UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

K-teoría de Milnor e cohomología de Galois

Elvis Torres Pérez

Dissertação de Mestrado do Programa de Pós-Graduação em
Matemática (PPG-Mat)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Elvis Torres Pérez

K-teoría de Milnor e cohomología de Galois

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Matemática. *EXEMPLAR DE DEFESA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Behrooz Mirzaii

USP – São Carlos
Março de 2019

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

T693k Torres Pérez, Elvis
 K-teoría de Milnor e cohomología de Galois / Elvis
 Torres Pérez; orientador Behrooz Mirzaii. -- São
 Carlos, 2019.
 74 p.

 Dissertação (Mestrado - Programa de Pós-Graduação
 em Matemática) -- Instituto de Ciências Matemáticas
 e de Computação, Universidade de São Paulo, 2019.

 1. K-Teoria Algébrica. 2. Cohomología de Galois.
 3. Grupo de Brauer. 4. Corpos Globais. I. Mirzaii,
 Behrooz, orient. II. Título.

Elvis Torres Pérez

Milnor K-theory and Galois cohomology

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of the Master Program in Mathematics. *EXAMINATION BOARD PRESENTATION COPY*

Concentration Area: Mathematics

Advisor: Prof. Dr. Behrooz Mirzaii

USP – São Carlos
March 2019

*Este trabalho é dedicado aos cientistas que amam a matemática,
e especialmente àqueles que aman e respeitam os números
tanto quanto ou até mais do que eu.*

AGRADECIMENTOS

Os agradecimentos principais são direcionados a minha família e amigos, gracias a eles não poderia estar aqui. Ao professor Carlos Ivorra Castillo¹ da Universidad de Valencia em España cujos livros são minha principal inspiração.

Agradecimentos especiais são direcionados ao Instituto de Ciências Matemáticas e de Computação (ICMC) por acreditar em mim, e à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pois graças a eles eu posso pesquisar sem mais preocupações.

¹ <<http://www.uv.es/ivorra>>

*“Há homens que lutam um dia e são bons.
Há outros que lutam um ano e são melhores.
Há aqueles que lutam muitos anos e são muito bons.
Mas há aqueles que lutam todas as suas vidas, esses são os essenciais.”*
(Bertolt Brecht)

RESUMO

PÉREZ, E. T. **K-teoría de Milnor e cohomología de Galois**. 2019. 74 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Aa presente dissertação é dedicada ao estudo de uma conexão profunda entre o K -grupo K_2 para um corpo global F e a cohomología de Galois de seu grupo de Galois absoluto $G = \text{Gal}(F^{\text{sep}}/F)$ com coeficientes no G -módulo $\mathbf{Z}_l(2) = \mathbf{Z}_l(1) \otimes_{\mathbf{Z}_l} \mathbf{Z}_l(1)$ onde $\mathbf{Z}_l$ é o grupo dos inteiros l -adicos, $\mathbf{Z}_l(1) = \varprojlim \mu_{l^i}$ e μ_{l^i} é o grupo das raízes l^i -ésimas da unidade. O objetivo principal é expresar $K_2 F$ como soma direita de $H^2(G, \mathbf{Z}_l(2))$ onde l recorre todos os primos diferentes da característica de F , em outras palavras.

$$K_2 F = \bigoplus_{l: \text{primo}, l \neq \text{char}(F)} H^2(G, \mathbf{Z}_l(2))$$

Palavras-chave: K-Teoria Algébrica, Cohomología de Galois, Grupo de Brauer, Corpos Globais.

ABSTRACT

PÉREZ, E. T. **Milnor K-theory and Galois cohomology**. 2019. 74 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

The present dissertation is concerned with a deep connection between the K -group K_2 for a global field F and the Galois cohomology of its absolute Galois group $G = \text{Gal}(F^{\text{sep}}/F)$ with coefficients in the G -module $\mathbf{Z}_l(2) = \mathbf{Z}_l(1) \otimes_{\mathbf{Z}_l} \mathbf{Z}_l(1)$ where $\mathbf{Z}_l$ is the group of l -adic integers, $\mathbf{Z}_l(1) = \varprojlim \mu_{l^i}$ and μ_{l^i} is the group of the l^i -roots of unity. The main objective is express K_2F as a direct sum of $H^2(G, \mathbf{Z}_l(2))$ where l runs over all the primes different from the characteristic of F , in other words.

$$K_2F = \bigoplus_{l:\text{prime}, l \neq \text{char}(F)} H^2(G, \mathbf{Z}_l(2))$$

Keywords: Algebraic K-Theory, Galois Cohomology, Brauer Group, Global Field.

SUMÁRIO

1	COHOMOLOGIA	17
1.1	Cohomología de Cocadeia Contínua	17
1.1.1	<i>Definição e exemplos</i>	17
1.1.2	<i>Propriedade da sequência exata longa</i>	18
1.1.3	<i>Produtos cup</i>	19
1.1.4	<i>Restrição y Transferência</i>	20
1.2	Cohomología l -ádica	20
2	TEORIA K ALGÉBRICA	25
2.1	O funtor K_0	25
2.2	O funtor K_1	27
2.3	O funtor K_2	29
2.4	O produto $K_1A \otimes K_1A \rightarrow K_2A$ e os símbolos de Steinberg	31
2.5	O homomorfismo de Transferência	33
3	ALGEBRAS SIMPLES CENTRAIS E O GRUPO DE BRAUER	37
3.1	Algebras cíclicas e o grupo de Brauer	37
3.2	Restrição e corpos de divisão	41
3.3	Grupo de Brauer cohomológico	43
3.4	Grupo de brauer de corpos locais e globais	46
4	O SIMBOLO DE GALOIS E A REPRESENTAÇÃO DE K_2 PARA UM CORPO GLOBAL	55
4.1	O Símbolo l -ádico	55
4.2	O morfismo h_1	57
4.2.1	<i>Criterio para a injetividade de h_1</i>	64
4.3	O teorema principal para corpos globais	69
	REFERÊNCIAS	73

COHOMOLOGIA

1.1 Cohomología de Cocadeia Contínua

1.1.1 Definição e exemplos

Nesta seção revisaremos as definições básicas e propriedades da teoria de cohomologia que precisamos para esta dissertação. Seja G um grupo topológico e M um G -módulo topológico. Para cada inteiro $n \geq 0$ denotamos por $C^n(G, M)$ ao grupo abeliano das funções contínuas de G^n (com $G^0 = e$) a M , criamos então um complexo com os seguintes homomorfismos:

$$d_n : C^n(G, M) \rightarrow C^{n+1}(G, M), \quad d_n(s_1, s_2, \dots, s_{n+1})$$

Dado por $(d_n \phi)(g_1, g_2, \dots, g_{n+1}) =$

$$g_1 \phi(g_2, \dots, g_{n+1}) + \sum_{j=1}^n (-1)^j \phi(g_1, \dots, g_j g_{j+1}, \dots, g_{n+1}) + (-1)^{n+1} \phi(g_1, \dots, g_n).$$

Note que isto lembra ao grupo de n -cocadeias não homogêneas de G com coeficientes em M visto na cohomologia de grupos (veja o capítulo II de (MILNE, 2013)), logo pela forma é um complexo (também se pode ver tras unos cálculos prolijos). Nesse contexto também podemos definir

$$Z^n(G, M) = \ker(d_n) \quad (\text{grupo de } n\text{-cociclos})$$

e

$$B^n(G, M) = \text{im}(d_{n-1}) \quad (\text{grupo de } n\text{-cofronteiras})$$

Então a cohomologia de grupos deste complexo é definido por $H^n(G, M) = Z^n(G, M) / B^n(G, M)$. Não é difícil mostrar que o grupo $H^0(G, M) = Z^0(G, M)$ é isomorfo a M^G (o subconjunto de M onde G age trivialmente) via o mapa $f \mapsto f(e)$.

Exemplo 1.1.1. 1. *Cohomología de grupos profinitos* Como se sabe, os grupos profinitos são grupos topológicos que vêm de limite projetivo de grupos finitos (discretos), estes são compactos e totalmente desconexos. Mostrar que um destes grupos G age continuamente sobre um grupo abeliano discreto M (e asi ter um G -módulo discreto) é equivalente a mostrar a igualdade $M = \bigcup M^H$ onde H recorre os subgrupos abertos de G , assim podemos ter $H^n(G, M)$. Sobre as propriedades da cohomología de Galois a ser usadas, pode encontrar mais informação nas seções *Cohomology* e *The Cohomology of Profinite Groups* de (MILNE, 2013).

2. *Cohomología de Galois* O grupo de Galois absoluto $G = \text{Gal}(F_s/F)$ para um corpo F (F_s denota a clausura separável de F) é um grupo profinito, pois é limite projetivo dos grupos correspondentes às subextensões finitas de Galois de F_s/F . Pelo teorema de Galois, as extensões finitas se correspondem com os subgrupos abertos, e se $x \in F_s$ então $x \in F_s^H$ com $H = \text{Gal}(F(x)/F)$ aberto em G . Assim G age continuamente sobre F_s e qualquer de seus subgrupos, e logo faz sentido escrever $H^n(G, F_s)$, $H^n(G, \mu_l)$ onde μ_l é o grupo das raízes l -ésimas da unidade, etc.

1.1.2 Propriedade da sequência exata longa

Proposição 1.1.1. Suponha que a seguinte sequência exata de G -módulos topológicos

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

é tal que a topología de L é induzida pela topología de M , e que o mapa $M \rightarrow N$ tem uma seção contínua (que não precisa ser um homomorfismo). Então a seguinte sequência de complexos

$$0 \longrightarrow C^\bullet(G, L) \longrightarrow C^\bullet(G, M) \longrightarrow C^\bullet(G, N) \longrightarrow 0$$

é exata, e logo obtemos uma sequência cohomológica exata

$$\cdots \longrightarrow H^n(G, M) \longrightarrow H^n(G, N) \xrightarrow{\delta} H^{n+1}(G, L) \longrightarrow H^{n+1}(G, M) \longrightarrow \cdots$$

Demonstração. Considere o diagrama comutativo

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & Z^n(G, L) & \longrightarrow & Z^n(G, M) & \longrightarrow & Z^n(G, N) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & C^n(G, L) & \longrightarrow & C^n(G, M) & \longrightarrow & C^n(G, N) \longrightarrow 0 \\
 & & \downarrow n & & \downarrow n & & \downarrow n \\
 0 & \longrightarrow & C^{n+1}(G, L) & \longrightarrow & C^{n+1}(G, M) & \longrightarrow & C^{n+1}(G, N) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \frac{Z^{n+1}(G, L)}{d_n C^n(G, L)} & \longrightarrow & \frac{Z^{n+1}(G, M)}{d_n C^n(G, M)} & \longrightarrow & \frac{Z^{n+1}(G, N)}{d_n C^n(G, N)} \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Usando no diagrama acima (sumando ou restando 1 convenientemente) pelo 'Snake Lemma' temos que as linhas horizontais do diagrama abaixo são exatas

$$\begin{array}{ccccccc}
 \frac{C^n(G, L)}{d_{n-1} C^{n-1}(G, L)} & \longrightarrow & \frac{C^n(G, M)}{d_{n-1} C^{n-1}(G, M)} & \longrightarrow & \frac{C^n(G, N)}{d_{n-1} C^{n-1}(G, N)} & \longrightarrow & 0 \\
 \downarrow d_n & & \downarrow d_n & & \downarrow d_n & & \\
 0 & \longrightarrow & Z^{n+1}(G, L) & \longrightarrow & Z^{n+1}(G, M) & \longrightarrow & Z^{n+1}(G, N)
 \end{array}$$

e como o núcleo de d_n em cada linha vertical é $H^n(G, \cdot)$ e o conúcleo é $H^{n+1}(G, \cdot)$ usando de novo o 'Snake Lemma' temos resultado. $\square$

Note que as condições do teorema são facilmente cumpridas quando L é um submódulo aberto de M já que $N = M/L$ com a topologia cociente é discreto (e toda seção é contínua).

1.1.3 Produtos cup

Suponha que $\cdot : M_1 \times M_2 \rightarrow M$ é um mapa contínuo e biaditivo tal que $(gx_1) \cdot (gx_2) = g(x_1 \cdot x_2)$ para $x_i \in M_i$, $s \in G$. Então para cada $m, n \geq 0$, $\cdot$ induz mapas biaditivos

$$C^m(G, M_1) \times C^n(G, M_2) \rightarrow C^{m+n}(G, M)$$

via as formulas bem conhecidas

$$(f \cup g)(s_1, \dots, s_{m+n}) = f(s_1, \dots, s_m) \cdot s_1 \cdots s_m g(s_{m+1}, \dots, s_{m+n})$$

Tras unos cálculos prolijos podemos provar a formula

$$\delta(f \cup g) = (\delta f) \cup g + (-1)^m f \cup (\delta g)$$

o que induz os mapas

$$H^m(G, M_1) \times H^n(G, M_2) \rightarrow H^{m+n}(G, M)$$

1.1.4 Restrição y Transferência

Seja H um subgrupo de G e M um G -módulo topológico, a *restrição* de cocadeias de G a H define homomorfismos de complexos $C^\bullet(G, M) \rightarrow C^\bullet(H, M)$ que logo induzem homomorfismos de *restrição*

$$\text{res} : H^n(G, M) \rightarrow H^n(H, M)$$

A restrição comuta com os mapas da sequência cohomológica exata (em particular com o morfismo de fronteira δ). Em dimensão 0 coincide com a inclusão $M^G \hookrightarrow M^H$.

Se H é aberto e de índice finito em G , então existe um homomorfismo de *transferência* na direção oposta à restrição. Seja R um conjunto de representantes das clases laterais direitas de H em G tal que $G = \cup_{r \in R} Hr$ é uma união disjunta. Com a ajuda de R definimos um homomorfismo de complexos $t_R : C^\bullet(H, M) \rightarrow C^\bullet(G, M)$ assim:

$$t_R f(s_1, \dots, s_n) = \sum_{r \in R} r_0^{-1} f(r_0 s_1 r_1^{-1}, r_1 s_2 r_2^{-1}, \dots, r_{n-1} s_n r_n^{-1})$$

onde $r_i \in R$ são determinado indutivamente em função de r e a n -upla $(s_1, \dots, s_n) \in G^n$ por

$$r_0 = r \quad \text{e} \quad r_{i-1} s_i \equiv r_i \pmod{H(\text{direita})}$$

Se R' é outro conjunto de representantes, temos que t_R e $t_{R'}$ são homotópicos, assim obtemos o homomorfismo de transferência (na proposição 2-5-2 de (WEISS, 1969) pode encontrar esta fórmula explícita).

$$\text{tr} : H^n(H, M) \rightarrow H^n(G, M)$$

Em dimensão 0 a transferencia é a traza $M^H \rightarrow M^G$ dada por $x \mapsto \sum_{x \in R} r^{-1} x$. Como é usual, a transferência comuta com os mapas da sequência cohomológica exata. No produto cup tras mais cálculos prolijos temos a fórmula:

$$\text{tr}(x \cup \text{res}(y)) = (\text{tr}(x)) \cup y \quad \text{para} \quad x \in H^m(H, M_1), \quad y \in H^n(G, M_2)$$

.

1.2 Cohomología l -ádica

Nesta seção, l é um número primo, $\mathbf{Z}_l$ é o anel dos inteiros l -ádicos e T é um G -módulo topológico tal que, como grupo topológico, é um $\mathbf{Z}_l$ -módulo finitamente gerado com a topología l -ádica e onde G age linearmente.

Proposição 1.2.1. Seja Y um $\mathbf{Z}_l$ -submódulo de $H^n(G, T)$ finitamente gerado. O grupo cociente $H^n(G, T)/Y$ não contém nenhum subgrupo l -divisível não nulo.

Demonstração. Seja Z um subgrupo l -divisível de $H^n(G, T)/Y$ e seja $x_0 + Y \in Z$, so precisamos mostrar que $x_0 \in Y$. Como Z é l -divisível podemos escrever $x_0 \equiv lx_1 \pmod{Y}$ para algum $x_1 + Y \in Z$, assim existem $x_i + Y \in Z$ onde $i \geq 0$, que satisfaz a equação $x_i \equiv lx_{i+1} \pmod{Y}$. Sejam também y_j , com $1 \leq j \leq m$, os geradores de Y . Para cada $i \geq 0$ seja f_i o n -cociclo representante de x_i e o $(n-1)$ -cociclo h_i , para $1 \leq j \leq m$ seja g_j o n -cociclo representante de y_j e logo para cada $i \geq 0$.

$$f_i = lf_{i+1} + \sum_{j=1}^m a_{ij}g_j + dh_i$$

Multiplicando a equação por l^i e somando sobre i temos.

$$\sum_{i \geq 0} l^i f_i = \sum_{i \geq 1} l^i f_i + \sum_{i \geq 0} \sum_{j=1}^m l^i a_{ij}g_j + \sum_{i \geq 0} l^i dh_i$$

Reordenando termos

$$f_0 = \sum_{j=1}^m \left(\sum_{i \leq 0} l^i a_{ij} \right) g_j + d \left(\sum_{i \leq 0} l^i h_i \right)$$

Fazendo $a_j = \sum_{i \leq 0} l^i a_{ij}$ e $h = \sum_{i \leq 0} l^i h_i$ temos

$$f_0 = \sum_{j=1}^m a_j g_j + dh$$

Finalmente passando à cohomologia temos que

$$x_0 = \sum_{j=1}^m a_j y_j$$

E assim $x_0 \in Y$. □

Observação 1.2.1. Como estamos trabalhando em $\mathbf{Z}_l$ -módulos e $\mathbf{Z}_l$ é noetheriano (de fato é um domínio de ideais principais) temos que $\varprojlim T/l^i T \simeq \hat{T} \simeq^* \hat{\mathbf{Z}}_l \otimes_{\mathbf{Z}_l} T \simeq \mathbf{Z}_l \otimes_{\mathbf{Z}_l} T \simeq T$ e isto logo implica que

$$C^n(G, T) = \varprojlim C^n(G, T/l^k T)$$

Logo temos que todo $f_i \in C^n(G, T)$ é de fato $(f_i^k)_{k \in \mathbb{N}}$ com $f_i^k : G \rightarrow T/l^k T$, e assim

$$\sum_{i \leq 0} l^i f_i = \left(\sum_{i=0}^{k-1} l^i f_k^i \right)_{k \in \mathbb{N}}$$

o que justifica as somas infinitas na prova acima. O isomorfismo $*$ pode encontra-lo em (ATIYAH; MACDONALD, 2016) (Proposição 10.13).

Corolário 1.2.1. O $\mathbf{Z}_l$ -módulo $H^n(G, T)$ é finitamente gerado se e somente se $H^n(G, T)/lH^n(G, T)$ é finito.

Demonstração. Suponha que $H^n(G, T)/lH^n(G, T) = \{x_i + lH^n(G, T) \mid i = 1, \dots, n\}$, definimos $Y = \langle x_i \mid i = 1, \dots, n \rangle$ então $H^n(G, T) = lH^n(G, T) + Y$ e tomando cociente conseguimos

$$H^n(G, T)/Y = l(H^n(G, T)/Y)$$

o que implica que $H^n(G, T)/Y$ é l -divisível. Usando a proposição temos que

$$H^n(G, T) = Y$$

y assim $H^n(G, T)$ é finitamente gerado. Agora suponha que $H^n(G, T) = \langle x_i \mid i = 1, \dots, n \rangle$, seja $x \in H^n(G, T)$ então $x = \sum_{i=1}^n a_i x_i$ com $a_i \in \mathbf{Z}_l$. Mas $a_i = b_i + l\hat{a}_i$ com $0 \leq b_i < l$. Assim

$$x = \sum_{i=1}^n b_i x_i + l \left(\sum_{i=1}^n \hat{a}_i x_i \right)$$

E como b_i só admite um número finito de valores, temos que $H^n(G, T)/lH^n(G, T)$ é finito. $\square$

Proposição 1.2.2. Para cada $n > 0$, existe uma sequência exata (os limites inversos são tomados em i).

$$0 \longrightarrow \varprojlim^1 H^{n-1}(G, T/l^i T) \longrightarrow H^n(G, T) \longrightarrow \varprojlim H^n(G, T/l^i T) \longrightarrow 0 \quad (1.1)$$

Demonstração. Para cada $i \geq 0$ considere o mapa

$$u_i : C^n(G, T/l^{i+1}T) \rightarrow C^n(G, T/l^i T)$$

com $u_i(f) = \pi_i f$ onde $\pi_i : T/l^{i+1}T \rightarrow T/l^i T$ é a projeção canônica. Definimos agora

$$\Delta : \prod_{i \geq 1} C^n(G, T/l^i T) \rightarrow \prod_{i \geq 1} C^n(G, T/l^i T)$$

com $\Delta((f_i)_{i \geq 0}) = (f_i - u_i f_{i+1})_{i \geq 0}$. Como qualquer seção de π_i é contínua, temos que u_i é sobrejetora logo Δ é sobrejetora (a prova disto é recursiva e pode encontra-lo na construção do limite inverso, proposição 10.2 de (ATIYAH; MACDONALD, 2016)). Assim, pela construção temos que $\ker \Delta = \varprojlim C^n(G, T/l^i T)$ e logo:

$$0 \longrightarrow \varprojlim C^n(G, T/l^i T) \xrightarrow{j} \prod_{i \geq 1} C^n(G, T/l^i T) \xrightarrow{\Delta} \prod_{i \geq 1} C^n(G, T/l^i T) \longrightarrow 0 \quad (1.2)$$

E como $\prod_{i \geq 1} C^\bullet(G, T/l^i T)$ é um complexo e $C^n(G, T) = \varprojlim C^n(G, T/l^i T)$ a propriedade da sequência exata longa e a propriedade do producto de cohomologias nos dá.

$$\begin{aligned} \cdots &\longrightarrow \prod_{i \geq 1} H^{n-1}(G, T/l^i T) \xrightarrow{H^{n-1}(\Delta)} \prod_{i \geq 1} H^{n-1}(G, T/l^i T) \\ &\xrightarrow{\delta} H^n(G, T) \xrightarrow{H^n(j)} \prod_{i \geq 1} H^n(G, T/l^i T) \xrightarrow{H^n(\Delta)} \prod_{i \geq 1} H^n(G, T/l^i T) \longrightarrow \cdots \end{aligned}$$

Logo cortando a sequência

$$0 \longrightarrow \ker(H^n(j)) \longrightarrow H^n(G, T) \longrightarrow \operatorname{im}(H^n(j)) \longrightarrow 0$$

Agora, é fácil mostrar que $H^r(\Delta)$ tem a mesma forma que Δ , isto significa que $\operatorname{coker}(H^{n-1}(\Delta)) = \varprojlim^1 H^{n-1}(G, T/l^i T)$ e $\ker(H^{n-1}(\Delta)) = \varprojlim H^{n-1}(G, T/l^i T)$. Também, da sequência exata longa acima é fácil mostrar que $\operatorname{coker}(H^{n-1}(\Delta)) \simeq \ker(H^n(j))$ e $\operatorname{im}(H^n(j)) = \ker(H^n(\Delta))$ o que da imediatamente o resultado. $\square$

Corolário 1.2.2. Se os grupos $H^{n-1}(G, T/l^i T)$ são finitos para cada i ou se os mapas $H^{n-1}(G, T/l^{i+1} T) \rightarrow H^{n-1}(G, T/l^i T)$ são sobrejetoras para cada i , então $H^n(G, T) \simeq \varprojlim_i H^n(G, T/l^i T)$.

