Universidade Federal do Amazonas

Instituto de Ciências Exatas

Programa de Pós–Graduação em Matemática

Mestrado em Matemática

O teorema de Brauer sobre o índice e o período de álgebras simples centrais

Eduardo Bruno Lima Pedrozo

Manaus – AM
Setembro de 2017

Universidade Federal do Amazonas

Instituto de Ciências Exatas

Programa de Pós–Graduação em Matemática

Mestrado em Matemática

O teorema de Brauer sobre o índice e o período de álgebras simples centrais

por

Eduardo Bruno Lima Pedrozo

sob a orientação do

Prof. Dr. Wilhelm Alexander Cardoso Steinmetz

Orientador

Manaus – AM
Setembro de 2017

O teorema de Brauer sobre o índice e o período de álgebras simples centrais

por

Eduardo Bruno Lima Pedrozo

Dissertação apresentada ao Corpo Docente do Programa de Pós–Graduação em Matemática da Universidade Federal do Amazonas como requisitos necessários para a obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada em 1 de setembro de 2017.

Banca Examinadora:

SLA.

Prof. Dr. Wilhelm Alexander Cardoso Steinmetz – (Orientador)
Universidade Federal do Amazonas - UFAM

Germán Benitez Monsalve.

Prof. Dr. Germán Alonso Benitez Monsalve – (Membro Interno)
Universidade Federal do Amazonas - UFAM

Prof. Dr. Oscar Francisco Márquez Sosa – (Membro Externo)
Universidade Federal de Santa Maria - UFSM

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Pedrozo, Eduardo Bruno Lima

P372t O Teorema de Brauer sobre o índice e o período de álgebras simples centrais / Eduardo Bruno Lima Pedrozo. 2017

66 f.: il.; 31 cm.

Orientador: Wilhelm Alexander Cardoso Steinmetz

Dissertação (Mestrado em Matemática Pura e Aplicada) - Universidade Federal do Amazonas.

1. Algebras Simples Centrais. 2. Grupo de Brauer. 3. Cohomologia galoisiana. 4. Índice. 5. Período. I. Steinmetz, Wilhelm Alexander Cardoso II. Universidade Federal do Amazonas III. Título

"Mas é preciso você tentar, talvez alguma coisa muito nova possa lhe acontecer"(Raul Seixas).

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado a capacidade suficiente para conseguir a realização deste trabalho.

Agradeço aos meus pais Arnoldo e Marta por toda dedicação e paciência para que tiveram comigo (não foi fácil!), aos meus irmãos Alex, Aline e Ariane que cresceram comigo e desfrutaram também da mesma educação que obtive, ao meu sobrinho Ismael e ao meu filho Carlos Eduardo.

A minha esposa Ivanize pela sua fundamental importância dentro da minha vida, fazendo-me amadurecer, fazendo-me enxergar e tentar corrigir os meus defeitos e com isso tornando-me alguém melhor.

Ao colegas de trabalho do Instituto de Saúde e Biotecnologia de Coari - ISB, em particular aos professores Deniz Mota, Fábio Junior, Ricardo Augusto, Adriano Guilherme, Jéferson Ferreira, Charles Falcão, Mestre Ademar Vieira, Tiago Gonçalves e professor Élder.

Ao professor Domingos Anselmo por tudo que fez por mim, pelas grandes oportunidades que me destes e por sempre ter acreditado em mim, por ter sido o grande mestre que me ensinou muito além dos teoremas.

A todos os meus professores que lecionaram nas disciplinas deste mestrado e no nivelamento, professores: Flávia Morgana, Roberto Cristóvão, Stefan Ehbauer, Dmitry Logachev, Inês Padilha, Maria Rosilene, Alfredo Wagner, Nikos Georgiou e José Nazareno.

Aos colegas da minha turma de mestrado por tantos momentos de dedicação e estudos para enfim chegarmos na conclusão do mesmo.

Agradecer ao meu orientador professor Alexander por ter tido bastante paciência comigo, por ter me inserido numa área tão interessante e com muitas aplicações bonitas.

Agradeço também a todos aqueles que de forma direta ou indireta me ajudaram a chegar até aqui.

RESUMO

O TEOREMA DE BRAUER SOBRE O ÍNDICE E O PERÍODO DE ÁLGEBRAS SIMPLES CENTRAIS

Neste trabalho provamos um teorema de Richard Brauer sobre o índice e o período de álgebras simples centrais. Uma álgebra simples central é uma álgebra de dimensão finita sobre um corpo que se torna isomorfa a uma álgebra de matrizes após extensão de escalares a uma extensão finita de corpos. O teorema de Wedderburn nos permite definir um invariante de uma tal álgebra, dito o índice e o grupo de Brauer fornece uma classificação destas álgebras sobre um corpo dado. O período de uma álgebra simples central é a ordem da sua classe no grupo de Brauer. O teorema de Brauer de 1929 mostra que o período de uma álgebra simples central sempre divide o seu índice, que é o resultado principal deste trabalho. Este teorema permite compreender melhor a estrutura destas álgebras. A nossa prova é baseada em técnicas da cohomologia galoisiana.

