.

Verificaremos agora os subgrupos $D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle$ e $D_F\langle 1,-c\rangle \cap D_F\langle 1,-e\rangle$ de $F^\times$ são não comparáveis. E a demonstração desse fato será surpreendentemente longa.

Observemos inicialmente que, pelo item (2) do **Teorema 4.1.1**, $D_F\langle 1,-d\rangle D_F\langle 1,-e\rangle = F^\times$. Agora, usando o Teorema do Isomorfismo para grupos, temos que

$$D_F\langle 1,-d\rangle/D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle \simeq (D_F\langle 1,-d\rangle)(D_F\langle 1,-e\rangle)/D_F\langle 1,-e\rangle \simeq F^\times/D_F\langle 1,-e\rangle.$$

Portanto $(D_F\langle 1,-d\rangle : D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle) = 2 = (D_F\langle 1,-e\rangle : D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle)$. Isso implica que $(F^\times : D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle) = 4$. Como $D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle \subset D_F\langle 1,-de\rangle$ e $(F^\times : D_F\langle 1,-de\rangle) = 2$, vemos que $D_F\langle 1,-d\rangle$, $D_F\langle 1,-e\rangle$, e $D_F\langle 1,-de\rangle$ são os únicos subgrupos com índice 2 em $F^\times$ que contém $D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle$. Esse 3 subgrupos são distintos pelo item (2) do **Teorema 4.1.1**.

Consideremos agora $D_F\langle 1,-c\rangle(D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle)$. Se esse subgrupo de $F^\times$ for igual a $D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle$ teremos que $D_F\langle 1,-c\rangle \subset D_F\langle 1,-d\rangle$ (também $D_F\langle 1,-c\rangle \subset D_F\langle 1,-e\rangle$), o

que contradiz item (2) do **Teorema 4.1.1** pois d (também e) não está presente na decomposição de c.

Caso esse subgrupo seja igual a um dos subgrupos de $F^\times$ com índice 2, teremos também uma contradição com o item (2) do **Teorema 4.1.1**. Logo a única possibilidade é $D_F\langle 1,-c\rangle(D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle) = F^\times$. Dessa forma $(D_F\langle 1,-c\rangle : D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle) = (F^\times : D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle) = 4$.

Procurando por uma contradição vamos supor que os subgrupos $D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle$ e $D_F\langle 1,-c\rangle \cap D_F\langle 1,-e\rangle$ são comparáveis. Assumimos, sem perda de generalidade, que $D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle \subset D_F\langle 1,-c\rangle \cap D_F\langle 1,-e\rangle$. Logo $D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle = D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle$, implicando $2 = (D_F\langle 1,-c\rangle : D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle) = (D_F\langle 1,-c\rangle : D_F\langle 1,-c\rangle \cap D_F\langle 1,-d\rangle \cap D_F\langle 1,-e\rangle) = 4$. Resultando na contradição desejada.

A igualdade $D_K\langle 1,-d\rangle D_K\langle 1,-e\rangle = K^\times$ é imediata. De fato, como $Q_F(c) = Q_F(d)$ e $cd \notin R(F)$, $D_K\langle 1,-d\rangle \neq D_K\langle 1,-e\rangle$, pelo **Lema 3.2.10**. De $(F^\times : D_F\langle 1,-d\rangle) = 2$ temos a igualdade.

Para cada $z \in K^\times$ existem, pela primeira parte do lema, $x \in D_K\langle 1,-d\rangle$, e $y \in D_K\langle 1,-e\rangle$ tais que $N(z) = N(x)N(y) = N(xy)$. Portanto existe $u \in K^\times$ tal que $z = (\sigma(u)/u)xy = N(u)u^{-2}xy$. Como $N(u) \in D_F\langle 1,-c\rangle$, pelo que demonstramos no início desta parte do lema, existem $a \in D_F\langle 1,-d\rangle \cap D_F\langle 1,-c\rangle$ e $b \in D_F\langle 1,-e\rangle \cap D_F\langle 1,-c\rangle$ tais que $N(u) = ab$. Logo $a \in D_K\langle 1,-d\rangle$ e $b \in D_K\langle 1,-e\rangle$ e assim $z = (ax)(byu^{-2}) \in D_K\langle 1,-d\rangle D_K\langle 1,-e\rangle$, como queríamos. □

(4) Seja $e \in F_\lambda \smallsetminus R(F)$. Caso $e = dr$, para algum $r \in R(F)$, como $R(F) \subset R(K)$ trivialmente $Q_K(e) = Q_K(d)$. Também se tivermos d, $e \in c_\lambda R(F)$, então $Q_K(d) = \{0\} = Q_K(e)$, pois pelo item 4 do **Teorema 4.1.1**, $c_\lambda R(F) \subset R(K)$.

Consideremos finalmente o caso não trivial, $ed \notin R(F)$ e se $\lambda \in I$, d, $e \notin c_\lambda R(F)$. Nesse caso pelo **Lema 4.1.6** acima, $D_K\langle 1,-d\rangle D_K\langle 1,-e\rangle = K^\times$. Logo $(K^\times : D_K\langle 1,-e\rangle) = (D_K\langle 1,-d\rangle : D_K\langle 1,-d\rangle \cap D_K\langle 1,-e\rangle)$.

Por outro lado, as condições impostas a e fazem com que $de \in F_\lambda \smallsetminus R(F)$. Logo os itens (1) e (2) aplicam-se a de. Vamos apresentar nas tabelas abaixo as possibilidades.

λ	$(K^\times : D_K\langle 1,-d\rangle) = (K^\times : D_K\langle 1,-e\rangle)$	$(K^\times : D_K\langle 1,-d\rangle \cap D_K\langle 1,-e\rangle)$
$\lambda \in I$	2	4
$\lambda \notin I$	4	16

λ	$(K^\times : D_K\langle 1,-de\rangle)$
$\lambda \in I$	2
$\lambda \notin I$	4

Temos então que

$$|Q_K(d) \cap Q_K(e)| = (D_K\langle 1,-de\rangle : D_K\langle 1,-d\rangle \cap D_K\langle 1,-e\rangle) = \begin{cases} 2 & \text{se } \lambda \in I \\ 4 & \text{se } \lambda \notin I \end{cases}$$

Portanto $|Q_K(d)| = |Q_K(e)| = |Q_K(d) \cap Q_K(e)|$ nos dois casos acima. Resulta então que $Q_K(d) = Q_K(e)$, como afirmado. □

Vamos a seguir demonstrar o análogo do **Teorema 3.2.14** do capítulo anterior.

Teorema 4.1.7. *Seja $c = \prod_{i\in I} c_i$ em $F^\times$, onde $I \subset \Lambda$ e $c_i \in F_i \smallsetminus R(F)$, para todo $i \in I$, como na* ***Observação 4.1.3****. Considere ainda $K = F(\sqrt{c})$. Desta forma, temos que:*

1. *Para todo $d = \prod_{j\in J} d_j$ em $F^\times$, onde $J \subset \Lambda$ e $d_j \in F_j \smallsetminus R(F)$, para todo $j \in J$ temos que*

$$Q_K(d) = \bigoplus_{j\in J_1\cup C_1} Q_K(d_j),$$

   onde J_1 e C_1 definidos na ***Observação 4.1.3****.*

2. *Mais geralmente, dado $J \subset \Lambda$ e $d_j \in F_j \smallsetminus R(F)$, para todo $j \in J$, e se $j \in I$, então $d_j \notin c_j R(F)$, temos que*

$$\sum_{j\in J} Q_K(d_j) = \bigoplus_{j\in J} Q_K(d_j).$$

3. *Para todo d como no item 1 acima vale*

$$D_K\langle 1, -d\rangle = \bigcap_{j\in J} D_K\langle 1, -d_j\rangle$$

Demonstração. (1) Dado $x \in K^\times$ temos em ${}_2\mathrm{Br}(K)$ que

$$(x, d)_K = \sum_{j\in J_1\cup C_1} (x, d_j)_K \in \sum_{j\in J_1\cup C_1} Q_K(d_j).$$

Logo

$$Q_K(d) \subset \sum_{j\in J_1\cup C_1} Q_K(d_j).$$

Como, pela **Proposição 4.1.4**, $\dim_{\mathbb{F}_2} K^\times/D_K\langle 1, -d\rangle = 2\#J_1 + \#C_1$, temos que $\dim_{\mathbb{F}_2} Q_K(d)$ é também igual a $2\#J_1 + \#C_1$.

Por outro lado $\dim_{\mathbb{F}_2} \sum_{j\in J_1\cup C_1} Q_K(d_j) \leq \sum_{j\in J_1\cup C_1} \dim_{\mathbb{F}_2} Q_K(d_j) = 2\#J_1 + \#C_1$. Desta forma temos uma igualdade entre $\dim_{\mathbb{F}_2} Q_K(d)$ e $\dim_{\mathbb{F}_2} \sum_{j\in J_1\cup C_1} Q_K(d_j)$, o que implica que $Q_K(d) = \sum_{j\in J_1\cup C_1} Q_K(d_j)$.

Observe agora que temos naturalmente um homomorfismo sobrejetor

$$\prod_{j\in J_1\cup C_1} Q_K(d_j) \to \sum_{j\in J_1\cup C_1} Q_K(d_j).$$

Vimos acima que os dois espaços tem a mesma dimensão. Logo esse homomorfismo é um isomorfismo e obtemos a validade do item (1)

$$Q_K(d) = \sum_{j\in J_1\cup C_1} Q_K(d_j) = \bigoplus_{j\in J_1\cup C_1} Q_K(d_j).$$

(2) Basta aplicarmos o item (1) a $d = \prod_{j\in J} d_j$. Observe que a escolha dos elementos d_j implica que $C_2 = \emptyset$ e assim $J = J_1 \cup C_1$.

(3) Vamos inicialmente destacar que as considerações acima sobre dimensão implicam que $Q_K(d_\lambda) \cap Q_K(d_j) = \{\,0\,\}$ sempre que $\lambda \neq j$, pois o item (1) aplicando-se a qualquer $d \in K^\times$, aplica-se também a $d = d_\lambda d_j$. Resulta disso que $D_K\langle 1, -d_\lambda\rangle \cap D_K\langle 1, -d_j\rangle = D_K\langle 1, -d_\lambda d_j\rangle$, sempre que $\lambda \neq j$. Fica assim demonstrado o item (3) para o caso de $d = d_\lambda d_j$ ter dois fatores ($\#J_1 + \#C_1 = 2$). Vamos demonstrar o caso geral por indução sobre $\#J_1 + \#C_1$. Observe que no item (3) basta tomarmos $j \in J_1 \cup C_1$, pois $D_K\langle 1, -d_j\rangle = K^\times$, para todo $j \in C_2$ ($d_j \in R(K) \cap F$, para $j \in C_2$).

Para $\lambda \in J_1 \cup C_1$ seja

$$d^{(\lambda)} = \prod_{\substack{j\in J_1\cup C_1\\ j\neq\lambda}} d_j.$$

Pelo que vimos acima, temos

$$Q_K(d^{(\lambda)}) = \bigoplus_{\substack{j\in J_1\cup C_1\\ j\neq\lambda}} Q_K(d_j) \quad \text{e} \quad Q_K(d) = \bigoplus_{j\in J_1\cup C_1} Q_K(d_j).$$

Logo $Q_K(d^{(\lambda)}) \cap Q_K(d_\lambda) = \{\,0\,\}$. Tendo-se em conta que $d = d^{(\lambda)}d_\lambda$ vamos obter $D_K\langle 1, -d\rangle = D_K\langle 1, -d^{(\lambda)}\rangle \cap D_K\langle 1, -d_\lambda\rangle$. Assim, pela hipótese de indução

$$D_K\langle 1, -d\rangle = \left(\bigcap_{\substack{j\in J_1\cup C_1\\ j\neq\lambda}} D_K\langle 1, -d_j\rangle\right) \cap D_K\langle 1, -d_\lambda\rangle = \bigcap_{j\in J} D_K\langle 1, -d_j\rangle$$

como queríamos. □

Vejamos agora um lema que já apareceu implicitamente na literatura inclusive em [**L**]. Vamos apresentá-lo aqui em uma formulação que é conveniente para o trabalho.

Lema 4.1.8. *Consideremos uma extensão $K = F(\sqrt{c})$ com $c \in F^\times \smallsetminus (F^\times)^2$ de um corpo F. Seja*

$$B_o = \sum_{a\in F^\times} Q_K(a)$$

o subgrupo de ${}_2\mathrm{Br}(K)$ gerado pela álgebras de quatérnios da forma $(x, a)_K$, com $x \in K^\times$ e $a \in F^\times$. Temos que $B_o = {}_2\mathrm{Br}(K)$.

Demonstração. Pelo famoso resultado de Merkurjev basta mostrarmos que para toda álgebra de quatérnios $(u,v)_K$ sobre K, $u, v \in K^\times$ sua classe satisfaz $(u,v)_K \in B_o$. Como $\dim_F K = 2$, temos que o conjunto $\{u,v\}$ pode ser linearmente dependente ou independente sobre F. Caso seja linearmente dependente, temos que $v = au$ para algum $a \in F$ e consequentemente $(u,v)_K = (u,au)_K = (u,a)_K + (u,u)_K = (u,a)_K + (u,-1)_K$, pois $(u,u)_K \simeq (u,-1)_K$. Logo $(u,v)_K \in B_o$.

Suponhamos agora que o conjunto $\{u,v\}$ seja linearmente independente sobre F. Logo $\{u,v\}$ é uma base de K sobre F e portanto existem $a, b \in F$ tais que $au + bv = 1$. Temos então que $(au,bv)_K = 0$ e desenvolvendo obteremos que $0 = (u,v)_K + (u,b)_K + (a,v)_K + (a,b)_K$. Portanto, $(u,v)_K = (u,b)_K + (a,v)_K + (a,b)_K \in B_o$, ficando assim demonstrado o lema. □

Teorema 4.1.9. *Seja F com base distinguida e sejam F_λ, $\lambda = 1,\dots,m$, os subgrupos correspondentes a partição principal, como introduzidos anteriormente. Se $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$, para todo $\lambda = 1,\dots,m$, então $\operatorname{cd} G_2(F) = 2$.*

Para F com $\operatorname{cd} G_2(F) = 2$ todo elemento de F é uma soma de no máximo 4 quadrados.

Demonstração. Assumimos agora que $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$, para todo $\lambda = 1,\dots,m$. Dados $a = \prod_{i\in I} a_i$ e $b = \prod_{j\in J} b_j$ em $F^\times$, onde $I, J \subset \Lambda$ e $a_i \in F_i \smallsetminus R(F)$, para todo $i \in I$, e $b_j \in F_j \smallsetminus R(F)$, para todo $j \in J$, respectivamente, sejam I_1, J_1 e C_1 como na **Observação 4.1.3**. Recordemos que $C_2 = \{\, \beta \in I \cap J \mid a_\beta \in b_\beta R(F) \,\}$ é o conjunto de índices dos "fatores em comum" nas decomposições de a e b.

Afirmamos que exitem $x, y \in F^\times$ cujas decomposições não tem "fator em comum" e $(a,b)_F \simeq (x,y)_F$.

Observe inicialmente que

$$(a,b)_F \simeq \sum_{\alpha\in C_1} (a_\alpha, b_\alpha)_F + \sum_{\beta\in C_2} (a_\beta, b_\beta)_F,$$

pois $(a_i,b_j)_F = 0$ sempre que $i, j \notin I \cap J = C_1 \cup C_2$, pois neste caso $a_i \in F_i$ e $b_j \in F_j$, com $i \neq j$, onde F_i, F_j são grupos da partição principal da base de distinguida de F.

Ainda, para todo $\beta \in C_2$, $(a_\beta, b_\beta)_F \simeq (a_\beta, a_\beta)_F$ pois $a_\beta \in b_\beta R(F)$. Para todo $\beta \in C_2$ tal que $(a_\beta,a_\beta)_F \neq 0$, temos que $a_\beta \notin D_F\langle 1, -a_\beta\rangle$. Dessa forma, como $\dim_{\mathbb{F}_2} F_\beta/R(F) > 1$ e $(F_\beta : D_F\langle 1,-a_\beta\rangle \cap F_\beta) = 2$ podemos tomar $c_\beta \in a_\beta(D_F\langle 1,-a_\beta\rangle \cap F_\beta)$ com $c_\beta \notin a_\beta R(F)$. (Não pode acontecer $F_\beta \smallsetminus a_\beta R(F) \subset D_F\langle 1,-a_\beta\rangle \cap F_\beta = F_\beta \smallsetminus a_\beta(D_F\langle 1,-a_\beta\rangle \cap F_\beta)$, pois isso implicaria $a_\beta(D_F\langle 1,-a_\beta\rangle \cap F_\beta) \subset a_\beta R(F)$ e como $R(F) \subset D_F\langle 1,-a_\beta\rangle \cap F_\beta$ resultaria em $R(F) = D_F\langle 1,-a_\beta\rangle \cap F_\beta$ e assim $(F_\beta : R(F)) = 2$, contra hipótese.) (Caso $(a_\beta,a_\beta)_F = 0 \in {}_2Br(F)$, tomamos $c_\beta = b_\beta$). Com esse escolha de c_β vamos ter $(a_\beta;c_\beta)_F = (a_\beta;a_\beta)_F = (a_\beta;b_\beta)_F$ em ${}_2Br(F)$, para todo $\beta \in C_2$ tal que $(a_\beta,b_\beta)_F \neq 0$.