Demonstração. Qualquer das duas premissas satisfaz as condições de Mittag-Leffler (proposição 10.13 ([WEIBEL, 1994](#))) do sistema inverso $\{H^{n-1}(G, T/l^i T)\}_{i \geq 1}$, logo

$$\varprojlim^1 H^{n-1}(G, T/l^i T) = 0.$$

$\square$

Suponha agora que T é livre de torção (logo é um $\mathbf{Z}_l$ -módulo livre), tensorizando sobre $\mathbf{Z}_l$ com a sequência exata

$$0 \longrightarrow \mathbf{Z}_l \longrightarrow \mathbf{Q}_l \longrightarrow \mathbf{Q}_l/\mathbf{Z}_l \longrightarrow 0 \quad (1.3)$$

temos a sequência exata

$$0 \longrightarrow T \longrightarrow V \longrightarrow W \longrightarrow 0 \quad (1.4)$$

Se $T = \bigoplus_{i=1}^m \mathbf{Z}_l$ então $V = \mathbf{Q}_l \otimes_{\mathbf{Z}_l} T = \bigoplus_{i=1}^m \mathbf{Q}_l$ e $W = \mathbf{Q}_l/\mathbf{Z}_l \otimes_{\mathbf{Z}_l} T = \bigoplus_{i=1}^m \mathbf{Q}_l/\mathbf{Z}_l$, como $\mathbf{Z}_l$ é compacto (completo e totalmente limitado) em $\mathbf{Q}_l$ então T também é compacto, também $\mathbf{Q}_l$ é um espaço ultramétrico, assim $\mathbf{Z}_l$ é a bola fechada de raio 1, logo aberto.

Por outro lado, $\mathbf{Q}_l/\mathbf{Z}_l$ é l -divisível e l -primário então a soma direta finita também é, similarmente temos que $\mathbf{Z}_l$ é aberto então $\mathbf{Q}_l/\mathbf{Z}_l$ é discreto e a soma direta finita W também é.

Proposição 1.2.3. Suponha que G é compacto, então na sequência exata longa associada à sequência exata acima o núcleo do homomorfismo fronteira $\delta : H^{n-1}(G, W) \rightarrow H^n(G, T)$ é o subgrupo maximal divisível de $H^{n-1}(G, W)$ e sua imagem é o subgrupo de torção de $H^n(G, T)$.

Demonstração. Temos que $H^{n-1}(G, V)$ é um $\mathbf{Q}_l$ -espaço vetorial pois V também é, logo é divisível e sua imagem em $H^{n-1}(G, W)$ que é o núcleo de δ também é. Agora seja D é o subgrupo maximal divisível de $H^{n-1}(G, W)$ então $\ker(\delta) \subseteq D$, por outro lado $\delta(D)$ é em particular l -divisível em $H^n(G, T)$, mas este grupo não pode conter um subgrupo l -divisível não nulo, assim $\delta(D) = 0$ e $D \subseteq \ker(\delta)$. Para a outra parte da proposição, como G é compacto e W discreto toda cocadeia $f : G^{n-1} \rightarrow W$ assume um número finito de valores ($G^{n-1} = \bigcup_{y \in W} f^{-1}(y)$ é um cubrimento aberto de G^{n-1}) e como W é um grupo de torção as cocadeias tem ordem finito e logo $H^{n-1}(G, W)$ também é de torção. Agora, a imagem de $H^{n-1}(G, W)$ por δ é um subgrupo de torção de $H^n(G, T)$, por outro lado se x é um elemento de torção de $H^n(G, T)$ então sua imagem em $H^n(G, V)$ é também de torção mas este último é um $\mathbf{Q}_l$ -espaço vetorial e logo livre de torção, assim x pertence ao núcleo de $H^n(G, T) \rightarrow H^n(G, V)$ assim $x \in \text{im}(\delta)$. $\square$

TEORIA K ALGÉBRICA

A teoria K algébrica é uma das disciplinas más fructíferas da matemática, com conexões com a topologia, a geometria, e a teoria dos números. Nesta disciplina associamos a um anel A uma sequência de grupos abelianos chamados K -grupos, e como na homologia, estes grupos nos falam coisas acerca do anel, por exemplo, as propriedades dos módulos que se criam em ele, ou as propriedades do grupo de matrizes que se formam com seus elementos, etc.

Neste capítulo todo anel vai ter elemento unidade 1 e todos os morfismos de anéis cumpren $f(1) = 1$, com isto construiremos os grupos K_0 , K_1 e K_2 e as relações entre eles, mas estudaremos mais profundamente o funtor K_2 que é objeto desta dissertação.

2.1 O funtor K_0

Definição 2.1.1. Seja A um anel e M um A -módulo, dizemos que:

- (i) M é livre se é isomorfo a uma soma direita de copias de A , i.e. se Γ é um conjunto de índices e

$$M \simeq \bigoplus_{\lambda \in \Gamma} A_\lambda$$

com $A_\lambda = A$.

- (ii) M é projetivo se é sumando de um módulo livre, i.e. existe um A -módulo N tal que $F = M \oplus N$ é um modulo livre.

- (iii) Dois A -módulos M, N são estable-isomorfos se $M \oplus A^r \simeq N \oplus A^r$ para algum $r \geq 0$.

Observação 2.1.1. Se P é um modulo projetivo finitamente gerado e $\{b_i\} \subset P$ um conjunto gerador finito, considere o A -módulo livre (finitamente gerado) com base $\{b_i\}$ e um

morfismo (sobrejetor) $F \rightarrow P$. Tomando o núcleo N temos

$$0 \longrightarrow N \longrightarrow F \longrightarrow P \longrightarrow 0$$

Se sabe que um A -módulo projetivo tem a propriedade (equivalente à definição) que toda sequência exata curta com P ao final se divide (i.e. que o morfismo $F \rightarrow P$ tem inverso a direita), assim $F = P \oplus N$. Tomando o morfismo de projeção ao módulo N e o teorema de isomorfismo temos que $N \simeq F/P$ é finitamente gerado e pela soma direita também é projetivo. Assim temos que tanto o módulo livre F como o sumando N são finitamente gerados e N também é projetivo.

Definição 2.1.2. Seja A um anel, o grupo abeliano K_0A é a **completação de Grothendieck** do monoide formado pelas classes $[P]$ de isomorfismos (que chamamos **geradores**) de A -módulos projetivos finitamente gerados com a operação $[P] + [Q] = [P \oplus Q]$, com elemento identidade $[0]$.

Lembre que a completção de Grothendieck de um monoide S (estrutura com operação associativa e com elemento identidade) é o cociente $S \times S / \sim$ onde $(m_1, m_2) \sim (m_3, m_4)$ se e somente se existe $c \in S$ tal que $m_1 + m_4 + c = m_2 + m_3 + c$. O objetivo desta completção é modelar o conjunto das diferenças formais de elementos de S . Assim podemos representar cada elemento de K_0A na forma $[P] - [Q]$.

Observação 2.1.2. Duas geradores $[P], [Q]$ são iguais se e somente se $P \simeq Q$, mas em K_0A temos que $[P] - [0] = [Q] - [0]$ se e somente se existe T tal que $[P] + [0] + [T] = [Q] + [0] + [T]$, mas seja T' tal que $T \oplus T' = A^n$ então

$$[P \oplus A^n] = [P \oplus T \oplus T'] = [Q \oplus T \oplus T'] = [Q \oplus A^n]$$

e logo P e Q são estable-isomorfos. O converso é fácil.

Agora, se $f : A \rightarrow A'$ e um homomorfismo entre os anéis A e A' , e dado M um A -módulo temos o A' -módulo $f_{\#}M = A' \otimes_A M$ (A' é um A -módulo direito com a operação $a' \cdot a = a'f(a)$ para $a \in A$ e $a' \in A'$) com o produto $b' \cdot (a' \otimes m) = (b'a') \otimes m$. É fácil mostrar que se M é livre, finitamente gerado ou projetivo então $[f_{\#}M]$ é livre, finitamente gerado ou projetivo respetivamente. Assim, pela propriedade universal da completção de Grothendieck, o morfismo $[P] \mapsto [f_{\#}P]$ se estende a $f_* : K_0A \rightarrow K_0A'$, que dá a K_0 propriedades funtoriais, i.e. $(Id)_* = Id$ e $(f \circ g)_* = f_* \circ g_*$.

Exemplo 2.1.1. Em qualquer corpo F todo F -módulo finitamente gerado é um espaço vetorial de dimensão finita, e sabemos que dois F -espaços vetoriais de dimensão finita são isomorfos se e somente se tem a mesma dimensão, assim podemos identificar aos geradores com números naturais correspondentes à dimensão, finalmente a completção de Grothendieck de $\mathbf{N}$ é o conjunto $\mathbf{Z}$ dos números inteiros. Por tanto $K_0F = \mathbf{Z}$.

Quando anel A é comutativo, podemos transformar K_0A em um anel comutativo com o produto $[P] \cdot [Q] = [P \otimes Q]$, é claro que cumpre as propriedades correspondentes. O elemento identidade deste produto é o gerador $[A]$.

2.2 O funtor K_1

Seja A um anel, para cada $n \in \mathbf{N}$ denotamos com $GL(n, A)$ ao grupo das matrizes de ordem $n \times n$ invertíveis, o conjunto destes grupos formam um sistema direito usando os morfismos da forma

$$T \mapsto \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix}$$

e logo usando o limite direito criamos o grupo $GL(A)$ chamado **grupo linear geral**, lembre que isto é intuitivamente uma 'união' de todos os $GL(n, A)$ tal que quando queremos multiplicar dois matrizes de diferente dimensão so temos que 'aumentar' a dimensão de uma delas agregando 1's à diagonal. Abelianizando obtemos

Definição 2.2.1. Seja A um anel, definimos o grupo K_1A como a abelianização do grupo $GL(A)$, i.e.

$$K_1A = GL(A)/[GL(A), GL(A)]$$

Agora, um teorema devido a Whitehead diz que o comutador de $GL(A)$ é o grupo $E(A)$ que é a 'união' dos grupos $E(n, A) \subset GL(n, A)$ gerados pelas matrizes elementares $E_{ij}(\lambda)$ que são matrizes com o valor $\lambda \in A$ no lugar (i, j) com $i \neq j$, i.e.

$$E(n, A) = \langle E_{ij}(\lambda) \mid i \neq j, \lambda \in A \rangle$$

(note que não precisamos explicitar a dimensão), o enunciamos formalmente.

Teorema 2.2.1 (Whitehead). Seja A um anel, então

$$[GL(A), GL(A)] = E(A) = \varinjlim E(n, A)$$

Demonstração. Veja em (MILNOR, 1972) (lema 3.1 em §3). □

Com isto temos que $K_1A = GL(A)/E(A)$, mais ainda se $f : A \rightarrow A'$ é um homomorfismo de anéis, temos um morfismo $f_* : K_1A \rightarrow K_1A'$ aplicando o morfismo a cada elemento da matriz, e como a imagem de uma matriz elementar em A e de novo uma matriz elementar em A' temos que o morfismo f_* está bem definido, daqui é fácil mostrar que K_1 também é um funtor.

Agora vamos a definir uma operação $K_0A \otimes K_1A \rightarrow K_1A$, para iso criamos um homomorfismo $\text{Aut}(P) \rightarrow K_1A$ assim. Seja $\alpha \in \text{Aut}(P)$ e seja Q um módulo projetivo finitamente gerado tal que $P \oplus Q$ seja livre de base finita (observação 2.1.1), fazendo $\alpha \oplus I_Q$ temos

um automorfismo em $P \oplus Q$ e escolhendo uma base de r elementos representamos $\alpha \oplus I_Q$ com uma matriz em $GL(r, A)$. Vamos a mostrar que em $K_1 A$ a classe pelo comutador não depende da escolha da base (mais ainda, pode ser de cardinal diferente) nem da escolha do módulo Q .

Lema 2.2.1. O seguinte mergulho

$$\text{Aut}(P) \subset \text{Aut}(P \oplus Q) \simeq GL(r, A) \subset GL(A)$$

está bem definido salvo conjugação.

Demonstração. Usando a mesma notação do parágrafo acima, seja $\{b_i\}_{i=1}^r$ e $\{b'_i\}_{i=1}^s$ (onde possivelmente $r \neq s$). Tomando $b'_i = \sum c_{ij} b_j$, a matriz $C = (c_{ij})$ de dimensão $s \times r$ que é a matriz de mudança de base (leva das coordenadas em uma base de qualquer elemento às coordenadas na outra base) é invertível, chamemos a sua inversa C^{-1} . Seja A a matriz de $\alpha \oplus I_Q$ na base $\{b_i\}$, logo em $GL(r+s, A)$

$$\begin{pmatrix} C & 0 \\ 0 & C^{-1} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} C & 0 \\ 0 & C^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} CAC^{-1} & 0 \\ 0 & I \end{pmatrix}$$

que é equivalente (em $GL(A)$) a $CAC^{-1} \in GL(s, A)$ que é a matriz de $\alpha \oplus I_Q$ na base b'_i . Assim uma mudança de base só altera a matriz do automorfismo por uma conjugação e é fácil mostrar que se duas matrizes são conjugadas então representam ao mesmo elemento em $K_1 A = GL(A)/[GL(A), GL(A)]$. Agora seja Q' outro A -módulo projetivo tal que $P \oplus Q' = A^t$ então temos $Q \oplus A^t \simeq Q' \oplus A^r$, e se g é o isomorfismo é fácil mostrar que o seguinte diagrama

$$\begin{array}{ccc} P \oplus Q \oplus A^t & \xrightarrow{I_P \oplus g} & P \oplus Q' \oplus A^r \\ \downarrow \alpha \oplus I_{Q \oplus A^t} & & \downarrow \alpha \oplus I_{Q' \oplus A^r} \\ P \oplus Q \oplus A^t & \xrightarrow{I_P \oplus g} & P \oplus Q' \oplus A^r \end{array}$$

é comutativo e logo (escolhendo uma base qualquer para $P \oplus Q' \oplus A^r \simeq P \oplus Q \oplus A^t \simeq A^{r+t}$) temos que a matriz dos morfismos $\alpha \oplus I_{Q \oplus A^t}$ e $\alpha \oplus I_{Q' \oplus A^r}$ são conjugadas. $\square$

Continuando com a definição do produto $K_0 A \otimes K_1 A \rightarrow K_1 A$, seja $[P]$ um gerador de $K_0 A$ e $\alpha \in \text{Aut}(A^n) \simeq GL(n, A)$, a correspondência $\alpha \mapsto I_P \otimes \alpha$ transforma α num elemento de $\text{Aut}(P \otimes A^n)$ que por o lema acima podemos mergulhar em $K_1 A$. Fazendo a composta destes morfismos obtemos $h(P) : K_1 A \rightarrow K_1 A$. A distributividade do produto tensorial (e o fato de que obter a matriz de um homomorfismo fixando uma base é um homomorfismo) nos dá a identidade

$$h(P \oplus P') = h(P) + h(P')$$

que mostra que $h(P) = h(P')$ se P e P' são estable-isomorfos e assim h está bem definido em $K_0 A$ (olha em 2.1.2). Finalmente tomamos limite direito e abelianizamos (isto último é

posível pelo lema 2.2.1) e assim obtemos um morfismo $K_1A \rightarrow K_1A$ que depende somente do gerador $[P]$ em K_0A e logo (pela identidade acima e a distributividade do produto tensorial) a operação produto $K_0A \otimes K_1A \rightarrow K_1A$ que simbolizamos com $[P] \cdot k$ para o gerador $[P] \in K_0A$ e $k \in K_1A$.

Exemplo 2.2.1. Sabemos que K_0F para um corpo é $\mathbb{Z}$, e a cada gerador $[P]$ corresponde um número natural $n = \dim(P)$, logo o produto criado acima corresponde a multiplicar por n .

Seja A um anel comutativo, podemos definir a aplicação determinante em $GL(A)$ e a propriedade multiplicativa deste permite a boa definição em K_1A (duas matrizes são conjugadas se e somente se definem o mesmo elemento em K_1). Seja $SL(A)$ o kernel do morfismo determinante, assim temos

$$1 \longrightarrow SL(A)/E(A) \longrightarrow K_1A \xrightarrow{\det} A^\bullet \longrightarrow 1$$

a inclusão $A^\bullet \subset GL(1, A) \subset GL(A)$ escinde a sequência acima, logo

$$K_1A = A^\bullet \oplus [SL(A)/E(A)]$$

o segundo sumando é denotado por $SK_1(A)$.

Exemplo 2.2.2. No caso de um corpo F temos que toda matriz com determinante 1 é produto de matrizes elementares, logo SK_1F é trivial e assim $K_1F = F^\bullet$.

2.3 O funtor K_2

Seja A um anel, considere as matrizes elementares $E_{ij}(\lambda) \in GL(n, A)$, tentaremos modelar as relações 'não triviais' entre estas, as 'triviais' a considerar são $E_{ij}(\lambda)E_{ij}(\mu) = E_{ij}(\lambda + \mu)$ (e logo $E_{ij}(\lambda)^{-1} = E_{ij}(-\lambda)$) e as seguintes relações certas

$$[E_{ij}(\lambda), E_{kl}(\mu)] = \begin{cases} 1 & \text{if } j \neq k, i \neq l \\ E_{il}(\lambda\mu) & \text{if } j = k, i \neq l \\ E_{kj}(-\mu\lambda) & \text{if } j \neq k, i = l \end{cases}$$

note que nestas fórmulas não consideramos o caso $j = k, i = l$ já que sua expressão não é tão 'trivial'. Definimos agora a abstração destas matrizes elementares com símbolos com o mesmo comportamento.

Definição 2.3.1. Definimos para $n \geq 3$ o grupo de Steinberg $St(n, A)$ gerado pelos símbolos $X_{ij}(\lambda)$ onde $i, j \leq n$, $i \neq j$ e $\lambda \in A$ tais que cumpren as seguintes relações

$$1. X_{ij}(\lambda)X_{ij}(\mu) = X_{ij}(\lambda + \mu)$$

2. $[X_{ij}(\lambda), X_{jl}(\mu)] = X_{il}(\lambda\mu)$ se $i \neq l$
3. $[X_{ij}(\lambda), X_{kl}(\mu)] = 1$ se $j \neq k, i \neq l$

A correspondência $X_{ij}(\lambda) \mapsto E_{ij}(\lambda)$ cria um homomorfismo canônico $\phi : \text{St}(n, A) \rightarrow GL(n, A)$, a boa definição está garantida pelas relações da definição acima, logo no limite direito temos (com o mesmo nome) $\phi : \text{St}(A) \rightarrow GL(A)$, e que pelo teorema 2.2.1 a imagem de ϕ é $E(A) = [GL(A), GL(A)]$.

Definição 2.3.2. O núcleo do morfismo $\phi : \text{St}(A) \rightarrow GL(A)$ vai ser chamado K_2A .

Teorema 2.3.1. O grupo $K_2A = \ker(\phi)$ é igual ao centro do grupo de Steinberg $\text{St}(A)$

Demonstração. Veja em (MILNOR, 1972) (teorema 5.1 em §5) □

Com isto temos a seguinte sequência exata de grupos abelianos

$$1 \longrightarrow K_2A \longrightarrow \text{St}(A) \xrightarrow{\phi} GL(A) \longrightarrow K_1A \longrightarrow 1$$

e se temos um homomorfismo $f : A \rightarrow A'$ aplicando este ao $\lambda \in A$ em cada símbolo $X_{ij}(\lambda)$ temos símbolos em $\text{St}(A')$, agora usando a propriedade universal do kernel da sequência de A' temos que existe $f_* : K_2A \rightarrow K_2A'$, assim K_2 é também um funtor covariante e

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K_2A & \longrightarrow & \text{St}(A) & \xrightarrow{\phi} & GL(A) & \longrightarrow & K_1A & \longrightarrow & 1 \\ & & \downarrow f_* & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K_2A' & \longrightarrow & \text{St}(A') & \xrightarrow{\phi'} & GL(A') & \longrightarrow & K_1A' & \longrightarrow & 1 \end{array}$$

Então, se temos uma $A \subset B$ anéis a inclusão $f : A \rightarrow B$ define um homomorfismo $f_* : K_2A \rightarrow K_2B$, o lema e o teorema abaixo, o que pode encontrar em (MILNOR, 1972) (lema 5.9 e teorema 5.10 em §5) nos ajudará a definir mais tarde o homomorfismo oposto de transferência $f^* : K_2B \rightarrow K_2A$ quando B é um A -módulo projetivo finitamente gerado.

Lema 2.3.1. O multiplicador de schur é um funtor, logo se $h : G_1 \rightarrow G_2$ é um homomorfismo de grupos, temos $h_* : H_2G_1 \rightarrow H_2G_2$. Se h é um automorfismo interno de G então h_* é a identidade em H_2G . Se G é limite direito de uma sequência

$$G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow \cdots$$

de grupos perfeitos (que são iguais a seu comutador), então H_2G é o limite direito da sequência

$$H_2G_1 \rightarrow H_2G_2 \rightarrow H_2G_3 \rightarrow \cdots$$

Observação 2.3.1. O multiplicador de Schur de um grupo G , é segundo grupo de homologia $H_2(G; \mathbf{Z})$ quando G age trivialmente sobre $\mathbf{Z}$.