Palavras-chave: Álgebras Simples Centrais, Grupo de Brauer, Cohomologia Galoisiana, Índice, Período.

ABSTRACT

BRAUER'S THEOREM ON THE INDEX AND THE PERIOD OF A CENTRAL SIMPLE ALGEBRA

In this work we will prove a theorem of Richard Brauer on the index and the period of central simple algebras. A central simple algebra is a finite-dimensional algebra over a field that becomes isomorphic to a matrix algebra after extending scalars to a finite field extension. Wedderburn's theorem allows us define an invariant of such an algebra, called the index and the Brauer group provides a classification of central simple algebras over a given field. The period of a central simple algebra is the order of its class in the Brauer group. Brauer's theorem of 1929 shows that the period of a central simple algebra always divides its index, which is the main result of this work. Our proof is based on techniques from Galois cohomology.

Keywords: Central Simple Algebras, Brauer Group, Galois Cohomology, Index, Period.

Sumário

Capítulo 1

Introdução

Este trabalho tem como foco principal o teorema de Richard Brauer sobre o índice e o período de álgebras simples centrais, as quais são objetos muito estudados em várias áreas da álgebra, da teoria dos números, tendo também aplicações na matemática aplicada, por exemplo na teoria de códigos e da comunicação. Historicamente a primeira álgebra simples central não-comutativa de dimensão finita sobre um corpo descoberta foi a álgebra dos quatérnions de Hamilton. Uma álgebra simples central generaliza várias propriedades da álgebra de quatérnios em dimensões superiores. Uma outra maneira de enxergar as álgebras simples centrais é como álgebras sobre um corpo que ficam isomorfas a uma álgebra de matrizes após extensão dos escalares a uma extensão finita de corpos.

O capítulo 1 é dedicado ao desenvolvimento da teoria das álgebras simples centrais e ao grupo de Brauer, que foi introduzido por Richard Brauer no ano de 1929 e que fornece uma classificação de álgebra centrais simples sobre um corpo. O período por sua vez é simplesmente a ordem da classe de uma álgebra simples central no grupo de Brauer. O índice de uma álgebra simples central é calculado da seguinte maneira: Pelo teorema de Wedderburn, para toda álgebra simples central A sobre k, existe uma única (a menos de isomorfismo) k-álgebra de divisão D, tal que $A \cong M_n(D)$ - o índice de A então é o grau de D, ou seja, a raiz quadrada (que é sempre inteira, como veremos) da dimensão de D como k-álgebra.

A questão naturalmente surge se o índice é suficiente para determinar a classe de uma certa álgebra simples central no grupo de Brauer. Richard Brauer provou em 1929 [1], que período de uma álgebra simples central sempre divide o seu índice. Este é o teorema principal deste

trabalho. A questão inversa, se o índice divide o período é muito mais delicada e ainda está aberta em geral. Existem alguns resultados parciais.

Para provar o teorema de Brauer usaremos técnicas da teoria da cohomologia galoisiana, que serão exploradas no segundo capítulo. Esta teoria foi desenvolvida nos anos 1950 por John Tate e Jean-Pierre Serre entre outros. No capítulo 3, veremos que as álgebras simples centrais definem classes em conjuntos de cohomologia galoisiana. Será também identificado o grupo de Brauer com um grupo de cohomologia desta teoria. Estas identificações deixam alguns argumentos mais fáceis, por exemplo a prova que o grupo de Brauer é de torção, graças às propriedades funtoriais da cohomologia galoisiana.

Capítulo 2

Álgebras Simples Centrais

Neste capítulo introduzimos a noção de álgebra simples central, principal objeto deste trabalho. Provaremos algumas propriedades básicas, assim como uma caracterização destas álgebras em termos de extensões galoisianas de corpos. Definiremos também as noções de índice e o período de uma álgebra simples central e o grupo de Brauer que classifica estas álgebras sobre um corpo dado. As referências principais para este capitulo são [3] e [6].

2.1 Convenções e Conceitos Básicos

Nesta primeira seção deste capitulo iremos lembrar alguns conceitos sobre **álgebras de dimensão finita** e estabeleceremos algumas convenções para o nosso trabalho:

Definição 2.1.1. *Dizemos que um conjunto $A \neq \emptyset$ é uma* ***k-álgebra*** *quando for um k-espaço vetorial e munido de uma multiplicação $(a, b) \longmapsto a \cdot b$ para todos $a, b \in A$ que satisfaz as seguintes propriedades:*

1) *Para todos $a, b, c \in A$ temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*

2) *Para todos $a, b, c \in A$ temos $(a + b) \cdot c = a \cdot c + b \cdot c$ e $a \cdot (b + c) = a \cdot b + a \cdot c$*

3) *Para todos $a, b \in A$ e $\lambda \in k$ temos que $\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$*

Quando para todo elemento $a \in A$ existir um elemento $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$, dizemos que A é uma k-álgebra **com unidade**. Se para todos $a, b \in A$ tivermos que $a \cdot b = b \cdot a$, então A é dita uma k-álgebra **comutativa**. Quando A satisfaz estas duas propriedades agora

acima mencionadas dizemos que A é uma k-álgebra **comutativa com unidade**.
Uma k**-subálgebra** B de uma k-álgebra A, é um k-subespaço vetorial $B \leq A$, que é fechado para a operação da multiplicação. Se A é com unidade, B precisa conter a unidade também.