Tomando-se $C_3 = \{\beta \in C_2;\ (a_\beta,b_\beta)_F \neq 0 \in {}_2Br(F)\}$,

$$x = \prod_{i\in I_1} a_i \prod_{\alpha\in C_1} a_\alpha \prod_{\beta\in C_3} a_\beta$$

$$y = \prod_{j\in J_1} b_j \prod_{\alpha\in C_1} b_\alpha \prod_{\beta\in C_3} c_\beta$$

vamos, por construção, ter que

$$(a,b)_F = (x,y)_F \text{ em } {}_2Br(F).$$

Logo $(a,b)_F \simeq (x,y)_F$ e x, y não tem "fatores em comum", comprovando a afirmação. Resulta do isomorfismo entre as álgebras que $\langle\langle a,b\rangle\rangle \simeq \langle\langle x,y\rangle\rangle$ e portanto $D_F(\langle\langle -a,-b\rangle\rangle) = D_F(\langle\langle -x,-y\rangle\rangle)$.

Pelo item (3) do **Teorema 4.1.1** temos que $D_F\langle 1,-x\rangle D_F\langle 1,-y\rangle = F^\times$. Logo $D_F(\langle\langle -a,-b\rangle\rangle) = F^\times$. Isto é, para todo para a, $b \in F^\times$ a forma $\langle\langle -a,-b\rangle\rangle$ é universal. Resulta disso que toda 3-forma de Pfister é isotrópica, portanto hiperbólica, implicando $I^3F = 0$, pelo [**L**]. Novamente pelos resultados de Voevodsky ([**OVV**], [**V1**],[**V2**]) podemos concluir que $H^3(F) = 0$ e portanto $\operatorname{cd} G_2(F) = 2$. Observe que $\operatorname{cd} G_2(F) \neq 1$, pois caso $\operatorname{cd} G_2(F)$ fosse igual a 1, teríamos $H^2(F) \simeq {}_2Br(F) = 0$ implicando toda 1-forma de Pfister universal, isto é, $R(F) = F^\times$, contrariando a hipótese $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$.

Finalmente, se $\langle 1,1,1,1\rangle$ for anisotrópica, será universal, pois acabamos de observar que toda 2-forma de Pfister anisotrópica é universal. Como toda forma quadrática isotrópica é universal, podemos concluir que $\langle 1,1,1,1\rangle$ é universal em qualquer caso. Logo todo elemento de F é soma de no máximo 4 quadrados. □

Corolário 4.1.10. *Sejam F, c, e K como no **Teorema 4.1.7** e assuma que $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$, para todo $\lambda \in I$. Considere $d = \prod_{\lambda\in\Lambda} d_\lambda \in F^\times$, onde $d_\lambda \in F_\lambda \smallsetminus R(F)$ para todo $\lambda \in \Lambda$, e $d_\lambda \notin c_\lambda R(F)$. Nestas condições temos*

$$Q_K(d) = \bigoplus_{\lambda\in\Lambda} Q_K(d_\lambda) = {}_2\mathrm{Br}(K).$$

Demonstração. Para esse d temos $C_2 = \emptyset$ e $C_1 = I$. Logo

$$Q_K(d) = \bigoplus_{\lambda\in\Lambda} Q_K(d_\lambda) = {}_2\mathrm{Br}(K),$$

onde a segunda igualdade é dada pelo **Teorema 3.2.14**.

□

Proposição 4.1.11. *Seja $c = \prod_{i\in I} c_i$ em $F^\times$, onde $I \subset \Lambda$ e $c_i \in F_i \smallsetminus R(F)$, para todo $i \in I$.*

Assumiremos ainda que $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$, para todo $\lambda = 1,\ldots,m$ e $e = \prod_{\lambda\in\Lambda} e_\lambda \in F^\times$, onde $e_\lambda \in F_\lambda \smallsetminus R(F)$ para todo $\lambda \in \Lambda$ e, se $\lambda \in I$, escolhemos $e_\lambda \notin c_\lambda R(F)$.

Sejam ainda $K = F(\sqrt{c})$, $G = Gal(K/F) = \{1,\sigma\}$ e $N : K \to F$ a função norma. Nessas condições temos

$${}_2\mathrm{Br}(K)^G = \mathrm{Im}\ \mathrm{Res} \oplus \left(\bigoplus_{i\in I} Q_K(e_i)\right) \quad e \quad \mathrm{Im}\,\mathrm{Res} = \left(\bigoplus_{\substack{\lambda\in\Lambda\\ \lambda\notin I}} Q_K(e_\lambda)\right)^G = \bigoplus_{\substack{\lambda\in\Lambda\\ \lambda\notin I}} Q_K(e_\lambda)^G.$$

Demonstração. Para todo $x \in F^\times$ e $y \in K^\times$ temos que $(x,y)_K^\sigma = (x,\sigma(y))_K$. Desta forma, $\sigma(Q_K(x)) = Q_K(x)$ e $Q_K(x)$ é um G-módulo. Sabemos pelo **Corolário 4.1.10** que

$$Q_K(e) = \bigoplus_{\lambda\in\Lambda} Q_K(e_\lambda) = {}_2\mathrm{Br}(K).$$

Logo

$${}_2\mathrm{Br}(K)^G = Q_K(e)^G = \bigoplus_{\lambda\in\Lambda} Q_K(e_\lambda)^G \tag{4.1.7}$$

Observe agora que para todo $i \in I,\ |Q_K(e_i)| = 2$, pelo item (2) da **Proposição 4.1.5**. Logo

$$Q_K(e_i)^G = Q_K(e_i), \tag{4.1.8}$$

para todo $i \in I$.

Sabemos pelo item (3) da **Proposição 4.1.5** que $D_K\langle 1,-e_\lambda\rangle \cap F = D_F\langle 1,-e_\lambda\rangle$. Pelos Teoremas do Isomorfismo para grupos, temos que

$$F^\times D_K\langle 1,-e_\lambda\rangle / D_K\langle 1,-e_\lambda\rangle \cong F^\times / \left(F^\times \cap D_K\langle 1,-e_\lambda\rangle\right) \cong F^\times / D_F\langle 1,-e_\lambda\rangle.$$

Portanto $(F^\times D_K\langle 1,-e_\lambda\rangle : D_K\langle 1,-e_\lambda\rangle) = (F^\times : D_F\langle 1,-e_\lambda\rangle) = 2$ e podemos então tomar $u \in K \smallsetminus F^\times D_K\langle 1,-e_\lambda\rangle$. Logo $N(u) \notin D_K\langle 1,-e_\lambda\rangle$, pelo Princípio da Norma. Logo, $(u,e_\lambda)_K \in Q_K(e_\lambda)$ e

$$(u,e_\lambda)_K + (u,e_\lambda)_K^\sigma \simeq (u,e_\lambda)_K + (\sigma(u),e_\lambda)_K =$$
$$(N(u),e_\lambda)_K \simeq \mathrm{Res}((N(u),e_\lambda)_F) \in \mathrm{Im}\,\mathrm{Res}$$

e $(u,e_\lambda)_K + (u,e_\lambda)_K^\sigma \neq 0 \in {}_2Br(K)$, pois $(N(u),e_\lambda)_F \neq 0 \in {}_2Br(F)$, pela escolha de u. Mas isso mostra que $(u,e_\lambda)_K \neq (u,e_\lambda)_K^\sigma$. Como $|Q_K(e_\lambda)| = 4$, pelo item (2) da **Proposição 4.1.5**, concluímos que $Q_K(e_\lambda) = \{\,0,(u,e_\lambda)_K,(u,e_\lambda)_K^\sigma,(N(u),e_\lambda)_K\,\}$ e assim $Q_K(e_\lambda)^G = \{\,0,(N(u),e_\lambda)_K\} = \mathrm{Res}(Q_F(e_\lambda))$. Desta maneira, temos que

$$\left(\bigoplus_{\substack{\lambda\in\Lambda\\ \lambda\notin I}} Q_K(e_\lambda)\right)^G \subset \mathrm{Im}\,\mathrm{Res}\,.$$

Por outro lado, como ${}_2\mathrm{Br}F = \bigoplus_{\lambda\in\Lambda} Q_F(e_\lambda)$ temos que

$$\mathrm{Im}\,\mathrm{Res} = \bigoplus_{\lambda\in\Lambda} \mathrm{Res}(Q_F(e_\lambda)) \subset \left(\bigoplus_{\substack{\lambda\in\Lambda\\ \lambda\notin I}} G_K(e_\lambda)\right)^G,$$

pois pelo ítem 3 da **Proposição 4.1.5** $F \subseteq D_K\langle 1,-e_i\rangle$ e assim $\mathrm{Res}(Q_F(e_i)) = \mathrm{Res}(Q_F(c_i)) = 0$, para todo $i \in I$. Juntando-se as duas inclusões obtemos

$$\mathrm{Im}\,\mathrm{Res} = \left(\bigoplus_{\substack{\lambda\in\Lambda\\ \lambda\notin I}} Q_K(e_\lambda)\right)^G$$

que juntamente com as equações (4.1.7) e (4.1.8) implicam o resultado. □

Proposição 4.1.12. *Seja F com base distinguida completa tal que $\dim_{\mathbb{F}_2} F_j/R(F) > 1$, para algum $j \in I$. Para cada $\lambda \in \Lambda$ seja $\{a_{\lambda,1}, \ldots, a_{\lambda,r_\lambda}\}$ uma base de F_λ módulo $R(F)$. Sabemos então que $\bigcup_{\lambda=1}^{m} \{a_{\lambda,1}, \ldots, a_{\lambda,r_\lambda}\}$ é uma base distinguida de F e que cada base distinguida de F pode ser decomposta nessa forma.*

*Seja agora $K = F(\sqrt{c})$ onde $c = \prod_{i\in I} c_i$ com $I \subset \Lambda$ e $c_i \in F_i \smallsetminus R(F)$, para todo $i \in I$, como na **Proposição 4.1.11** acima. Seja*

$$R_o = \bigcap_{\substack{\lambda\in\Lambda \\ j=1,\ldots,r_\lambda}} D_K\langle 1, -a_{\lambda,j}\rangle.$$

*Então $R_o \neq R(K)$, diferentemente do que ocorre no caso $F(\sqrt{r})$ com $r \in R(F)$, conforme visto no **Teorema 2.2.4**.*

Demonstração. Pelo item (4) da **Teorema 4.1.1** sabemos que $\dim_{\mathbb{F}_2} (R(K) \cap F)/R(F) = \#I$.

Vejamos agora $R_o \cap F$. Para isso observe que pelo item (3) da **Proposição 4.1.5** temos $D_K\langle 1, -a_{\lambda,j}\rangle \cap F = F^\times$ para todo $\lambda \in I$ e $j = 1, \ldots, r_\lambda$.

Por outro lado, $D_K\langle 1, -a_{\lambda,j}\rangle \cap F = D_F\langle 1, -a_{\lambda,j}\rangle$ para todo $\lambda \notin I$ e $j = 1, \ldots, r_\lambda$, pelo mesmo item (3) mencionado. Logo

$$R_o \cap F = \bigcap_{\substack{\lambda\notin I \\ j=1,\ldots,r_\lambda}} D_F\langle 1, -a_{\lambda,j}\rangle.$$

Pelo item 2(a) do **Teorema 3.2.11** temos $F_i \subset D_F\langle 1, -a_{\lambda,j}\rangle$, para todo $\lambda \notin I$ e $j = 1, \ldots, r_\lambda$. Dessa forma $F_i \subset R_o \cap F$, para todo $i \in I$ e assim $\dim_{\mathbb{F}_2} (R_o \cap F)/R(F) \geq \sum_{i\in I} r_i$. Como para $r_i \geq 1$ para todo $i \in I$ e existe $j \in I$ com $r_j > 1$ temos que $\dim_{\mathbb{F}_2} R_o \cap F/R(F) > \#I = \dim_{\mathbb{F}_2} R(K) \cap F/R(F)$. Logo $R_o \neq R(F)$, como afirmado. □

Nos últimos resultados apresentados, usamos como hipótese que $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$, para algum $\lambda \in \Lambda$.

Vamos agora apresentar alguns resultados onde assumiremos que $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$, para algum $\lambda = 1, \ldots, m$.

4.1.1 O Caso formalmente real

Nesta parte do trabalho vamos ver que um corpo com base distinguida ou bem corresponde ao caso $\operatorname{cd} G_2(F) = 2$ que acabamos de ver ou então corresponde a um corpo formalmente real com propriedades muito fortes. Vamos iniciar com um resultado técnico.

Proposição 4.1.13. *Sejam F um corpo com base distinguida completa e F_λ, $\lambda \in \Lambda = \{1, \ldots, m\}$ os subgrupos ligados a partição principal. Suponha que exista $\lambda \in \Lambda$, $1 \leq \lambda \leq m$, tal que $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$. Então para $c \in F_\lambda \smallsetminus R(F)$ a aplicação $\chi_c \cup \_ : H^2(F) \to H^3(F)$ não pode ser nula.*

Em particular, $\operatorname{cd} G_2(F) \geq 3$ e $c \notin D_F\langle 1, 1, 1, 1\rangle$.

Demonstração. Buscando por uma contradição seja $c \in F_\lambda \smallsetminus R(F)$ e suponhamos que a aplicação $\chi_c \cup \_ : H^2(F) \to H^3(F)$ seja nula. Aplicando-se então a sequência exata

$$\cdots \to H^1(F) \to H^1(K) \to H^1(F) \stackrel{\chi_a \cup \_}{\to} H^2(F) \to H^2(K) \to H^2(F) \stackrel{\chi_a \cup \_}{\to} H^3(F) \to \cdots,$$

[**A**], à extensão $K = F(\sqrt{c})$ temos sequência exata

$$\cdots \to H^1(F) \stackrel{\chi_c \cup}{\longrightarrow} H^2(F) \stackrel{\text{Res}}{\longrightarrow} H^2(K) \stackrel{\text{Cor}}{\longrightarrow} H^2(F) \stackrel{\chi_c \cup}{\longrightarrow} H^3(F) \to \cdots.$$

Nossa hipótese sobre a nulidade de $\chi_c \cup \_$ implica que Cor é sobrejetiva. Mais ainda, tem núcleo =ImRes.

Por outro lado Res tem núcleo $= \chi_c \cup (H^1(F)) = Q_F(c)$. Deduzimos então da sequência exata acima que $\dim_{\mathbb{F}_2} H^2(K) = \dim_{\mathbb{F}_2} H^2(F) + (\dim_{\mathbb{F}_2} H^2(F) - \dim_{\mathbb{F}_2} Q_F(c)) = 2 \dim_{\mathbb{F}_2} {}_2\text{Br}(F) - 1$, pois $Q_F(c)$ tem ordem 2 em $F^\times$, pois $c \in F_\lambda$.

Vamos aplicar a **Proposição 4.1.5** na extensão $K = F(\sqrt{c})$. Para todo $j \neq \lambda$ e todo $d_j \in F_j \smallsetminus R(F)$ temos $\dim_{\mathbb{F}_2} Q_K(d_j) = 2$, pelo item (2) da referida proposição. Temos também, pelo item (4) que $Q_K(e) = Q_K(d_j)$ para todo $e \in F_j \smallsetminus R(F)$.

Por outro lado, como $\dim_{\mathbb{F}_2} F_\lambda / R(F) = 1$, não vai ocorrer a possibilidade $j = \lambda$ e $d_\lambda \notin cR(F)$.

Seja $d = \prod_{j \in J} d_j$ em $F^\times$, com $J \subset \Lambda$ e $d_j \in F_j \smallsetminus R(F)$ para todo $j \in J$, um elemento genérico de $F^\times$. Com a notação da **Observação 4.1.3** temos $I = \{\lambda\}$ e as seguintes alternativas:

$$\begin{array}{lll} J_1 = J,\ C_1 = \emptyset = C_2, & \text{se} & \lambda \notin J \\ J_1 = J \smallsetminus \{\lambda\},\ C_1 = \emptyset,\ C_2 = \{\lambda\} & \text{se} & \lambda \in J \end{array}.$$

Mais ainda, se $\lambda \in J$, então pelo item (4) do **Teorema 4.1.1**, $d_\lambda \in R(K)$ e $Q_K(d_\lambda) = \{0\}$. Podemos então concluir que para todo $d \in F^\times$,

$$Q_K(d) = \bigoplus_{\substack{j \in J \\ j \neq \lambda}} Q_K(d_j) \subset \bigoplus_{\substack{j \in \Lambda \\ j \neq \lambda}} Q_K(e_j),$$

onde tomamos $e_j \in F_j \smallsetminus R(F)$ para todo $j \in \Lambda$, $j \neq \lambda$.

Logo, com a notação do **Lema 4.1.8**, temos

$${}_2\text{Br}(K) = B_o \subset \bigoplus_{\substack{j \in \Lambda \\ j \neq \lambda}} Q_K(e_j).$$

Ou melhor

$${}_2\text{Br}(K) = \bigoplus_{\substack{j \in \Lambda \\ j \neq \lambda}} Q_K(d_j).$$

A igualdade acima implica que $\dim_{\mathbb{F}_2} {}_2\text{Br}(K) = 2(m-1)$, pois pelo **Teorema 4.1.5** $\dim_{\mathbb{F}_2} Q_K(d_j) = 2$ para todo j.

Combinado os dois cálculos feitos de $\dim_{\mathbb{F}_2} {}_2\mathrm{Br}(K)$ chegamos a contradição $2m-2=2m-1$. Logo a aplicação $\chi_c \cup \_$ não pode ser nula, conforme afirmado.