Teorema 2.3.2. Seja A um anel, então K_2A é $H_2E(A)$ que é o multiplicador de Schur de $E(A)$

Agora, vamos a definir uma operação externa $K_0A \otimes K_2A \rightarrow K_2A$ e converter K_2A num K_0A -módulo do mesmo jeito que em K_1 , seja $[P]$ um gerador em K_0 e Q tal que $P \oplus Q \simeq A^r$, então temos $h(P) : GL(n, A) \rightarrow GL(rn, A) \subset GL(A)$ o que faz $\alpha \mapsto I_P \otimes \alpha$ e está bem definido salvo automorfismos internos (lema 2.2.1), este leva o grupo perfeito (para $n \geq 3$) $E(n, A)$ em $E(A)$ que satisfaz $h(P \oplus P') = h(P) + h(P')$. Então aplicando o multiplicador de Schur temos o morfismo

$$h(P)_* : H_2E(n, A) \rightarrow H_2E(A)$$

bem definido. Mais ainda pela propriedade da homologia temos $h(P \oplus Q)_* = h(P)_* + h(Q)_*$ e usando o lema 2.3.1 podemos passar ao limite e ter o homomorfismo $[P] \cdot (\bullet) : K_2A \rightarrow K_2A$. No caso de um corpo F , ao igual que em K_1 a operação se reduce a multiplicar o elemento de K_2A pela dimensão de F .

2.4 O produto $K_1A \otimes K_1A \rightarrow K_2A$ e os símbolos de Steinberg

O objetivo desta seção é construir um simbolo $\{a, b\} \in K_2A$ com $a, b \in A^\bullet$ para gerar os elementos de K_2A e enunciar o Teorema de Matsumoto que faz uma apresentação de K_2A usando estos simbolos.

Vamos começar construindo elemetos de K_2 a partir de dois matrices comutaveis $A, B \in E(A)$, sejam $a, b \in \text{St}(A)$ suas respectivas preimagens por $\phi : \text{St}(A) \rightarrow GL(A)$, o comutador $[a, b] = aba^{-1}b^{-1}$ é um elemento de K_2A que denotamos assim

$$A \star B = aba^{-1}b^{-1} \in K_2A$$

Como $\ker(\phi)$ é o centro do grupo de Steinberg, então se $\phi(a) = \phi(\bar{a})$ e $\phi(b) = \phi(\bar{b})$ então $\bar{a} = ac$ e $\bar{b} = ad$ com $c, d \in \ker(\phi)$, assim

$$[\bar{a}, \bar{b}] = acbd(ac)^{-1}(bd)^{-1} = [a, b]$$

com isto temos que $A \star B$ não depende das preimagens escolhidas. O seguinte lema lista algumas propriedades desta operação.

Lema 2.4.1. A operação $\star$ satisfaz

1. É antisimetrica i.e. $(A \star B)^{-1} = B \star A$
2. É bímultiplicativa i.e. $(A_1A_2) \star B = (A_1 \star B)(A_2 \star B)$

3. É invariante por automorfismos internos de $E(A)$ i.e. $(PAP^{-1}) \star (PBP^{-1}) = A \star B$

Demonstração. Estas propriedades se deduzem imediatamente das seguintes identidades do comutador ($a^b = aba^{-1}$)

1. $[a, b]^{-1} = [b, a]$
2. $[ab, c] = [b, c]^a [a, c]$
3. $[a^p, b^p] = [a, b]^p$

e do fato que os comutadores pertencem ao centro do grupo de Steinberg. $\square$

Agora suponha que A é comutativo e seja $u, v \in A^\bullet$, então as matrizes abaixo

$$D_u = \begin{pmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} D'_v = \begin{pmatrix} v & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & v^{-1} \end{pmatrix}$$

comutam, mais ainda $D_u, D'_v \in E(3, A)$ já que

$$D_u = E_{12}(u)E_{21}(-u^{-1})E_{12}(u)E_{12}(-1)E_{21}(1)E_{12}(-1) \in E(3, A)$$

e

$$D_v = E_{13}(v)E_{31}(-v^{-1})E_{13}(v)E_{13}(-1)E_{31}(1)E_{13}(-1) \in E(3, A)$$

Agora podemos definir o simbolo principal desta seção.

Definição 2.4.1. O comutador $D_u \star D'_v \in K_2 A$ será denotado por $\{u, v\}$

Proposição 2.4.1. O simbolo $\{u, v\}$ é antisimétrico e bímultiplicativo

Demonstração. Seja $P \in GL(3, A)$

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

de fato $P = E_{21}(1)E_{12}(-1)E_{23}(-1)E_{31}(-1)E_{32}(1)E_{23}(-1)E_{21}(1)E_{13}(1)E_{31}(-1)E_{13}(1) \in E(3, A)$, e é fácil ver que $PD_u P^{-1} = D'_u$ e $PD'_v P^{-1} = D_v$, então

$$\{u, v\}^{-1} = (D_u \star D'_v)^{-1} = D'_v \star D_u = (PD'_v P^{-1}) \star (PD_u P^{-1}) = D_v \star D'_u = \{v, u\}$$

A outra propriedade é óbvia pela bímultiplicatividade de $\star$. $\square$

Precisamos uma propriedade adicional do simbolo $\{a, b\}$, a prova pode encontrá-lo em (MILNOR, 1972) (lema 9.8 em §9) a prova é para uma generalização deste simbolo usando os geradores do grupo de Steinberg.

Proposição 2.4.2. Seja $u \in A^\bullet$ tal que $1 - u \in A^\bullet$, então $\{u, 1 - u\} = 1$. Mais ainda para qualquer $u \in A^\bullet$, temos que $\{u, -u\} = 1$.

Agora vamos a definir o produto entre elementos de K_1 usando $\star$, novamente seja A comutativo e dadas as matrizes $X \in GL(n, A)$ e $Y \in GL(m, A)$ comutáveis, logo as matrizes

$$\alpha = \text{diag}(X \otimes I_m, A^{-1} \otimes I_m, I_n \otimes I_m)$$

$$\beta = \text{diag}(Y \otimes I_m, I_n \otimes I_m, Y^{-1} \otimes I_m)$$

pertencem a $E(3mn, A)$ (tem a mesma forma que D_u e D'_v) e são comutáveis. Definimos $\{A, B\} = \alpha \star \beta$. Observe que esta é uma generalização do produto $\{u, v\}$ quando $m = n = 1$. Como pode-se esperar, temos o seguinte teorema que dá a boa definição deste produto e suas propriedades, veja a prova em (MILNOR, 1972) (lema 8.6 em §8).

Teorema 2.4.1. Seja A um anel comutativo e $X, Y \in K_1 A$, então o produto $\{X, Y\}$ está bem definido, é antisimétrico e bímultiplicativo.

Agora que temos definido o símbolo $\{u, v\}$ para duas unidades do anel A comutativo, o seguinte teorema, cuja prova pode encontrar in (MILNOR, 1972) (teorema 11.1 em §11), dá uma apresentação de K_2 para um corpo F , e permite criar morfismos saindo de K_2 chamados *símbolos de Steinberg*.

Teorema 2.4.2 (Matsumoto). Seja F um corpo, o grupo abeliano $K_2 F$ tem uma apresentação em termos dos símbolos $\{a, b\}$ com $a, b \in F^\bullet$ que satisfazem as relações seguintes.

- i (Bilinearidade) $\{ab, c\} = \{a, c\}\{b, c\}$, $\{a, bc\} = \{a, b\}\{a, c\}$ para $a, b, c \in F^\bullet$
- ii (Identidade de Steinberg) $\{x, 1 - x\} = 1$ para $x \in F^\bullet - \{1\}$

Ja que é uma apresentação, qualquer mapa $c : F^\bullet \times F^\bullet \rightarrow G$ onde G é um grupo abeliano, que satisfaz as propriedades acima, pode gerar um único homomorfismo $\bar{c} : K_2 F \rightarrow G$ que cumpre $\bar{c}(\{a, b\}) = c(a, b)$. Podemos ver exemplos no capítulo seguinte.

2.5 O homomorfismo de Transferência

Nesta seção, A, B anéis tais que $B \supset A$ e onde B é um A -módulo esquerdo projetivo finitamente gerado, denotaremos o morfismo definido pela inclusão por $f_* : K_i A \rightarrow K_i B$ para $i = 0, 1, 2$. Definiremos um morfismo $f^* : K_i B \rightarrow K_i A$ tal que cumpra a seguinte propriedade cuja prova está em (MILNOR, 1972) (teorema 14.1 em §14).

Teorema 2.5.1 (Fórmula de projeção). Se B é comutativo e $i, j \leq 2$, então se satisfaz a identidade

$$f^*(x \cdot f_*(y)) = f^*(x) \cdot y$$

onde $\cdot$ representa a operação que corresponde em cada caso estudado nas seções anteriores.

Observação 2.5.1. Nas seções acima, mostramos que podemos definir operações para transformar a K_0 em um anel e a K_1 e K_2 em K_0 -módulos e logo a operação $\cdot$ acima pode-se interpretar como a operação correspondente em cada caso, por exemplo, num corpo F temos que $K_1 F = F^\bullet$ e logo o produto $\cdot$ se interpreta como o simbolo $\{\cdot, \cdot\}$ que é o produto de duas unidades de um anel comutativo definido na seção anterior. Outro exemplo, seja L/F uma extensão de corpos finita, e $\dim_F(L) = n$, seja $x \in F^\bullet$, então $f^*(f_*(x)) = f^*([L] \cdot f_*(x)) = f^*([L]) \cdot x$, logo veremos que $f^*([L]) = n$.

Vamos agora a definir o mapa transferência, em K_0 , K_1 e K_2 , começamos por K_0 . Para definir $f^* : K_0 B \rightarrow K_0 A$, seja $[P]$ um gerador em $K_0 B$, mas P também pode ser visto como um A -módulo projetivo e finitamente gerado (por hipotesis sobre $B \supset A$) que denotamos por P_A , então $f^*([P]) = [P_A]$. Por exemplo, numa extensão de corpos L/F de grau n temos que $f^*([L]) = [F^n] = n$.

Para definir f^* em K_1 e K_2 precisamos definir antes uma função $f^\# : GL(n, B) \rightarrow GL(A)$ assim, seja $X \in GL(n, B)$ que dá lugar a um automorfismo (com o mesmo nome) X de B^n . Escolha um módulo projetivo C finitamente gerado tal que $B \oplus C$ seja livre sobre A gerado por r elementos. Então $B^n \oplus C^n$ é também livre e podemos ampliar o automorfismo X a um automorfismo de $B^n \oplus C^n$ assim.

$$X \oplus I_{Q^n}$$

Escolha uma A -base para $B^n \oplus C^n$ e representamos o automorfismo acima pela matriz

$$f^\#(X) \in GL(nr, A) \subset GL(A)$$

E como na prova do lema 2.2.1 temos que $f^\#$ está bem definido salvo automorfismos internos de $GL(A)$, logo podemos abelianizar e fazer o limite direito e obtemos $f^* : K_1 B \rightarrow K_1 A$.

Agora, fazendo a restrição de $f^\#$ a $E(n, B) \subset [GL(B), GL(B)]$ a imagem também fica em $E(A) = [GL(A), GL(A)]$ (pela construção de $f^\#$), então tomando o multiplicador de Schur e fazendo limite direito (2.3.1) temos $f^* : H_2 E(B) = K_2 B \rightarrow H_2 E(A) = K_2 A$.

Observação 2.5.2. Pela definição acima, temos então que se L/F é uma extensão de corpos de grau n então $f^*([L]) = n$, e logo pela observação 2.5.1 temos para todo $x \in K_2 F$

$$f^*(f_*(x)) = nx$$

Precisamos agora uma propriedade do transfer que dá uma fórmula para $f_*(f^*(y))$ para $y \in K_2 L$, para isto precisamos do seguinte lema cuja prova num contexto mais geral pode encontrar na página 387 de (BASS; TATE, 1973).

Lema 2.5.1. Seja $F' = F(\alpha)$ uma extensão algébrica simples de F , e L/F uma extensão algébrica qualquer de F . Seja $\pi \in F[t]$ o polinômio mínimo e seja

$$\pi = \prod_i \pi_i^{e_i}$$

sua decomposição em fatores mônicos irreducíveis em $L[t]$. Seja também $L_i = L[t]/(\pi_i)$, α_i a classe de $t \in L[t]$ (e logo $L_i = L(\alpha_i)$) e $j_i : F(\alpha) \rightarrow L_i$ tal que $j_i(\alpha) = \alpha_i$ então o seguinte diagrama

$$\begin{array}{ccc} \bigoplus_i K_2 L(\alpha_i) & \xrightarrow{\Sigma f_{L_i/L}^*} & K_2 L \\ (e_i \cdot j_i)_i \uparrow & & \uparrow f_{*L/F} \\ K_2 F(\alpha) & \xrightarrow{f_{F'/F}^*} & K_2 F \end{array}$$

é comutativo.

Teorema 2.5.2. Seja L/F uma extensão Galois e $G = \text{Gal}(L/F)$, então

$$f_*(f^*(x)) = \sum_{\sigma \in G} \sigma x$$

para todo $x \in K_1 L$.

Demonstração. Se L/F é Galois, então $L = F[\alpha]$ pelo teorema do elemento primitivo e o polinômio mínimo $\pi \in F[t]$ de α se decompõe assim

$$\pi = \prod_{\sigma \in G} (t - \sigma(\alpha))$$

então, o lema acima nos dá o diagrama comutativo

$$\begin{array}{ccc} \bigoplus_{\sigma \in G} K_2 L & \xrightarrow{\Sigma f_{L_i/L}^*} & K_2 L \\ (\sigma_*)_i \uparrow & & \uparrow f_{*L/F} \\ K_2 L & \xrightarrow{f_{L/F}^*} & K_2 F \end{array}$$

Agora, como $L_i = L$ usando a fórmula de projeção (2.5.1) temos que $f_{L_i/L}^*$ é a identidade e então usando a comutatividade do diagrama

$$f_{*L/F}(f_{L/F}^*(y)) = \sum_{\sigma \in G} \sigma y$$

para todo $y \in K_2 L$. □

Para finalizar este capítulo, definiremos uma aplicação norma que generaliza a norma entre extensões de anéis.

Definição 2.5.1. Se A é um anel comutativo, a composição dos morfismos

$$B^\bullet \longrightarrow K_1 B \xrightarrow{f^*} K_1 A \xrightarrow{\det} A^\bullet \quad (2.1)$$

definimos a aplicação $\text{Nm} : B^\bullet \rightarrow A^\bullet$ chamada **norma**.

Exemplo 2.5.1. Se B é um A -módulo livre, então pela definição do transfer para K_1 temos que para calcular a norma de um elemento γ temos que calcular a determinante da aplicação $x \mapsto \gamma x$, para isto temos que escolher uma A -base $\{b_i\}$ e fazer $\gamma b_i = \sum_j a_{ij} b_j$, então o determinante da matriz (a_{ij}) nos dá a norma (olha no capítulo 2, seção *Review norms and traces* de (MILNE, 2017)).

O exemplo acima mostra que no caso de uma extensão de corpos L/F , a norma definida coincide com norma da teoria de corpos, neste contexto (na verdade, um poquinho mais geral) vamos a mostrar uma propriedade que vai ser de utilidade depois.

Proposição 2.5.1. Seja n um inteiro e F um corpo, se $\alpha \in F^\bullet$ pertence à imagem da norma

$$\text{Nm} : L^\bullet \rightarrow F^\bullet$$

onde $L = F[x]/(x^n - \beta)$, então o elemento $\{\alpha, \beta\} \in K_2 F$ tem uma raiz n -ésima (usando notação multiplicativa) em $K_2 F$.

Observação 2.5.3. L não necessariamente é um corpo, já que o polinômio $x^n - \beta$ não necessariamente é irreduzível, mas $F[x]$ tem fatoração única e usando o teorema chinês L é produto finito de corpos ou anéis locais e é conhecido que para estes últimos o grupo K_1 coincide com seu grupo de unidades. Logo $K_1 L = L^\bullet$.

Demonstração. Pela observação acima, temos que a norma é de fato o morfismo de transferência $f^* : L^\bullet \rightarrow F^\bullet$, logo a fórmula de projeção 2.5.1 tem a forma (veja a observação 2.5.1).

$$f^*(\gamma \cdot f_* \beta) = \{\text{Nm} \gamma, \beta\}$$

onde $\gamma \in L^\bullet$, $\beta \in F^\bullet$. Se $\alpha = \text{Nm}(\gamma)$ e $\beta = \theta^n$ com $\theta \in L$ temos que

$$\{\alpha, \beta\} = f^*(\gamma \cdot f_* \beta) = f^*(\gamma \cdot \theta^n) = (f^*\{\gamma, \theta\})^n \in (K_2 F)^n$$

o que conclui a prova. □

ALGEBRAS SIMPLES CENTRAIS E O GRUPO DE BRAUER

3.1 Algebras cíclicas e o grupo de Brauer

Definição 3.1.1. Seja k um corpo, um k -álgebra A é um anel com k contido em seu centro (que denotamos com $C(A)$), que é um k -espaço vetorial de dimensão finita. Se o k -álgebra A é também um anel de divisão (onde todo elemento não nulo tem inverso multiplicativo), é chamado *álgebra de divisão*. Um k -álgebra é *simples* se não tem ideais bilaterais não-triviais e é *central* se tem centro igual a k .

Observação 3.1.1. Um álgebra de divisão sempre é simples pois qualquer ideal não nulo tem um elemento invertível, logo o ideal é tudo.

O exemplo mais trivial para nós será a álgebra de matrizes sobre um corpo k que denotamos com $M_n(k)$, de fato não é difícil mostrar que é um k -álgebra simples central, nós vamos trabalhar principalmente com as álgebras cíclicas como no exemplo abaixo.

Exemplo 3.1.1. Seja n um inteiro positivo e k um corpo que contém uma raiz n -ésima primitiva da unidade ω e sejam $a, b \in k^\bullet$, a álgebra $A_\omega(a, b)$ gerada por os elementos x e y é o k -espaço vetorial de dimensão n^2 com base $\{x^i y^j \mid 1 \leq i, j \leq n\}$, com o produto definido pelas identidades

$$x^n = a, \quad y^n = b, \quad yx = \omega xy$$

O álgebra acima é um caso particular de álgebras cíclicas, o objetivo deste capítulo é mostrar que algumas álgebras simples centrais sobre um corpo global tem esta forma.

Seja K/k uma *extensão cíclica* que é uma extensão finita de Galois com grupo de Galois $G = \text{Gal}(K/k)$ cíclico. Seja $n = |G| = [K : k]$, um elemento $\chi \in \text{Hom}(G, \frac{1}{n}\mathbf{Z}/\mathbf{Z})$ é

chamado um *caracter*, por cardinalidade sabemos que um caracter sobrejetivo é também bijetivo e logo podemos escolher um gerador $\sigma \in G$ tal que $\chi(\sigma) = \frac{1}{n}$.

Definição 3.1.2. Seja K/k uma extensão cíclica de grau n e G o grupo de Galois, seja $a \in k^\bullet$ e χ um caracter sobrejetivo. Denotemos por σ o gerador de G tal que $\chi(\sigma) = \frac{1}{n}$. A k -álgebra cíclica de grau n denotado por (χ, a) é o K -espaço vetorial

$$(\chi, b) = \bigoplus_{i=0}^{n-1} Ke^i$$

com base $1, e, e^2 \dots e^{n-1}$ e o produto definido pelas relações

$$\begin{aligned} e^i e^j &= e^{i+j}, & i+j < n \\ e^i e^j &= e^{i+j-n}, & i+j > n \\ e\lambda &= \sigma(\lambda)e, & \lambda \in K \\ e^n &= a \end{aligned}$$

Seja $n \in \mathbf{Z}$ coprimo com a característica de k , seja a álgebra $A_\omega(a, b)$ com $a, b \in k^\bullet$ e $\omega \in k$ uma raiz n -ésima primitiva da unidade, sejam x e y os geradores de $A_\omega(a, b)$ e considere a extensão cíclica $k[x]/k$ com grupo de Galois G . O mapa $\chi_a : G = \langle \sigma \rangle \rightarrow \frac{1}{n}\mathbf{Z}/\mathbf{Z}$ definido por $\chi_a(\sigma) = J_\omega(\sigma(x)/x)$ onde J_ω é o isomorfismo entre o grupo μ_n das raízes n -ésimas da unidade e $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ (que faz $\omega \mapsto \frac{1}{n}$), é um caracter e define a álgebra cíclica

$$(\chi_a, b) = \bigoplus_{j=0}^{n-1} Ky^j \subset A_\omega(a, b)$$

(note que as operações são compatíveis e logo a inclusão é um homomorfismo), de fato tomando dimensões temos que $(\chi_a, b) \simeq A_\omega(a, b)$. O recíproco se cumpre quando n é um número primo.

Proposição 3.1.1. Seja K/k uma extensão cíclica de grau n primo diferente da característica de k e G o grupo de Galois, seja $\omega \in k$ uma raiz primitiva n -ésima da unidade e seja $\chi : G \rightarrow \frac{1}{n}\mathbf{Z}/\mathbf{Z}$ um caracter sobrejetor, então a álgebra cíclica (χ, b) com $b \in k^\bullet$ tem a forma $A_\omega(a, b)$ para um $a \in k^\bullet$.

Demonstração. Seja K/k a extensão cíclica e $\sigma \in G$ um gerador tal que $\chi(\sigma) = \frac{1}{n}$, considere a álgebra cíclica

$$(\chi, b) = \bigoplus_{j=0}^{n-1} Ky^j$$

com as operações como na definição 3.1.2. Como $\text{Nm}(\omega) = 1$ o lema abaixo, cuja prova pode encontrar em (MILNE, 2013) (corolário 1.23 na seção *Cohomologia* do capítulo II), implica que existe $x \in K^\bullet$ tal que $\omega = \sigma(x)/x$, assim $\sigma(x) = \omega x$ (observe que $x \notin k$ e que $x^n \in k^\bullet$). Considere agora a extensão intermediária $k \subset k[x] \subset K$, como $n = [K : k]$ é

primo temos que $K = k[x]$. Por outro lado seja $a = x^n \in k^\bullet$, o caracter $\chi_a : G \rightarrow \frac{1}{n}\mathbf{Z}/\mathbf{Z}$ com $\chi_a(\tau) = J_\omega(\tau(x)/x)$ para todo $\tau \in G$ (note que $\tau \in \langle \sigma \rangle$ e logo $\tau(x)/x \in \mu_n$), assim $\chi(\sigma) = \frac{1}{n} = J_\omega(\omega) = J_\omega(\sigma(x)/x) = \chi_a(\sigma)$. Finalmente, podemos construir o algebra $A_\omega(a, b) \subset (\chi, b)$ e não é difícil ver que as operações são compatíveis (so interprete a relação $yx = \omega xy$ em $A_\omega(a, b)$ como $yx = \sigma(x)y$ em (χ_a, b)) e por igualdade de dimensões são isomorfos. $\square$

Lema 3.1.1. Seja K/k uma extensão cíclica, e seja $\sigma \in \text{Gal}(K/k)$ um gerador. Se $\text{Nm}(\omega) = 1$ para algum $\omega \in K$ então existe $x \in K^\bullet$ tal que

$$\omega = \sigma(x)/x$$

Podemos ver também em (GILLE; SZAMUELY, 2017) (olha a construção 2.5.1) que as algebras cíclicas da forma (χ, a) e com base $\{1, e, e^2, \dots, e^{n-1}\}$ são simples centrais, para mostrar que são centrais so precisamos tomar um elemento central arbitrario c e usar a equação $c = ece^{-1}$ e a independência linear para concluir que os coeficientes de c são de fato elementos do corpo base k . Para mostrar que so temos um elemento independente temos que usar o teorema de Hilbert da base normal e encontrar um elemento $\lambda \in K$ tal que $\{\sigma^j(\lambda) \mid 0 \leq j < n\}$ são linearmente independentes, multiplicando convenientemente por λ e de novo usando a independência linear chegamos a uma contradição ao suponer que algum coeficiente diferente ao término independente é não nulo. Mostrar que as álgebras cíclicas são simples é mais complicado mas também pode encontrar uma prova elementar do caso particular $A_\omega(a, b)$ em (MILNOR, 1972) (teorema 15.1 em §15).