Definição 2.1.2. *Sejam A e B duas k-álgebras e $f : A \longrightarrow B$ uma aplicação entre elas, dizemos que f é um k-**homomorfismo de álgebras** quando:*
1) $f(1) = 1$.
2) *f for uma transformação linear.*
3) *Para todos $a, b \in A$ temos que $f(a \cdot b) = f(a) \cdot f(b)$.*

Se tivermos para todos $a, b \in A$ que $f(a \cdot b) = f(b) \cdot f(a)$, diremos que f é um **anti-homomorfismo de k-álgebras**.
Sejam A e B duas k-álgebras dizemos que elas são **equivalentes** quando existir um isomorfismo entre elas, ou seja, $A \cong B$. Quando existir um k-anti-isomorfismo entre elas dizemos que são **recíprocas**.
Temos alguns exemplos de k-álgebras, como: os números complexos, os números reais, o espaço das transformações lineares, e a álgebra dos quatérnios ao qual estudaremos com mais detalhes à frente neste nosso texto.
Seja I um subconjunto não vazio de A, dizemos que I será um **ideal à esquerda de** A se for um k-subespaço vetorial de A e invariante em relação à multiplicação à esquerda por elementos de A ($ab \in I$ para todo $a \in A$ e $b \in I$), de modo análogo define-se **ideal à direita**. Quando o ideal for à direita e a esquerda simultaneamente chamamos de **ideal bilateral**.

Chamamos uma k-álgebra D de **álgebra com divisão** quando todo elemento $x \in D$, não nulo possui inverso. Se A é um módulo à esquerda (à direita) sobre D, então dizemos que A é um D-**espaço vetorial à esquerda (à direita)**.
Sejam A e B duas k-álgebras. Seja $A \otimes_k B$ o produto tensorial entre A e B como espaços vetoriais sobre k. Definimos uma multiplicação sobre $A \otimes_k B$ da seguinte forma

$$(a_1 \otimes_k b_1)(a_2 \otimes_k b_2) = a_1 a_2 \otimes_k b_1 b_2.$$

Sejam A, B e C três k-álgebras. Então $(A \otimes_k B) \otimes_k C \cong A \otimes_k (B \otimes_k C)$ e $A \otimes_k B \cong B \otimes_k A$.
Sejam A, A', B e B' quatro k-álgebras e sejam $f : A \longrightarrow A'$ e $g : B \longrightarrow B'$ dois k-

homomorfismos, então a aplicação $f \otimes g : A \otimes_k B \longrightarrow A' \otimes_k B'$ definida pela lei

$$(f \otimes g)(a \otimes_k b) = f(a) \otimes_k g(b),$$

é um homomorfismo.
Finalmente, se B possui unidade, a aplicação $a \longmapsto a \otimes_k 1$ é um homomorfismo injetivo de A em $A \otimes_k B$. Assim, podemos identificar A com $A \otimes_k 1$. De modo análogo, se A possui unidade podemos identificar B com $1 \otimes_k B$.

2.2 Álgebras de quatérnios

A noção de uma álgebra de quatérnios é um dos exemplos mais triviais de uma álgebra simples central. Todos os conceitos (cindimento ou normas reduzidas, que definiremos em seguida de forma mais geral) podem ser definidos para álgebra de quatérnios de forma mais elementar. Além disso, historicamente o primeiro exemplo de uma álgebra de dimensão finita sobre um corpo foi a álgebra dos quatérnios sobre $\mathbb{R}$, descoberta por Hamilton em 1843 e definida da seguinte forma:

Definição 2.2.1. *A **álgebra dos quatérnios de Hamilton** $\mathbb{H}$ é o espaço vetorial real de dimensão 4 de base $\{1, i, j, k\}$, munido das relações $i^2 = -1$, $j^2 = -1$ e $ij = -ji = k$. Um elemento desta álgebra é dito um **quatérnio de Hamilton**.*

Cada quatérnio de Hamilton se escreve da forma $q = x + yi + zj + wk$, onde $x, y, z, w \in \mathbb{R}$. O conjugado de um quatérnio de Hamilton q é $\bar{q} := x - yi - zj - wk$ e a sua norma é dada por $N(q) := q.\bar{q} = x^2 + y^2 + z^2 + w^2$ respectivamente. Se $q \neq 0$, q possui um inverso, dado pela fórmula $q^{-1} = \dfrac{\bar{q}}{N(q)}$, assim vemos que os quatérnios de Hamilton formam uma álgebra com divisão. Podemos generalizar o conceito de uma álgebra de quatérnios sobre um corpo qualquer. Como esta seção é meramente ilustrativa e introdutória, nos limitamos aqui nesta seção a partir de agora a um corpo k de característica diferente de 2.