A primeira das duas últimas afirmações da proposição é clara, pois se $\operatorname{cd} G_2(F) = 2$, então $H^3(F) = 0$, implicando na nulidade de $\chi_c \cup \_$. Vejamos agora a última afirmação, isto é, se $c \in D_F\langle 1,1,1,1\rangle$, então $\chi_c \cup \_$ é nula, contradizendo o que acabamos de demonstrar.

Recordemos inicialmente que a aplicação $\langle 1,-a\rangle \otimes \langle 1,-b\rangle \mapsto (a,b)_F$ de I^2F em ${}_2\mathrm{Br}(F)$ induz, conforme Merkurjev, um isomorfismo $I^2F/I^3(F) \cong {}_2\mathrm{Br}(F)$. No nosso caso, todo elemento de ${}_2\mathrm{Br}(F)$ é uma soma de álgebras de quatérnios, isto é, todo elemento de $H^2(F) \cong {}_2\mathrm{Br}(F)$ é da forma $(a,b)_F$. Recordemos que $H^1(G_2(F))$ pode ser identificado com o grupo dos homomorfismos contínuos $\{\, \chi : G_2(F) \to \mathbb{Z}/2\mathbb{Z} \,\}$. Para cada $d \in F^\times$ seja $\chi_d \in H^1(G_2(F))$ o homomorfismo cujo núcleo é $G_2(F(\sqrt{d}))$. Temos então a identificação canônica entre $F^\times/(F^\times)^2$ e $H^1(G_2(F))$ que associa à classe $d(F^\times)^2$ o homomorfismo χ_d. Prosseguindo nessa linha de identificações vamos identificar $(a,b)_F$ com o *produto cup* $\chi_a \cup \chi_b$, veja por exemplo [**Se**], páginas 204-207.

Voltando a demonstração do resultado, dados $a,\, b \in F^\times$ e tomando-se a decomposição $a = \prod_{i\in I} a_i$ e $b = \prod_{j\in J} b_j$, onde $I,\, J \subset \Lambda$ e $a_i \in F_i \smallsetminus R(F)$, para todo $i \in I$, e $b_j \in F_j \smallsetminus R(F)$, para todo $j \in J$, respectivamente, como na **Observação 4.1.3** temos que

$$(a,b)_F \simeq \sum_{\alpha\in C_1} (a_\alpha, b_\alpha)_F + \sum_{\beta\in C_2} (a_\beta, a_\beta)_F,$$

pois $(a_\beta, b_\beta)_F \simeq (a_\beta, a_\beta)_F$ no caso $a_\beta \in b_\beta R(F)$. Usando a notação do "cup" temos

$$\chi_a \cup \chi_b = \sum_{\alpha\in C_1} \chi_{a_\alpha} \cup \chi_{b_\alpha} + \sum_{\beta\in C_2} \chi_{a_\beta} \cup \chi_{a_\beta}.$$

Como o produto "cup" é associativo e distributivo em relação a soma temos que

$$\chi_a \cup \chi_b \cup \chi_c = \sum_{\alpha\in C_1} \chi_{a_\alpha} \cup \chi_{b_\alpha} \cup \chi_c + \sum_{\beta\in C_2} \chi_{a_\beta} \cup \chi_{a_\beta} \cup \chi_c.$$

Recordemos agora que para todo $\alpha \in C_1$ e todo $\beta \in C_2$ temos $\chi_{a_\alpha} \cup \chi_{b_\alpha} \cup \chi_c = 0$ e $\chi_{a_\beta} \cup \chi_{a_\beta} \cup \chi_c = 0$ a menos que $\alpha = \lambda$, ou $\beta = \lambda$. Como $a_\alpha \notin b_\alpha R(F)$, para todo $\alpha \in C_1$ e $(F_\lambda : R(F)) = 2$, vamos ter que $\alpha \neq \lambda$ para todo $\alpha \in C_1$. Mais ainda, no caso $\beta = \lambda$ podemos também assumir que $a_\beta = c$. Concluímos assim que para todo $z \in H^2(F)$ vale

$$z \cup \chi_c = 0 \qquad \text{ou} \qquad z \cup \chi_c = \chi_c \cup \chi_c \cup \chi_c. \tag{4.1.9}$$

Observe a seguir que para todo $c \in D_F\langle 1,1,1,1\rangle$ a 3-forma de Pfister $\langle 1,-c\rangle \otimes \langle 1,-c\rangle \otimes \langle 1,-c\rangle$ é isotrópica e portanto hiperbólica. Logo sua classe no anel de Witt de F é nula. Aplicando-se os resultados de Voevodsky, [**OVV**], [**V1**], [**V2**], ou mesmo por [**A**], de que aplicação $e_3 : I^3F/I^4F \to H^3(K)$, cuja ação estende

$$e_3(\langle 1,-a_1\rangle \otimes \langle 1,-a_2\rangle \otimes \langle 1,-a_3\rangle) = \chi_{a_1} \cup \chi_{a_2} \cup \chi_{a_3}, \quad \text{para quaisquer } \ a_1,\, a_2,\, a_3 \in F^\times,$$

está bem definida e é um isomorfismo, concluímos que $\chi_c \cup \chi_c \cup \chi_c = e_3(\langle 1,-c\rangle \otimes \langle 1,-c\rangle \otimes \langle 1,-c\rangle) = 0$. Portanto, devido a equação (4.1.9) temos que a aplicação $\chi_c \cup \_$ é nula, contradizendo a primeira parte da demonstração. □

Vamos agora aprofundar o estudo dos corpos onde ocorre $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$, para algum $\lambda = 1, \ldots, m$. Antes porém, a última afirmação do resultado (4.1.13) sugere o lema técnico a seguir que será usado várias vezes nas demonstrações.

Lema 4.1.14. *Seja F com base distinguida completa e os subgrupos F_λ, $\lambda = 1, \ldots, m$, correspondentes a partição principal como introduzido anteriormente. Para todo $1 \leq \lambda \leq m$ e todo $c \in F_\lambda \smallsetminus R(F)$ temos que uma das seguintes possibilidades ocorre: c é uma soma de no máximo quatro quadrados ou $D_F\langle 1, -c\rangle + D_F\langle 1, -c\rangle \subset D_F\langle 1, -c\rangle$.*

Demonstração. Dado $c \in F_\lambda \smallsetminus R(F)$, caso $c \in D_F\langle 1, 1\rangle$ o resultado vale. Assumindo-se $c \notin D_F\langle 1, 1\rangle$ temos que a 2-forma forma de Phister $\langle 1, -c, 1, -c\rangle$ é anisotrópica, e portanto $D_F\langle 1, -c, 1, -c\rangle \subset F^\times$. Como $D_F\langle 1, -c\rangle \subset D_F\langle 1, -c, 1, -c\rangle$ e $(F^\times : D_F\langle 1, -c\rangle) = 2$ temos duas possibilidades: $D_F\langle 1, -c\rangle = D_F\langle 1, -c, 1, -c\rangle$, ou $D_F\langle 1, -c, 1, -c\rangle = F^\times$. Resulta do primeiro caso que $D_F\langle 1, -c\rangle + D_F\langle 1, -c\rangle \subset D_F\langle 1, -c\rangle$, ocorrendo uma das possibilidades anunciadas. No segundo caso $-1 \in D_F\langle 1, -c, -c, 1\rangle$ e assim $\langle -1\rangle\langle 1, -c, -c, 1\rangle \simeq \langle 1, -c, -c, 1\rangle$, por [**L**]. Isto é

$$\langle 1, -c, -c, 1\rangle \simeq \langle -1, c, c, -1\rangle.$$

Somando-se $\langle 1, 1\rangle + \langle c, c\rangle$ dos dois lados dessa igualdade temos

$$\langle 1, 1\rangle + \langle c, c\rangle + \langle 1, -c, -c, 1\rangle \simeq \langle 1, 1\rangle + \langle c, c\rangle + \langle -1, c, c, -1\rangle.$$

Rearranjando os termos das formas quadráticas obtemos

$$\langle 1, 1, 1, 1\rangle + \langle c, c, -c, -c\rangle \simeq \langle c, c, c, c\rangle + \langle 1, -1, 1, -1\rangle.$$

Cancelando-se $2\langle 1, -1\rangle$ dos dois lados obtemos

$$\langle 1, 1, 1, 1\rangle \simeq \langle c, c, c, c\rangle \simeq \langle\, c\rangle\langle 1, 1, 1, 1\rangle,$$

do que resulta $c \in D_F\langle 1, 1, 1, 1\rangle$, novamente por ([**L**]),terminando a demonstração do lema. □

Usaremos nos próximos resultados conceitos e propriedades sobre corpos formalmente reais introduzidos na parte final do Capítulo 3.

Teorema 4.1.15. *Seja F com base distinguida completa e conservemos a notação e os objetos já introduzidos. Sejam F_λ, $\lambda = 1, \ldots, m$, os subgrupos correspondentes a partição principal. Suponhamos que para algum $1 \leq \lambda \leq m$ temos $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$ e seja $c \in F_\lambda \smallsetminus R(F)$. Então:*

1. *$-1 \notin D_F\langle 1, -c\rangle$, ou então, equivalentemente, $c \notin D_F\langle 1, 1\rangle$.*
2. *Seja agora $-1 = c_1 \cdots c_r$ a decomposição de -1 em relação a partição principal, onde $c_i \in F_{\lambda_i} \smallsetminus R(F)$, para todo $i = 1, \ldots, r$. Então existe $1 \leq i \leq r$ tal que $c_i \in cR(F)$. Consequentemente, $D_F\langle 1, 1\rangle \subset D_F\langle 1, -c\rangle$.*

3. *$P = D_F\langle 1, -c\rangle$ é o cone positivo de uma ordem definida em F e portanto F é formalmente real.*

Demonstração. (1) Como vimos no item 2(a) do **Teorema 3.2.11** que $(F_\lambda : F_\lambda \cap D_F\langle 1, -c\rangle) = 2$, podemos concluir que $R(F) = F_\lambda \cap D_F\langle 1, -c\rangle$. Como $c \notin R(F)$, então $c \notin D_F\langle 1, -c\rangle$, e equivalentemente $-1 \notin D_F\langle 1, -c\rangle$.

(2) Para a decomposição de $-1 = c_1 \cdots c_r$ em relação a partição principal assumimos, sem perda de generalidade, que $\{ 1, \ldots, r \}$ são os $r \leq m$ primeiros elementos de Λ. Ainda pelo item 2(a) do **Teorema 3.2.11** temos que

$$L_j \subset D_F\langle 1, 1\rangle = \bigcap_{i=1}^{r} D_F\langle 1, -c_i\rangle,$$

para todo $j > r$, caso $r < m$. Como $c \notin D_F\langle 1, 1\rangle$, concluímos que $\lambda \leq r$. Isto é, existe $1 \leq \lambda \leq r$ para o qual podemos assumir que $c_\lambda = c$, pois $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$.

(3) Temos que $P = D_F\langle 1, -c\rangle$ é multiplicativamente fechado e já temos $(F^\times : D_F\langle 1, -c\rangle) = 2$, pois $c \in F_\lambda$. Também pelo item (1), $-1 \notin P$. Por outro lado, a **Proposição 4.1.13** implica que $c \notin D_F\langle 1, 1, 1, 1\rangle$, e assim, pelo **Lema 4.1.14**, $P + P \subset P$ e então P é o cone de uma ordem sobre F. □

Veremos a seguir a recíproca do último resultado e também a descrição do espaço de ordens de um corpo com base distinguida completa. Caso F seja formalmente real, recordemos que $\sum F^2$ é um subgrupo de $F^\times$, tal que $-1 \notin \sum F^2$ e $\sum F^2 + \sum F^2 \subset \sum F^2$. Propriedades essas que caracterizam uma *pré-ordem*. Para um corpo não formalmente real F, temos $\sum F^2 = F$.

No caso de F ser formalmente real denotaremos por X_F o espaço de ordens de F. Recordemos que X_F pode ser topologizado tomando-se como base de abertos as interseções finitas dos conjuntos de Harrison: $H(a) = \{ P \in X_F \mid a \in P \}$. Com essa topologia X_P é compacto e totalmente desconexo.

Os corpos formalmente reais com base distinguida têm propriedades aritméticas muito particulares, podendo mesmo serem caracterizados por elas. Seguindo Elman e Prestel [**EP**] dizemos que um corpo formalmente real F tem a propriedade

(S_1): *se $w \in \sum F^2$, então $D_F\langle 1, -w\rangle \sum F^2 = F^\times$.*

Vamos também, como de costume, dizer que um corpo formalmente real F tem a propriedade SAP, ou que X_F tem SAP (*strong approximation property*), caso para todo par A, B de fechados disjuntos de X_F exista $a \in F^\times$ tal que $A \subset H(a)$ e $B \subset H(-a) = X_F \setminus H(a)$. A propriedade SAP está bem estudada e pode ser facilmente encontrada na literatura. Para maiores detalhes sobre ela sugerimos, por exemplo, [**P**].

Recordamos a seguir um resultado que combina as duas propriedades introduzidas acima com uma propriedade do grupo de Galois $G_2(F)$. Os grupos profinitos *reais livre* foram introduzidos em [**HJ**], embora já tivessem aparecido em [**Er**] onde foram denominados *quase livres*. São os grupos que podem ser descritos como o produto livre $\mathcal{F} * (*_X \mathbb{Z}/2\mathbb{Z})$, onde $\mathcal{F}$ é um pro-2 grupo livre e $*_X \mathbb{Z}/2\mathbb{Z}$ é um produto livre sobre um espaço Booleano X, conforme descrito em [**Er**] ou [**H**]. No caso $G_2(F) \cong \mathcal{F} * (*_X \mathbb{Z}/2\mathbb{Z})$, para algum corpo F, temos que $X \cong X_F$ é homeomorfo ao

espaço de ordens de F e $\mathcal{F} \cong G(F_{pyth}/F)$ corresponde ao grupo de Galois do fecho pitagórico de F em relação a F.

Particularmente para corpos com um número finito de ordens, dizer que $G_2(F)$ é real livre significa que $G_2(F) \cong \mathcal{F} * C_1 * \cdots * C_n$ é produto livre usual na categoria dos pro-2 grupos, onde C_i tem ordem 2 para todo i.

Os corpos considerados no **Teorema 4.1.16** abaixo não tem X_F necessariamente finitos.

Teorema 4.1.16. *Para um corpo formalmente real F denotaremos por F_{pyth} seu fecho pitagórico. As seguintes condições são equivalentes:*

1. *F tem SAP e tem S_1.*
2. *F_{pyth} tem SAP*
3. *$G_2(F_{pyth}) \cong \mathcal{F} * (*_X \mathbb{Z}/2\mathbb{Z})$ é real livre.*

Demonstração. A equivalência entre os itens (1) e (2) é consequência de [**PW**]. A equivalência entre os itens (2) e (3) corresponde ao [**Er**] no caso de F ser pitagórico (de forma mais explícita [**Er**]). □

O resultado acima será aplicado no estudo dos corpos com base distinguida.

Teorema 4.1.17. *Seja F com base distinguida completa e sejam F_λ, $\lambda = 1, \ldots, m$, os subgrupos correspondentes a partição principal. Então, F é formalmente real se e somente se existe $1 \leq \lambda \leq m$ tal que $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$.*

Assumindo-se agora que F é formalmente real temos:

1. *Para todo $P \in X_F$ existe um único $\lambda \in \Lambda$ e $c_\lambda \in F_\lambda \smallsetminus R(F)$, único módulo $R(F)$, tais que $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$ e $P = D_F\langle 1, -c_\lambda\rangle$. Mais ainda, todos os elementos de X_F são dessa forma. Vamos então escrever P_λ para a ordem $D_F\langle 1, -c_\lambda\rangle$ onde $1 \leq \lambda \leq m$, $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$, e $c_\lambda \in F_\lambda \smallsetminus R(F)$.*
2. *Seja $d = \prod c_\lambda$ onde $P_\lambda = D_F\langle 1, -c_\lambda\rangle$ é uma ordem de F. Então $D_F\langle 1, -d\rangle = \sum F^2$. Assim $\dim_{\mathbb{F}_2} F^\times/\sum F^2 = \#X_F$. Mais ainda, todo elemento de $\sum F^2$ é uma soma de no máximo quatro quadrados.*
3. *X_F tem as propriedades SAP e S_1.*

Demonstração. Pelo item (3) do **Teorema 4.1.15**, $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$ para algum $1 \leq \lambda \leq m$ implica que F é formalmente real. Reciprocamente, se $P \in X_F$ é uma ordem, como $P \neq F^\times$, existe $1 \leq \lambda \leq m$ tal que $F_\lambda \not\subset P$. Para $c \in F_\lambda$ com $c \notin P$ temos $-c \in P$. Logo $D_F\langle 1, -c\rangle \subset P$. Dessa forma $D_F\langle 1, -c\rangle \neq F^\times$ implicando que $c \notin R(F)$. Mais ainda, como $(F^\times : D_F\langle 1, -c\rangle) = 2$ temos que $P = D_F\langle 1, -c\rangle$.

Observe agora que como $D\langle 1, 1\rangle \subset P$, pelo item (1) do **Teorema 4.1.1** temos $c \in c_j R(F)$, onde $-1 = c_1 \cdots c_r$ é a decomposição de -1 em relação a partição principal, com $c_i \in F_{\lambda_i} \smallsetminus R(F)$,

para todo $i = 1, \ldots, r$. Sem perda de generalidade vamos novamente adotar a numeração dos F_j de forma que $\lambda_1, \ldots, \lambda_r$ são os r primeiros elementos de Λ. Podemos também assumir que $c = c_j$.