Agora nos proponemos a definir o grupo de Brauer, para isso precisamos de fatos muito conhecidos sobre algebras simples, do centro e do produto tensorial, comencamos com o conhecido teorema de Wedderburn cuja prova pode encontrar em (GILLE; SZAMUELY, 2017) (teorema 2.1.13).

Teorema 3.1.1 (Wedderburn). Seja A um k -álgebra simples, então existe um inteiro $n \geq 1$ e uma álgebra de divisão $D \supset k$ tais que $A \simeq M_n(D)$. Mais ainda, a álgebra de divisão D é única salvo isomorfismo (se $A \simeq M_n(D) \simeq M_m(D')$ então $D \simeq D'$).

Definição 3.1.3. Dizemos que as álgebras simples centrais são *Brauer equivalentes* se existem m, n tais que

$$M_m(A) \simeq M_m(k) \otimes_k A \simeq M_n(k) \otimes_k B \simeq M_n(B)$$

O produto tensorial sobre corpo base k pode ser definido como um k -algebra com a operação

$$(a \otimes b) \cdot (a' \otimes b') = (aa' \otimes bb')$$

mas precisamos também que o produto de dois álgebras simples centrais seja também simples central, isso é consequência imediata do lema abaixo cuja prova pode encontrar em (TENGAN, 2009) (no lema 3.3).

Lema 3.1.2. Seja k um corpo e A e B dois k -álgebras

1. $C(A \otimes_k B) = C(A) \otimes_k C(B)$
2. Se A e B são simples e A é central, então $A \otimes_k B$ é também simples com centro $C(B)$.

Não é difícil mostrar que a equivalência de Brauer definida acima é de fato uma relação de equivalência, a transitividade se deduz das identidades

1. $M_m(A) \otimes_k B \simeq M_m(A \otimes_k B)$
2. $M_m(M_n(B)) \simeq M_{mn}(B)$

para dois k -álgebras arbitrárias A e B .

Proposição 3.1.2. Seja k um corpo e seja A um k -álgebra simples central, considere o anel oposto A^{opp} então $A \otimes_k A^{\text{opp}}$ é Brauer equivalente a k .

Demonstração. Seja V igual a A visto como um k -espaço vetorial e considere o homomorfismo de k -álgebras

$$a \otimes a' \mapsto (v \mapsto av a') : A \otimes_k A^{\text{opp}} \rightarrow \text{End}_k(V)$$

como $A \otimes_k A^{\text{opp}}$ é simples (olha o lema 3.1.2 acima) e $1 \otimes 1$ não está no núcleo temos que o mapa acima é injetora, agora considerando dimensões

$$[A \otimes_k A^{\text{opp}} : k] = [A : k]^2 = [\text{End}_k(V) : k]$$

temos finalmente que é um isomorfismo, assim $A \otimes_k A^{\text{opp}}$ é Brauer equivalente a k . $\square$

Definição 3.1.4 (Grupo de Brauer). Seja k um corpo, definimos o grupo de Brauer $\text{Br}(k)$ como o conjunto cociente da família de k -álgebras simples centrais com a relação de equivalência 3.1.3 e com o produto

$$[A] \cdot [B] = [A \otimes_k B]$$

a associatividade está garantida pela associatividade do produto tensorial, o elemento neutro é $[k]$ e o inverso de A é $[A^{\text{opp}}]$ como foi mostrado acima.

Exemplo 3.1.2. Seja k um corpo algebricamente fechado, então veamos que $\text{Br}(k)$ é trivial, para isso considere primeramente um k -álgebra de divisão central D e seja $a \in D$, temos que $k[a]$ é um corpo e a extensão $k[a]/k$ é finita (pois D é finito-dimensional sobre k) e logo algebrica, mas k é algebricamente fechado e logo $k[a] = k$ e assim $D = k$. Agora seja A um k -álgebra simples central, pelo teorema de Wedderburn $A \simeq M_n(D)$ para um k -álgebra de divisão D , mas temos que $C(D) = C(A) = k$ e assim D é um k -álgebra de divisão central e pelo anterior $D = k$. Assim temos que $A \simeq M_n(k)$ que é o elemento trivial do grupo de Brauer.

Exemplo 3.1.3. Seja k um corpo com uma raiz n -ésima primitiva da unidade ω , classes das álgebras cíclicas da forma $A_\omega(a, b)$ com $a, b \in k^\bullet$ no grupo de Brauer são bilineares, i.e.

$$[A_\omega(a, c)] \cdot [A_\omega(b, c)] = [A_\omega(ab, c)] \quad e \quad [A_\omega(a, b)] \cdot [A_\omega(a, c)] = [A_\omega(a, bc)]$$

Para todos os $a, b, c \in k^\bullet$, a prova pode encontra-lo em (MILNOR, 1972) (no meio da prova do teorema 15.1 em §15, página 146).

3.2 Restrição e corpos de divisão

Definição 3.2.1. Seja k um corpo e seja A um k -álgebra simples central, o produto $A \otimes_k K$ por uma extensão de corpos K/k (que denotamos por A_K) produce um K -álgebra simples central pelo lema 3.1.2, esta operação define um homomorfismo

$$\begin{aligned} \text{res} : \text{Br}(k) &\rightarrow \text{Br}(K) \\ [A] &\mapsto [A_K] \end{aligned}$$

chamado *homomorfismo de restrição*. Denotamos por $\text{Br}(K/k)$ ao núcleo deste homomorfismo.

Lembre que para nos a álgebra mais trivial sobre um corpo k é a álgebra de matrizes sobre este corpo, então se uma extensão de corpos K/k faz

$$A \otimes_k K \simeq M_n(K)$$

dizemos que a extensão *divide* o trivializa ao álgebra e se o interpretamos com o conceito acima temos que $[A]$ pertence ao núcleo do homomorfismo de restrição.

Exemplo 3.2.1. Seja k um corpo e A um k -álgebra simples central, veamos que o fecho algébrico k^{al} divide a A . Como $A \otimes_k k^{\text{al}}$ é um álgebra simples central sobre k^{al} temos que este é isomorfo a $M_n(k^{\text{al}})$ para algum n pelo exemplo 3.1.2. Uma consequência deste exemplo é a proposição abaixo que permite definir o grau de um álgebra simples central.

Proposição 3.2.1. Sea k um corpo e A um k -álgebra simples central, a dimensão de A como k -espaço vetorial sempre é um cuadrado.

Demonstração. Claramente $[A : k] = [A \otimes_k k^{\text{al}} : k^{\text{al}}]$, mas $A \otimes_k k^{\text{al}} \simeq M_n(k^{\text{al}})$ para algum n . □

Definição 3.2.2. Seja k um corpo e A um k -álgebra simples central, definimos o *grau* $\text{Deg}(A)$ de A como a raiz cuadrada de $[A : k]$.

Procurando corpos mais pequenos que dividem a um álgebra simples central encontramos a seguinte proposição.

Teorema 3.2.1. Seja k um corpo e A um simples central k -álgebra de grau n , então se K é um corpo conteudo em A tal que $[A : K] = n$ temos que K divide a A .

Demonstração. Considere o mapa da prova de 3.1.2

$$a \otimes a' \mapsto (v \mapsto av a') : A \otimes_k A^{\text{opp}} \rightarrow \text{End}_k(A)$$

que é um isomorfismo, a restrição deste mapa ao subálgebra $A \otimes_k K$ nos dá um homomorfismo injetivo onde o contradomínio é $\text{End}_K(A)$ (olha à maiúscula) pois a imagem de $d \otimes \lambda$ para $d \in A$ e $\lambda \in K$ é o mapa K -linear (por direita) $x \mapsto dx\lambda$. Considerando dimensões temos que

$$[A \otimes_k K : K] = [A : k] = n^2 = [\text{End}_K(A) : K]$$

e assim a restrição do mapa acima a $A \otimes_k K$ é um isomorfismo. $\square$

Observação 3.2.1. O teorema acima implica que se K/k é uma extensão cíclica e χ é um caracter sobrejetivo então as álgebras cíclicas da forma (χ, b) para $b \in k^\bullet$ são divididas por a própria extensão cíclica K/k . Mais adiante veremos que o recíproco também é certo, para isso precisamos conectar o grupo de Brauer com a cohomologia.

Agora veremos que um álgebra siempre pode dividir-se por uma extensão separável, pode encontrar a prova em (TENGAN, 2009)(teorema 4.6).

Teorema 3.2.2. Seja k um corpo e D um k -álgebra central de divisão, então existe $\theta \in D$ tal que a extensão $k[\theta]/k$ é separável e tem grau $\text{Deg}(D)$.

O teorema acima implica que toda álgebra central de divisão sobre um corpo k é dividido por uma extensão separável K/k , mais ainda usando o teorema de Wedderburn podemos dividir qualquer álgebra simples central A sobre k , seja agora K/k a extensão separável que divide a A e L/k o fecho normal, então L/k é Galois e temos a cadeia de isomorfismos (olha as maiúsculas)

$$A \otimes_k L \simeq A \otimes_k (K \otimes_K L) \simeq (A \otimes_k K) \otimes_K L \simeq M_n(K) \otimes_K L \simeq M_n(L)$$

por tanto L/k divide a k -álgebra simples central A . Uma consequência desto é a seguinte proposição

Proposição 3.2.2. Seja k um corpo, então

$$\text{Br}(k) = \bigcup \text{Br}(K/k)$$

onde K percorre todas as extensões finitas de Galois de k em uma clausura algébrica fixa.

Demonstração. A discussão acima implica que todo k -álgebra simples central A pode ser dividido por uma extensão de Galois K/k , logo $[A] \in \text{Br}(K/k)$. $\square$

3.3 Grupo de Brauer cohomológico

Nesta seção apresentamos a relação entre o grupo de Brauer e a cohomologia de grupos, isto aporta muitas consequências importantes que usaremos mais adiante. Começamos por o teorema principal desta seção cuja prova pode encontrar em (TENGA, 2009)(teorema 6.5).

Teorema 3.3.1. Seja k um corpo e $G_k = \text{Gal}(k_{\text{sep}}/k)$ o grupo de Galois sobre a clausura separável k_{sep} , então

$$\text{Br}(k) \simeq H^2(G_k, k_{\text{sep}})$$

este homomorfismo é compatível com o homomorfismo de restrição, i.e. para qualquer extensão K/k temos que o diagrama abaixo é comutativo

$$\begin{array}{ccc} \text{Br}(K) & \xrightarrow{\simeq} & H^2(G_K, K_{\text{sep}}^\bullet) \\ \text{res} \uparrow & & \uparrow \text{res} \\ \text{Br}(k) & \xrightarrow{\simeq} & H^2(G_k, k_{\text{res}}^\bullet) \end{array}$$

Uma primeira consequência é que podemos calcular também o grupo $\text{Br}(K/k)$ para alguma extensão finita de Galois K/k .

Corolário 3.3.1. Seja K/k uma extensão de Galois com $G = \text{Gal}(K/k)$. Então temos um isomorfismo

$$\text{Br}(K/k) \simeq H^2(G, K^\bullet)$$

Demonstração. Como $K_{\text{sep}} = k_{\text{sep}}$, $(K_{\text{sep}}^\bullet)^{G_K} = K^\bullet$, $G = G_K/G_k$ e $H^1(G_K, K_{\text{sep}}^\bullet)$ é trivial pelo teorema 90 de Hilbert, considere então a sequência exata de inflação-restrição (olha a proposição 1.34 de (MILNE, 2013))

$$0 \longrightarrow H^2(G, K^\bullet) \xrightarrow{\text{inf}} H^2(G_k, k_{\text{sep}}^\bullet) \xrightarrow{\text{res}} H^2(G_K, K_{\text{sep}}^\bullet)$$

logo $H^2(G, K^\bullet)$ é isomorfo ao núcleo do mapa de restrição $\text{res} : \text{Br}(k) \rightarrow \text{Br}(K)$. $\square$

Mas pela proposição 3.2.2 todo elemento de $\text{Br}(k)$ pertence a algum $\text{Br}(K/k) = H^2(G, K^\bullet)$, e como sabemos que este grupo é $|G|$ -torção (corolário 1.31 de (MILNE, 2013)) temos provado.

Corolário 3.3.2. Seja k um corpo, então o grupo de Brauer $\text{Br}(k)$ é de torção.

Agora considere a seguinte sequência exata (μ_n é o grupo das raízes n -ésimas da unidade)

$$1 \longrightarrow \mu_n \longrightarrow k_{\text{sep}}^\bullet \xrightarrow{n} k_{\text{sep}}^\bullet \longrightarrow 1$$

onde n representa a 'exponenciação por n ', considere agora o fragmento da sequência exata longa de cohomologia (o teorema 90 de Hilbert nos dá que $H^1(G_k, k_{\text{sep}}^\bullet)$ é trivial).

$$1 = H^1(G_k, k_{\text{sep}}^\bullet) \longrightarrow H^2(G_k, \mu_n) \longrightarrow H^2(G_k, k_{\text{sep}}^\bullet) \xrightarrow{n} H^2(G_k, k_{\text{sep}}^\bullet)$$

se chamamos $\text{Br}_n(k)$ ao subgrupo de n -torção de $\text{Br}(k)$ então a sequência acima nos dá.

Corolário 3.3.3. Seja k um corpo, logo

$$\text{Br}_n(k) \simeq H^2(G_k, \mu_n)$$

O seguinte teorema nos dá uma condição suficiente para que um k -álgebra simples central seja de fato uma álgebra cíclica da forma definida em 3.1.2. Omitiremos a prova da parte 1 da prova pois tem detalhes técnicos que não precisaremos. mas daremos uma referência. Haremos uso da cohomologia de Tate que define $H^r(G, M)$ para um grupo G finito, um G -módulo e $r \in \mathbf{Z}$, saiba mais em (MILNE, 2013) (na seção *The Tate Groups* no capítulo II).

Teorema 3.3.2. Seja K/k uma extensão cíclica de grau n com $G = \text{Gal}(K/k)$.

1. Seja $\chi \in H^1(G, \frac{1}{n}\mathbf{Z}/\mathbf{Z}) = \text{Hom}(G, \frac{1}{n}\mathbf{Z}/\mathbf{Z})$ um caracter sobrejetivo visto como elemento de $H^1(G, \mathbf{Q}/\mathbf{Z}) = \text{Hom}(G, \mathbf{Q}/\mathbf{Z})$. Considere o mapa de fronteira $\delta : H^1(G, \mathbf{Q}/\mathbf{Z}) \rightarrow H^2(G, \mathbf{Z})$ associada à sequência exata de G -módulos (com ação trivial)

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Q} \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

então para qualquer $b \in k^\bullet = H^0(G, K^\bullet)$ temos que o produto cup

$$b \cup \delta(\chi) \in H^2(G, K^\bullet) = \text{Br}(K/k)$$

é igual à classe do oposto da álgebra cíclica (χ, b) , i.e. $(\chi, b)^{\text{opp}}$.

2. Um k -álgebra simples central A é Brauer equivalente a um álgebra cíclica se e somente se existe uma extensão cíclica K/k que divide a A .

Demonstração. 1. Pode encontrar a prova em (TENGAN, 2009) (parte 1 do teorema 6.10)

2. Sabemos pela observação 3.2.1 que as álgebras cíclicas são divididas pela mesma extensão cíclica. Reciprocamente suponha que K/k divide a A , então $[A] \in \text{Br}(K/k) \simeq H^2(G, K^\bullet)$. Seja $\chi \in \text{Hom}(G, \frac{1}{n}\mathbf{Z}/\mathbf{Z})$ um caracter sobrejetivo. Como G é cíclico o produto cup definido na parte 1 coincide com o isomorfismo de grupos de cohomologia de Tate (olha na observação 3.5 do capítulo II, seção *The Tate Groups* em (MILNE, 2013)).

$$\frac{k^\bullet}{N_{K/k}K^\bullet} = H_T^0(G, K^\bullet) \xrightarrow{\cup \delta(\chi)} H_T^2(G, K^\bullet) = \text{Br}(K/k)$$

□

Exemplo 3.3.1. Vamos a calcular o grupo de Brauer de $\mathbf{R}$, como o corpo dos números complexos é algébricamente fechado, então so precisamos calcular $\text{Br}(\mathbf{C}/\mathbf{R}) = H^2(G, \mathbf{C}^\bullet)$, onde $G = \text{Gal}(\mathbf{C}/\mathbf{R}) = \{\text{Id}, \sigma\}$ é cíclico. Usando a cohomologia de Tate (que usamos acima)

$$H_T^2(G, \mathbf{C}^\bullet) = H_T^0(G, \mathbf{C}^\bullet) = \frac{\mathbf{R}^\bullet}{N_{\mathbf{C}/\mathbf{R}} \mathbf{C}^\bullet} = \{\pm 1\}$$

Observação 3.3.1. Da prova da parte 2 também podemos deduzir que o álgebra cíclica (χ, b) é trivial se e somente se b é imagem da norma da extensão K/k .

Veamos que as álgebras $(\chi_x, 1-x) = A_\omega(x, 1-x)$ quando $x \neq 0, 1$ e $(\chi_x, -x) = A_\omega(x, -x)$ com $x \neq 0$ são triviais (ω é uma raiz l -ésima primitiva da unidade). Se χ_x é o caracter da extensão $k[\alpha]/k$ com $\alpha^l = x$, temos que

1. No primer caso

$$\text{Nm}(1-\alpha) = (1-\alpha)(1-\omega\alpha)\cdots(1-\omega^{l-1}\alpha) = (1-x)$$

e assim $(\chi_x, 1-x)$ é trivial.

2. No segundo caso devemos diferenciar quando $l=2$ e $l>2$. Quando $l=2$ temos que $\text{Nm}(\alpha) = (\alpha)(-\alpha) = -x$, mas quando $l>2$ temos que

$$\text{Nm}(-\alpha) = (-\alpha)(-\omega\alpha)\cdots(-\omega^{l-1}\alpha) = -\omega^{l(l-1)/2}\alpha^l = -x$$

e por tanto $(\chi_x, -x) = A_\omega(x, -x)$ é trivial.

Assim podemos mostrar que $[A_\omega(a, b)] \cdot [A_\omega(b, a)]$ é necessariamente trivial. Veamos, pela bilinearidade (olha 3.1.3)

$$[A_\omega(a, b)] \cdot [A_\omega(b, a)] = [A_\omega(a, b)] \cdot [A_\omega(a, -a)] \cdot [A_\omega(b, a)] \cdot [A_\omega(b, -b)]$$

e logo

$$[A_\omega(a, b)] \cdot [A_\omega(a, -a)] \cdot [A_\omega(b, a)] \cdot [A_\omega(b, -b)] = [A_\omega(a, -ba)] \cdot [A_\omega(b, -ab)] = [A_\omega(ab, -ab)]$$

assim $[A_\omega(a, b)] \cdot [A_\omega(b, a)]$ é trivial.

Sumando a observação acima com o teorema de Matsumoto em K_2 temos de maneira muito obvia.

Proposição 3.3.1. Seja F um corpo, l um número primo e $\omega \in F$ uma raiz l -ésima da unidade, então existe um único homomorfismo

$$\rho : K_2 F \rightarrow \text{Br}_l(F)$$

fazendo $\rho(a, b) = [A_\omega(a, b)]$ para todo $a, b \in F^\bullet$.

3.4 Grupo de brauer de corpos locais e globais

Definição 3.4.1. Seja k um corpo, um *valor absoluto* o *módulo* em k é uma função $|\cdot| : k \rightarrow \mathbf{R}$ tal que para todo $x, y \in k$

$$(a) \quad |x| > 0 \text{ salvo que } x = 0$$

$$(b) \quad |xy| = |x||y|$$

$$(c) \quad |x + y| \leq |x| + |y|$$

se a condição mais forte

$$(c') \quad |x + y| \leq \max\{|x|, |y|\}$$

é cumprida então $|\cdot|$ é chamado valor absoluto *não arquimediano*, no outro caso chamamos *arquimediano*. O valor absoluto que faz $|x| = 1$ para todo $x \neq 0$ é chamado *valor absoluto trivial*.

Note que pela definição $|\cdot|$ é um homomorfismo de grupos de $k^\bullet$ em $\mathbf{R}_{>0}$ então temos que $|1| = 1$, logo como $\mathbf{R}_{>0}$ é livre de torção temos que a imagem das raízes n -ésimas da unidade por $|\cdot|$ é sempre 1. Em particular temos $|-1| = 1$ e $|-x| = |x|$ para todo x .

Exemplo 3.4.1. Seja K um corpo numérico e $\mathfrak{p}$ um ideal primo, como o anel dos inteiros algébricos $\mathcal{O}_K$ é um domínio de Dedekind, então existe a fatoração única de ideais e dado $c \in K^\bullet$ seja $v(c)$ o expoente de $\mathfrak{p}$ na fatoração de (c) , defina

$$|c|_{\mathfrak{p}} = \left(\frac{1}{N\mathfrak{p}} \right)^{v_{\mathfrak{p}}(c)}$$

onde $N\mathfrak{p}$ é a norma do ideal $\mathfrak{p}$ (número de elementos do cociente $\mathcal{O}_K/\mathfrak{p}$ que é finito para os corpos numéricos).

Veamos um criterio para decidir se um valor absoluto é não arquimediano.

Proposição 3.4.1. Um valor absoluto $|\cdot|$ num corpo k é não arquimediano se e somente se o conjunto $\{m1 \mid m \in \mathbf{Z}\}$ é limitado.