Definição 2.2.2. *Sejam $a, b \in k^\times$. Definimos a **álgebra de quatérnios** (generalizada) (a, b), como sendo o espaço vetorial sobre k de dimensão 4 de base $\{1, i, j, ij\}$, com as relações*

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

Observação 2.2.1. *Toda álgebra de quatérnios é determinada unicamente por a e b, a menos de multiplicação de a ou b por um quadrado de k.*

Definição 2.2.3. *Seja $q = x + yi + zj + wij$ um elemento da álgebra (a, b), podemos assim definir o* ***conjugado*** *de q por*

$$\overline{q} = x - yi - zj - wij$$

e sua ***norma*** *como sendo:*

$$N(q) = q \cdot \overline{q} = x^2 - ay^2 - bz^2 + abw^2.$$

A aplicação $(a, b) \longrightarrow (a, b)$ definida por $q \longmapsto \overline{q}$ é um anti-homomorfismo da k-álgebra (a, b) e temos que $\overline{\overline{q}} = q$ para quaisquer $q \in (a, b)$. A norma define uma aplicação dada por $N : (a, b) \longrightarrow k$ e assim obtemos o seguinte resultado:

Proposição 2.2.1. *O quatérnio q é inversível quando $N(q)$ for diferente de zero. Daí (a, b) é uma k-álgebra com divisão quando $N(q) = 0 \Rightarrow q = 0$.*

Na verdade, é possível se dar uma definição intrínseca da conjugação (que serve também na norma) em uma álgebra de quatérnios (a, b), que não depende da escolha da base $(1, i, j, ij)$. Chamaremos o elemento $q \in (a, b)$ de um **quatérnio puro** se $q^2 \in k$ mas q não pertence a k e um simples cálculo nos mostra que o quatérnio $q = x + yi + zj + wij \neq 0$ é puro se, e somente se $x = 0$, podendo assim escrever $q = q_1 + q_2$ de forma única com $q_1 \in k$ e q_2 puro, e temos também que seu conjugado será dado por $\overline{q} = q_1 - q_2$. Além disso, um quatérnio q quando puro satisfaz $N(q) = -q^2$.

Observação 2.2.2. *Se $k = \mathbb{R}$, a norma definida acima não é uma norma no sentido usual. Se $\lambda \in \mathbb{R}$ e $q \in (a, b)$, nós não temos $N(\lambda \cdot q) = \lambda \cdot N(q)$, porém temos que $N(\lambda \cdot q) = \lambda^2 \cdot N(q)$.*

Exemplo 2.2.1. *A k-álgebra de matrizes $M_2(k)$.*
A k-álgebra de matrizes $M_2(k)$ é também uma álgebra de quatérnios. Seja $b \in k^\times$.
Definimos:

$$I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ e } J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}.$$

Logo, as matrizes

$$id=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ I=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ J=\begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} \text{ e } IJ=\begin{bmatrix} 0 & b \\ -1 & 0 \end{bmatrix},$$

formam uma base de $M_2(k)$ como k-espaço vetorial de dimensão 4. Além disso temos:

$$I^2 = id\ ,\ J^2 = b \cdot id \text{ e } IJ = -JI.$$

Logo, $M_2(k)$ pode ser vista como uma k-álgebra de quatérnios $(1, b)$, ao identificar $k^\times$ com o centro de $M_2(k)$.

Definição 2.2.4. *Uma k-álgebra de quatérnios é dita **cindida** quando ela é isomorfa a $M_2(k)$, isto é, $(a, b) \cong M_2(k)$.*

Vamos agora dar uma caracterização de álgebras de quatérnios sobre k.

Proposição 2.2.2. *Para a álgebra dos quatérnios (a, b) as seguintes afirmações são equivalentes:*

1. A álgebra (a, b) é cindida.

2. A álgebra (a, b) não é uma álgebra com divisão.

Demonstração. Se (a, b) é cindida, $(a, b) \cong M_2(k)$, logo basta tomarmos uma matriz de $M_2(k)$ que não seja invertível para ver que não é uma álgebra com divisão. Para a implicação inversa veja [6] proposição 1.1.7. ■

Lembramos a definição do centro de uma álgebra:

Definição 2.2.5. *Para A uma k-álgebra o conjunto $Z(A) = \{x \in A |\, x \cdot a = a \cdot x; \forall a \in A\}$ é chamado o **centro** de A. Este conjunto é uma k-subálgebra de A.*

Lema 2.2.1. *Seja D uma k-álgebra tal que:*

(i) D é de dimensão 4 como k-espaço vetorial.

(ii) O centro de D é igual a k.

(iii) D contém uma k-álgebra comutativa A, tal que $A \cong k[\sqrt{a}]$, onde $k[\sqrt{a}]$ é uma extensão de corpos quadrática não trivial de k.