Acabamos de ver que se $F_j \not\subset P$, então $1 \leq j \leq r$ e $c = c_j$ é a única componente (módulo $R(F)$) de -1 em F_j. Consequentemente, para todo $x \in F_j$ tal que $x \notin P$ temos $x \in cR(F)$ (pois x estará na fatoração -1 que é única módulo $R(F)$). Isto é, $F_j \setminus P \cap F_j = cR(F)$. Como $F_j = (P \cap F_j) \cup c(P \cap F_j)$ (pois $(F_j : P \cap F_j) = 2$) concluímos que $c(P \cap F_j) = cR(F)$, ou então $P \cap F_j = R(F)$ e $(F_j : R(F)) = 2$. Logo $X_F \neq \emptyset$ implica que existe $1 \leq \lambda \leq m$ tal que $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$.

Por outro lado, para todo $1 \leq i \leq m$ com $i \neq j$ temos $F_i \subset D_F\langle 1, -c\rangle = P$. Logo, temos um único $j \in \{1, \ldots, m\}$ tal que $P = D_F\langle 1, -c\rangle$, com $c \in F_j$ e $c \notin P$. Fica assim demonstrado a primeira parte do teorema e também o item (1).

A primeira parte do item (2) é imediato pois $\sum F^2 = \bigcap_{P \in X_F} P$. Vamos demonstrar a segunda parte junto com o item seguinte. Como $D_F\langle 1, -d\rangle = \sum F^2$, pelo **Teorema 3.2.14** temos que $\dim_{\mathbb{F}_2} F^\times/\sum F^2 = \#X_F$. Essa igualdade implica que F tem SAP pelo Teorema 17.4 de [**L2**].

Usaremos agora a decomposição $-1 = c_1 \cdots c_r$ em fatores de F_λ e mantemos também a convenção de que $1, \ldots, r$ são os r primeiros elementos de Λ. Decorre de $D_F\langle 1, 1\rangle \subset D_F\langle 1, -d\rangle$ que podemos adotar a decomposição de d, módulo $R(F)$, na forma $d = c_1 \cdots c_s$, com $s \leq r$, pelo item (1) do **Teorema 4.1.1**. Feito isso, dado $w \in \sum F^2$, como $D_F\langle 1, -w\rangle \not\subset P$, para todo $P \in X_F$, podemos concluir pelo item (1) do **Teorema 4.1.1**, para todo $1 \leq j \leq s$, que c_j não comparece na decomposição de w. Logo d e w não tem "termos em comum", conforme descrito no item (3) do **Teorema 4.1.1**. Por esse mesmo item obtemos então $D_F\langle 1, -d\rangle D_F\langle 1, -w\rangle = F^\times$, mostrando que vale S_1, conforme afirmado. Fica assim demonstrado o item (3).

Finalmente, para completarmos a demonstração do item (2), tomemos a decomposição de $w = e_1 \cdots e_\ell$, com $e_k \in L_{\lambda_k} \setminus R(F)$. Vimos no parágrafo anterior que $\lambda_k > s$, para todo $k = 1, \ldots, \ell$. Logo $D_F\langle 1, -e_k\rangle$ não é uma ordem sobre F. Caso ocorra $-1 \in D_F\langle 1, -e_k\rangle$, então $e_k \in D_F\langle 1, 1\rangle$. Caso $-1 \notin D_F\langle 1, -e_k\rangle$, como $D_F\langle 1, -e_k\rangle$ é multiplicativamente fechado e tem índice 2 em $F^\times$, a única maneira de $D_F\langle 1, -e_k\rangle$ não ser uma ordem é não ser aditivamente fechado. Nesse caso, pelo **Lema 4.1.14**, $e_k \in D_F\langle 1, 1, 1, 1\rangle$. Conclusão, e_k é uma soma de no máximo 4 quadrados, para todo k. Como $D_F\langle 1, 1, 1, 1\rangle$ é multiplicativamente fechado, resulta também $w \in D_F\langle 1, 1, 1, 1\rangle$. completando a demonstração do item (2). □

A pesar de não alcançarmos o objetivo inicial, isto é, mostrar que para todo corpo F com base distinguida completa o grupo de Galois $G_2(F)$ é decomponível como um produto livre, na categoria dos pro-2 grupos, de um número finito de parcelas de Demushkin e um parcela livre, conseguimos mostrar para um caso particular de corpos com base distinguida.

Teorema 4.1.18. *Seja F formalmente real tal que $\dim_{\mathbb{F}_2} F^\times/R(F)$ é finita. Assumindo-se as mesmas notações do* ***Teorema 4.1.17*** *temos que as seguintes afirmações são equivalentes:*

1. *F tem base distinguida e $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$, para todo $\lambda = 1, \ldots, m$.*
2. *$R(F) = \sum F^2$ e F tem SAP.*
3. *$G_2(F)$ é real livre.*

Demonstração. Valendo (1) temos que $\dim_{\mathbb{F}_2} F^\times/R(F) = m$. Por outro lado, resulta dos itens (2) e (3) do **Teorema 4.1.17** que F tem SAP e $\dim_{\mathbb{F}_2} F^\times/\sum F = \#X_F = m$. Como $R(F) \subset D_F\langle 1,1\rangle \subset \sum (F^\times)^2$, podemos concluir das duas igualdades que $R(F) = \sum (F^\times)^2$, demonstrando (2).

Assumindo (2), temos que a igualdade $R(F) = \sum (F^\times)^2$ permite usar a equivalência (5)⇔(1) do Teorema E, pg. 295, de [**ELP**] para aplicar o Teorema F, pg. 296 de [**ELP**]. Como F tem SAP, pela equivalência (7)⇔(1) desse último resultado, implicam que toda forma quadrática totalmente indefinida com coeficientes em F que tenha dimensão ≥ 3 é indefinida (isto é, F tem invariante de Hasse ≤ 2, como foi introduzido em [**EL**]). Segue então de [**Er**] que $G_2(F)$ é real livre.

Finalmente, como F é formalmente real com $\dim_{\mathbb{F}_2} F^\times/R(F)$ finita temos que X_F é finito. Logo $G_2(F) \cong \mathcal{F} * C_1 * \cdots * C_m$, onde C_i tem ordem 2 para todo i. Resulta então do **Teorema 3.1.6** que F tem base distinguida. Por outro lado, sejam, como no parágrafo logo após o **Teorema 3.1.1**, página 32, L_o o corpo fixo de $\mathcal{F}$ e para cada $i = 1, \ldots, m$, L_i o corpo fixo de C_i. Observe que para $i \geq 1$, L_i é um corpo euclidiano e $(L_1^\times)^2 \cap F$ é uma ordem de F. Mais ainda, como por [**HR**] todo elemento de ordem 2 de $G_2(F)$ deve ser conjugado ao gerador de algum C_i temos que toda ordem de F é induzida por algum L_i. Logo $X_F = \{\, (L_1^\times)^2 \cap F, \ldots, (L_m^\times)^2 \cap F \,\}$.

Obtemos, como no **Corolário 3.1.5**, que $R(F) = F \cap (L_1^\times)^2 \cap \cdots \cap (L_m^\times)^2$. Logo $R(F) = \sum F^2$, pelo que vimos acima. Assim pelo item *2.* do **Teorema 3.1.6**, $\dim_{\mathbb{F}_2} F_\lambda/R(F) = 1$, para todo $\lambda = 1, \ldots, m$. □

Os resultados acima também permitem completar o **Teorema 4.1.9**. A saber,

Observação 4.1.19. *O resultado acima mostra que a decomposição que desejávamos mostrar em geral vale para corpos com base distinguida completa bem específicos. Mas é válido ressaltar que se F é um corpo tal que $\dim_{\mathbb{F}_2} F^\times/R(F) = 1$, então $\dim_{\mathbb{F}_2} {}_2Br(F) = 1$ e o grupo de Galois é decomponível. Isto é um caso particular de corpos com duas álgebras de quatérnios, a menos de isomorfismo, e nos incentiva a continuar trabalhando para demonstrarmos o caso geral.*

Teorema 4.1.20. *Seja F com base distinguida e sejam F_λ, $\lambda = 1, \ldots, m$, os subgrupos correspondentes a partição principal, como descrito na introdução. Nessas condições temos que $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$, para todo $\lambda = 1, \ldots, m$ se, e somente, se $\operatorname{cd} G_2(F) = 2$.*

Para F com $\operatorname{cd} G_2(F) = 2$ todo elemento de F é uma soma de no máximo 4 quadrados.

Demonstração. Precisamos somente mostrar um dos lados da primeira afirmação, veja **Teorema 4.1.9**. Se $\operatorname{cd} G_2(F) = 2$, então F não é formalmente real. Portanto, pelo **Teorema 4.1.17**, $\dim_{\mathbb{F}_2} F_\lambda/R(F) > 1$, para todo $\lambda = 1, \ldots, m$.

□

Capítulo 5

Bases distinguidas - parte III Extensões não radicais de corpos com base distinguida

Como já adiantado na introdução, apresentaremos neste capítulo resultados gerais sobre 2-extensões de corpos com base distinguida completa. Apresentaremos aqui o Teorema 90 de Hilbert para extensões não radicais de corpos com base distinguida, versão para o radical de Kaplansky. E finalmente a construção de uma base para extensões quadráticas não radicais de corpos com base distinguida completa.

5.1 Extensões não radicais de corpos com base distinguida completa

Apresentaremos inicialmente dois lemas técnicos que usaremos nas demonstrações de vários resultados deste capítulo.

Lema 5.1.1. *Sejam F um corpo qualquer e $K = F(\sqrt{c})$ uma extensão não radical de F.*

1. *Dados x, $y \in K^\times$ linearmente independentes sobre F, teremos que existem a, $b \in F^\times$ tais que $ax + by = 1$. Logo*

   (a) $(x, by)_K = 0 \in {}_2Br(K)$ *do que resulta*

   $$(ax, y)_K = (a, b)_K + (a, y)_K + (b, x)_K \, em \, {}_2Br(F).$$

   (b) Caso $(x, y)_K \in {}_2\mathrm{Br}(K)^G$ *obtemos que, em* ${}_2Br(K)$, $(a, b)_K + (a, y)_K + (b, x)_K = (a, b)_K + (a, \sigma(y))_K + (b, \sigma(x))_K$ *e assim*

   $$(a, N(y))_K \simeq (b, N(x))_K \in Q_K(N(y)) \cap Q_K(N(x))$$

2. *Para $x \in K^\times$ se $F^\times \subset D_K\langle 1, -x\rangle$, então $N(x) \in R(F)$.*
   Reciprocamente, se $N(x) \in R(F)$, então existe $e \in F^\times$ tal que $F^\times \subset D_K\langle 1, -ex\rangle$.

Demonstração. O item (1) é imediato. Quanto ao item (2) observe que $F^\times \subset D_K\langle 1, -x\rangle$ se e somente se $x \in R_0$, onde R_0 é como no **Corolário 3.2.5**. Ainda, como vimos no **Corolário 3.2.5** que $N^{-1}(R(F)) = F^\times R_0$, então $N(x) \in R(F)$.

Reciprocamente, se $N(x) \in R(F)$, então, pelo mesmo **Corolário 3.2.5**, existe $e \in F^\times$ tal que $ex \in R_0$ e assim $F^\times \subset D_K\langle 1, -ex\rangle$. □

Lema 5.1.2. *Seja F um corpo com base distinguida completa $\{ a_1, \ldots, a_n \}$, partição principal I_λ, $1 \leq \lambda \leq m$ e os subgrupos F_λ e $Q_F(\lambda)$, como na **Definição 3.2.8**.*
Denotemos por $\Lambda = \{ 1, \ldots, m \}$ e seja $c = \prod_{i\in I} c_i \in F^\times$, onde $I \subset \Lambda$, $c_i \in F_i \smallsetminus R(F)$, para todo $i \in I$. Seja também $d = \prod_{j\in J} d_j \in F^\times$, onde $J \subset \Lambda$ e $d_j \in F_j \smallsetminus R(F)$ para todo $j \in J$. Se $d \in D_F\langle 1, -c\rangle$, então $d_j \in D_F\langle 1, -c\rangle$, para todo $j \in J$.

Demonstração. Pelo **Teorema 3.2.14** se $d \in D_F\langle 1, -c\rangle$, então $d \in D_F\langle 1, -c_i\rangle$, para todo $i \in I$. Para cada $i \in I$ fixado, temos pelo item 2(a) do **Teorema 3.2.11** que $d_j \in D_F\langle 1, -c_i\rangle$, para todo $j \neq i$. Como $d \in D_F\langle 1, -c_i\rangle$, resulta disso que se $i \in J$, também $d_i \in D_F\langle 1, -c_i\rangle$ que é um subgrupo de $F^\times$. Conclusão, $d_j \in D_F\langle 1, -c_i\rangle$, para todo $j \in J$, para cada $i \in I$, fixado. Mas então $d_j \in D_F\langle 1, -c_i\rangle$, para todo $i \in I$ e todo $j \in J$. Logo $d_j \in D_F\langle 1, -c\rangle$, para todo $j \in J$, novamente pelo **Teorema 3.2.14**. □

Proposição 5.1.3. *Seja $K = F(\sqrt{c})$, onde $c \in F^\times \smallsetminus (F^\times)^2$ e F é um corpo com base distinguida completa. Para todo $x \in \operatorname{Im} N_{K/F} = D_F\langle 1, -c\rangle$ existe $z \in K^\times$ tal que $N(z)x^{-1} \in (F^\times)^2$ e $D_K\langle 1, -z\rangle \cap F = D_F\langle 1, -x\rangle$.*

Demonstração. Consideremos primeiro o caso em que $x \in R(F)$ e seja $z' \in K^\times$ tal que $N(z') = x$. Pelo item (2) do **Lema 5.1.1**, existe $e \in F^\times$ tal que $F^\times \subset D_K\langle 1, -ez'\rangle$. Para $z = ez'$ teremos que $N(z)x^{-1} \in (F^\times)^2$. Pela escolha de z temos que

$$D_K\langle 1, -z\rangle \cap F = F^\times = D_F\langle 1, -N(z)\rangle = D_F\langle 1, -x\rangle, \text{ pois } x \in R(F),$$

demonstrando o resultado para $x \in R(F)$.

Consideremos a seguir o caso em que $(F^\times : D_F\langle 1, -x\rangle) = 2$. Isto é, podemos ter uma base distinguida $a_1, \ldots, a_n$ para F onde $a_1 = x$. Tomemos também $\{ b_1, \ldots, b_n \}$ uma base dual de $\{ a_1, \ldots, a_n \}$ em F, conforme visto na **Proposição 3.2.7**. Para cada $i = 1, \ldots, n$ temos que $\{ b_1 \ldots, b_{i-1}, b_{i+1}, \ldots, b_n \}$ geram $D_F\langle 1, -a_i\rangle$, módulo $R(F)$. Mais ainda, conforme essa mesma proposição temos que $a_i \in D_F\langle 1, -b_j\rangle$, para todo $j \neq i$. Logo, se $z' \in K^\times$ é tal que $N(z') = a_1 = x$, teremos pelo Princípio da Norma que

$$z' \in \bigcap_{j\neq i} F^\times D_K\langle 1, -b_j\rangle = F^\times \left(\bigcap_{j\neq i} D_K\langle 1, -b_j\rangle \right),$$

onde a igualdade vale pelo item (4) da **Proposição 3.2.4.** Concluímos então que existem $a \in F^\times$ e $y \in \bigcap_{j\neq i} D_K\langle 1, -b_j\rangle$ tais que $z' = ay$. Portanto $a^{-1}z' = y \in D_K\langle 1, -b_j\rangle$, para todo $j \neq i$. Dessa

forma $b_j \in D_K\langle 1, -a^{-1}z'\rangle$ para todo $j \neq i$. Consequentemente, $b_j \in D_K\langle 1, -a^{-1}z'\rangle \cap F^\times$ para todo $j \neq i$. Obtemos como consequência que $\dim_{\mathbb{F}_2}\left(D_K\langle 1, -a^{-1}z'\rangle \cap F^\times\right)/R(F) \geq n-1$ $(*)$.

Seja $z = a^{-1}z'$ e observe que $N(z)x^{-1} = a^{-2} \in (F^\times)^2$.

Afirmamos que $F^\times \not\subset D_K\langle 1, -z\rangle$. De fato, se $d \in D_K\langle 1, -z\rangle$ para todo $d \in F^\times$, então $z \in D_K\langle 1, -d\rangle$ para todo $d \in F^\times$. Pelo Princípio da Norma, **Teorema 1.1.9**, resultaria que $N(z) \in D_F\langle 1, -d\rangle$, para todo $d \in F^\times$. Isto é $N(z) \in R(F)$, contrário a hipótese $x \notin R(F)$.

Resulta da desigualdade $(*)$ e da afirmação acima que $\dim_{\mathbb{F}_2}\left(D_K\langle 1, -z\rangle \cap F^\times\right)/R(F) = n-1$ e portanto $(F^\times : D_K\langle 1, -z\rangle \cap F^\times) = 2$.

Por outro lado, $D_K\langle 1, -z\rangle \cap F^\times \subset D_F\langle 1, -N(z)\rangle = D_F\langle 1, -x\rangle$, pelo Princípio da Norma, **Teorema 1.1.9**. Como acabamos de ver que $(F^\times : D_K\langle 1, -z\rangle \cap F^\times) = 2$ e $D_F\langle 1, -x\rangle \neq F^\times$ (pois estamos assumindo que $(F^\times : D_F\langle 1, -x\rangle) = 2$), resulta na igualdade $D_K\langle 1, -z\rangle \cap F^\times = D_F\langle 1, -x\rangle$ que queríamos demonstrar.