Demonstração. Se $|\cdot|$ é não arquimediano então para $m > 0$

$$|m1| = |1 + 1 + \cdots + 1| \leq |1| = 1$$

e pela observação baixo da definição de valor absoluto temos que $|-1| = |1|$ e logo $|-m1| = |m1| \leq 1$. Reciprocamente, suponha que $|m1| \leq N$ para todo m . Então pelo binomio de Newton

$$|x + y|^n = \left| \sum \binom{n}{r} x^r y^{n-r} \right| \leq \sum_r \binom{n}{r} |x|^r |y|^{n-r}$$

mas $|x|^r|y|^{n-r} \leq \max\{|x|^n, |y|^n\} = \max\{|x|, |y|\}^n$ e $\binom{n}{r}$ é um inteiro temos usando a hipotesis que

$$|x+y|^n \leq N(n+1)\max\{|x|, |y|\}^n$$

tomando raízes

$$|x+y| \leq N^{1/n}(n+1)^{1/n}\max\{|x|, |y|\}$$

e tomando $n \rightarrow \infty$ temos o resultado. $\square$

Se k é um corpo e $|\cdot|$ é um valor absoluto, então é fácil ver que a função $d : k \times k \rightarrow \mathbf{R}_{\geq 0}$ definida por

$$d(x, y) = |x - y|$$

é uma métrica em k logo define uma topología, esto nos permite definir.

Definição 3.4.2. Seja k um corpo, dizemos que dois valores absolutos $|\cdot|_1$ e $|\cdot|_2$ são equivalentes se geram a mesma topología.

A seguinte proposição nos da uma forma útil de saber se dois valores absolutos são equivalentes, pode encontrar a prova em (MILNE, 2017) (proposição 7.8).

Proposição 3.4.2. Sejam $|\cdot|_1$ e $|\cdot|_2$ valores absolutos num corpo k , então as proposições abaixo são equivalentes:

- (a) $|\cdot|_1, |\cdot|_2$ são valores absolutos equivalentes.
- (b) $|\alpha|_1 < 1$ implica que $|\alpha|_2 < 1$.
- (c) $|\cdot|_2 = |\cdot|_1^a$ para algum $a > 0$.

Exemplo 3.4.2. 1. O exemplo acima nos permite definir a topología $\mathfrak{p}$ -ádica em o corpo numérico K .

2. Para o corpo $\mathbf{Q}$ dos números racionais temos pelo conhecido teorema de Ostrowski que existen so 2 tipos de valores absolutos

- a) Se $|\cdot|$ é arquimediato, então $|\cdot|$ é equivalente ao valor absoluto usual (que denotamos por $|\cdot|_\infty$)
- b) Se $|\cdot|$ é não arquimediato, então este é equivalente ao valor absoluto p -ádico para algum primo p (que definimos no exemplo acima e denotamos com $|\cdot|_p$).

Para o objetivo deste capítulo precisamos o teorema de aproximação fraco, cuja prova pode encontrar em (MILNE, 2017) (teorema 7.20 no capítulo 7), começamos com o conceito de completitude de um corpo.

Definição 3.4.3. Seja k um corpo com um valor absoluto $|\cdot|$ não trivial. Uma sequência (a_n) de elementos de k é chamado *sequência de Cauchy* se para todo $\varepsilon > 0$, existe N tal que para todo $m, n \geq N$

$$|a_m - a_n| < \varepsilon$$

Um corpo k é dito *completo* se toda sequência de Cauchy converge a um elemento de k .

Agora, a proposição abaixo diz que todo corpo com um valor absoluto está imerso em um corpo completo, a prova é a mesma que no caso geral de espaços métricos e será omitida.

Proposição 3.4.3. Seja k um corpo com um valor absoluto $|\cdot|$. Então existe um corpo com valor absoluto completo $(\hat{k}, |\cdot|)$ e um homomorfismo $k \rightarrow \hat{k}$ que preserva o valor absoluto tal que cumpre a seguinte propriedade universal: Dado um homomorfismo $k \rightarrow \bar{k}$ de k a um corpo com valor absoluto completo $(\bar{k}, |\cdot|)$ que preserve o valor absoluto, este se estende a um único homomorfismo $\hat{k} \rightarrow \bar{k}$ que preserve o valor absoluto. Graficamente o diagrama abaixo é comutativo.

$$\begin{array}{ccc} k & \xrightarrow{\quad} & \hat{k} \\ & \searrow & \downarrow \\ & & \bar{k} \end{array}$$

Observação 3.4.1. 1. Como no caso de espaços métricos, a completção $\hat{k}$ e o homomorfismo $k \rightarrow \hat{k}$ são únicos salvo um único isomorfismo pela propriedade universal.

2. A imagem de k em $\hat{k}$ pelo homomorfismo dado pelo teorema é denso em $\hat{k}$, pois o fecho da imagem $\bar{k}$ é completo também e tem a mesma propriedade universal.

Exemplo 3.4.3. A completção do corpo dos racionais $\mathbf{Q}$ por o valor absoluto $|\cdot|_\infty$ é o corpo $\mathbf{R}$ dos números reais. Se usamos o valor absoluto p -ádico obtemos o corpo $\mathbf{Q}_p$.

Teorema 3.4.1 (Teorema de aproximação fraco). Sejam $|\cdot|_1, |\cdot|_2, \dots, |\cdot|_n$ valores absolutos não triviais e não equivalentes num corpo k , sejam $a_1, a_2, \dots, a_n$ elementos de k . Para todo $\varepsilon > 0$, existe um elemento $a \in k$ tal que $|a - a_i|_i < \varepsilon$

Corolário 3.4.1. Sejam $|\cdot|_1, |\cdot|_2, \dots, |\cdot|_n$ valores absolutos não triviais e não equivalentes num corpo k , sejam $a_1, a_2, \dots, a_n$ elementos das completções k_i . Para todo $\varepsilon > 0$, existe um elemento $a \in k$ tal que $|a - a_i|_i < \varepsilon$

Demonstração. Seja $\varepsilon > 0$, como k é denso em k_i então podemos encontrar para cada i um elemento b_i tal que $|b_i - a_i|_i < \varepsilon/2$, logo usando o teorema podemos encontrar $a \in k$ tal que $|a - b_i|_i < \varepsilon/2$. Por tanto

$$|a - a_i|_i = |a - b_i + b_i - a_i|_i < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

□

Agora vamos estudar o grupo de Brauer dos corpos que são matéria deste trabalho, começamos com os corpos locais.

Definição 3.4.4. Um corpo local é um corpo k com um valor absoluto não trivial que é localmente compacto (e logo completo).

Veamos as propriedades dos corpos localmente compactos que precisamos para nossa discussão.

Proposição 3.4.4. Seja k um corpo local

1. Todas as bolas fechadas são compactas.
2. O conjunto k^n é fechado em k para qualquer n .

Demonstração. 1. A traslação é um homeomorfismo e o produto por uma constante é contínua, logo so precisamos mostrar que as bolas fechadas centradas em 0 são compactas. Como o valor absoluto é não trivial temos que existe α tal que $|\alpha| > 1$, como k é localmente compacto existe uma bola fechada compacta centrada em 0 , logo todas as bolas fechadas de raio menor são também compactas. Multiplicando convenientemente por uma potência de α podemos recorrer todos os raios possíveis.

2. Seja (x_k^n) que converge a $a \in k$, logo a sequência (x_k) é limitada e contida em uma bola que é compacta pela parte 1, tomando uma subsequência (x_{k_j}) que converge a $x \in k$ temos pela continuidade da potência n -ésima que $(x_{k_j}^n)$ converge a $x^n = a$.

□

Observação 3.4.2. É possível classificar todos os corpos locais, pode encontrar esta classificação em (MILNE, 2017) na observação 7.49, também pode ver uma prova em (WEIL, 1995) na parte §3 do capítulo I.

- (a) Se um corpo k é completo com um valor absoluto arquimediano $|\cdot|$ então k é isomorfo a $\mathbf{R}$ ou $\mathbf{C}$ (o corpo dos números complexos). O valor absoluto é equivalente ao valor absoluto usual.
- (b) Um corpo local não arquimediano k de característica 0 é isomorfo a uma extensão finita de $\mathbf{Q}_p$, e o valor absoluto é equivalente a uma extensão (que veremos depois que é única) do valor absoluto p -ádico.
- (c) Um corpo local não arquimediano k de característica $p > 0$ é isomorfo ao corpo das séries formais de Laurent $k_q((T))$ sobre um corpo com q elementos k_q cujos elementos tem a forma

$$f = \sum_{i \geq -n}^{\infty} a_i T^i$$

O valor absoluto está definido pelo ideal primo $\mathfrak{p} = (T)$, é fácil ver que a norma (que é análogo ao caso do corpo numérico) $N_{\mathfrak{p}}$ é igual a q , logo o valor absoluto do elemento acima é

$$|f|_{\mathfrak{p}} = \left(\frac{1}{q}\right)^{v_{\mathfrak{p}}(f)} = q^n$$

Observação 3.4.3. Para um corpo K qualquer com um valor absoluto $|\cdot|$ não arquimediano podemos definir os seguintes 3 conjuntos:

$$A = \{a \in K \mid |a| \leq 1\}$$

$$U = \{a \in K \mid |a| = 1\}$$

$$\mathfrak{m} = \{a \in K \mid |a| < 1\}$$

Onde A é um subanel de K , U é seu grupo de unidades e $\mathfrak{m}$ é o único ideal maximal, se sabe que $|K^\bullet|$ é um subconjunto discreto de $\mathbb{R}_{>0}$ se e somente se $\mathfrak{m}$ é principal (proposição 7.6 de (MILNE, 2017)) e seu gerador é chamado *o parâmetro uniformizador* de K , precisamente os corpos locais não arquimedianos satisfazem isto, também podemos ver em (MILNE, 2017) (proposição 7.26) que todo elemento de um corpo local (que é completo) se pode escrever (de um jeito único) em forma de serie

$$\sum_{i \geq -n}^{\infty} a_i \pi^i$$

onde $n \in \mathbb{Z}$, a_i são representantes do cociente $A/\mathfrak{m}$. Daqui que o parâmetro uniformizador não pode ter raiz m -ésima no corpo K para qualquer m , vamos a mostrar isso último.

Seja $\pi \in \mathfrak{m}$ o parâmetro uniformizador, então $|\pi| < 1$, veamos que π não pode ter raiz m -ésima para $m \geq 2$. Suponha que sim e seja $\pi = x^m$, x não pode ser uma unidade pois $1 > |\pi| = |x|^m = 1$ absurdo. Logo pela representação acima existe $r > 0$ tal que $x\pi^r$ é uma unidade, veamos os casos.

1. No caso $r > 0$ temos que $\pi = (\pi^{-r} \pi^r x)^m = \pi^{-mr} u^m$ onde $u \in U$, logo tomando valores absolutos temos

$$|\pi|^{mr+1} = 1$$

com $mr+1 > 0$ o que é uma contradição.

2. No caso $r < 0$ temos que $\pi = (\pi^{-r} \pi^r x)^m = \pi^{-mr} u^m$ onde $u \in U$, logo

$$|\pi|^{-mr-1} = 1$$

mas $m \geq 2$ e logo $-mr-1 \geq 1$ o que é uma contradição.

Proposição 3.4.5. Seja k um corpo com um valor absoluto $|\cdot|$, e seja K/k uma extensão finita separável, seja $K = k[\alpha]$ e $|\cdot|'$ uma extensão de $|\cdot|$ a K . Então a completção $\hat{K} = \hat{k}[\alpha]$.

Demonstração. Considere primeramente o diagrama

$$\begin{array}{ccccc}
 (K, |\cdot|') & \hookrightarrow & (\hat{K}, \|\cdot\|') & \xlongequal{\quad} & (\hat{k}[\alpha], \|\cdot\|') \\
 \uparrow & & \uparrow & \nearrow & \\
 (k, |\cdot|) & \hookrightarrow & (\hat{k}, \|\cdot\|) & &
 \end{array}$$

Explicaremos passo a passo as setas que de fato são mergulhos, para as linhas horizontais do quadro esquerdo é claro pois são dadas pelas respectivas completações. A primeira linha vertical esquerda está dada pela inclusão da extensão K/k . A linha vertical do meio é consequência de que $\hat{K}$ contem a k e é completo com a extensão $\|\cdot\|'$ do valor absoluto $|\cdot|$ de k , pela propriedade universal existe um morfismo $\hat{k} \rightarrow \hat{K}$ que preserva o valor absoluto.

A linha em diagonal é a inclusão da extensão $\hat{k}[\alpha]/\hat{k}$ e podemos u. Para a seta $\hat{k}[\alpha] \rightarrow \hat{K}$ observe que pela seta do meio temos que $\hat{K}$ contem a $\hat{k}$, mas contem a α e logo contem a $\hat{k}[\alpha]$ e podemos usar o valor absoluto $\|\cdot\|'$ para ele.

O morfismo $\hat{K} \rightarrow \hat{k}[\alpha]$ é consequência de que $\hat{k}[\alpha]$ contem K e é completo (pois é finito dimensional sobre $\hat{k}$) e com valor absoluto que estende ao valor absoluto de K , assim podemos usar a propriedade universal e definir o morfismo $\hat{K} \rightarrow \hat{k}[\alpha]$ que preserva o valor absoluto. Finalmente fazendo a composta destes últimos morfismos temos um morfismo $\hat{K} \rightarrow \hat{K}$ mas o único morfismo que satisfaz é a identidade e como os morfismos são injetivos vemos que são de fato isomorfismos. $\square$

Os corpos locais tem um grupo de Brauer simples, mas a partir daqui podemos usá-los para obter informação de outro tipo de corpos, os corpos globais, que são matéria desta dissertação, o teorema abaixo e sua prova pode encontrar-lo em (TENGGAN, 2009) (teorema 3.6).

Teorema 3.4.2. Seja k um corpo local não arquimediano, então o grupo de Brauer é isomorfo a $\mathbf{Q}/\mathbf{Z}$.

Exemplo 3.4.4. Seja k um corpo local não arquimediano, seja n um número natural, o subgrupo $\text{Br}_n(k)$ é isomorfo ao subgrupo de n -torção de $\mathbf{Q}/\mathbf{Z}$, i.e. $\frac{1}{n}\mathbf{Z}/\mathbf{Z} \simeq \mathbf{Z}/n\mathbf{Z}$, logo é cíclico.

No caso arquimediano $\text{Br}(\mathbf{R}) = \frac{1}{2}\mathbf{Z}/\mathbf{Z}$, logo em geral temos que nos corpos locais $\text{Br}_n(k)$ é cíclico.

Començamos agora com o estudo do grupo de Brauer para corpos globais, começamos com a definição.

Definição 3.4.5. Dizemos que um corpo k é *global* se cair em uma das categorias indicadas abaixo.

1. Um corpo numérico, i.e. Uma extensão finita de $\mathbf{Q}$.
2. Uma extensão do corpo de funções racionais $k_q(T)$ e uma variável sobre um corpo finito com q elementos k_q .

É claro que a equivalência de valores absolutos definida em 3.4.2 é de fato uma relação de equivalência, logo podemos definir.

Definição 3.4.6. Seja k um corpo global um *primo* ou *place* de k é uma classe de equivalência de valores absolutos. Se v é um primo de k , denotamos por k_v à completção de k por um representante de v . Se K/k é uma extensão e k_v é a completção por um place v , então vamos a denotar por K^v à completção de K por uma extensão qualquer de um representante de v .

Agora precisamos de um teorema da teoria de corpos de classes chamado principio local-global para las álgebras simples centrais, pode encontrar em (TENGAN, 2009) (teorema 2.3.5).

Teorema 3.4.3 (Principio local-global para álgebras simples centrais). Seja K/k uma extensão de Galois de corpos globais com $G = \text{Gal}(K/k)$ a seguinte sequência (onde C_K é a *grupo de classes idéle* do corpo K)

$$0 \longrightarrow \text{Br}(K/k) \longrightarrow \bigoplus_v \text{Br}(K^v/k_v) \longrightarrow H^2(G, C_K) \longrightarrow 0$$

é um complexo que é exato nos dois primeiros termos, mas se G é cíclico então a sequência inteira é exata. Em particular, se tomamos o limite sobre todas as extensões Galois K/k temos

$$0 \longrightarrow \text{Br}(k) \longrightarrow \bigoplus_v \text{Br}(k_v)$$

Observação 3.4.4. Para os objetivos desta dissertação so precisamos os dois primeiros termos das sequências do teorema, o primer morfismo não trivial (nas dois sequências) é o morfismo que aplica a um $\alpha \in \text{Br}(k)$ todos os morfismos de restrição

$$\text{res}_v : \text{Br}(k) \rightarrow \text{Br}(k_v)$$

e suma os resultados. O primero que observamos é que para todo $\alpha \in \text{Br}(k)$ existe uma quantidade finita de primos tais que a restrição $\text{res}_v(\alpha)$ é não trivial, assim se precisamos saber se um álgebra simples central é trivial, so temos que provar num número finito primos se a restrição é trivial, a injetividade do morfismo nos da que α também é.

Agora olha a primera sequência, observamos que se $\alpha \in \text{Br}(k)$ e extensão K/k é tal que para os finitos v onde $\text{res}_v(\alpha)$ é não trivial temos que K^v o divide, então K divide a α , a proposição 3.4.5 nos da que se K/k é uma extensão separavel, então K e K_v tem a mesma 'forma'.

Agora vamos a mostrar o teorema principal deste capítulo: 'Os elementos de $\text{Br}_l(k)$, com k um corpo global e l um número primo diferente de sua característica, são Brauer equivalentes a um álgebra cíclica'. Precisamos da lei de reciprocidade local (olha em (MILNE, 2013))(teorema 1.1 no capítulo I).

Lema 3.4.1. Seja l um número primo, considere que os corpos tem característica diferente de l e contem as raízes primitivas l -ésimas da unidade, então

1. Para todo corpo local não arquimediano k e para todo $d \notin k^l$, existe $b \in k$ tal que o grupo cíclico (χ_d, b) é não trivial.
2. Se $l = 2$ então para todo corpo local diferente de $\mathbf{C}$ e $d \notin k^l$, existe $b \in k$ tal que o grupo cíclico (χ_d, b) é não trivial.

Demonstração. Seja $K = k[d^{1/l}]$ a extensão cíclica (em particular abeliana) gerada por d , $G = \langle \sigma \rangle$ o grupo de Galois e χ_d o caracer correspondente que faz $\chi_d(\sigma) = \frac{1}{l}$.

1. Pela lei de reciprocidade local temos que o grupo

$$\frac{k^\bullet}{\text{Nm}_{K/k}(K^\bullet)} \simeq G$$

Mas $|G| = l$, logo podemos encontrar $b \in k^\bullet$ tal que não seja norma de algum elemento em $K^\bullet$, assim (χ_d, b) é não trivial pela observação 3.3.1.

2. No caso arquimediano so temos $\mathbf{R}$ e a extensão K é necessariamente $\mathbf{C}$, logo os números negativos não podem ser norma, assim sempre podemos escolher um número negativo b e formar a álgebra cíclica não trivial (χ_d, b) usando de novo a observação 3.3.1. No caso não arquimediano, usamos o item anterior.

□

Teorema 3.4.4. Seja k um corpo global e l um número primo diferente da característica de k , suponha que k contem uma raiz primitiva da unidade ω . Seja $\alpha_1, \dots, \alpha_r$ elementos de $\text{Br}_l(k)$, então existe d tal que é brauer equivalente a um álgebra cíclica da forma $A_\omega(a, d)$.

Demonstração. Denotemos por $(\alpha_i)_v$ as imagens pela restrição res_v que vimos na observação 3.4.4, seja S o conjunto de primos onde $(\alpha_i)_v$ é não nulo para algum i .

Primero observamos que no caso $l > 2$ so podemos tomar o caso não arquimediano ja que $(\alpha_i)_v$ é também de l -torção, assim o ordem do elemento divide a l , mas no caso arquimediano so temos $\mathbf{R}$ cujo grupo de Brauer tem ordem 2, logo $(\alpha_i)_v$ so pode ser trivial.

Logo no caso $l > 2$ todos os k_v com $v \in S$ são não arquimedianos, assim podemos tomar o parâmetro uniformizador (olha a observação 3.4.3) que não tem raiz l -ésima, mas pela proposição 3.4.4 temos que $(k_v)^n$ é fechado e logo fora de ele podemos encontrar um ε_v e uma bola desse raio onde ninguém tem raiz l -ésima.

Pelo teorema da aproximação fraca temos que existe $d \in k$ no interior das bolas de raio ε_v e logo não tem raiz l -ésima em k_v . Pela parte 1 do lema 3.4.1 acima temos que existe uma álgebra cíclica não trivial (χ_d, c_v) com a extensão cíclica $k_v[d^{1/l}]/k_v$, como $\text{Br}_l(k_v)$ é cíclico de ordem l temos que $(\alpha_i)_v$ é gerado por (χ_d, c_v) para qualquer i , e logo $k_v[d^{1/l}]/k_v$ divide a ele. Finalmente pelo princípio local-global α_i é dividido pela extensão $k[d^{1/d}]/k$ (olha 3.4.5) e logo usamos a parte 2 do teorema 3.3.2 e concluimos que α_i é um álgebra cíclica que é o oposto (no grupo de Brauer) da álgebra $(\chi_d, a) = A_\omega(d, a)$, i.e. $A_\omega(a, d)$.

No caso $l = 2$, temos que S tem primos arquimedianos, no caso de $k_v = \mathbf{R}$ os números negativos não tem raiz quadrada, no caso não arquimediano temos igualmente o uniformizador (olha a observação 3.4.3), logo como no caso $l > 2$ podemos encontrar ε_v tal que a bola desse raio tem so elementos sem raiz l -ésima em k_v . Finalmente podemos repetir o procedimento do parágrafo acima usando a parte 2 do lema 3.4.1. $\square$

O SIMBOLO DE GALOIS E A REPRESENTAÇÃO DE K_2 PARA UM CORPO GLOBAL

4.1 O Símbolo l -ádico

Seja F um corpo, F_s uma clausura separável de F e $G_F = \text{Gal}(F_s/F)$ o grupo de Galois da extensão F_s/F . Seja $m \geq 1$ coprimo com a característica de F , o polinômio $x^m - 1$ é separável e suas raízes ficam em F_s .

Agora, como G_F é um grupo profinito, pelo exemplo 1.1.1 temos que G_F age continuamente sobre $F_s^\bullet$ (como grupo topológico discreto).

Considere agora $l \neq \text{char}(F)$ um primo, para cada $i \geq 0$ temos o seguinte diagrama comutativo de G_F -módulos discretos.