Então $D \cong (a, b)$ para algum $b \in k^\times$.

Demonstração. Seja A uma tal k-subálgebra de D. Como $A \cong k(\sqrt{a})$, então existe $q \in D\backslash k$ tal que $q^2 = a \in k$. Por hipótese, temos que q não pertence ao centro k de D. O automorfismo interno $\Phi : D \longrightarrow D$ tal que $x = q^{-1}xq$ é exatamente de ordem 2, pois fazendo a composição $\Phi \circ \Phi : D \longrightarrow D$ temos $x \longmapsto q^{-1} \cdot (q^{-1}xq) \cdot q = (q)^{-2}xq^2 = x$ e como $q^2 \in k = Z(D)$, temos $\Phi \circ \Phi = id_D$. Este k-automorfismo possui então -1 como um de seus valores próprios, assim, existe um $r \in D$ com $qr + rq = 0$. Observamos que q e qr anticomutam, pois $qqr = -qrq$. Um cálculo simples mostra que $1, r, q, qr$ são linearmente independentes. O automorfismo $x \longmapsto r^{-2}xr^2$ deixa os quatro elementos $1, r, q, rq$ fixos. Assim r^2 pertence ao centro de D que é igual a k, por hipótese. Pondo $r^2 = b \in k^\times$, podemos verificar que $D \cong (a, b)$. ■

Temos o seguinte resultado:

Proposição 2.2.3. *Toda k-álgebra com divisão D, de centro $k^\times$ e de dimensão 4 é isomorfa a alguma álgebra de quatérnios.*

Demonstração. Seja $d \in D\backslash k$, e como D é de dimensão finita sobre k, temos que $\{1, d, d^2, ...\}$ são linearmente dependentes, logo temos que D é algébrico sobre k existindo assim um polinômio $f \in k[x]$ com $f(d) = 0$, isto é d é algébrico sobre k. Como D é uma álgebra com divisão, não há divisores de zero, então podemos supor f irredutível, isto significa que o homomorfismo $k[x]/(f) \to D$, $p(x) \mapsto p(d)$ é um homomorfismos de k-álgebras que faz o corpo $k(d)$ ser uma k-subálgebra de D. Observando que o grau de $[k(d) : k]$ não pode ser 1 pois $d \notin k$ e também não pode ser 4 pois D é não comutativa, logo temos que $[k(d) : k] = 2$ e $k(d)$ é uma extensão quadrática, assim pelo lema anterior, temos que $D \cong (a, b)$. ■

2.3 Álgebras Simples Centrais

Nesta seção definiremos a noção de álgebra simples central que pode ser visto como generalização de álgebra de quatérnio para dimensões superiores. Primeiro mostraremos que toda álgebra simples central é isomorfa a uma álgebra de matrizes sobre uma álgebra com divisão D através do teorema de Wedderburn. Em seguida mostraremos que uma k-álgebra é simples central se ela virar isomorfa a uma álgebra de matrizes depois de uma extensão de escalares a uma extensão galoisiana de k. Em parte seguimos de perto [6, Chap. 2], mas para fins de exaustividade retomamos a teoria detalhadamente.

Definição 2.3.1. *Uma k-álgebra A é dita* ***simples*** *quando seus únicos ideais bilaterais são os triviais, ou seja,* 0 *e A.*

Definição 2.3.2. *Uma k-álgebra A é dita* ***central*** *quando seu centro for igual ao corpo k, ou seja,* $Z(A) = k$*, e esta é dita* ***simples central*** *quando A for simples.*

Exemplo 2.3.1. *Uma k-álgebra com divisão D é claramente uma álgebra simples. Seu centro* $Z(D)$ *é um corpo. Seja* $x \in Z(D)^{\times}$*, logo para todo* $y \in D^{\times}$*, nós temos* $xy = yx$*. Invertendo esta relação temos que* $y^{-1}x^{-1} = x^{-1}y^{-1}$*. Logo* $x^{-1} \in Z(D)^{\times}$*. Daí D é uma álgebra simples central sobre* $Z(D)$*.*

Lema 2.3.1. *Se D uma k-álgebra com divisão, então o anel* $M_n(D)$ *é simples central sobre* $Z(D)$*, para* $n \geq 1$*.*

Demonstração. Provaremos esta afirmação mostrando que o ideal bilateral $< M >$ de $M_n(D)$, onde $< M >$ é gerado por uma matriz não nula, é o próprio $M_n(D)$. Para isso, vamos considerar as matrizes E_{ij} que tem 1 na sua ij-ésima posição e 0 nas demais posições. Como todo elemento de $M_n(D)$ pode ser escrito de forma única como combinação D-linear desses E_{ij}, é suficiente mostrar que a matriz $E_{ij} \in < M >$ para quaisquer i, j. Nós temos a seguinte relação $E_{ki} \cdot E_{ij} \cdot E_{jl} = E_{kl}$ para quaisquer índices i, j, k, l, assim é suficiente mostrar que um dos E_{ij} esteja em $< M >$. Pois então todos os outros estarão em $< M >$ também. Vamos escolher i, j tais que a ij-ésima posição de M não seja zero e seja α o escalar não-nulo nesta posição, então a relação, $\alpha^{-1}E_{ii}ME_{jj} = E_{ij}$, nos garante que $E_{ij} \in < M >$, portanto $< M >= M_n(D)$. O centro de $M_n(D)$ são as matrizes escalares que tem elementos de $Z(D)$ na diagonal e podemos concluir que a álgebra $M_n(D)$ é então simples central sobre $Z(D)$. ■