Seja agora $x \in F^\times$, qualquer, e tomemos sua representação $x = x_1 \cdots x_k$ onde $x_i \in F_i \smallsetminus R(F)$, para todo $i = 1, \ldots, k$. Pelo **Lema 5.1.2**, $x_1, \ldots, x_k \in D_F\langle 1, -c\rangle$ e pelo caso anterior, existem $z_1, \ldots, z_k \in K^\times$ tais que $N(z_i)x_i^{-1} \in (F^\times)^2$ e $D_K\langle 1, -z_i\rangle \cap F = D_F\langle 1, -x_i\rangle$, para todo $i = 1, \ldots, k$. Seja $z = z_1 \cdots z_k$. Então $N(z)x^{-1} \in (F^\times)^2$, como queríamos. Vejamos que z também satisfaz a outra condição.

Pelo Princípio da Norma, **Teorema 1.1.9**, $D_K\langle 1, -z\rangle \cap F \subset D_F\langle 1, -N(z)\rangle = D_F\langle 1, -x\rangle$. Para demonstrarmos a inclusão inversa tomemos $y \in D_F\langle 1, -x\rangle$. Pelo **Teorema 3.2.14** sabemos que $D_F\langle 1, -x\rangle = \bigcap_{i=1}^{k} D_F\langle 1, -x_i\rangle$. Logo $y \in D_F\langle 1, -x_i\rangle$, para todo $i = 1, \ldots, k$, resultando que $y \in D_K\langle 1, -z_i\rangle$, para todo $i = 1, \ldots, k$. Vemos então que

$$(y, z)_K = \sum_{i=1}^{k} (y, z_i)_K = 0 \in {}_2Br(F).$$

Dessa forma $y \in D_K\langle 1, -z\rangle$, implicando a outra inclusão e portanto vale a igualdade procurada. □

Vamos a seguir ver um resultado da mesma natureza da **Proposição 3.2.4**, caso não radical.

Proposição 5.1.4. *Seja $K = F(\sqrt{c})$, onde F é um corpo com base distinguida completa e $c \in F^\times \smallsetminus (F^\times)^2$. Sejam agora $a_1, \ldots, a_r \in F^\times$ tais que para todo subconjunto $\{ i_1, \ldots, i_s\} \subset \{ 1, \ldots, r \}$ e para todo $j \in \{ 1, \ldots, r \} \smallsetminus \{ i_1, \ldots, i_s\}$*

$$\left(\bigcap_{t=1}^{s} D_F\langle 1, -a_{i_t}\rangle\right) D_F\langle 1, -a_j\rangle = F^\times.$$

Sejam também $z_1, \ldots, z_r \in K^\times$ tais que $D_K\langle 1, -z_i\rangle \cap F = D_F\langle 1, -a_i\rangle$, para todo $i = 1, \ldots, r$. Nessa condições, para um subconjunto $\{ i_1, \ldots, i_s\} \subset \{ 1, \ldots, r \}$, vale que

$$\left(\bigcap_{t=1}^{s} F^\times D_K\langle 1, -z_{i_t}\rangle\right) = F^\times \left(\bigcap_{t=1}^{s} D_K\langle 1, -z_{i_t}\rangle\right).$$

Demonstração. A inclusão $F^\times\left(\bigcap_{t=1}^{s} D_K\langle 1,-z_{i_t}\rangle\right) \subset \left(\bigcap_{i=1}^{s} F^\times D_K\langle 1,-z_{i_t}\rangle\right)$ é claramente verdadeira. Temos que mostrar que a inclusão inversa também vale. Vamos verificar isso recursivamente, i.e., para todo $1 \leq k \leq s$ e todo $x \in \left(\bigcap_{t=1}^{k} F^\times D_K\langle 1,-z_{i_t}\rangle\right)$ existem $a \in F^\times$ e $y \in \left(\bigcap_{t=1}^{k} D_K\langle 1,-z_{i_t}\rangle\right)$ tais que $x = ay$. Para $k = 1$ a inclusão é obvia. Suponhamos indutivamente que para todo $k = 1, \ldots, n < s$ a inclusão está demonstrada e tomemos $x \in \left(\bigcap_{t=1}^{n+1} F^\times D_K\langle 1,-z_{i_t}\rangle\right)$.

Por hipótese de indução existem $a \in F^\times$ e $y \in \left(\bigcap_{t=1}^{n} D_K\langle 1,-z_{i_t}\rangle\right)$ tais que $x = ay$. Mas como também temos $x \in F^\times D_K\langle 1,-z_{i_{n+1}}\rangle$ existem $b \in F^\times$ e $w \in D_K\langle 1,-z_{i_{m+1}}\rangle$ satisfazendo $x = bw$.

Por outro lado, como por hipótese vale a igualdade

$$\left(\bigcap_{t=1}^{n} D_F\langle 1,-a_{i_t}\rangle\right) D_F\langle 1,-a_{i_{n+1}}\rangle = F^\times,$$

existem y_1, $w_1 \in \bigcap_{t=1}^{n} D_F\langle 1,-a_{i_t}\rangle$ e a_1, $b_1 \in D_F\langle 1,-a_{i_{n+1}}\rangle$ tais que $a = a_1y_1$ e $b = b_1w_1$.

Temos como consequência de uma das hipóteses da proposição que

$$\bigcap_{t=1}^{n} D_K\langle 1,-z_{i_t}\rangle \bigcap F = \bigcap_{t=1}^{n} D_F\langle 1,-a_{i_t}\rangle \quad \text{e} \quad D_K\langle 1,-z_{i_{n+1}}\rangle \cap F = D_F\langle 1,-a_{i_{n+1}}\rangle.$$

Logo y_1, $w_1 \in \bigcap_{t=1}^{n} D_K\langle 1,-z_{i_t}\rangle$ e a_1, $b_1 \in D_K\langle 1,-z_{i_{n+1}}\rangle$. Juntando as informações temos que

$$a_1y_1y = x = b_1w_1w. \text{ Logo temos } u = y_1yw_1^{-1} = a_1^{-1}b_1w \in \bigcap_{t=1}^{n+1} D_K\langle 1,-z_{i_t}\rangle.$$

Tomemos em seguida $d = a_1w_1 \in F^\times$ e vamos concluir que

$$x = du \in F^\times \left(\bigcap_{t=1}^{m+1} D_K\langle 1,-z_{i_t}\rangle\right),$$

com queríamos. Logo, para $k = s$ obtemos a que a inclusão inversa vale, completando a demonstração da igualdade.

□

Lema 5.1.5. *Sejam F um corpo com base distinguida completa e $K = F(\sqrt{c})$, $c \in F^\times \smallsetminus (F^\times)^2$. Dados x, $y \in K^\times$, temos:*

1. *Se $N(x)N(y)^{-1} \notin (F^\times)^2$, então existem a, $b \in F^\times$ tais que $ax + by = 1$.*
2. *Assumido-se que $D_K\langle 1,-x\rangle \cap F = D_F\langle 1,-N(x)\rangle$ (ou $D_K\langle 1,-y\rangle \cap F = D_F\langle 1,-N(y)\rangle$), então $Q_K(x) \cap \operatorname{Im}\operatorname{Res} = \{0\}$ (ou $Q_K(y) \cap \operatorname{Im}\operatorname{Res} = \{0\}$).*
3. *Suponhamos que $N(x) \in D_K\langle 1,-y\rangle$ e $N(y) \in D_K\langle 1,-x\rangle$. Então $(x,y)_K \in {}_2\mathrm{Br}(K)^G$.*

   Particularmente se $D_K\langle 1,-x\rangle \cap F = D_F\langle 1,-N(x)\rangle$, $D_K\langle 1,-y\rangle \cap F = D_F\langle 1,-N(y)\rangle$, $N(x) \in F_\lambda$, $N(y) \in F_\gamma$, e mais ainda, caso $\lambda = \gamma$, então $N(x) \in D_F\langle 1,-N(y)\rangle$, então $(x,y)_K \in {}_2\mathrm{Br}(K)^G$.

Demonstração. (1) Por hipótese temos que $N(x)N(y)^{-1} \notin (F^\times)^2$, e daí x, y são linearmente independentes em relação a F.Logo existem a, $b \in F^\times$ tais que $ax + by = 1$.

(2) decorre de $D_K\langle 1, -x\rangle \cap F = D_F\langle 1, -N(x)\rangle$ devido a **Teorema 3.2.17.**

(3) Como $x\sigma(x) = N(x) \in D_K\langle 1, -y\rangle$, resulta que $(x, y)_K \simeq (\sigma(x), y)_K$. Analogamente temos que $(\sigma(x), y)_K \simeq (\sigma(x), \sigma(y))_K$, pois $N(y) = \sigma(N(y)) \in \sigma(D_K\langle 1, -x\rangle) = D_K\langle 1, -\sigma(x)\rangle$. Dessa forma $(x, y)_K \simeq (\sigma(x), \sigma(y))_K \simeq (x, y)_K^\sigma \in {}_2\mathrm{Br}(K)^G$, conforme afirmado.

Caso $\lambda \neq \gamma$, então $F_\lambda \subset D_F\langle 1, -N(y)\rangle \subset D_K\langle 1, -y\rangle$. Logo $N(x) \in D_K\langle 1, -y\rangle$ e igualmente e igualmente $N(y) \in D_K\langle 1, -x\rangle$. Se $\lambda = \gamma$, então $N(x) \in D_F\langle 1, -N(y)\rangle$ por hipótese. Assim as hipóteses do item (3) valem nesse caso particular. □

Nos próximos resultados vamos sempre manter as seguintes notações:
F é
Seja também $c = \prod_{j\in J} c_j$ onde $J \subset \Lambda$ e $c_j \in F_j \setminus R(F)$, para todo $j \in J$.

Teorema 5.1.6. *Considere F um corpo com base distinguida completa $\{a_1, \ldots, a_n\}$, partição principal I_λ, $\lambda \in \Lambda = \{1, \ldots, m\}$ e os subgrupos F_λ e $Q_F(\lambda)$ como na **Definição 3.2.8**. Sejam $c = \prod_{j\in J} c_j$ onde $J \subset \Lambda$ e $c_j \in F_j \setminus R(F)$, para todo $j \in J$ e $K = F(\sqrt{c})$.*

Para todo $z \in K$ com $N(z) \in F_\lambda \setminus R(F)$ existe $f \in F^\times$ tal que $D_K\langle 1, -fz\rangle \cap F = D_F\langle 1, -N(z)\rangle$ e $(K^\times : D_K\langle 1, -fz\rangle) = 2$. Mais ainda, $f \in \prod_{j\in J} F_j$.

Demonstração. Pela **Proposição 5.1.3** podemos assumir que $D_K\langle 1, -z\rangle \cap F = D_F\langle 1, -N(z)\rangle$.

Seja a aplicação sobrejetiva $K^\times/(K^\times)^2 \xrightarrow{\overline{N}} D_F\langle 1, -c\rangle/(F^\times)^2$ induzida pela norma. Nosso objetivo é demonstrar que para um conveniente $f \in F^\times$, existe $x \in D_K\langle 1, -fz\rangle$ tal que $\overline{N}(x(K^\times)^2) = d(F^\times)^2$ e $D_K\langle 1, -fz\rangle \cap F = D_F\langle 1, -N(z)\rangle$.

Como o núcleo de $\overline{N}$ é $F^\times(K^\times)^2/(K^\times)^2$ vamos ter, para esse f, que $F^\times D_K\langle 1, -fz\rangle = K^\times$. Logo $(K^\times : D_K\langle 1, -fz\rangle) = (F^\times : D_K\langle 1, -fz\rangle \cap F) = (F^\times : D_F\langle 1, -N(z)\rangle)$. Finalmente, como $(F^\times : D_F\langle 1, -N(z)\rangle) = 2$ vamos obter o resultado desejado.

Pelo **Lema 5.1.2**, temos que $d = \prod_{\gamma\in\Gamma} d_\gamma \in D_F\langle 1, -c\rangle$, onde $\Gamma \subset \Lambda$ e $d_\gamma \in F_\gamma \setminus R(F)$ para todo $\gamma \in \Gamma$, basta demonstrarmos que para todo d_γ existe $x_\gamma \in D_K\langle 1, -z\rangle$ tal que $\overline{N}(x_\gamma(K^\times)^2) = d_\gamma(F^\times)^2$. Logo para $x = \prod_{\gamma\in\Gamma} x_\gamma$ vamos obter $x \in D_K\langle 1, -z\rangle$ e $\overline{N}(x(K^\times)^2) = d(F^\times)^2$.

Obtemos assim uma simplificação do problema. Vamos demonstrar que existe $f \in F^\times$ de forma que para todo $d \in D_F\langle 1, -c\rangle \cap F_\gamma$ e todo $\gamma \in \Lambda$, existe $x \in D_K\langle 1, -fz\rangle$ tal que $\overline{N}(x(K^\times)^2) = d(F^\times)^2$ e as outras condições requeridas também valem. Demonstrar esse fato é um pouco longo e vamos dividir a demonstração em vários casos. Observe que caso $d(F^\times)^2 = N(z)(F^\times)^2$, basta tomar $x = -z$, pois $N(-z) = N(z)$ e $-z \in D_K\langle 1, -z\rangle$ e a existência de x vale trivialmente. Logo vamos considerar somente o caso $dN(z)^{-1} \notin (F^\times)^2$. Dessa forma, pelo **Lema 5.1.5** as fórmulas dos itens (1a) e (1b) do **Lema 5.1.1** valem.

Como o argumento a seguir é longo convém destacarmos o seguinte: o índice λ é fixo e $N(z) \in F_\lambda$. Já o índice γ assume todos os valores de Λ.

Caso I: $d \in R(F)$ ou $d \in F_\gamma$ com $\gamma \notin J$ e sem restrições sobre λ.
Nessas condições demonstraremos que existe $x \in D_K\langle 1, -z\rangle$ tal que $\overline{N}(x(K^\times)^2) = d(F^\times)^2$. Isto é, tomamos $f = 1$ no caso I.

IA: seja $d \in R(F)$. Pelo item (2) do **Lemma 5.1.1** podemos escolher $x \in K^\times$ tal que $N(x)d^{-1} \in (F^\times)^2$ e $F^\times \subset D_K\langle 1, -x\rangle$. Usando a fórmula (1a) do **Lema 5.1.1** temos

$$(x, z)_K \simeq (a, b)_K + (a, z)_K + (x, b)_K.$$

Como $F^\times \subset D_K\langle 1, -x\rangle$, conforme nossa escolha, $(b, x)_K = 0 \in {}_2Br(K)$. Logo $(x, z)_K \simeq (a, b)_K + (a, z)_K$, implicando que $(ax, z)_K = (a, b)_K \in Q_K(z) \cap \operatorname{Im}\operatorname{Res} = \{0\}$, pelo item (2) do **Lema 5.1.5**. Assim $(ax, z)_K = 0 \in {}_2Br(K)$ e $ax \in D_K\langle 1, -z\rangle$. Como $N(ax)d^{-1} = a^2N(x)d^{-1} \in (F^\times)^2$, obtemos $\overline{N}(ax(K^\times)^2) = d(F^\times)^2$, como queríamos.

Antes de prosseguirmos vamos fixar alguns fatos que serão usados nos casos seguintes.

Dado $d \in F_\gamma$ podemos escolher, pela **Proposição 5.1.3**, $x \in K$ tal que $D_K\langle 1, -x\rangle \cap F = D_F\langle 1, -d\rangle$, e $N(x)d^{-1} \in (F^\times)^2$. Como estamos procurando por representantes das classes de $F^\times$ módulo $(F^\times)^2$ podemos assumir que existe $x \in K^\times$ tal que $D_K\langle 1, -x\rangle \cap F = D_F\langle 1, -d\rangle$ e $N(x) = d$. Posteriormente vamos trocar x por gx, com $g \in F^\times$ ou por $\sigma(x)$. Em ambos os casos a norma do novo elemento é igual a $N(x)$, módulo $(F^\times)^2$.

Sejam agora $a = \prod_{i\in I_1} a_i$ e $b = \prod_{i\in I_2} b_i$, onde I_1, $I_2 \subset \Lambda$ e $a_i \in F_i \smallsetminus R(F)$ para todo $i \in I_1$ e $b_i \in F_i \smallsetminus R(F)$ para todo $i \in I_2$, as decomposições de a e b, respectivamente.

Pelo item 2(a) do **Teorema 3.2.11** para todo $i \in I_1$ tal que $i \neq \lambda$ temos $F_i \subset D_F\langle 1, -N(z)\rangle = D_K\langle 1, -z\rangle \cap F$ e para todo $i \in I_2$ tal que $i \neq \gamma$ temos $F_i \subset D_F\langle 1, -N(x)\rangle = D_K\langle 1, -x\rangle \cap F$ concluímos então que $(a, z)_K \simeq (a_\lambda, z)_K \in Q_K(a_\lambda)$ e $(b, x)_K \simeq (b_\gamma, x)_K \in Q_K(b_\gamma)$. Logo

$$(x, z)_K \simeq (a, b)_K + (a_\lambda, z)_K + (b_\gamma, x)_K. \tag{5.1.1}$$

Vamos manter essas escolhas e usar suas consequências em todos os casos a seguir.