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \mu_{l^i} & \longrightarrow & F_s^\bullet & \xrightarrow{l^i} & F_s^\bullet \longrightarrow 0 \\
 & & \uparrow l & & \uparrow l & & \parallel \\
 0 & \longrightarrow & \mu_{l^{i+1}} & \longrightarrow & F_s^\bullet & \xrightarrow{l^{i+1}} & F_s^\bullet \longrightarrow 0
 \end{array} \tag{4.1}$$

Onde os morfismos l e l^i são potências. Como $\mu_{l^{i+1}} \rightarrow \mu_{l^i}$ é sobrejetivo temos no limite projetivo a sequência exata

$$0 \longrightarrow \mathbf{Z}_l(1) \longrightarrow \varprojlim F_s^\bullet \longrightarrow F_s^\bullet \longrightarrow 0 \tag{4.2}$$

Onde $\mathbf{Z}_l(1) = \varprojlim \mu_{l^i}$, e como $\mu_{l^i} \simeq \mathbf{Z}/l^i\mathbf{Z}$ como $\mathbf{Z}_l$ -módulo, temos no limite projetivo $\mathbf{Z}_l(1) \simeq \mathbf{Z}_l$, assim $\mathbf{Z}_l(1)$ é livre de posto 1.

Definimos $\mathbf{Z}_l(2) = \mathbf{Z}_l(1) \otimes \mathbf{Z}_l(1)$ que é também um G_F -módulo com a ação dagonal $g(a \otimes b) = ga \otimes gb$. Com respeito a isso temos algumas observações.

1. G_F age $\mathbf{Z}_l$ -linearmente sobre $\mathbf{Z}_l(1)$
2. O mapa $\otimes : \mathbf{Z}_l(1) \times \mathbf{Z}_l(1) \rightarrow \mathbf{Z}_l(2)$ é contínuo com a topología natural.

Vamos agora a mudar a notação, nos vamos a escrever $H^r(F, M)$ no lugar de $H^r(G_F, M)$ para denotar o grupo de cohomología de cocadeia contínua de G_F com coeficientes em M . Como $F_s^\bullet$ é discreto qualquer seção da sequência acima é contínua e podemos obter a sequência exata longa. Em particular o morfismo de fronteira

$$d_F : F^\bullet = H^0(F, F_s^\bullet) = F_s^\bullet{}^{G_F} \rightarrow H^1(F, \mathbf{Z}_l(1)) \quad (4.3)$$

O Teorema de Matsumoto nos permite construir um único morfismo de K_2F a partir de um símbolo de Steinberg, nós vamos a contruir o símbolo $(a, b)_F := d_F a \cup d_F b$. A bilinearidade está garantida pela bilinearidad do produto cup, so falta mostrar que para todo $a \in F^\bullet - \{1\}$ tem se $(a, 1 - a)_F = 0$, se chamamos

$$D_F = \langle \text{tr}_{E/F}(a, 1 - a)_E \mid E/F \text{ subextensão finita de } F_s/F \rangle \subseteq H^2(F, \mathbf{Z}_l(2))$$

mostraremos que é suficiente provar que $(a, 1 - a)_F \in D_F$ e que $D_F = 0$, mas pela proposção 1.2.1 é suficiente mostrar que D_F é l -divisível. Para tudo isso precisamos do seguinte lema.

Lema 4.1.1. Se E/F é uma subextensão finita de F_s/F seja $a \in F^\bullet$ e $b \in E^\bullet$ então $\text{tr}_{E/F}(a, b)_E = (a, N_{E/F}b)_F$.

Demonstração. Temos que mostrar que

$$\text{tr}_{E/F}(d_E a \cup d_E b) = d_F a \cup d_F N_{E/F} b$$

Lembre que $N_{E/F}$ é o mapa de transferência em dimensão 0 e que comuta com o morfismo de fronteira de cohomología, logo da identidade $\text{tr}(\text{res}(\alpha) \cup \beta) = \alpha \cup \text{tr}(\beta)$ temos

$$\text{tr}_{E/F}(\text{res}(d_F a) \cup d_E b) = d_F a \cup \text{tr}_{E/F}(d_E b) = d_F a \cup d_F N_{E/F}(b)$$

□

Teorema 4.1.1. Existe um único homomorfismo $h_F : K_2F \rightarrow H^2(F, \mathbf{Z}_l(2))$ tal que $h_F(\{a, b\}) = d_F a \cup d_F b$ para cada par de elementos a, b em $F^\bullet$.

Demonstração. Seguimos com a notação de D_F de antes do lema, seja $a \in F^\bullet - \{1\}$ onde E/F é uma subextensão finita de F_s/F . Considere o polinomio separavel $X^l - a = \prod_i f_i(X)$ com $f_i(X)$ mónico e irreducível em $E[X]$. Para cada i , seja a_i uma raiz de $f_i(X)$ e seja $E_i = E(a_i)$, vamos a mostrar que $f_i(1) = N_{E_i/E}(1 - a_i)$. Sabemos que $N_{E_i/E}(1 - a_i) = \prod_{\sigma \in S} (1 -$

σa_i) com S um conjunto de representantes de $\text{Gal}(F_s/E)/\text{Gal}(F_s/E_i)$ (lembre que S é finito pois $\text{Gal}(F_s/E_i)$ é aberto), se b_i é outra raiz de $f_i(X)$, existe $\sigma \in \text{Gal}(F_s/E)$ com $\sigma(a_i) = b_i$, assim $\{\sigma(a_i) \mid \sigma \in S\}$ é o conjunto de todas as raízes de $f_i(X)$, logo $f_i(X) = \prod_{\sigma \in S} (X - \sigma a_i)$ na clausura separável, avaliando temos $f_i(1) = \prod_{\sigma \in S} (1 - \sigma a_i) = \prod_{\sigma \in S} \sigma(1 - a_i) = N_{E_i/E}(1 - a_i)$. Agora, $1 - a = \prod_i f_i(1) = \prod_i N_{E_i/E}(1 - a_i)$, então

$$(a, 1 - a)_E = (a, \prod_i N_{E_i/E}(1 - a_i))_E = \prod_i (a, N_{E_i/E}(1 - a_i))_E$$

e usando o lema

$$(a, 1 - a)_E = \prod_i \text{tr}_{E_i/E}(a, 1 - a_i)_{E_i} = \prod_i \text{tr}_{E_i/E}(a_i^l, 1 - a_i)_{E_i} = \prod_i (\text{tr}_{E_i/E}(a_i, 1 - a_i))^l$$

temos então que, em notação multiplicativa, $(a, 1 - a)_E$ é combinação linear de transferências de extensões finitas deste corpo. Assim, o mostrado acima tem dois consequências.

1. Todo $(a, 1 - a)_F \in D_F$, para isto so basta trocar E por F no raciocínio acima.
2. D_F é l -divisível

Com isto, o teorema está demonstrado. $\square$

4.2 O morfismo h_1

Agora vamos a construir um morfismo auxiliar a partir de h_F , as propriedades deste morfismo são de vital importância para nosso objetivo como poderá apreciar o leitor.

No seguinte diagrama $E = F(\mu_l)$ e $\Delta = \text{Gal}(E/F)$, os morfismos serão explicados abaixo.

$$\begin{array}{ccccccc} (\mu_l \otimes E^\bullet)^\Delta & \xrightarrow{\gamma} & K_2 F & \xrightarrow{l} & K_2 F & \xrightarrow{\pi} \twoheadrightarrow & K_2 F / lK_2 F \\ \downarrow i & & \downarrow h & & \downarrow h & & \downarrow h_1 \\ H^1(F, \mu_l \otimes \mu_l) & \xrightarrow{\delta} & H^2(F, \mathbf{Z}_l(2)) & \xrightarrow{l} & H^2(F, \mathbf{Z}_l(2)) & \xrightarrow{k} & H^2(F, \mu_l \otimes \mu_l) \end{array} \quad (4.4)$$

A linha inferior é parte da sequência exata longa associada à sequência abaixo (o que significa que k é $H^2(\pi_1 \otimes \pi_1)$)

$$0 \longrightarrow \mathbf{Z}_l(2) \xrightarrow{l} \mathbf{Z}_l(2) \xrightarrow{\pi_1 \otimes \pi_1} \mu_l \otimes \mu_l \longrightarrow 0 \quad (4.5)$$

De fato, esta sequência é exata. O morfismo l é injetor pois $\mathbf{Z}_l(2)$ é um módulo livre sobre um domínio íntegro, logo é livre de torção. Por outro lado o mapa $\mathbf{Z}_l(2) \rightarrow \mu_l \otimes \mu_l$ é dado por $\pi_1 \otimes \pi_1$ onde $\pi_1 : \mathbf{Z}_l(1) \rightarrow \mu_l$ é a projeção à primeira componente, logo é sobrejetor.

Veamos que $\text{im}(l) = \ker(\pi_1 \otimes \pi_1)$, suponha que ω é a raiz primitiva l -ésima da unidade, então considere $\pi_1(a) = \omega^\alpha$ e $\pi_1(b) = \omega^\beta$, se $\pi_1(a) \otimes \pi_1(b)$ é a identidade, então

pelo isomorfismo $\mu_l \otimes \mu_l \simeq \mu_l$ que mostraremos abaixo (lema 4.2.1), $l|a$ ou $l|b$, assim $\pi_1(a) = 1$ ou $\pi_1(b) = 1$. Suponha que $\pi_1(a) = 1$, como $a = (\omega_i^{\alpha_i})_{i \in \mathbb{N}}$ é uma sequência coerente (ω_i é uma raiz l^i -ésima da unidade) temos que $1 = \omega_1^{\alpha_1} = l^{i-1} \omega_i^{\alpha_i} = \omega_i^{l^{i-1} \alpha_i}$, assim $l|\alpha_i$ para todo i e $a \otimes b = la' \otimes b$ para algum $a' \in \mathbb{Z}_l(1)$. A outra inclusão é óbvia.

Voltando ao diagrama 4.4, a linha superior não é necessariamente exata em $K_2 F$ da esquerda, mas é exata no resto. Vamos a construir γ com $\text{im}(\gamma) \subset \ker(l)$ e o isomorfismo i , para isso tomamos dois casos. Considere primeramente que $\mu_l \subset F$, isto implica que $E = F$ e $\Delta = 1$, neste caso definimos $\gamma(z \otimes a) = \{z, a\}$ (note que está bem definido pela bilinearidade de $\{\cdot, \cdot\}$ e que $\text{im}(\gamma) \subset \ker(l)$ já que $l\gamma(z \otimes b) = l\{z, b\} = \{z^l, b\} = \{1, b\} = 1$). Do mesmo jeito definimos $i(z \otimes a) = z \cup d_1 a$ onde $d_1 : F^\bullet \rightarrow H^1(F, \mu_l)$ é o conector da sequência exata longa correspondente à sequência exata:

$$0 \longrightarrow \mu_l \longrightarrow F_s^\bullet \xrightarrow{l} F_s^\bullet \longrightarrow 0 \quad (4.6)$$

Ainda sem usar $\mu_l \subset F$ temos a sequência

$$\mu_l^{G_F} \longrightarrow F \xrightarrow{l} F \xrightarrow{d_1} H^1(F, \mu_l)$$

Logo $\mathbb{Z}/l\mathbb{Z} \otimes F \simeq F/lF \simeq H^1(F, \mu_l)$ e como $\mu_l \simeq \mathbb{Z}/l\mathbb{Z}$ temos $\mu_l \otimes F \simeq H^1(F, \mu_l)$. Para continuar precisamos dois fatos.

Lema 4.2.1. Se μ_l é o grupo cíclico das raízes l -ésimas da unidade, temos o seguinte:

1. $\mu_l \otimes \mu_l \simeq \mu_l$
2. Se $\mu_l \subset F$ então para todo $r \geq 0$ se cumpre $\mu_l \otimes H^r(F, \mu_l) \simeq H^r(F, \mu_l \otimes \mu_l)$.

Demonstração. Para o item 1, considere a aplicação bilinear $(\omega^a, \omega^b) \mapsto \omega^{ab}$ onde ω é uma raiz l -ésima primitiva. Se $l|a - a'$ e $l|b - b'$ então $\omega^{ab} = \omega^{(a'+la'')(b'+lb'')} = \omega^{a'b'}$, assim a aplicação está bem definida. Logo existe $\hat{p} : \mu_l \otimes \mu_l \rightarrow \mu_l$ tal que $\hat{p}(\omega^a \otimes \omega^b) = \omega^{ab}$. Considere agora $\hat{q} : \mu_l \rightarrow \mu_l \otimes \mu_l$ com $\hat{q}(z) = \omega \otimes z$, é fácil ver que é o inverso de $\hat{p}$. Para o item 2, considere $A : H^r(F, \mu_l \otimes \mu_l) \rightarrow \mu_l \otimes H^r(F, \mu_l)$ com $A(\bar{f}) = \omega \otimes \overline{\hat{p} \circ f}$. Como $\mu_l \subset F$ então G_F age trivialmente sobre μ_l e $\hat{p}$ é um homomorfismo de grupos, logo $\hat{p}$ comuta com δ . Assim se $f - g = \delta h$ (usando notação aditiva para os cociclos, as cohomologias e no produto $\mu_l \otimes \mu_l$)

$$\omega \otimes \overline{\hat{p} \circ (f - g)} = \omega \otimes \overline{\hat{p} \circ (\delta h)} = \omega \otimes \overline{\delta(\hat{p} \circ h)} = 0$$

o que mostra a boa definição de A . Por outro lado, para definir $B : \mu_l \otimes H^r(F, \mu_l) \rightarrow H^r(F, \mu_l \otimes \mu_l)$ com $B(\omega^a \otimes \bar{f}) = \overline{\hat{q} \circ (af)}$ precisamos que se $l|a - a'$ e $f - g = \delta h$

$$\overline{\hat{q} \circ (af)} = \overline{\hat{q} \circ [(a' + la'')(g + \delta h)]} = \overline{\hat{q} \circ (a'g)} + \overline{\hat{q} \circ (a''\delta h)}$$

mas $\mu_l \subset F$ e G_F age trivialmente sobre $\mu_l \otimes \mu_l$ e ja que $\hat{q}$ é um homomorfismo de grupos comuta com δ , assim $\overline{\hat{q} \circ (a''\delta h)} = \overline{\delta(a''\hat{q} \circ h)} = 0$. Assim B está bem definido e do item anterior temos que $\hat{p}$ e $\hat{q}$ são inversos, daqui é fácil mostrar que A e B são inversos. $\square$

Usando o lema temos o isomorfismo:

$$\mu_l \otimes F \xrightarrow{\hat{q} \otimes \text{Id}} \mu_l \otimes \mu_l \otimes F \xrightarrow{\text{Id} \otimes \hat{f}} \mu_l \otimes H^1(F, \mu_l) \xrightarrow{B} H^1(F, \mu_l \otimes \mu_l) \quad (4.7)$$

Onde $\hat{f}$ é a composição dos isomorfismos $\mu_l \otimes F^\bullet \simeq F^\bullet / lF^\bullet \simeq H^1(F, \mu_l)$. Evaluando a função na composta 4.7 vemos que este é necessariamente o morfismo i (propriedade universal do produto tensorial). Para definir i e γ no caso geral, considere o seguinte diagrama

$$\begin{array}{ccccc} H^1(F, \mu_l \otimes \mu_l) & \xleftarrow{i} & (\mu_l \otimes E^\bullet)^\Delta & \xrightarrow{\gamma} & (K_2 F)_l \\ \downarrow \text{res} & & \downarrow \text{incl} & & \downarrow f \\ H^1(E, \mu_l \otimes \mu_l) & \xleftarrow{i_E} & \mu_l \otimes E^\bullet & \xrightarrow{\gamma_E} & (K_2 E)_l \end{array} \quad (4.8)$$

Onde i_E e γ_E estão definidos pelo caso anterior ($\mu_l \subset E$), nós procedemos a definir i e γ . Notemos que a ação de G_F sobre $H^1(E, \mu_l \otimes \mu_l)$ é equivalente à ação de $\Delta = \text{Gal}(E/F) \simeq G_F/G_E$ ja que sabemos que G_E age trivialmente sobre $H^1(E, \mu_l \otimes \mu_l)$. O isomorfismo de G_F/G_E a Δ é a restrição de um representante qualquer.

Os morfismos verticais de 4.8 são isomorfismos se restringimos os contradomínios $H^1(E, \mu_l \otimes \mu_l)$ e $(K_2 E)_l$ a $H^1(E, \mu_l \otimes \mu_l)^\Delta$ e $(K_2 E)_l^\Delta$ da esquerda e direita respectivamente, isso será mostrado depois do lema 4.2.2 abaixo. Logo para terminar a definição de i e γ temos que mostrar que $\text{im}(i_E \circ \text{incl}) = H^1(E, \mu_l \otimes \mu_l)^\Delta$ e $\text{Im}(\gamma_E \circ \text{incl}) \subset (K_2 E)_l^\Delta$. O segundo caso é fácil, seja $z \otimes a \in (\mu_l \otimes E^\bullet)^\Delta$, então $\theta(z \otimes a) = z \otimes a$, assim.

$$\theta \gamma_E(z \otimes a) = \{\theta z, \theta a\} = \gamma_E(\theta z \otimes \theta a) = \gamma_E(\theta(z \otimes a)) = \gamma_E(z \otimes a)$$

Para o primer caso é suficiente mostrar que se $\theta \in \Delta = G_F/G_E$ então

$$\theta \cdot (i_E(z \otimes a)) = i_E(\theta^{-1}(z \otimes a))$$

Seja $\sigma \in G_E$

$$(\theta \cdot (z \otimes d_1 a))(\sigma) = \theta^{-1}(z \otimes d_1 a(\theta \sigma \theta^{-1})) = \theta^{-1} z \otimes \theta^{-1} \left(\frac{\theta \sigma \theta^{-1} s(a)}{s(a)} \right)$$

Onde $s(a)$ é uma raiz l -ésima de a qualquer. Agora, usando o fato de que α é uma raiz de $x^l - a$ se e somente se $\theta \alpha$ é uma raiz de $x^l - \theta a$ temos que.

$$\theta^{-1} z \otimes \frac{\sigma \theta^{-1} s(a)}{\theta^{-1} s(a)} = \theta^{-1} z \otimes \frac{\sigma s(\theta^{-1} a)}{s(\theta^{-1} a)} = [\theta^{-1} z \otimes d_1(\theta^{-1} a)](\sigma)$$

Finalmente

$$[\theta^{-1} z \otimes d_1(\theta^{-1} a)](\sigma) = i_E(\theta^{-1} z \otimes \theta^{-1} a)(\sigma) = i_E(\theta^{-1}(z \otimes a))(\sigma)$$

Lema 4.2.2. Seja L/F uma extensão finita de Galois de grau n com grupo de Galois G . Então o núcleo e o co-núcleo dos mapas $f : K_2F \rightarrow (K_2E)^G$ e $f : H^r(F, M) \rightarrow H^r(G, M)^G$ para qualquer inteiro r e qualquer G -módulo M é aniquilado por n .

Demonstração. Tanto em K_2 (olha em 2.5.2 e 2.5.2) como em cohomologia (olha na proposição 9.5 em (BROWN, 1982)) existe o mapa de transferência $\mathbf{tr}$ na direção oposta que cumpre:

$$\mathbf{tr}(f(x)) = nx$$

e

$$f(\mathbf{tr}(y)) = \sum_{s \in G} sy$$

para $x \in K_2F$ ou $x \in H^r(F, M)$ e para $y \in K_2E$ ou $y \in H^r(L, M)$. Logo se $x \in \ker(f)$ então $nx = 0$ e se $y + \text{im}(f) \in \text{coker}(f)$ então $ny \in \text{im}(f)$. $\square$

Como foi dito acima do lema, para concluir a definição de i e γ , falta mostrar que os morfismos

$$H^1(F, \mu_l \otimes \mu_l) \xrightarrow{f=\text{res}} H^1(E, \mu_l \otimes \mu_l)^\Delta$$

e

$$(K_2F)_l \xrightarrow{f} (K_2E)_l^\Delta$$

são de fato, isomorfismos. Veamos, se $x \in \ker(\text{res})$ então $|\Delta|x = (l-1)x = 0$ e como $H^1(E, \mu_l \otimes \mu_l)$ é l -torção temos que $x = 0$ e res é injetora. Agora se $y \in H^1(E, \mu_l \otimes \mu_l)^\Delta$ então $f(\mathbf{tr}(y)) = (l-1)y = -y$, logo $y = f(\mathbf{tr}(-y))$ e res é sobrejetora. Do mesmo jeito $f : (K_2F)_l \rightarrow (K_2E)_l^\Delta$ é um isomorfismo.

Agora vamos a analisar a comutatividade do diagrama 4.4 e empezamos com o quadro esquerdo que é o piso do diagrama seguinte

$$\begin{array}{ccccc}
 & (\mu_l \otimes E^\bullet) & \xrightarrow{\gamma_E} & (K_2E)_l & \hookrightarrow K_2E \\
 & \uparrow & & \uparrow & \uparrow \\
 H^1(E, \mu_l \otimes \mu_l) & \xleftarrow{i_E} & & \xleftarrow{h_E} & \\
 & \delta_E & \rightarrow & H^2(E, \mathbf{Z}_l(2)) & \\
 & \downarrow & & \downarrow & \downarrow \\
 & (\mu_l \otimes E^\bullet)^\Delta & \xrightarrow{\gamma} & (K_2F)_l & \hookrightarrow K_2F \\
 & \uparrow & & \uparrow & \uparrow \\
 H^1(F, \mu_l \otimes \mu_l) & \xleftarrow{i} & & \xleftarrow{h_F} & \\
 & \delta & \rightarrow & H^2(F, \mathbf{Z}_l(2)) & \\
 & \uparrow & & \uparrow & \uparrow \\
 & \text{res} & & \text{res} &
 \end{array} \tag{4.9}$$

Deste diagrama temos que resaltar que:

1. O mapa $\text{res} : H^2(F, \mathbf{Z}_l(2)) \rightarrow H^2(E, \mathbf{Z}_l(2))$ é injetivo pois para todo $x \in \ker(\text{res})$ temos pelo lema 4.2.2 que $(l-1)x = 0$ e daí que $x = lx$ o que nos diz que $\ker(\text{res})$ é l -divisível e por a proposição 1.2.1 res é injetivo.
2. O quadro lateral direito é comutativo. Pois se $\{a, b\} \in K_2F$ com $a, b \in F^\bullet$ temos que $\text{res}(h_F(\{a, b\})) = \text{res}(d_F a \cup d_F b) = d_E a \cup d_F b = h_E(f(\{a, b\}))$
3. A parede da esquerda junto com a parede da frente é o diagrama 4.8 onde definimos γ e i , logo estes são comutativos.
4. A comutatividade dos demais quadros laterais é fácil de mostrar, logo fazendo as contas temos que a injetividade de res nos dá que se o quadro do teto é comutativo então o piso também é.