Como preparação para o Teorema de Wedderburn iremos recordar alguns fatos da teoria de módulos e também enunciar e demonstrar dois lemas importantes.

Definição 2.3.3. *Um A-módulo à esquerda* $M \neq 0$ *é* ***simples*** *quando o mesmo possui apenas* 0 *e M como A-submódulos à esquerda.*

Observação 2.3.1. *Seja D uma k-álgebra com divisão. Observamos que a D-álgebra* $M_n(D)$ *(*$n \in \mathbb{N}$*) é simples como D-álgebra, mas não é simples como D-espaço vetorial à esquerda. Logo, se A é uma k-álgebra, uma A-álgebra simples não é necessariamente simples como A-módulo.*

Observação 2.3.2. *Seja A um anel e M um módulo à esquerda sobre este anel, então $End_A(M)$ é um anel. Sua soma é definida por $(\varphi+\psi)(m)=\varphi(m)+\psi(m)$ para todo $m \in M$ e seu produto é a composição de funções usual e se A for uma k-álgebra teremos que $End_A(M)$ será uma álgebra também. Quando A é uma k-álgebra com divisão, então M é um espaço vetorial à esquerda sobre A, logo $End_A(M) \cong M_n(A)$, onde n é a dimensão de M sobre A. Assim temos que M se torna um $End_A(M)$-módulo à esquerda com a multiplicação definida por $\varphi \cdot x = \varphi(x)$ para todo $\varphi \in End_A(M)$ e $x \in M$.*

Lema 2.3.2. *(Lema de Schur)*
Se M uma A-módulo simples sobre uma k-álgebra A, então $End_A(M)$ é uma álgebra com divisão.

Demonstração. Para mostrar que $End_A(M)$ é uma k-álgebra de divisão precisamos mostrar que todo $0 \neq f \in End_A(M)$ possui inverso.
Seja então $f : M \to M$ um elemento de $End_A(M)$, $f \neq 0$, logo $\ker f \neq M$ e $Imf \neq 0$. Ora M é simples e núcleo e a imagem são submódulos de M, assim o $\ker f = \{0\}$ e $Imf = M$, portanto f é inversível. ■

Agora, sejam M um A-módulo à esquerda e $D = End_A(M)$ o anel de endomorfismos. Pela observação 2.3.2, temos que M é naturalmente um D-módulo à esquerda, consideremos então o anel de endomorfismos $End_D(M)$. Logo podemos definir a aplicação

$$\begin{aligned} \lambda_M : A &\longrightarrow End_D(M) \\ a &\longmapsto (\phi_a : M \longrightarrow M) \\ & \qquad x \longmapsto a \cdot x. \end{aligned}$$

Esta aplicação é bem-definida, pois ϕ_a é um D-homomorfismo de anéis: Com efeito seja $x \in M$ então $\phi \cdot ax = \phi(ax) = a \cdot \phi(x) = a\phi \cdot x$, para todo $x \in M$.

Lema 2.3.3. *(Lema de Rieffel)*
Sejam $L \neq 0$ um ideal à esquerda de uma k-álgebra simples A, e $D = End_A(L)$. Então, $\lambda_L : A \longrightarrow End_D(L)$, definido acima, é um isomorfismo.

Demonstração. O núcleo de λ_L é um ideal bilateral de A, como $\lambda_L \neq 0$ e A é simples o seu núcleo é trivial, portanto λ_L é injetiva.

Para mostrar a sobrejetividade, vamos mostrar primeiro que $\lambda_L(L)$ é um ideal à esquerda de $End_D(L)$. Para $\phi \in End_D(L)$ e $l \in L$, então, temos que $\phi\lambda_L(L)$ é a aplicação que leva $x \to \phi(lx)$, para todo $x \in L$. A aplicação $y \to yx$ é um A-endomorfismos de L, ou seja, um elemento de D, como ϕ é um D-endomorfismo, temos que $\phi(lx) = \phi(l)x$ e assim $\phi\lambda_L(l) = \lambda_L(\phi(l))$.