IB: $\gamma \notin J$ e $\gamma \neq \lambda$. Nesse caso, pelo item (2a) do **Teorema 3.2.11** temos $F_\gamma \subset D_F\langle 1, -N(z)\rangle$ e $F_\lambda \subset D_F\langle 1, -N(x)\rangle$. Logo, pelo item (3) do **Lema 5.1.5** temos que $(x, z)_K \in {}_2\mathrm{Br}(K)^G$. Então usando a equação (5.1.1), teremos

$$(a, b)_K + (a_\lambda, z)_K + (b_\gamma, x)_K \simeq (a, b)_K + (a_\lambda, \sigma(z))_K + (b_\gamma, \sigma(x))_K$$

e assim

$$(a_\lambda, N(z))_K \simeq (b_\gamma, N(x))_K \in Q_K(N(z)) \cap Q_K(N(x)) = \{0\},$$

onde a última igualdade está no item (1) do **Teorema 4.1.7**, pois $\gamma \neq \lambda$. Então, como $\gamma \notin J$, pelo item (3) da **Proposição 4.1.5**

$$b_\gamma \in D_K\langle 1, -N(x)\rangle \cap F = D_F\langle 1, -N(x)\rangle = D_K\langle 1, -x\rangle \cap F,$$

implicando que $(b_\gamma, x)_K = 0 \in {}_2Br(K)$, pois que $N(x) = d$.

Logo $(x,z)_K \simeq (a,b)_K + (a_\lambda, z)_K$ resultando que

$$(a_\lambda x, z)_K \simeq (x,z)_K + (a_\lambda, z)_K \simeq (a,b)_K \in Q_K(z) \cap \operatorname{Im}\operatorname{Res} = \{\,0\,\},$$

pelo item (2) do **Lema 5.1.5**. Portanto $(a_\lambda x, z)_K = 0$ e $a_\lambda x \in D_K\langle 1, -z\rangle$. Como $\overline{N}(a_\lambda x(K^\times)^2) = \overline{N}(x(K^\times)^2)$, o CasoIB fica demonstrado trocando-se x por $a_\lambda x$.

IC: $\gamma = \lambda \notin J$. Para $d \in F_\lambda$ dividimos a demonstração em duas alternativas.

IC$_1$: $d \in F_\lambda \cap D_F\langle 1, -N(z)\rangle$. Como no Caso IB, pelo item (3) do **Lema 5.1.5** $(x,z)_K \in {}_2Br(K)^G$. Portanto, o item (b) do **Lema 5.1.1** implica

$$(a_\lambda, N(z))_K = (b_\lambda, N(x))_K \in Q_K(N(z)).$$

Se $(a_\lambda, N(z))_F = 0$ (ou simetricamente $(b_\lambda, N(x)_F = 0)$, então, como $\lambda \notin J$,

$$a_\lambda \in D_F\langle 1, -N(z)\rangle \simeq D_K\langle 1, -N(z)\rangle \cap F = D_K\langle 1, -z\rangle \cap F, \tag{5.1.2}$$

pelo item (3) da **Proposição 4.1.5**.

Vemos então que se $(a_\lambda, N(z))_F = 0$, então $0 = (a_\lambda, N(z))_K = (b_\lambda, N(x)_K$. E consequentemente, $b_\lambda \in D_K\langle 1, -N(x)\rangle \cap F = D_F\langle 1, -N(x)\rangle = D_F\langle 1, -x\rangle$, pelo item (3) da **Proposição 4.1.5**. Logo $(b_\lambda, x)_K = 0$ e também $(b_\lambda, N(x))_F = 0$. Concluímos assim que em ${}_2Br(F)$:

$$(a_\lambda, N(z))_F = 0 \quad \text{implica} \quad (b_\lambda, N(x))_F = 0,$$

e simetricamente

$$(b_\lambda, N(x))_F = 0 \quad \text{implica} \quad (a_\lambda, N(z))_F = 0,$$

Por outro lado, como vimos também em (5.1.2) que $a_\lambda \in D_K\langle 1, -z\rangle$, $(a_\lambda, z)_K = 0$.

Resumindo a discussão acima, temos que: se $(a_\lambda, N(z))_F = 0$ ou $(b_\lambda, N(x)_F = 0$, então $(b_\lambda, x)_K = 0$ e $(a_\lambda, z)_K = 0$.

Consequentemente $(x,z)_K \simeq (a,b)_K \in Q_K(z) \cap \operatorname{Im}\operatorname{Res} = \{\,0\,\}$, pelo item (2) do **Lema 5.1.5**. Assim $x \in D_K\langle 1, -z\rangle$, como afirmado.

Consideremos agora a situação em que $(a_\lambda, N(z))_F \neq 0$ que implica em $(b_\lambda, N(x))_F \neq 0$, como vimos acima.

Nesse caso, como $N(z)$, $N(x) \in F_\lambda$, temos que $(a_\lambda, N(z))_F = (b_\lambda, N(x))_F$, pois $Q_F(N(z)) = Q_F(N(x))$ tem ordem 2, por definição de F_λ. Conforme vimos na demonstração da **Proposição 4.1.13** podemos identificar a cada classe $(a,b)_K$ com o produto "cup" $\chi_a \cup \chi_b$, para $a, b \in K$. No caso das classes $(a_\lambda, z)_K$ e $(b_\lambda, z)_K$, como $a_\lambda, b_\lambda \in F$ essa identificação pode ser escrita, respectivamente, nas formas $\operatorname{Res}(\chi_{a_\lambda}) \cup \chi_z$ e $\operatorname{Res}(\chi_{b_\lambda}) \cup \chi_z$, com χ_{a_λ}, $\chi_{b_\lambda} \in H^1(G_2(F))$ e $\chi_z \in H^1(G_2(K))$. Dessa identificação obtemos por [**RZ**] que $\operatorname{Cor}((a_\lambda, z)_K) = (a_\lambda, N(z))_F$ e $\operatorname{Cor}((b_\lambda, z)_K) = (a_\lambda, N(z))_F$. Podemos então concluir que $\operatorname{Cor}((x,z)_K) = 0$. Como $\ker\operatorname{Cor} = \operatorname{Im}\operatorname{Res}$, $(x,z)_K \in Q_K(z) \cap \operatorname{Im}\operatorname{Res} = \{\,0\,\}$, pelo item (2) do **Lema 5.1.5**. Podemos então concluir que $x \in D_K\langle 1, -z\rangle$ conforme afirmado.

Caso IC$_2$ Tomemos agora $d \in F_\lambda$, mas $d \notin D_F\langle 1, -N(z)\rangle$. Recordemos que

$$(x,z)_K \simeq (a,b)_K + (a_\lambda, z)_K + (b_\lambda, x)_K$$

(lembrar que agora $\gamma = \lambda$). Aplicando-se Cor temos

$$\mathrm{Cor}((x,z)_K) = \mathrm{Cor}((a_\lambda, z))_K + \mathrm{Cor}((b_\lambda, x)_K) = (a_\lambda, N(z))_F + (b_\lambda, N(x))_F.$$

Caso $(a_\lambda, N(z))_F = 0$ teremos $a_\lambda \in D_F\langle 1, -N(z)\rangle = D_K\langle 1, -z\rangle \cap F$ implicando $(a_\lambda, z)_K = 0$. Resulta disso que $(x,z)_K = (a,b)_K + (b_\lambda, x)_K$. Como $(x,z)_K$, $(b_\lambda, x)_K \in Q_K(x)$ e $Q_K(x) \cap \mathrm{Im\,Res} = \{0\}$, devido a escolha de x, temos que $(a,b)_K = 0$ e assim $(x,z)_K = (b_\lambda, x)_K$. Se $(x,z)_K \neq 0$, como $Q_K(z) \cap \mathrm{Im\,Res} = \{0\}$ e $\ker \mathrm{Cor} = \mathrm{Im\,Res}$, resulta que $\mathrm{Cor}((x,z)_K) \neq 0$. Por outro lado $\mathrm{Cor}((x,z)_K) = \mathrm{Cor}((b_\lambda, x))_K = (b_\lambda, N(x))_F$, implicando que $(b_\lambda, N(x))_F \neq 0$. Logo $b_\lambda \notin D_F\langle 1, -N(x)\rangle$. Por hipótese $N(x) = d \notin D_F\langle 1, -N(z)\rangle$ e assim também $N(z) \notin D_F\langle 1, -N(x)\rangle$, pelo **Lema 1.1.1**. Como $(F_\lambda : D_F\langle 1, -N(x)\rangle \cap F_\lambda) = 2$, pelo item 2(a) do **Teorema 3.2.11**, vamos ter que $b_\lambda = N(z)g$, para algum $g \in D_F\langle 1, -N(x)\rangle = D_K\langle 1, -x\rangle \cap F$. Portanto $(b_\lambda, x)_K = (K, N(z))_x$, resultando que $(z,x)_K = (N(z), x)_K = (z,x)_K + (\sigma(z), x)_K$. Temos como consequência que $(\sigma(z), x)_K = 0$ implicando $(z, \sigma(x))_K = 0$. Assim $\sigma(x) \in D_K\langle 1, -z\rangle$. Como $N(\sigma(x)) = N(x)$ a afirmação fica demonstrada nesse caso.

Caso $(b_\lambda, N(x))_F = 0$, teremos como acima que $b_\lambda \in D_F\langle 1, -N(x)\rangle = D_K\langle 1, -x\rangle$, implicando em $(b_\lambda, x)_K = 0$. Como no caso anterior essa igualdade nos leva a $(a,b)_K = 0$ e portanto $(x,z)_K = (a_\lambda, z)_K$. Resulta disso que $(a_\lambda x, z)_K = 0$ e então $a_\lambda x \in D_K\langle 1, -z\rangle$. Como $d = N(x) = a_\lambda^{-2} N(a_\lambda x)$ teremos um representante da classe $d(F^\times)^2$ em $D_K\langle 1, -z\rangle$, conforme afirmado.

Assumimos finalmente que $(a_\lambda, N(z))_F \neq 0$ e $(b_\lambda, N(x))_F \neq 0$. Como $Q_F(N(z)) = Q_F(N(x))$ tem ordem 2, isso implica que $(a_\lambda, N(z))_F \simeq (b_\lambda, N(x))_F$. Logo $0 = (a_\lambda, N(z))_F + (b_\lambda, N(x))_F = \mathrm{Cor}((x,z)_K)$. Mas $\ker \mathrm{Cor} = \mathrm{Im\,Res}$ e $Q_K(z) \cap \mathrm{Im\,Res} = \{0\}$, pela escolha de z, logo $(x,z)_K = 0$ e temos novamente $x \in D_K\langle 1, -z\rangle$.

Fica assim demonstrado o **Caso I**.

Caso II: $\gamma \in J$.

Afirmação: *Para todo* $d \in D_F\langle 1, -c\rangle \cap F_\gamma$ *existe* $x \in K^\times$ *com* $D_K\langle 1, -x\rangle \cap F = D_F\langle 1, -d\rangle$ *e* $N(x)d^{-1} \in (F^\times)^2$ *tal que* $z \in F^\times D_K\langle 1, -x\rangle$ *(sem nenhuma restrição sobre* λ*).*

Vamos considerar duas situações.

IIA: $\lambda \in J$. Observe inicialmente que $(a_\lambda, b_\gamma)_K = 0$, pois $F^\times \subset D_K\langle 1, -a_\lambda\rangle$ já que $\lambda \in J$, pelo item (3) da **Proposição 4.1.5**.

Rearranjando a equação (5.1.1) temos que $(x,z)_K + (a_\lambda, z)_K = (a,b)_K + (a_\lambda, b_\gamma)_K + (b_\gamma, x)_K$. Logo $(a_\lambda x, z)_K + (b_\gamma, a_\lambda x)_K = (a,b)_K \in Q_K(a_\lambda x) \cap \mathrm{Im\,Res}$.

Pelo **Lema 1.1.3** temos que $D_K\langle 1, -a_\lambda\rangle \cap D_K\langle 1, -x\rangle = D_K\langle 1, -a_\lambda\rangle \cap D_K\langle 1, -a_\lambda x\rangle$ de forma que

$$F \cap D_K\langle 1, -a_\lambda\rangle \cap D_K\langle 1, -x\rangle = F \cap D_K\langle 1, -a_\lambda\rangle \cap D_K\langle 1, -a_\lambda x\rangle.$$

Como $F^\times \subset D_K\langle 1, -a_\lambda\rangle$, resulta que

$$F \cap D_K\langle 1, -x\rangle = F \cap D_K\langle 1, -a_\lambda x\rangle.$$

Recorde agora que $F \cap D_K\langle 1, -x\rangle = D_F\langle 1, -N(x)\rangle$, pela escolha de x. Como $D_F\langle 1, -N(x)\rangle = D_F\langle 1, -N(a_\lambda x)\rangle$ vamos obter também $F \cap D_K\langle 1, -a_\lambda x\rangle = D_F\langle 1, -N(a_\lambda x)\rangle$. Dessa forma podemos trocar x por $a_\lambda x$ na escolha do representante da classe $d(F^\times)^2$. Com essa escolha obtemos a igualdade $(x,z)_K - (b_\gamma, x)_K = (a,b)_K \in Q_K(x) \cap \operatorname{Im}\operatorname{Res} = \{0\}$, pelo **Teorema 3.2.17**. Concluímos assim que $(x,z)_K = (b_\gamma, x)_K$. Logo $(x, b_\gamma z)_K = 0$, implicando que $b_\gamma z \in D_K\langle 1, -x\rangle$. Logo $z \in F^\times D_K\langle 1, -x\rangle$, conforme afirmado.

IIB: $\lambda \notin J$. Logo $\gamma \neq \lambda$ para todo $\gamma \in J$ e assim pelo item (3) do **Lema 5.1.5** temos que $(x,z)_K \in {}_2\mathrm{Br}(K)^G$. Consequentemente, usando a equação (5.1.1), teremos

$$(a,b)_K + (a_\lambda, z)_K + (b_\gamma, x)_K \simeq (a,b)_K + (a_\lambda, \sigma(z))_K + (b_\gamma, \sigma(x))_K$$

e assim

$$(a_\lambda, N(z))_K = (b_\gamma, N(x))_K = 0 \in {}_2Br(K),$$

pois, como $N(x) \in F_\gamma$, com $\gamma \in J$, temos pelo item (3) da **Proposição 4.1.5** que $F^\times \subset D_K\langle 1, -N(x)\rangle$. Logo

$$a_\lambda \in D_K\langle 1, -N(z)\rangle \cap F = D_F\langle 1, -N(z)\rangle = D_K\langle 1, -z\rangle \cap F,$$

a primeira igualdade decorre do item (3) da **Proposição 4.1.5** e a segunda da escolha de z. Resulta então que $(a_\lambda, z)_K = 0$ e assim

$$(x,z)_K = (a,b)_K + (b_\gamma, x)_K.$$

Logo

$$(x, b_\gamma z)_K = (a,b)_K \in Q_K(x) \cap \operatorname{Im}\operatorname{Res} = \{0\},$$

pelo item (2) do **Lema 5.1.5**. Consequentemente, $(x, b_\gamma z)_K = 0$. Novamente obtemos $b_\gamma z \in D_K\langle 1, -x\rangle$ e assim $z \in F^\times D_K\langle 1, -x\rangle$, como queríamos.

Fica assim demonstrada a **Afirmação**.

Vamos a seguir tomar $d_1, \ldots, d_{n-t} \in D_F\langle 1, -c\rangle$ de forma que se $I(j) = \{\, 1 \leq i \leq n-t \mid d_i \in F_j \cap D_F\langle 1, -c\rangle \,\}$, então o conjunto $\{\, d_i \mid i \in I(j) \,\}$ é uma base de $F_j \cap D_F\langle 1, -c\rangle$ módulo $R(F)$, para todo $j \in J$. Isto é, $\{\, d_1, \ldots, d_{n-t} \,\}$ é uma base de $\prod_{j\in J} F_j$ módulo $R(F)$, pois $\dim_{\mathbb{F}_2} F^\times / D_F\langle 1, -c\rangle = t = \#J$, pelo **Teorema 3.2.14.**

Para cada $i \in I = \bigcup_{j\in J} I(j)$ seja $x_i \in K^\times$ para o qual vale a Afirmação do Caso II, isto é, $D_K\langle 1, -x_i\rangle \cap F = D_F\langle 1, -d_i\rangle$, $N(x_i)d_i^{-1} \in (F^\times)^2$, e $z \in F^\times D_K\langle 1, -x_i\rangle$. Pela escolha dos elementos $d_1, \ldots, d_{n-t}$, com a mesma demonstração do item (2) da **Proposição 3.2.3**, obtemos que esse conjunto tem a seguinte propriedade:

Para todo subconjunto $\{\, j_1, \ldots, j_s\} \subset \{\, 1, \ldots, n-t \,\}$ *e para todo* $j \in \{\, 1, \ldots, n-t \,\} \smallsetminus \{\, j_1, \ldots, j_s\}$ *vale*

$$\left(\bigcap_{k=1}^{s} D_F\langle 1, -d_{j_k}\rangle\right) D_F\langle 1, -d_j\rangle = F^\times.$$

Consequentemente, pela **Proposição 5.1.4** temos que

$$\left(\bigcap_{i\in I} F^\times D_K\langle 1,-x_i\rangle\right) = F^\times\left(\bigcap_{i\in I} D_K\langle 1,-x_i\rangle\right)$$

Como

$$z \in \left(\bigcap_{i\in I} F^\times D_K\langle 1,-x_i\rangle\right),$$

pela igualdade acima existe $f \in F^\times$ e $u \in (\bigcap_{i\in I} D_K\langle 1,-x_i\rangle)$ tal que $z = fu$. Seja agora $f = \prod_{\delta\in\Delta} f_\delta$, onde $\Delta \subset \Lambda$ e $f_\delta \in F_\delta \smallsetminus R(F)$ para todo $\delta \in \Delta$, a decomposição de f. Recorde que para todo $\delta \notin J$ temos $f_\delta \in D_F\langle 1,-d_i\rangle \subset D_K\langle 1,-x_i\rangle$, para todo $i \in I$. Dessa forma vemos que

$$\left(\prod_{i\notin J} f_i\right) u \in \left(\bigcap_{i\in I} D_K\langle 1,-x_i\rangle\right).$$

Podemos então assumir, sem perda de generalidade, que $\Delta \subset J$ e $f \in \prod_{j\in J} F_j$.