Destas observações se desprende que so precisamos mostrar que o quadro do teto é comutativo o que significa que, sem perda de generalidade podemos supor que $\mu_l \subset F$.

Então, se $\mu_l \subset F$ considere o diagrama comutativo.

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \mathbf{Z}_l(1) & \hookrightarrow & \varprojlim F_s^\bullet & \xrightarrow{\Delta_l} & F_s^\bullet \longrightarrow 0 \\
 & & \downarrow \pi_1 & & \downarrow \pi_1 & & \parallel \\
 0 & \longrightarrow & \mu_l & \hookrightarrow & F_s^\bullet & \xrightarrow{l} & F_s^\bullet \longrightarrow 0
 \end{array} \tag{4.10}$$

Sejam agora ζ e α preimagens de z e a respectivamente em $\varprojlim F_s^\bullet$. Então (note que a comutatividade de π_1 e d é porque a ação de G_F em $\varprojlim F_s^\bullet$ é diagonal)

$$i(z \otimes a) = z \cup d\pi_1(\alpha) = \pi_1(l\zeta) \cup \pi_1 \circ (d\alpha) = (\pi_1 \otimes \pi_1) \circ (l\zeta \cup d\alpha)$$

Lembrando agora a sequência exata 4.5

$$0 \longrightarrow \mathbf{Z}_l(2) \xrightarrow{l} \mathbf{Z}_l(2) \xrightarrow{\pi_1 \otimes \pi_1} \mu_l \otimes \mu_l \longrightarrow 0$$

Temos que o cociclo $l^{-1}d(l\zeta \cup d\alpha) = d\zeta \cup d\alpha$ é o representante da imagem de $i(z \otimes a)$ pelo morfismo de fronteira δ da sequência acima, por outro lado $d\zeta \cup d\alpha$ é o representante de $h(\gamma(z \otimes a)) = d_F z \cup d_F a$. E assim o quadro esquerdo do diagrama 4.4 é comutativo.

O quadro do meio do diagrama 4.4 é obviamente comutativo e vamos a definir h_1 tal que o quadro da direita seja comutativo. Para isso observe o quadro direito aqui em baixo.

$$\begin{array}{ccc}
 K_2F & \xrightarrow{\pi} & K_2F / lK_2F \\
 \downarrow h & & \downarrow h_1 \\
 H^2(F, \mathbf{Z}_l(2)) & \xrightarrow{k} & H^2(F, \mu_l \otimes \mu_l)
 \end{array} \tag{4.11}$$

Definimos $h_1(x + lK_2F) = k \circ h(x)$, e se $x - x' = ly$ com $y \in K_2F$ então $k \circ h(x) = k \circ h(x' + ly) = k \circ h(x') + lk \circ h(y) = k \circ h(x')$, pois $H^2(F, \mu_l \otimes \mu_l)$ é de l -torção, e assim h_1 está bem definido e claramente o diagrama é comutativo

Observação 4.2.1. Uma descrição de h_1 mais fácil é a seguinte, seja $\{a, b\} + K_2F$ e sejam α e β as preimagens de a e b em $\varprojlim F_s^\bullet$ no diagrama 4.10, então o cociclo $d\alpha \cup d\beta$ representa a $h(\{a, b\})$ e aplicando $k = H^2(\pi_1 \otimes \pi_1)$ temos o cociclo $d(\pi_1\alpha) \cup d(\pi_1\beta)$, mas $\pi_1\alpha$ e $\pi_1\beta$ são preimagens de a e b na linha inferior do diagrama 4.10, por tanto $d(\pi_1\alpha) \cup d(\pi_1\beta)$ é um representante de $d_1a \cup d_1b \in H^2(F, \mu_l \otimes \mu_l)$.

O próximo teorema e seu corolário são resultados medulares para o teorema principal, para seu enunciado precisamos da notação seguinte para um grupo abeliano A

- $A_{l\text{-div}}$: O subgrupo maximal l -divisível.
- A_{l^n} : O dos elementos $a \in A$ tais que $l^n a = 0$.
- $A\{l\} = \bigcup_{n=1}^{\infty} A_{l^n}$: A parte l -primária de A .

Teorema 4.2.1. No diagrama 4.4 se cumpre o seguinte:

- (a) O kernel de h contém $(K_2F)_{l\text{-div}}$ e $h[(K_2F)_l] = H^2(F, \mathbf{Z}_l(2))_l$
- (b) Suponha que h_1 é injetivo. Então $\ker(h) = (K_2F)_{l\text{-div}}$ e $\text{coker}(h)$ é livre de l -torção.

Demonstração. (a) Temos que a imagem de $(K_2F)_{l\text{-div}}$ por h é também l -divisível, mas $H^2(F, \mathbf{Z}_l(2))$ não pode conter subgrupos l -divisíveis não nulos pela propriedade 1.2.1, logo $(K_2F)_{l\text{-div}} \subset \ker(h)$. Seja agora $x \in H^2(F, \mathbf{Z}_l(2))$ com $lx = 0$, então $x = \delta(y)$ com $y \in H^1(F, \mu_l \otimes \mu_l)$ e também $y = i(z)$ com $z \in (\mu_l \otimes E^\bullet)^\Delta$. Então $x = \delta(i(z)) = h(\gamma(z))$ e sabemos que $\text{im}(\gamma) \subset (K_2F)_l$. A outra inclusão é óbvia.

- (b) Suponha que h_1 é injetivo, pela parte (a) e pela definição de $(K_2F)_{l\text{-div}}$ é suficiente mostrar que $\ker(h)$ é l -divisível. Seja $x \in \ker(h)$, então $0 = k(h(x)) = h_1(\pi(x))$ e $\pi(x) = 0$, com isto temos que $x = ly$ com $y \in K_2F$. Agora $0 = h(x) = lh(y)$, então $h(y) = \delta(i(z)) = h(\gamma(z))$ e assim $y - \gamma(z) \in \ker(h)$, e como $\text{im}(\gamma) \subset (K_2F)_l$ temos que $x = ly = l(y - \gamma(z))$, concluímos que $\ker(h)$ é l -divisível.

Por outro lado, seja $y + \text{im}(h) \in \text{coker}(h)$, mostremos que se $l^n \in \text{im}(h)$ então $l^{n-1}y \in \text{im}(h)$ para $n \geq 1$. Seja então $l^n y = l(l^{n-1}y) = h(x)$, logo $h_1(\pi(x)) = k(h(x)) = 0$ e pela injetividade de h_1 temos que $x = lz$. Assim $l^n y = h(x) = lh(z)$ e $l(l^{n-1}y - h(z)) = 0$, então $l^{n-1}y - h(z) = \delta(i(\omega)) = h(\gamma(\omega))$, finalmente $l^{n-1}y = h(z + \gamma(\omega)) \in \text{im}(h)$. Seguindo o proceso concluímos que $y \in \text{im}(h)$.

□

Corolário 4.2.1. Se h_1 é injetivo, então $K_2F\{l\}$ é soma direita de seu subgrupo maximal divisível (que é aniquilado por h) e um subgrupo que é mapeado isomorficamente por h a $H^2(F, \mathbf{Z}_l(2))\{l\}$.

Demonstração. Como $\text{coker}(h)$ é livre de l -torção temos que $H^2(F, \mathbf{Z}_l(2))\{l\} \subset \text{im}(h)$. Seja $A = h^{-1}(H^2(F, \mathbf{Z}_l(2))\{l\})$, veamos que o mapa $h|_A$ define um isomorfismo

$$A/A_{l\text{-div}} \rightarrow H^2(F, \mathbf{Z}_l(2))\{l\}$$

pelo teorema de isomorfismo de grupos so precisamos mostrar que

$$\ker(h|_A) = A \cap (K_2F)_{l\text{-div}} = A_{l\text{-div}}$$

e que $h|_A$ é sobrejetivo e a sobrejetividade de $h|_A$ está dada pela inclusão

$$H^2(F, \mathbf{Z}_l(2))\{l\} \subset \text{im}(h)$$

Seja agora $x \in A \cap (K_2F)_{l\text{-div}}$ então $x = ly$ com $y \in (K_2F)_{l\text{-div}}$ e $0 = h(x) = lh(y)$, logo $h(y) \in H^2(F, \mathbf{Z}_l(2))\{l\}$ e $y \in A$. Assim $A \cap (K_2F)_{l\text{-div}}$ é l -divisível em A , então $x \in A \cap (K_2F)_{l\text{-div}} \subset A_{l\text{-div}}$. Por outro lado $A_{l\text{-div}} = A \cap A_{l\text{-div}} \subset A \cap (K_2F)_{l\text{-div}}$. Considere agora a sequência

$$0 \longrightarrow A_{l\text{-div}} \hookrightarrow A \xrightarrow{h|_A} H^2(F, \mathbf{Z}_l(2))\{l\} \longrightarrow 0.$$

mas $\text{EXT}(Y, X) = 0$ quando X é um grupo l -primário e Y é l -divisível (propriedade (I) na página 268 de (FUCHS, 2015)), o que significa que $A = A_{l\text{-div}} \oplus B$ com $B \subset A$ e $B \simeq H^2(F, \mathbf{Z}_l(2))\{l\}$.

Vamos a concluir o corolário, para decompor $K_2F\{l\}$ é suficiente mostrar a seguinte inclusão

$$K_2F\{l\} \subset (K_2F\{l\} \cap A_{l\text{-div}}) \oplus B$$

e que $K_2F\{l\} \cap A_{l\text{-div}} = (K_2F\{l\})_{l\text{-div}}$ pois a outra inclusão é trivial.

Seja $x \in K_2F\{l\} \subset A$, então $x = a + b$ com $a \in A_{l\text{-div}}$ e $b \in B$, tomando máximo temos que $l^m x = 0$ e $l^m b = 0$ para algum m . Logo $a \in K_2F\{l\} \cap A_{l\text{-div}}$.

Falta ver que $(K_2F\{l\})_{l\text{-div}} = K_2F\{l\} \cap A_{l\text{-div}}$, para isso note que a inclusão $K_2F\{l\} \subset A$ implica $(K_2F\{l\})_{l\text{-div}} \subset A_{l\text{-div}}$ e $(K_2F\{l\})_{l\text{-div}} \subset A_{l\text{-div}} \cap K_2F\{l\}$.

Seja agora $x \in A_{l\text{-div}} \cap K_2F\{l\}$, $x = ly$ com $y \in A_{l\text{-div}}$, mas $0 = l^n x = l^{n+1} y$ e assim $y \in K_2F\{l\}$ e $A_{l\text{-div}} \cap K_2F\{l\}$ é l -divisível e está contido em $K_2F\{l\}$, por tanto temos a outra inclusão e

$$K_2F\{l\} = (K_2F\{l\})_{l\text{-div}} \oplus B$$

□

Observação 4.2.2. Deste corolário podemos inferir que para dar uma representação K_2F de um corpo, precisamos o seguinte:

1. A injetividade de h_1
2. Que $K_2F\{l\}$ não tenha subgrupos l -divisíveis
3. Que K_2F seja um grupo de torção

A ultima condição permite que K_2F seja a soma direita das partes l -primárias, um resultado também da que K_2F não tem p -torção quando a característica de F é $p > 0$ (teorema 6.7 em (WEIBEL, 2013)). Na seguinte seção daremos condições para a injetividade de h_1 .

4.2.1 Criterio para a injetividade de h_1

O seguinte lema nos permite trabalhar com o caso $\mu_l \subset F$.

Lema 4.2.3. Seja $E = F(\mu_l)$ e $\Delta = \text{Gal}(E/F)$, se h_1^E é injetivo o bijetivo então h_1^F também é.

Demonstração. Considere o seguinte diagrama:

$$\begin{array}{ccccc}
 & (K_2E)^\Delta & \xrightarrow{\pi_E} & (K_2E/lK_2E)^\Delta & \\
 & \nwarrow h_E & \uparrow f & \nwarrow h_1^E & \\
 H^2(E, \mathbf{Z}_l(2)) & \xrightarrow{k^E} & H^2(E, \mu_l \otimes \mu_l)^\Delta & & \\
 \uparrow \text{res} & & \uparrow \text{res} & & \\
 & K_2F & \xrightarrow{\pi_F} & K_2F/lK_2F & \\
 & \nwarrow h_F & \uparrow k^F & \nwarrow h_1^F & \\
 H^2(F, \mathbf{Z}_l(2)) & \xrightarrow{k^F} & H^2(F, \mu_l \otimes \mu_l) & &
 \end{array} \tag{4.12}$$

É facil mostrar a comutatividade das paredes da esquerda, frente e atrás, o piso e o teto também são comutativas (são os quadros da direita no diagrama 4.4 no caso de F e E respectivamente) e π_F é sobrejetor, logo a comutatividade da parede esquerda implica a comutatividade da parede direita que detalhamos no seguinte dissenho:

$$\begin{array}{ccc}
 K_2F/lK_2F & \xrightarrow{\hat{f}} & (K_2E/lK_2E)^\Delta \\
 \downarrow h_1^F & & \downarrow h_1^E \\
 H^2(F, \mu_l \otimes \mu_l) & \xrightarrow{\text{res}} & H^2(E, \mu_l \otimes \mu_l)^\Delta
 \end{array} \tag{4.13}$$

So resta mostrar então que $\hat{f}$ e **res** são de fato isomorfismos, mas como na prova do lema 4.2.2 usamos o mapa **tr** tal que a composta $K_2F \xrightarrow{f} (K_2E)^\Delta \xrightarrow{\text{tr}} K_2F$ é multiplicar por $|\Delta| = l - 1$, pasando aos cocientes temos que se $0 = \hat{f}(x + lK_2F)$ então

$$0 = \widehat{\text{tr}}(\hat{f}(x + lK_2F)) = (l - 1)x + lK_2F = -x + lK_2F$$

Assim $x \in lK_2F$. Do mesmo jeito seja $y + lK_2E \in (K_2E/lK_2E)^\Delta$

$$\hat{f}(\widehat{\text{tr}}(y + lK_2E)) = \sum_{s \in \Delta} s(y + lK_2E) = (l-1)y + lK_2E = -y + lK_2E$$

Logo $y + lK_2E = \hat{f}(-\widehat{\text{tr}}(y + lK_2E))$ e assim $\hat{f}$ é sobrejetora. Do mesmo jeito fazemos para **res** na linha horizontal inferior. $\square$

A causa deste lema podemos considerar que $\mu_l \subset F$ para a discussão seguinte.

Sabemos que $H^2(F, \mu_l \otimes \mu_l) \simeq \mu_l \otimes H^2(F, \mu_l)$ por o lema 4.2.1, também por 3.3.3 se sabe que $H^2(F, \mu_l) \simeq \text{Br}_l F$ onde $\text{Br}_l F$ é o subgrupo do grupo de Brauer de F tal que seus elementos tem orden que divide a l . Então considere o diagrama.

$$\begin{array}{ccccc} K_2F & \xrightarrow{\pi} & K_2F/lK_2F & & \\ \downarrow h & & \downarrow h_1 & & \\ \rho \circ H^2(F, \mathbf{Z}_l(2)) & \xrightarrow{k} & H^2(F, \mu_l \otimes \mu_l) & \xrightarrow{a} & \mu_l \otimes H^2(F, \mu_l) \\ & & & & \downarrow b \\ & & & & \mu_l \otimes \text{Br}_l F \\ & & & \xleftarrow{c} & \text{Br}_l F \end{array} \quad (4.14)$$

Onde b vem do isomorfismo $H^2(F, \mu_l) \simeq \text{Br}_l F$ (logo é isomorfismo) e c é o isomorfismo dado por $c(\omega^t \otimes \alpha) = \alpha^t$ (é fácil mostrar que está bem definido e seu inverso é $c^{-1}(\alpha) = \omega \otimes \alpha$), por outro lado o morfismo ρ é dado pelo símbolo $\rho(\{a, b\}) = (a, b)$ (olha em 3.3.1) onde (a, b) é a classe de equivalência no grupo de Brauer de F do algebra cíclica $A_\omega(a, b)$ (definido no exemplo 3.1.1). Pela unicidad do símbolo ρ temos a igualdade $cbakh(x) = \rho(x)$, mas $kh(x) = h_1\pi(x) = h_1(x + lK_2F)$ y assim $bah_1(x + lK_2F) = c^{-1}\rho(x)$.

Pelo descrito acima, podemos trabalhar com $\mu_l \otimes \text{Br}_l F$ no lugar de $H^2(F, \mu_l \otimes \mu_l)$ e mudar a notação e bah_1 pode pasar a ser h_1 . Com isto temos $h_1(\{a, b\} + lK_2F) = c^{-1}\rho(x)$ e a equação:

$$h_1(\{a, b\} + lK_2F) = c^{-1}\rho(\{a, b\}) = c^{-1}(a, b) = \omega \otimes (a, b) \quad (4.15)$$

Proposição 4.2.1. Para $a, b \in F^\bullet$ as seguintes afirmações são equivalentes.

- (i) $\{a, b\} \in lK_2F$
- (ii) $h_1(\{a, b\} + lK_2F) = 0$
- (iii) $(a, b) = 0$
- (iv) b é a imagem da norma da extensão $F(a^{1/l})$

Demonstração. (i) implica (ii) é trivial, (ii) e (iii) são equivalentes pelo isomorfismo c do diagrama 4.14, para (iii) implica (iv) podemos usar 3.3.1 e para (iv) implica (i) usamos 2.5.1. $\square$

O seguinte teorema caracteriza o núcleo do mapa h_1 e seus corolários dan condições suficientes sobre o simbolo $(\cdot, \cdot)$ para a injetividade de h_1 .

Teorema 4.2.2. Se $\mu_l \subset F$ o núcleo do mapa h_1 no diagrama 4.4 é isomorfo a $\ker(u)/(\ker(u))'$ onde $u : F^\bullet \otimes F^\bullet \rightarrow \text{Br}_l F$ é o mapa dado pelo algebra cíclica $a \otimes b \mapsto (a, b)$ e $(\ker(u))'$ é o subgrupo de $\ker(u)$ gerado pelos elementos descomponíveis de $\ker(u)$. Em particular h_1 é injetivo se $\ker(u)$ é gerado por seus elementos descomponíveis.

Demonstração. O objetivo é usar o teorema do isomorfismo, para isso definiremos o (único) homomorfismo $t : F^\bullet \otimes F^\bullet \rightarrow K_2 F / lK_2 F$ com $t(a \otimes b) = \{a, b\} + lK_2 F$ e trabalharemos com sua restrição $t|_{\ker(u)}$, mostraremos que a imagem de esta restrição é igual a $\ker(h_1)$ e seu núcleo é $(\ker(u))'$.

Primero, veamos que $\ker(t)$ é gerado por elementos descomponíveis, de fato $\ker(t) = S + T$ onde $S = \{a \otimes b \mid a, b \in F^\bullet, a + b = 1\}$ e $T = \{la \otimes b \mid a, b \in F^\bullet\}$. Considere o único isomorfismo $v : \frac{F^\bullet \otimes F^\bullet}{S} \rightarrow K_2 F$ com $v(a \otimes b + S) = \{a, b\}$ com inversa $v^{-1}(\{a, b\}) = a \otimes b + S$ e considere a composta:

$$F^\bullet \otimes F^\bullet \xrightarrow{\pi_S} \frac{F^\bullet \otimes F^\bullet}{S} \xrightarrow{v} K_2 F \xrightarrow{\pi} K_2 F / lK_2 F$$

Pela unicidade de t temos que $t = \pi v \pi_S$. Agora seja $x \in \ker(t)$, então $0 = \pi v \pi_S(x) = \pi v(x + S)$, que implica que $x + S = lv^{-1}(y)$ com $y \in K_2 F$. Seja $y = \prod_{i=1}^n \{a_i, b_i\}$, com isto temos $x = \sum_{i=1}^n l(a_i \otimes b_i) + S \in T + S$. A outra inclusão é óbvia, e assim temos que $\ker(t)$ é gerado por elementos descomponíveis em ele.

Agora, usando a proposição 4.2.1 temos que $0 = t(a \otimes b)$ se e somente se $0 = (a, b) = u(a \otimes b)$, com isto temos que os elementos descomponíveis do núcleo de t são os mesmos que os elementos descomponíveis do núcleo de u , logo $\ker(t) = (\ker(u))' \subset \ker(u)$.

Finalmente podemos definir $\hat{t} = t|_{\ker(u)} : \ker(u) \rightarrow \ker(h_1)$ com $\ker(\hat{t}) = \ker(u) \cap \ker(t) = \ker(t)$, para a sobrejetividade seja $\prod_{i=1}^n \{a_i, b_i\} \bmod lK_2 F \in \ker(h_1)$, então $0 = h_1(\prod_{i=1}^n \{a_i, b_i\} \bmod lK_2 F) = z \otimes \prod_{i=1}^n (a_i, b_i)$. Logo pelo isomorfismo $\mu_l \otimes \text{Br}_l F \simeq \text{Br}_l F$ temos que $0 = \prod_{i=1}^n (a_i, b_i) = u(\sum_{i=1}^n a_i \otimes b_i)$. $\square$

Corolario 4.2.2. Se o símbolo $(\cdot, \cdot)$ satisfaz as seguintes duas condições, então h_1 é injetora.

- (i) Sejam $a, b, c, d \in F^\bullet$ tais que $(a, b) = (c, d)$, exist elementos $x, y \in F^\bullet$ tais que

$$(a, b) = (x, b) = (x, y) = (c, y) = (c, d)$$

- (ii) Sejam $a_1, a_2, b_1, b_2 \in F^\bullet$, existem $c_1, c_2, d \in F^\bullet$ tais que

$$(a_1, b_1) = (c_1, d) \text{ e } (a_2, b_2) = (c_2, d)$$

Demonstração. Suponha que (i) e (ii) são satisfeitos. Por (i) se $(a, b) = (c, d)$ então

$$a \otimes b - c \otimes d = \left(\frac{a}{x} \otimes b\right) + \left(x \otimes \frac{b}{y}\right) + \left(\frac{x}{c} \otimes y\right) + \left(c \otimes \frac{y}{d}\right) \in \ker(u)$$

pois como $(a, b) = (x, b)$ então $0 = u(a \otimes b - x \otimes b) = u(\frac{a}{x} \otimes b)$ e $\frac{a}{x} \otimes b \in \ker(u)$, de igual forma com os demais sumandos. Assim $a \otimes b - c \otimes d \in (\ker(u))'$.