Como L é um ideal à esquerda, então o ideal LA é um ideal bilateral, logo, $LA = A$, pois A é simples. Em particular temos que $1 = \sum l_i a_i$ com $l_i \in L$, $a_i \in A$. Portanto para $\phi \in End_D(L)$ temos $\phi = \phi \circ id_L = \phi \circ \lambda_L(1) = \phi \circ \lambda_L(\sum l_i a_i) = \sum \phi \circ \lambda_L(l_i) \circ \lambda_L(a_i)$. Como $\lambda_L(L)$ é um ideal à esquerda de $End_A(L)$, logo $\phi \circ \lambda_L(l_i) \in \lambda_L(L)$, então $\phi \circ \lambda_L(l_i) = \lambda_L(l_i')$ para algum $l_i' \in L$. Temos assim que $\phi = \sum \lambda_L(l_i') \circ \lambda_L(a_i) = \sum \lambda_L(l_i' \cdot a_i)$ e $\phi \in \lambda_L(A)$. Logo λ_L é sobrejetiva. ■

Teorema 2.3.1. *(Teorema de Wedderburn)*
Seja A uma k-álgebra simples de dimensão finita. Temos que existe um inteiro $n \geq 1$ e uma álgebra de divisão $D \supset k$ de tal modo que A seja isomorfa ao anel de matriz $M_n(D)$. Além disso, a álgebra com divisão D é determinada unicamente, a menos de isomorfismo.

Demonstração. Como A é de dimensão finita, toda cadeia descendente de ideais à esquerda estabiliza. Seja L um ideal minimal à esquerda e portanto um A-modulo simples. Pelo Lema de Schur $D = End_A(L)$ é uma álgebra com divisão e pelo Lema de Rieffel temos um isomorfismo $A \cong End_D(L)$, onde $D = End_A(L)$. Pelo o exemplo 2.2 e da observação 2.3.2 podemos concluir que $End_D(L)$ é um espaço vetorial, logo $End_D(L) \cong M_n(D)$, onde n é a dimensão de L sobre D, portanto $A \cong M_n(D)$.

Para mostrar a unicidade tomemos D' uma álgebra com divisão tal que $A \cong M_n(D) \cong M_m(D')$ onde m, n são inteiros, e L um ideal minimal de A, logo temos $D^n \cong L \cong D^m$, pois os ideais minimais de $M_n(D)$ são precisamente as matrizes que têm entradas não nulas em exatamente uma coluna (ver [6] exemplo 2.1.4), assim

$$D \cong End_A(D^n) \cong End_A(L) \cong End_A(D^m) \cong D'$$

. ■

Corolário 2.3.1. *Se k é um corpo algebricamente fechado, então cada k-álgebra simples central é isomorfa a $M_n(k)$, para algum $n \geq 1$.*

Demonstração. Seja A uma k-álgebra simples central, pelo teorema de Wedderburn temos que

$A \cong M_n(D)$ para alguma k-álgebra de divisão D, portanto resta provar que $D = k$. Seja $d \in D$, o conjunto $\{1, d, d^2, ...\}$ é linearmente dependente sobre k. Logo existe um polinômio $p(x)$ com coeficientes em k tal que $p(d) = 0$, isto é, d é algébrico sobre k. Como k é algebricamente fechado, $d \in k$, assim $D = k$. ■

2.3.1 Corpos de decomposição

Nesta seção será apresentada uma caracterização de álgebras simples centrais trivializada por uma extensão finita separável K/k do corpo k. Deste modo iremos caracterizar à mesma como uma matriz de ordem $n \times n$ com coeficientes nessa extensão K.

Lema 2.3.4. *Sejam A uma k-álgebra, $M_n(A)$ a álgebra das matrizes com coeficientes em A e $M_n(k)$ a álgebra das matrizes $n \times n$ sobre k. Então $M_n(A) \cong A \otimes_k M_n(k)$.*

Demonstração. Sejam E_{ij} as matrizes unitárias de $M_n(k)$, podemos escrever todos os elementos de $M_n(A)$ (pela adjunção de uma unidade caso seja necessário), de maneira única como $\sum a_{ij}E_{ij}$, $a_{ij} \in A$. Como consequência temos que a aplicação

$$\begin{aligned} M_n(A) &\longrightarrow A \otimes_k M_n(k) \\ \textstyle\sum a_{ij}E_{ij} &\longmapsto \textstyle\sum a_{ij} \otimes_k E_{ij}; \end{aligned}$$

é um isomorfismo. ■

Observação 2.3.3. *Um resultado importante é quando tivermos A uma k-álgebra simples e B uma k-álgebra arbitraria com unidade, vai existir sempre uma aplicação biunívoca*

$$\begin{aligned} f : B &\longrightarrow A \otimes_k B \\ I &\longmapsto A \otimes_k I, \end{aligned}$$

onde I é um ideal de B e $A \otimes_k I$ ideal de $A \otimes_k B$, para mais detalhes ver [3] teorema 28.1.

Definição 2.3.4. *Seja A uma k-álgebra e B uma k-subálgebra de A, chamamos conjunto $C_A(B) = \{a |\, a \cdot b = b \cdot a, \forall\, b \in B\}$ de centralizador de A em B.*

O centralizador de A em B é uma k-subálgebra da k-álgebra A. Quando A for simples podemos afirmar que o centralizador coincide com o centro de A, ou seja, $C_A(A) = Z(A)$.