Finalmente, como $z = fu$ temos que $fz = f^2u \in D_K\langle 1,-x_j\rangle$, para todo $j \in J$. Consequentemente $x_j \in D_K\langle 1,-fz\rangle$, para todo $j \in J$.

Vamos manter fixos os elementos $d_i,\ \ x_i,\ i \in I$ e f obtidos, para cada $D_F\langle 1,-c\rangle \cap F_\gamma$, com $\gamma \in J$.

Observe agora que dado $d \in F_\gamma \cap D_F\langle 1,-c\rangle$, com $\gamma \in J$, existem $\varepsilon_i \in \{0,1\}$ tais que $d = \prod_{i\in I(\gamma)} d_i^{\varepsilon_i} r$, com $r \in R(F)$, pois $\{d_i \mid i \in I(\gamma)\}$ é uma base de $F_\gamma \cap D_F\langle 1,-c\rangle$ módulo $R(F)$.

Veremos no fim que os elementos fz e $D_K\langle 1,-fz\rangle$ encontrados satisfazem as hipóteses do Caso I, logo pelo Caso IA existe $y \in D_K\langle 1,-fz\rangle$ tal que $N(y)r^{-1}(F^\times)^2$.

Tomamos a seguir $x = \prod_{i\in I(\gamma)} x_i^{\varepsilon_i} \in D_K\langle 1,-fz\rangle$ teremos que $N(xy)d^{-1} \in (F^\times)^2$, pela escolha dos elementos $x_i,\ i \in I(\gamma)$ e y. Podemos então concluir que $\overline{N}(xy(K^\times)^2) = d(F^\times)^2$.

Para terminarmos a demonstração lembremos que pelo item (3) do **Teorema 4.1.7**,

$$D_K\langle 1,-f\rangle = \bigcap_{\delta\in\Delta} D_K\langle 1,-f_\delta\rangle, \quad \text{onde} \quad \Delta \subset J.$$

Como cada $f_\delta \in F_\delta$ com $\delta \in J$, pelo item (3) da **Proposição 4.1.5**, temos $F^\times \subset D_K\langle 1,-f_\delta\rangle$. Logo $F^\times \subset D_K\langle 1,-f\rangle$. Dessa forma

$$F \cap D_K\langle 1,-z\rangle = F \cap D_K\langle 1,-f\rangle \cap D_K\langle 1,-z\rangle = F \cap D_K\langle 1,-f\rangle \cap D_K\langle 1,-fz\rangle = F \cap D_K\langle 1,-fz\rangle,$$

onde a igualdade do meio decorre do **Lema 1.1.3**. Ainda $D_F\langle 1,-N(z)\rangle = D_F\langle 1,-N(fz)\rangle$. Logo, pelo Caso I, para todo $r \in R(F)$ existe $y \in D_K\langle 1,-fz\rangle$ tal que $\overline{N}(y(K^\times)^2) = r(F^\times)^2$. Ficando assim demonstrado o teorema.

□

Corolário 5.1.7. *Sejam F e $K = F(\sqrt{c})$ como no **Teorema 5.1.6**.*

1. *Para todo $z \in K^\times$ tal que $N(z) \in F_\lambda \smallsetminus R(F)$ com $\lambda \notin J$ e satisfazendo as condições $D_K\langle 1,-z\rangle \cap F = D_F\langle 1,-N(z)\rangle$ e $(K^\times : D_K\langle 1,-z\rangle) = 2$, temos que $Q_K(N(z)) = Q_K(z) \oplus Q_K(\sigma(z))$.*

   Mais ainda, para todo $\lambda \in \Lambda$ com $\lambda \notin J$ e $d \in F_\lambda \smallsetminus R(F)$ existe $z \in K^\times$ com $N(z)d^{-1} \in (F^\times)^2$ e satisfazendo $D_K\langle 1,-z\rangle \cap F = D_F\langle 1,-d\rangle, (K^\times : D_K\langle 1,-z\rangle) = 2$.

2. *Para todo $z \in K^\times$ tal que $N(z) \in F_j \smallsetminus R(F)$ com $j \in J$ e satisfazendo as condições $D_K\langle 1,-z\rangle \cap F = D_F\langle 1,-N(z)\rangle$ e $(K^\times : D_K\langle 1,-z\rangle) = 2$, temos que $Q_K(z) = Q_K(e_j)$, onde $e_j \in F_j\mathcal{R}(F)$.*

   Mais ainda, para todo $j \in J$ e $d \in D_F\langle 1,-c\rangle \cap F_j$, $d \notin R(F)$, existe $z \in K^\times$ com $N(z)d^{-1} \in (F^\times)^2$ e satisfazendo $D_K\langle 1,-z\rangle \cap F = D_F\langle 1,-d\rangle$, $(K^\times : D_K\langle 1,-z\rangle) = 2$.

3. *Escolhendo-se $d_\lambda \in F_\lambda \smallsetminus R(F)$ com $d_\lambda \in D_F\langle 1,-c\rangle$ e assumindo-se que para $\lambda \in J$ podemos tomar $d_\lambda \notin c_\lambda R(F)$, então existem $z_\lambda \in K^\times$ tais que $D_K\langle 1,-z_\lambda\rangle \cap F = D_F\langle 1,-d_\lambda\rangle$ para os quais temos*

$$ {}_2\mathrm{Br}(K) = \left(\bigoplus_{\lambda\notin J} Q_K(z) \oplus Q_K)(\sigma(z))\right) \bigoplus \left(\bigoplus_{j\in J} Q_K(z_j)\right). $$

Demonstração. (1) Como $(K^\times : D_K\langle 1,-z\rangle) = 2$ temos que $|Q_K(z)| = 2$. Vamos verificar que $Q_K(N(z)) = Q_K(z) \oplus Q_K(\sigma(z))$. Pelo item 2(a) do **Teorema 3.2.11** sabemos que $(F_\lambda : D_F\langle 1,-N(z)\rangle \cap F_\lambda) = 2$ e portanto existe $e \in F_\lambda$ com $e \notin D_F\langle 1,-N(z)\rangle$. Logo $e \notin D_K\langle 1,-z\rangle$ e assim $0 \neq (e,z)_K \in Q_K(e) \cap Q_K(z)$. Como $|Q_K(z)| = 2$ resulta que $Q_K(z) \subset Q_K(e)$. Como $e \in F_\lambda$, o item (4) da **Proposição 4.1.5** nos diz que $Q_K(e) = Q_K(N(z))$. Já o item (2) dessa proposição garante que $|Q_K(N(z))| = 4$.

Por outro lado, como $Q_K(\sigma(z)) = Q_K(z)^\sigma$, temos que $|Q_K(\sigma(z))| = 2$. Logo basta mostrarmos que $Q_K(\sigma(z)) \neq Q_K(z)$ para concluirmos que $Q_K(\sigma(z)) \cap Q_K(z) = \{0\}$. Temos também $Q_K(\sigma(z)) \subset Q_K(N(z))$, pois $Q_K(N(z))^\sigma = Q_K(N(z))$. Assim $Q_K(N(z)) = Q_K(z) \oplus Q_K)(\sigma(z))$.

Observe que $D_K\langle 1,-\sigma(z)\rangle \cap F = D_K\langle 1,-z\rangle \cap F$. Portanto $(\sigma(z),e)_K \neq 0$. Se $Q_K(\sigma(z)) = Q_K(z)$, então $(\sigma(z),e)_K = (z,e)_K$, e consequentemente $(N(z),e)_K = 0$. Nesse caso concluímos $e \in D_K\langle 1,-N(z)\rangle$, um absurdo, devido a escolha de e.

Para completarmos a demonstração deste item basta observarmos que o **Teorema 5.1.6** garante a existência de z para o qual as condições exigidas valem.

(2) Observe inicialmente que $|Q_K(z)| = 2$, pois $(K^\times : D_K\langle 1,-z\rangle) = 2$. Por outro lado $(F_j : D_F\langle 1,-N(z)\rangle \cap F_j) = 2$, pelo item 2(a) do **Teorema 3.2.11**.

Logo existe $e \in F_j$ com $e \notin D_F\langle 1,-N(z)\rangle$, implicando também que $e \notin D_K\langle 1,-z\rangle$. Assim $0 \neq (e,z)_K \in Q_K(e) \cap Q_K(z)$.

Como $(e,z)_K \neq 0$, o item (4) do **Teorema 4.1.1** garante que $e \notin c_jR(F)$ e portanto, pelo item (2) da **Proposição 4.1.5**, $|Q_K(e)| = 2$. Resulta então que $Q_K(e) = Q_K(z)$.

Devido ao **Teorema 5.1.6**, para todo $j \in J$ e $d \in D_F\langle 1,-c\rangle \cap F_j$, $d \notin R(F)$, existe $z \in K^\times$ satisfazendo as condições exigidas.

(3) Pelo **Corolário 4.1.10**, para $d_\lambda \in F_\lambda \smallsetminus R(F)$ para todo $\lambda \in \Lambda$ e escolhendo $d_\lambda \notin c_\lambda R(F)$, para $\lambda \in J$, temos que

$$ {}_2\mathrm{Br}(K) = \bigoplus_{\lambda\in\Lambda} Q_K(d_\lambda). $$

Logo, pelos itens (1) e (2) acima, basta trocarmos d_λ pelos apropiados z_λ para obtermos o resultado. □

Vamos a seguir demonstrar o Teorema 90 de Hilbert, versão para o Radical de Kaplansky, para extensões quadrática não radicais de corpos com base distinguida completa.

Teorema 5.1.8. *Para F e K como no **Teorema 5.1.6** temos*

$$ N^{-1}(R(F)) = F^\times R(K) \quad e \quad F^\times R(K) = F^\times R_o, $$

onde $R_o = \bigcap_{a\in F^\times} D_K\langle 1, -a\rangle$. Mais ainda, se $u \in N^{-1}(R(F))$ é tal que $F^\times \subset D_K\langle 1, -u\rangle$, então existe $f \in \prod_{j\in J} F_j$ tal que $fu \in R(K)$. Dessa forma $R_o = (\prod_{j\in J} F_j)R(K)$.

Demonstração. Dado $x \in K^\times$ tal que $N(x) \in R(F)$ e $N(x) \notin (F^\times)^2$, pelo item (2) do **Lema 5.1.1** existe $e \in F^\times$ tal que $F^\times \subset D_K\langle 1, -ex\rangle$. Pelo **Lema 5.1.1** isso implica que $u = ex \in \bigcap_{a\in F^\times} D_K\langle 1, -a\rangle = R_o$.

Tomamos $\{ a_1, \ldots, a_{n-t} \}$ a parte de uma base distinguida de F que está na contida em $D_F\langle 1, -c\rangle$ e é uma base de $D_F\langle 1, -c\rangle$ módulo $R(F)$. Sejam $z_1, \ldots, z_{n-t}$, de acordo com os itens (1) e (2) do **Corolário 5.1.7**, tais que $N(z_i)a_i^{-1} \in (F^\times)^2$, $D_K\langle 1, -z_i\rangle \cap F = D_F\langle 1, -N(z_i)\rangle = D_F\langle 1, -a_i\rangle$, e $|Q_K(z_i)| = 2$.

Claramente $N(u)N(z_i)^{-1} \notin (F^\times)^2$, para cada $i = 1, \ldots, n-t$, e pelo **Lema 5.1.5** podemos tomar A_k, $B_k \in F^\times$ tais que $A_k u + B_k z_i = 1$. Obtemos então, como no **Lema 5.1.1**, $(u, z_i)_K = (A_k, B_k)_K + (A_k, z_i)_K + (B_k, u)_K$. Como vimos acima que $F^\times \subset D_K\langle 1, -u\rangle$, teremos $(B_k, u)_K = 0$ e como $(u, z_i)_K$ e $(A_k, z_i)_K$ estão em $Q_K(z_i)$ que pela escolha de z_i satisfaz $Q_K(z_i) \cap \mathrm{Im}\,\mathrm{Res} = \{ 0, 1 \}$ pelo item (2) do **Lema 5.1.5** , obtemos também $(A_k, B_k)_K = 0$. Assim $(u, z_i)_K = (A_k, z_i)_K$, implicando $(A_k u, z_i)_K = 0$.

Portanto $A_k u \in D_K\langle 1, -z_i\rangle$, ou então $u \in F^\times D_K\langle 1, -z_i\rangle$, para todo $i = 1, \ldots, n-t$. Pela **Proposição 5.1.4** existe $a \in F^\times$ tal que $au \in D_K\langle 1, -z_i\rangle$, para todo $i = 1, \ldots, n-t$. Fixemos então para uso futuro que

$$ z_i \in D_K\langle 1, -au\rangle, \text{ para todo } i = 1, \ldots, n-t. \tag{5.1.3} $$

Vamos agora denotar por σ o gerador do grupo de Galois $G(K; F)$. Como $\sigma(au)au = N(au) \in R(F) \subset R(K)$, resulta que $D_K\langle 1, -\sigma(au)\rangle = D_K\langle 1, -auN(au)(au)^{-2}\rangle = D_K\langle 1, -au\rangle$, onde a última igualdade é válida pelo **Corolário 2.1.4**. Logo $\sigma(D_K\langle 1, -au\rangle) = D_K\langle 1, -au\rangle$ e portanto

$$ N(D_K\langle 1, -au\rangle) \subset D_K\langle 1, -au\rangle \cap F. \tag{5.1.4} $$

Vamos agora escrever $a = a^{(1)} f$ onde

$$a^{(1)} = \prod_{\lambda \notin J} a_\lambda^{\varepsilon_\lambda} \quad \text{e} \quad f = \prod_{j \in J} a_j^{\varepsilon_j}$$

com ε_λ, $\varepsilon_j \in \{0, 1\}$. Observe que $F^\times \subset D_K\langle 1, -f\rangle$. Resultando então que $F^\times \subset D_K\langle 1, -f\rangle \cap D_K\langle 1, -u\rangle = D_K\langle 1, -f\rangle \cap D_K\langle 1, -fu\rangle$, pelo **Lema 1.1.3**.

Analogamente $D_K\langle 1, -a^{(1)}\rangle \cap D_K\langle 1, -fu\rangle \cap F = F \cap D_K\langle 1, -fu\rangle \cap D_K\langle 1, -a^{(1)}fu\rangle$, ou então $D_K\langle 1, -au\rangle \cap F = D_K\langle 1, -a^{(1)}\rangle \cap F$, pois $a = a^{(1)}f$ e $D_K\langle 1, -fu\rangle \cap F = F$. Podemos concluir do item (3) da **Proposição 4.1.5** e do item (3) do **Teorema 4.1.7** que $D_K\langle 1, -a^{(1)}\rangle \cap F = D_F\langle 1, -a^{(1)}\rangle$. Juntando-se as duas última igualdades obtemos

$$D_K\langle 1, -au\rangle \cap F = D_F\langle 1, -a^{(1)}\rangle.$$

Dessa forma, pela equação (5.1.4) obtemos

$$N(D_K\langle 1, -au\rangle) \subset D_F\langle 1, -a^{(1)}\rangle.$$

A equação acima junto com a equação (5.1.3) implicam que para conveniente $y_i \in F^\times$ teremos $a_i = N(z_i)y_i \in D_F\langle 1, -a^{(1)}\rangle$, para todo $i = 1, \ldots, n-t$.

Recorde agora que pela escolha de $a_1, \ldots, a_{n-t}$, todo elemento $e \in D_F\langle 1, -c\rangle$ pode ser escrito na forma $e = \prod_{i=1}^{n-t} a_i^{\varepsilon_i} r$, onde $r \in R(F)$ e $\varepsilon_i \in \{0, 1\}$, para todo i. Como $R(F) \subset D_F\langle 1, -a^{(1)}\rangle$ podemos concluir que $e \in D_F\langle 1, -a^{(1)}\rangle$, isto é, $D_F\langle 1, -c\rangle \subset D_F\langle 1, -a^{(1)}\rangle$. Mas essa inclusão contradiz o item (1) do **Teorema 4.1.1** devido as decomposições de c e $a^{(1)}$, sem termos comuns.

Resulta dessa contradição que $a = f \in \prod_{j \in J} F_j$ e na verdade $D_K\langle 1, -fu\rangle \cap F = F^\times$ assim como $N(D_K\langle 1, -fu\rangle) \subset D_F\langle 1, -c\rangle = \text{Im } N$. Voltando porém a equação (5.1.3) vemos que para todo $i = 1, \ldots, n-t$ temos $a_i = N(z_i)y_i \in N(D_K\langle 1, -fu\rangle)$.