Agora, considerando (i) e (ii) sejam $a_1 \otimes b_1, a_2 \otimes b_2 \in F^\bullet \otimes F^\bullet$, sabemos que $(a_1, b_1) = (c_1, d)$ e $(a_2, b_2) = (c_2, d)$ então $(a_1, b_1)(a_2, b_2) = (c_1 c_2, d)$ e logo por o raciocínio acima $a_1 \otimes b_1 + a_2 \otimes b_2 - (c_1 c_2 \otimes d) = (a_1 \otimes b_1 - c_1 \otimes d) + (a_2 \otimes b_2 - c_2 \otimes d) \in (\ker(u))'$, assim $a_1 \otimes b_1 + a_2 \otimes b_2 \equiv (c_1 c_2 \otimes d) \pmod{(\ker(u))'}$. Usando indução temos $a_1 \otimes b_1 + \dots + a_n \otimes b_n \equiv x_0 \otimes y_0 \pmod{(\ker(u))'}$, se $a_1 \otimes b_1 + \dots + a_n \otimes b_n \in \ker(u)$ então $x_0 \otimes y_0 \in \ker(u)$ e logo $x_0 \otimes y_0 \in (\ker(u))'$. Assim se $x = \sum_{i=1}^n a_i \otimes b_i \in \ker(u)$ então $x \in (\ker(u))'$ e h_1 é injetivo. $\square$

Observação 4.2.3. 1. A condição ii) significa que dois algebras l-cíclicas siempre tem um corpo común $F(d^{1/l})$ que os escinde, e se sabe que estos são exatamente da forma (c, d) para algum $c \in F^\bullet$.

2. A condição i) pode ser obviamente reemplazado por a seguinte: Dados $a, b, c, d \in F^\bullet$, existem $x_i, y_i \in F^\bullet, 1 \leq i \leq n$, tais que

$$(a, b) = (x_1, b) = (x_1, y_1) = (x_2, y_1) = (x_2, y_2) = \dots = (x_n, y_n) = (c, y_n) = (c, d)$$

3. Para $l = 2$ a condição i) sempre é satisfeito inclusive com $y = d$. De fato, seja D o algebra de quaternões sobre F cuja clase é $(a, b) = (c, d)$. Seja D^0 o subespaço de elementos de traza 0 ($\text{tr}(r + si + tj + uk) = 2r = 0$ tem dimensão 3). Definamos uma forma bilinear simétrica não degenerada $\langle \alpha, \beta \rangle = \frac{1}{2}(\alpha\beta + \beta\alpha)$, um cálculo fácil nos da que a imagem esta contido em F . Para que D seja da clase (a, b) é necesario e suficiente que existam $\alpha, \beta \in D^0$ tais que $a \perp b$ e que $a\alpha^2 = a$ e $\beta^2 = b$ (o isomorfismo será dado por $i \mapsto \alpha, j \mapsto \beta$). Seja então $\alpha, \beta \in D^0$ ditos elementos para (a, b) e $\gamma, \delta \in D^0$ os que corresponden a (c, d) . Como D^0 é 3-dimensional temos que existe $0 \neq \xi \in D^0$ tal que $\xi \perp \alpha$ e $\xi \perp \beta$ e seja $x = \langle \xi, \xi \rangle \in F^\bullet$. Logo

$$(a, b) = (x, b) = (x, d) = (c, d)$$

Proposição 4.2.2. Se $\text{Br}_l F$ é cíclico, então as condições i) e ii) da proposição anterior se satisfacem e h_1 é injetivo.

Demonstração. A condição ii) é obvia. Para a condição i) se $\text{Br}_l F = 0$ não temos nada que mostrar, veamos então o caso $\text{Br}_l F = \mathbf{Z}/l\mathbf{Z}$.

Seja $\alpha := (a, b) = (c, d) \in \text{Br}_l F$, debemos encontrar $x, y \in F^\bullet$ tais que

$$\alpha = (a, b) = (x, b) = (x, y) = (c, y) = (c, d)$$

Se $\alpha = 0$ podemos tomar $x = y = 1$ e estamos pronto. Para o caso $\alpha \neq 0$ para cada $z \in F^\bullet$ vamos a definir a funcional linear $A_z : F^\bullet / lF^\bullet \rightarrow \mathbf{Z}/l\mathbf{Z}$ dado por $\bar{x} \mapsto (x, z)$. Logo como $\alpha \neq 0$ as funcionais A_b e A_d são não nulos e para istos vamos a dividir a prova em dois casos.

a) **A_b, A_d são L.I. ou iguais.** Neste caso vamos a escolher $y = d$, para o caso da igualdade qualquer $x \in F^\bullet$ é válido para a condição i), mas se são L.I. temos que procurar $x \in F^\bullet$ tal que

$$(a, b) = (x, y) = (x, d) = (c, d)$$

Como A_b e A_d são L.I os núcleos não estão contidos entre si, logo existe $x_0 \in \ker(A_b)$ tal que $x_0 \notin \ker(A_d)$ então para qualquer $x \in F^\bullet / lF^\bullet$ temos

$$x - \frac{A_d(x)}{A_d(x_0)} x_0 \in \ker(A_d)$$

e assim $\ker(A_b) + \ker(A_d) = F^\bullet / lF^\bullet$ e logo $(a + \ker(A_b)) \cap (c + \ker(A_d)) \neq \emptyset$ (um exercicio básico de algebra linear), assim existe $x \in F^\bullet / lF^\bullet$ tal que

$$\alpha = (a, b) = A_b(a) = A_b(x) = A_d(x) = A_d(c) = (c, d)$$

b) **A_b e A_d são L.D e diferentes**

Agora se A_b e A_d são L.D. e diferentes, então $A_b = \gamma A_d$ com $\gamma \neq 0, 1$. Por outro lado, o caso $l = 2$ já foi resuelto na observação acima e podemos supor então que $l > 2$, logo a forma bilinear $(\cdot, \cdot)$ é alternada pois qualquer $e \in F^\bullet$ é uma potência l -ésima o a norma de $e^{1/l}$ da extensão $F(e^{1/l})/F$ e assim $(e, e) = 0$ (veja 4.2.1).

As formas $A_b = \gamma A_d$ e A_{cd} são L.I. avaliando convenientemente em b e cd na equação $mA_b + nA_{cd} = 0$. Logo escolha $y = cd$ e temos $(c, y) = (c, cd) = (c, d) = \alpha$ e como no caso a), a independência linear de A_b e A_{cd} nos permite resolver

$$(a, b) = (x, b) = A_b(x) = \alpha = A_{cd}(x) = (x, cd) = (c, cd) = (c, d)$$

□

A exigência da proposição acima pode ser muito forte para corpos em geral, mas o objetivo deste trabalho es estudar corpos globais cujas completções por valores absolutos dan como resultado os corpos locais, istos tem o grupo Br_l cíclico. Na proxima seção estudaremos os corpos globais pasando por seus corpos locais usando o principio local-global de Hasse.

4.3 O teorema principal para corpos globais

Nesta seção, F denotará um corpo global como no definido em 3.4.5.

Teorema 4.3.1. Para um corpo global F o mapa h_1 no diagrama 4.4 é bijetivo.

Demonstração. Pelo lema 4.2.3 podemos considerar que $\mu_l \subset F$. Empecemos escrevendo a propriedade do morfismo $h_1 : K_2F/lK_2F \rightarrow \mu_l \otimes \text{Br}_l(F)$ escolhendo a raiz primitiva l -ésima da unidade ω que diz

$$h_1(\{a, b\} + lK_2F) = \omega \otimes (a, b)$$

para todo $a, b \in F^\bullet$. Para mostrar a sobrejetividade, temos que mostrar que qualquer $\alpha \in \text{Br}_l(F)$ tem a forma (a, b) já que uma preimagem pode ser $\{a, b\} + lK_2F$, mas isso é dado pelo teorema 3.4.4 do capítulo anterior, inclusive nos diz que dados $\alpha_1, \dots, \alpha_r$ em $\text{Br}_l(F)$ todos eles tem uma forma comun, i.e.

$$\alpha_i = (a_i, d)$$

para todo $0 \leq i \leq r$. Isto nos dá a condição (ii) do corolário 4.2.2 para a injetividade de h_1 , agora trabalharemos na primeira condição que diz que dados $(a, b) = (c, d)$ com $a, b, c, d \in F^\bullet$ temos que encontrar $x, y \in F^\bullet$ tais que

$$(a, b) = (x, b) = (x, y) = (c, y) = (c, d). \quad (4.16)$$

Então, seja $\alpha = (a, b) = (c, d)$, seja S o conjunto de primos onde $\alpha_v = \text{res}_v(\alpha)$ é não trivial, tomando $v \in S$, temos que F_v é um corpo local e sabemos por 3.4.4 que $\text{Br}_l(F_v)$ é cíclico e pela proposição 4.2.2 temos que em F_v a condição (i) é cumprida, assim existem $x_v, y_v \in F_v$ tais que

$$(a, b)_v = (x_v, b)_v = (x_v, y_v)_v = (c, y_v)_v = (c, d)_v. \quad (4.17)$$

Pela última igualdade temos que $(c, y_v/d)$ é trivial e logo por 4.2.1 $y_v/d = N_v t_v$ com $t_v \in F_v[c^{1/l}]$. Agora, como é conhecido nos corpos locais temos que $(F_v^\bullet)^l$ é aberto em $F_v^\bullet$, assim existe $\varepsilon > 0$ tal que a bola de raio ε e centro em t_v^l esta contido em $(F_v^\bullet)^l$, como F é denso em F_v tomamos $t \in F[c^{1/l}]$ tal que

$$|t - t_v^{l+1}|_v < \varepsilon |t_v|_v$$

Logo $|t/t_v - t_v^l| < \varepsilon$ e $t/t_v = s_v^l$ com $s_v \in F_v[d^{1/l}]$. Então escolhemos $y = dNt$, onde N é a norma da extensão $F[c^{1/l}]/F$ (c não pode ser raiz l -ésima em F_v pois α_v é não trivial), assim

$$(c, y) = (c, dNt) = (c, d) + (c, Nt) = (c, d) \quad (4.18)$$

e

$$(c, y)_v = (c, dNt)_v = (c, y_v N_v t_v^{-1} N_v t)_v = (c, y_v)_v + (c, N_v(t/t_v)) = (c, y_v)_v + (c, N_v s_v^l)_v = (c, y_v)_v \quad (4.19)$$

para $v \in S$. Então reemplazando 4.19 em 4.17 temos que x_v é solução local da equação

$$(x, b) = (x, y) = \alpha$$

nos primos $v \in S$ e se para $v \notin S$ colocamos a solução trivial $x_v = 1$ temos solução local para todos os primos. O lema abaixo (lema 5.2 em (TATE, 1976)) nos diz que existe uma solução global da equação acima, o que conclui o teorema. $\square$

Lema 4.3.1. Sejam $\alpha_1, \dots, \alpha_r \in \text{Br}_l(F)$ e sejam $a_1, \dots, a_r \in F^\bullet$. Se para cada primo v de F existe $x_v \in F_v^\bullet$ tal que $(a_i, x_v) = (\alpha_i)_v = \text{res}_v(\alpha_i)$ para cada i , então existe $x \in F^\bullet$ tal que $(a_i, x) = \alpha_i$ para cada i .

Seja v um primo não arquimediano de F , como na observação 3.4.3 definimos os conjuntos

$$A_v = \{a \in F \mid |a| \leq 1, |\cdot| \in v\} \quad \mathfrak{m}_v = \{a \in F \mid |a| < 1, |\cdot| \in v\} \quad k(v) = A_v / \mathfrak{m}_v$$

mas o último conjunto $k(v)$ é chamado *corpo residual* de F , é conhecido para os corpos globais que $k(v)$ sempre é finito.

Seja agora S um conjunto finito de primos de F que inclui os arquimedianos. O conjunto dos $x \in F$ tais que $|x| \leq 1$ para os representantes dos $v \notin S$ (a desigualdade é a mesma para os equivalentes segun a proposição 3.4.2) é denotado por O_S e é chamado conjunto de S -inteiro em F . Seja $d_v : K_2 F \rightarrow k(v)^\bullet$ o *tame symbol* em v (definido no lema 11.5 de (MILNOR, 1972)). Como $k(v)$ é um corpo finito, então $k(v)^\bullet$ é um grupo cíclico finito, fazendo a soma direta e juntando todos os d_v com $v \notin S$ com a propriedade universal temos o mapa d^S

$$K_2 F \xrightarrow{d^S} \bigoplus_{v \notin S} k(v)^\bullet$$

que por um teorema debido a C. Moore (MOORE, 1968) é sobrejetivo, agora pelo morfismo dado pela inclusão $O_S \subset F$ podemos criar o diagrama

$$K_2 O_S \longrightarrow K_2 F \xrightarrow{d^S} \bigoplus_{v \notin S} k(v)^\bullet \longrightarrow 0$$

Bass em (BASS, 1969) mostrou que $\ker(d^S)$ é a imagem de $K_2 O_S$, logo o diagrama é exato. Garland em (GARLAND, 1971) usando isso mostrou a finitude de $\ker(d^S)$ no caso dos corpos numéricos, u outro caso foi resuelto por Bass e Tate em (BASS; TATE, 1973), eles mostraron que $\ker(d^S)$ é finito e de ordem coprimo com sua característica. Finalmente Quillen em (QUILLEN, 1973) depois mostrou que de fato $\ker(d^S) \simeq K_2 O_S$, com isso último temos a sequência exata

$$0 \longrightarrow K_2 O_S \longrightarrow K_2 F \xrightarrow{d^S} \bigoplus_{v \notin S} k(v)^\bullet \longrightarrow 0 \quad (4.20)$$

Aqui nós só precisamos a finitude de $\ker(d^S)$, a sequência 4.20 nos diz que K_2F é uma extensão de uma soma direta de grupos cíclicos finitos por um grupo finito e o lema 4.3.2 abaixo nos diz que K_2F é um subgrupo de torção sem subgrupos divisíveis não triviais. O lema 4.3.3 abaixo nos diz que $K_2F\{l\}$ não pode ter subgrupos l -divisíveis. O último lema 4.3.4 abaixo com a proposição 1.2.1 nos diz que $H^2(F, \mathbf{Z}_l(2))$ só pode ter l -torção. Por tanto, somando tudo do acima com o teorema 4.3.1 e o corolário 4.2.1 (olha a observação 4.2.2) hemos probado o teorema.

Teorema 4.3.2. Para um corpo global F o mapa h do teorema 4.1.1 induz um isomorfismo da parte l -primária de K_2F e o subgrupo de torção de $H^2(F, \mathbf{Z}_l(2))$.

Dito de outro modo, como sabemos que se a característica de F é $p > 0$, então K_2F não tem p -torção (teorema 6.7 em (WEIBEL, 2013)) e que K_2F é a soma direta de suas partes l -primárias então

$$K_2F = \bigoplus_{l:\text{primo}, l \neq \text{char}(F)} H^2(F, \mathbf{Z}_l(2))$$

Lema 4.3.2. Considere a seguinte sequência exata

$$0 \longrightarrow F \longrightarrow A \xrightarrow{\pi} \bigoplus_{\lambda \in I} C_\lambda \longrightarrow 0$$

Onde F é um grupo finito de ordem $|F|$, I é um conjunto arbitrário de índices e C_λ é cíclico de ordem $|C_\lambda|$. Então A é um grupo de torção sem nenhum subgrupo divisível.

Demonstração. Seja $C_\lambda = \langle \omega_\lambda \rangle$ para todo $\lambda \in I$. Seja $D \subset A$ um subgrupo divisível e seja $x \in D$, logo $\pi(x) = \sum_{\lambda \in S} a_\lambda \omega_\lambda$ com $S \subset I$ finito e $a_\lambda \neq 0$. Considere agora

$$n = \prod_{\lambda \in S} |C_\lambda|$$

Como a imagem de um conjunto divisível é também divisível, temos que $\pi(x) = ny$ com

$$y = \sum_{\lambda \in S'} b_\lambda \omega_\lambda$$

com $S' \subset I$ finito e $b_\lambda \neq 0$. Agora, afirmo que $S \cap S' = \emptyset$ já que se $\lambda \in S \cap S'$ então quando se multiplica com n na equação $\pi(x) = ny$ temos na esquerda uma componente $a_\lambda \neq 0$ mas na direita temos a componente de λ igual a 0. Assim temos que a representação de $\pi(x) - ny$ tem todos os subíndices diferentes, por tanto todas as componentes são zeros e $\pi(x) = 0$.

Assim $x \in F$ e como x foi arbitrário, temos que $D \subset F$, mas isso é impossível pois se temos $y \in D$, então $y = |F|z = 0$ e por tanto $D = 0$.

Agora veamos que é de torção, seja $x \in A$, então $\pi(x)$ é de torção pois se

$$\pi(x) = \sum_{\lambda \in S} a_\lambda \omega_\lambda$$

com $S \subset I$ finito, logo se $n = \prod_{\lambda \in S} |C_\lambda|$ então $\pi(nx) = n\pi(x) = 0$. Assim $nx \in F$ e logo $|F|nx = 0$. Por tanto $x \in A$ é de torção. $\square$

Lema 4.3.3. Seja A um grupo sem grupos divisíveis não nulos, então se l é primo $A\{l\}$ não tem subgrupos l -divisíveis.

Demonstração. Suponha que $D \subset A\{l\}$ é um subgrupo l -divisível, vamos a mostrar que D é divisível.

1. *n é coprimo com l :* Seja n coprimo com l , logo é coprimo com qualquer potência de l , seja $x \in D$ e como $D \subset A\{l\}$ então a ordem de x é uma potência de l (não é difícil, usar o teorema de Bezout), agora se $o(x) = l^r$ então como $(n, l^r) = 1$ então existem $r, s \in \mathbf{Z}$ tais que $nr + sl^r = 1$, então $x = (nr + l^r s)x = nrx$. Assim D é n -divisível para todo n coprimo com l .
2. *Caso geral:* Seja n inteiro, logo $n = l^r s$ com s coprimo com l e $r \geq 1$, então $x = sy$ com $y \in D$ mas D é l -divisível, logo $y = l^r z$ com $z \in D$ e finalmente $x = l^r sz = nz$ e D é divisível.

$\square$

Lema 4.3.4. Se um grupo abeliano A e l primo, se A não pode ter subgrupos l -divisíveis então não pode ter n -torção com $(n, l) = 1$.

Demonstração. Seja A_n o subgrupo de n -torção de A , seja $x \in A_n$, então $nr + ls = 1$, logo

$$x = nrx + lsx = lsx$$

assim A_n é l -divisível, logo $A_n = 0$. $\square$

REFERÊNCIAS

ATIYAH, M. F.; MACDONALD, I. G. **Introduction to commutative algebra**. economy. [S.l.]: Westview Press, Boulder, CO, 2016. ix+128 p. (Addison-Wesley Series in Mathematics). For the 1969 original see [MR0242802]. ISBN 978-0-8133-5018-9; 0-201-00361-9; 0-201-40751-5. Citado nas páginas 21 e 22.

BASS, H. **K_2 of global fields**. AMS taped lecture, Cambridge, Mass., Oct. 1969. 1969. Citado na página 70.

BASS, H.; TATE, J. The Milnor ring of a global field. Springer, Berlin, p. 349–446. Lecture Notes in Math., Vol. 342, 1973. Citado nas páginas 34 e 70.

BROWN, K. S. **Cohomology of Groups**. 1st edition. ed. [S.l.]: Springer-Verlag New York 1982, 1982. (Graduate Texts in Mathematics). ISBN 978-1-4684-9329-0. Citado na página 60.

FUCHS, L. **Abelian Groups**. Springer International Publishing, 2015. Disponível em: <<https://doi.org/10.1007/978-3-319-19422-6>>. Citado na página 63.

GARLAND, H. A finiteness theorem for K_2 of a number field. **Annals of Mathematics**, Annals of Mathematics, v. 94, n. 3, p. 534–548, 1971. ISSN 0003486X. Disponível em: <<http://www.jstor.org/stable/1970769>>. Citado na página 70.

GILLE, P.; SZAMUELY, T. **Central simple algebras and Galois cohomology**. [S.l.]: Cambridge University Press, Cambridge, 2017. v. 165. xi+417 p. (Cambridge Studies in Advanced Mathematics, v. 165). Second edition of [MR2266528]. ISBN 978-1-316-60988-0; 978-1-107-15637-1. Citado na página 39.

MILNE, J. **Class Field Theory**. 2013. Disponível em: <<http://www.jmilne.org/math/CourseNotes/CFT.pdf>>. Acesso em: 01/03/2018. Citado nas páginas 17, 18, 38, 43, 44 e 53.

_____. **Algebraic Number Theory**. 2017. Disponível em: <<http://www.jmilne.org/math/CourseNotes/ANT.pdf>>. Acesso em: 01/03/2018. Citado nas páginas 36, 47, 49 e 50.

MILNOR, J. **Introduction to Algebraic K-Theory**. (AM-72). 1972. Citado nas páginas 27, 30, 32, 33, 39, 41 e 70.

MOORE, C. Group extensions of p -adic and adelic linear groups. **Institut des Hautes Études Scientifiques. Publications Mathématiques**, n. 35, p. 157–222, 1968. ISSN 0073-8301. Citado na página 70.

QUILLEN, D. **Higher algebraic K-theory: I**. 1973. 85-147 p. Citado na página 71.

TATE, J. Relations between K_2 and Galois Cohomology. **Inventiones mathematicae**, v. 36, p. 257–274, 1976. Disponível em: <<http://eudml.org/doc/142421>>. Citado na página 70.

TENGAN, E. **Central Simple Algebras an the Brauer Group**. 2009. Disponível em: https://www.ime.usp.br/~xviiiicla/pdf_files/cft.pdf. Acesso em: 01/02/2019. Citado nas páginas 39, 42, 43, 44, 51 e 52.

WEIBEL, C. A. **An introduction to homological algebra**. [S.l.]: Cambridge University Press, Cambridge, 1994. v. 38. xiv+450 p. (Cambridge Studies in Advanced Mathematics, v. 38). ISBN 0-521-43500-5; 0-521-55987-1. Citado na página 23.

_____. **The K-book**. [S.l.]: American Mathematical Society, Providence, RI, 2013. v. 145. xii+618 p. (Graduate Studies in Mathematics, v. 145). An introduction to algebraic K -theory. ISBN 978-0-8218-9132-2. Citado nas páginas 64 e 71.

WEIL, A. **Basic number theory**. [S.l.]: Springer, 1995. (Classics in mathematics). ISBN 9783540586555. Citado na página 49.

WEISS, E. **Cohomology of groups**. [S.l.]: Academic Press, New York-London, 1969. x+274 p. (Pure and Applied Mathematics, Vol. 34). Citado na página 20.