Vamos agora verificar que $R(F) \subset N(D_K\langle 1, -fu\rangle)$, módulo $(F^\times)^2$. Dado $r \in R(F)$, se $r \in N(u)(F^\times)^2$, temos $-fu \in D_K\langle 1, -fu\rangle$ tal que $N(fu)r^{-1} \in (F^\times)^2$. Para $r \in R(F)$ com $N(u)r^{-1} \notin (F^\times)^2$ seja $y \in K^\times$ tal que $N(y)r^{-1} \in (F^\times)^2$ e $F^\times \subset D_K\langle 1, -y\rangle$, conforme o item (2) do **Lema 5.1.1**. Sejam também e, $g \in F^\times$ tais que $e(fu) + gy = 1$ implicando que

$$(y, fu)_K = (e, g)_K + (e, y)_K + (fu, g)_K.$$

Como $F^\times \subset D_K\langle 1, -y\rangle$, conforme nossa escolha, $(e, y)_K = 0$. Vimos acima que $F^\times \subset D_K\langle 1, -fu\rangle$ também, logo $(fu, g)_K = 0$, restando $(y, fu)_K = (e, g)_K$. Pela **Proposição 3.2.15** existe $h \in F^\times$ tal que $(y, fu)_K = (h, fu)_K$. Novamente, como $h \in F$, temos que $(h, fu)_K = 0$. Dessa forma $(y, fu)_K = 0$ e $y \in D_K\langle 1, -fu\rangle$. (Na verdade $(F^\times)^2 = N(F^\times) \subset N(D_K\langle 1, -fu\rangle)$.)

Os dois últimos parágrafos implicam que

$$\overline{N}(D_K\langle 1, -fu\rangle/(K^\times)^2) = D_F\langle 1 - c\rangle/(F^\times)^2 = \overline{N}(K^\times/(K^\times)^2)$$

. Finalmente, como o núcleo de $\overline{N} = F^\times(K^\times)^2/(K^\times)^2$ está contido em $D_K\langle 1, -fu\rangle/(K^\times)^2$ vamos concluir que $D_K\langle 1, -fu\rangle = K^\times$. Assim $fu \in R(K)$ e como temos $f \in \prod_{j \in J} F_j$ resulta que $u \in \left(\prod_{j \in J} F_j\right) R(K)$, ficando demonstrado o resultado.

□

Corolário 5.1.9. *Com as mesmas hipótese do* ***Teorema 5.1.8*** *acima temos que*

$$\dim_{\mathbb{F}_2} K^\times/R(K) = 2(\dim_{\mathbb{F}_2} F^\times/R(F) - t)$$

onde $t = \#J = \dim_{\mathbb{F}_2} F^\times/D_F\langle 1, -c\rangle$.

Demonstração. Observe que o **Teorema 5.1.8** implica que a seguinte sequência é exata

$$1 \to (R(K)\cap F)/R(F) \to F^\times/R(F) \to K^\times/R(K)\xrightarrow{\overline{N}} D_F\langle 1, -c\rangle/R(F) \to 1,$$

onde $\overline{N}$ é induzida pela norma. Pelo **Teorema 3.2.14** temos que $\dim_{\mathbb{F}_2} D_F\langle 1, -c\rangle/R(F) = \dim_{\mathbb{F}_2} F^\times/R(F) - t$. Por outro lado, $\dim_{\mathbb{F}_2} (R(K)\cap F)/R(F) = t$, pelo item (4) do **Teorema 4.1.1**. Logo $\dim_{\mathbb{F}_2} \ker \overline{N} = \dim_{\mathbb{F}_2} F^\times/R(F) - t$ implicando o resultado proposto.

□

5.1.1 Base distinguida para uma 2-extensão finita de um corpo com base distinguida completa.

No **Teorema 3.2.27**, apresentamos a construção de uma base distinguida completa para uma extensão quadrática radical de um corpo F que possui base distinguida completa. Apresentaremos agora uma versão estendida desse fato, isto é, mostraremos que se F possui base distinguida completa, então toda $2-$extensão finita de de F também possui base distinguida completa.

Começaremos por fazer a construção, a partir do **Corolário 5.1.7**, da base para o caso de K ser uma extensão quadrática não radical de F.

Teorema 5.1.10. *Sejam F um corpo com base distinguida completa e uma extensão não radical $K = F(\sqrt{c})$, onde $c = \prod_{i\in I} c_i$ com $c_i \in F_i \smallsetminus R(F)$ e $I \subseteq \Lambda$, onde $\Lambda = \{1, \ldots, m\}$ é a partição principal. Então $K = F(\sqrt{c})$ possui base distinguida completa.*

Demonstração. Como no **Teorema 3.2.27**, a construção da base distinguida para o corpo K será a partir de uma base distinguida de F.

Vamos mostrar inicialmente que o conjunto $\{c_i;\, i \in I\}$, é linearmente independente sobre $R(F)$. Sem perda da generalidade, vamos supor que $I = \{1, \ldots, t\}$.

Suponhamos que $\prod_{j=1}^t c_j^{\varepsilon_j} = r \in R(F)$, com $\varepsilon_j \in \{0, 1\}$ para todo j. Sabemos, pelo item 2(a) do **Teorema 3.2.11**, para cada j temos que $(F_j : D_F\langle 1, -c_j\rangle \cap F_j) = 2$. Logo, novamente para cada j, existe $g_j \in F_j$ tal que $g_j \notin D_F\langle 1, -c_j\rangle$ e portanto $(c_j, g_j)_K \neq 0$. Por outro lado

$$0 = (g_j, c)_K = \sum_{i=1}^{t} (g_j, c_i)_K^{\varepsilon_i} = (g_j, c_j)_K^{\varepsilon_j},$$

pois $g_j \in D_F\langle 1, -c_i\rangle$ para todo $i \neq j$. Logo $\varepsilon_j = 0$. Como o argumento acima vale para todo j obtemos $\varepsilon_j = 0$ para todo $j = 1, \ldots, t$ e, consequentemente, o conjunto é linearmente independente.

Agora, podemos encontrar uma base distinguida completa de F que possui como subconjunto $\{c_1, \ldots, c_t\}$. Para tanto, consideremos os seguintes conjuntos:

- para cada $i = 1, \ldots, t$ seja $\{c_i, b_{i,1}, \ldots, b_{i,\lambda_i}\}$ uma base de $F_i/R(F)$
- para cada $j = t+1, \ldots, m$ seja $\{b_{j,1}, \ldots, b_{j,\lambda_j}\}$ uma base de $F_j/R(F)$.

Desta maneira, temos que

$$B = \left(\bigcup_{i=1}^{t} \{c_i, b_{i,1}, \ldots, b_{i,\lambda_i}\} \right) \cup \left(\bigcup_{j=t+1}^{m} \{b_{j,1}, \ldots, b_{j,\lambda_j}\} \right)$$

é uma base distinguida de $F^\times/R(F)$.

Agora, reordenando se necessário, podemos assumir que $c_1, \ldots, c_s$ são tais que $c_i \in D_F\langle 1, -c_i\rangle$ para todo $i = 1, \ldots, s$ e $c_i \notin D_F\langle 1, -c_i\rangle$ para $i = s+1, \ldots, t$. Ainda, para cada $i = 1, \ldots, s$ vamos assumir que $b_{i,1} \notin D_F\langle 1, -c_i\rangle$.

Faremos uso agora do **Corolário 5.1.7** para construir uma base de $K^\times/R(K)$ a partir da base B acima.

- Para cada c_i, com $i = 1, \ldots, s$, temos pelo **Corolário 5.1.7** que existe $z_i \in K^\times$ tal que $N(z_i) = c_i(F^\times)^2$ e $(K : D_K\langle 1, -z_i\rangle) = 2$. Ainda, temos que $Q_K(z_i) = Q_K(b_{i,1})$.
- Para cada $b_{i,k}$, onde $i = 1, \ldots, s$ e $k = 2, \ldots, \lambda_i$, novamente pelo **Corolário 5.1.7**, existe $z_{i,k} \in K^\times$ tal que $N(z_{i,k}) = b_{i,k}(F^\times)^2$, $(K : D_K\langle 1, -z_{i,k}\rangle) = 2$ e $Q_K(z_{i,k}) = Q_K(b_{i,k})$.
- Para cada $b_{i,k}$, onde $i = s+1, \ldots, t$ e $k = 1, \ldots, \lambda_i$, novamente pelo **Corolário 5.1.7**, existe $z_{i,k} \in K^\times$ tal que $N(z_{i,k}) = b_{i,k}(F^\times)^2$, $(K : D_K\langle 1, -z_{i,k}\rangle) = 2$ e $Q_K(z_{i,k}) = Q_K(b_{i,k})$.
- Para cada $b_{j,k}$, onde $j = t+1, \ldots, m$ e $k = 1, \ldots, \lambda_j$, novamente pelo **Corolário 5.1.7**, existe $z_{j,k} \in K^\times$ tal que $N(z_{j,k}) = b_{j,k}(F^\times)^2$, $(K : D_K\langle 1, -z_{i,k}\rangle) = (K : D_K\langle 1, -\sigma(z_{i,k})\rangle) = 2$ e $Q_K(b_{j,k}) = Q_K(z_{j,k}) \oplus Q_K(\sigma(z_{j,k}))$.

Considere agora os seguintes conjuntos:

- $C_1 = \bigcup_{i=1}^{s} \{z_i, z_{i,2}, \ldots, z_{i,\lambda_i}, b_{i,1}, \ldots, b_{i,\lambda_i}\}$
- $C_2 = \bigcup_{i=s+1}^{t} \{z_{i,1}, \ldots, z_{i,\lambda_i}, b_{i,1}, \ldots, b_{i,\lambda_i}\}$
- $C_3 = \bigcup_{i=t+1}^{m} \{z_{i,1}, \ldots, z_{i,\lambda_i}\}$
- $C_4 = \bigcup_{i=t+1}^{m} \{\sigma(z_{i,1}), \ldots, \sigma(z_{i,\lambda_i})\}$

Tomando $C = C_1 \cup \cdots \cup C_4$, temos que cada $z \in C$, temos que $(K : D_K\langle 1, -z\rangle) = 2$ e $\#C = 2(\dim_{\mathbb{F}_2} F^\times/R(F) - t) = \dim_{\mathbb{F}_2} K^\times/R(K)$, pelo **Corolário 5.1.9**. Ainda, pelo item (3) do **Corolário 5.1.7** que

$$ {}_2Br(K) = \bigoplus_{i=1}^{m} Q_K(b_{i,1}) = \left(\bigoplus_{i=1}^{t} Q_K(b_{i,1})\right) \oplus \left(\bigoplus_{i=t+1}^{m} Q_K(z_{i,1})\right) \oplus \left(\bigoplus_{i=t+1}^{m} Q_K(\sigma(z_{i,1}))\right). $$

Vamos mostrar que C é um conjunto gerador do $\mathbb{F}_2-$espaço vetorial $K^\times/R(K)$, para tanto, considere $z \in K^\times/R(K)$.

Caso I: Se $N(z) \in R(F)$, então pelo **Teorema 5.1.8**, temos que $z \in F^\times R(K)$, isto é, $z = fr$, onde $f \in F^\times/R(F)$. Desta maneira, temos que f pertence ao espaço gerado por

$$ \left(\bigcup_{i=1}^{t}\{c_i, b_{i,1}, \ldots, b_{i,\lambda_i}\}\right) \cup \left(\bigcup_{j=t+1}^{m}\{b_{j,1}, \ldots, b_{j,\lambda_j}\}\right). $$

Como $c_i \in R(K)$, para todo $i = 1, \ldots, t$ pelo ítem 4 do **Teorema 4.1.1**, temos então que f pode ser tomado no subespaço gerado por

$$ \left(\bigcup_{i=1}^{t}\{b_{i,1}, \ldots, b_{i,\lambda_i}\}\right) \cup \left(\bigcup_{j=t+1}^{m}\{b_{j,1}, \ldots, b_{j,\lambda_j}\}\right). $$

Portanto, temos que f pertence ao subespaço gerado por $\bigcup_{i=1}^{t}\{b_{i,1}, \ldots, b_{i,\lambda_i}\}, C_3, C_4$. Portanto z é gerado por C.

Caso II: Se $N(z) \notin R(F)$, então $N(z) \in x(F^\times)^2$, onde $x \in F^\times \setminus R(F)$ e consequentemente, x gerado pela base B de $F^\times \setminus R(F)$. Daí, $x = x_1 \cdots x_n$, onde $x_i \in B$ para $i = 1, \ldots, n$. Pela construção do conjunto C, existem $y_1, \ldots, y_n \in C$ tais que $N(y_i) = x_i$. Logo, $y = y_1 \cdots y_n$ é tal que $N(z) = N(y)(F^\times)^2$ e pelo **Teorema 1.1.4** segue que $z \in y(K^\times)^2$. Portanto, a classe de z em $K^\times/R(K)$ é também gerada por C.

Finalmente, como C é um conjunto gerador do $\mathbb{F}_2$-espaço vetorial $K^\times \setminus R(K)$ com $\#C = \dim_{\mathbb{F}_2} K^\times/R(K)$, temos que C é um base.

□

Finalmente, apresentaremos um Corolário que garante a existência de uma base distinguida para toda $2-$extensão finita de F.

Corolário 5.1.11. *Se F é um corpo com base distinguida completa, então toda $2-$extensão finita K de F possui base ditinguida completa.*

Demonstração. Sabemos, pelos **Teoremas 3.2.27 e 5.1.10**, que qualquer que seja M corpo com base distuinguida completa, então toda extensão quadrática L de M possui base distuinguida completa. Portanto, o resultado segue por indução sobre o grau da 2-extensão.

□

Bibliografia

[A] J. K. Arason, Cohomologische Invarianten quadratischer Formen. J. Algebra **36** (1975), 448-491.

[BNW] E. Binz, J. Neukirch, G.H. Wenzel, A subgroup theorem for free products of pro-finite groups. J. Algebra **19** (1971), 104-109.

[B] K. J. Becher, Le radical de Kaplansy. Théorie des nombres, Années 1998/2001, 27pp.

[C] C.M. Cordes, Kaplansky's radical and quadratic forms over non-real fields. Acta Arithmetica **28** (1975), 253-271.

[CR] C. M. Cordes, J. R. Ramsey Jr., Quadratic forms over quadratic extensios of fields with two quaternio algebras. Can. J. Math. **31** (1979), 1047-1058.

[EL] R. Elman, T.Y. Lam, Quadratic forms under algebraic extensions. Math. Ann. **219** (1976), 21-42.

[EL] R. Elman, T.Y. Lam, Quadratic forms over formally real fields and pythagorean fields. Amer. J. Math. **94**, (1972), 1155-1194.

[EP] R. Elman, A. Prestel, Reduced Stability Of The Witt Ring Of A Field And Its Pythagorean Closure. Amer. J. Math. **106** (1984), 1237-1260.

[ELP] R. Elman, T.Y. Lam, A. Pretel, On some Hasse principles over formally real fields. Math. Z. **134** (1973), 291-301.

[Er] Yu. L. Ershov, Galois groups of maximal 2-extensions. Mat. Zametki **36** (1984), 921-923 (Russian); Math. Notes **36** (1985), 956-961.

[H] D. Haran, On Closed Subgroups of Free Products of Profinite Groups. Proc. London Math. Soc **55** (1987), 266-298.

[HJ] D. Haran, M. Jarden, Real free groups and the absolute Galois group of $\mathbb{R}(t)$. J. Pure Appl. Algebra **37** (1985), 155-165.

[HR] W. N. Herfort, L. Ribes, Torsion elements and centralizers in free products of profinite groups. J. reine angew. Math. **358** (1985), 155-161.

[JW] B. Jacob, R. Ware, A recursive description of the maximal por-2 Galois group via Witt rings. *Math. Z.* **200** (1989) 379-396.

[K] I. Kaplansky, Fröhlich's local quadratic forms. J. reine angew. Math. **39/40** (1969), 74-77.

[KN] D. Kijima, M. Nishi, Kaplansky's radical and Hilbert Theorem 90 II, Hiroshima Math. J. **13** (1983), 29-37.

[KMRT] M.-A., Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, American Math. Soc. 1998.

[L] T. Y. Lam, The Algebraic Theory of Quadratic Forms. American Math. Soc. 2000.

[L2] T. Y. Lam, Orderings, Valuations and Quadratic Forms. Conference Board of the Mathematical Science, Number 52. Providence, RI: Amer. Math. Soc. 1983.

[La] Lang, S., Algebra. Springer-Verlag. 2002.

[LLMS] J. Labute, N. Lemire, J. Mináč, J. Swallow, Demushkin groups, Galois Modules, and the Elementary Type Conjecture, J. Algebra, **304** (2006), 1130-1146.

[M] M. Marshall, Abstract Witt rings, Queen's Papers in Pure and Appl. Math., Vol 57, Kingston, Ontario, 1980.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Springer 2000.

[OVV] D. Orlov, A. Vishik, V. Voedovsky, An exact sequence for Milnor's K-theory with applications to quadratic forms, preprint (2001), `arxiv.org/abs/math/0101023`

[P] A. Prestel, Lectures on Formally Real Fields, IMPA, Rio de Janeiro, 1975 (and Springer Lecture Notes **1093**).

[PW] A. Prestel, R. Ware, Almost isotropic quadratic forms. J. London Math. Soc. **19** (1979), 241-244.

[R] L. Ribes, Introduction of Profinite Groups and Galois Cohomology. Queen's Papers in Pure and Applied Math. N$^{\underline{0}}$ 24, 1970.

[RZ] L. Ribes, P. Zalesski, Profinite Groups, Springer 2000.

[Se] J.-P. Serre, Cohomologie Galoissienne. Cinquième édition, Springer-Verlag, 1994.

[S] S. S. Shatz, Profinite Groups, Arithmetic and Geometry. (Annals of Mathematics Studies, 67) Princeton: Princeton University Press 1972.

[V1] V. Voevodsky, Reduced power operations in motivic cohomology, Publ. Math. IHES **98** (2003), 1-57.

[V2] V. Voevodsky, Motivic cohomology with $\mathbb{Z}/2\mathbb{Z}$-coefficients, Publ. Math. IHES **98** (2003), 59-104.

[W] R. Ware, Witt rings and almost free pro-2 groups, J. Algebra, **132** (1990), 377-383.