Os seguintes lemas serão importantes para podermos mostrar que a propriedade de ser uma álgebra simples central sobre um corpo é estável em relação a extensões de escalares a extensões finitas de corpos.

Lema 2.3.5. *Para todos A, A' k-subálgebras e B, B' suas k-subálgebras respectivamente, temos que:*

$$C_{A\otimes_k A'}(B \otimes_k B') = C_A(B) \otimes_k C_{A'}(B').$$

Demonstração. $\Rightarrow$ Tomemos $u \in C_{A\otimes_k A'}(B \otimes_k B')$, faremos $u = \sum a_i \otimes_k a_i'$ onde a_i e a_i' são linearmente independente sobre o corpo k. Para todo $b \in B$, temos:

$$u \cdot (b \otimes_k 1) = (b \otimes_k 1) \cdot u \Rightarrow u \cdot (b \otimes_k 1) - (b \otimes_k 1) \cdot u = 0 \Rightarrow$$

$$\Rightarrow \left(\sum a_i \otimes_k a_i'\right)(b \otimes_k 1) - (b \otimes_k 1)\left(\sum a_i \otimes_k a_i'\right) = 0 \Rightarrow$$

$$\Rightarrow \sum (a_i b - b a_i) \otimes_k a_i' = 0$$

e sendo a_i' linearmente independente sobre k temos que $a_i \in C_A(B)$ para todos $a_i \in A$. Analisando similarmente para todo $b' \in B'$ obtemos $a_i' \in C_{A'}(B')$, logo $u \in C_A(B) \otimes_k C_{A'}(B')$. Assim, $C_{A\otimes_k A'}(B \otimes_k B') \subset C_A(B) \otimes_k C_{A'}(B')$.
$\Leftarrow$ Agora tomemos $y \in C_A(B) \otimes_k C_{A'}(B')$, $y = a \otimes_k a'$ tal que $b \cdot a = a \cdot b$ para todo $b \in B$ e $b' \cdot a' = a' \cdot b'$ para todo $b' \in B'$. Assim, $y \cdot (b \otimes_k b') = (a \otimes_k a')(b \otimes_k b') = (a \cdot b) \otimes_k (a' \cdot b') = (b \cdot a) \otimes_k (b' \cdot a') = (b \otimes_k b') \cdot (a \otimes_k a') = (b \otimes_k b') \cdot y$ portanto $y \in C_{A\otimes_k A'}(B \otimes_k B')$
Assim $C_A(B) \otimes_k C_{A'}(B') \subset C_{A\otimes_k A'}(B \otimes_k B')$.
Com isso temos o resultado. ■

Se A e B forem k-álgebras simples uma consequência imediata do lema anterior será o isomorfismo

$$Z(A \otimes_k B) \cong Z(A) \otimes_k Z(B).$$

Lema 2.3.6. *Sejam A uma k-álgebra de dimensão finita e K/k uma extensão finita de corpos. Então A é uma k-álgebra simples central se, e somente se, $A \otimes_k K$ é central simples sobre K.*

Demonstração. $\Rightarrow$ Suporemos que A seja uma k-álgebra simples centrais e usando o lema anterior, temos:

$$Z(A \otimes_k K) = Z(A) \otimes_k Z(K) = k \otimes_k K = K$$

e assim provamos que $A \otimes_k K$ é central sobre K. Agora mostraremos que é simples e assim:

$$A \otimes_k K \cong M_n(D) \otimes_k K \cong (D \otimes_k M_n(k)) \otimes_k K \cong M_n(D \otimes_k K) \cong M_n(K) \otimes_K (D \otimes_k K)$$

e com isso temos que $A \otimes_k K$ é simples. Assim temos que $A \otimes_k K$ é simples central.
$\Leftarrow$ Agora suporemos que $A \otimes_k K$ seja simples central e assim:

$$k \otimes_k K \cong K \cong Z(A \otimes_k K) \cong Z(A) \otimes_k K$$

e assim obtemos que $Z(A) = k$ e consequentemente vemos que A é central. Agora iremos supor que I seja um ideal não trivial de A e assim teremos que $A \otimes_k I$ é um ideal não trivial de $A \otimes_k B$ o que é uma contradição, pois por hipótese é simples e assim temos que A é simples também. ■

O próximo lema irá mostrar que a propriedade de ser uma álgebra simples central sobre um corpo é estável em relação a extensões de escalares a extensões finitas de corpos e assim podemos provar uma caracterização alternativa de álgebras simples centrais: elas são exatamente as álgebras que se tornam isomorfas a uma álgebra de matrizes após extensão dos escalares a uma extensão de corpos de grau finito.

Teorema 2.3.2. *Seja k um corpo e A uma k-álgebra de dimensão finita. A álgebra A é simples central sobre k se, e somente se, existirem inteiros $n \geq 1$, e uma extensão finita de corpos K/k para a qual $A \otimes_k K \cong M_n(K)$.*

Demonstração. $\Rightarrow$ Supomos que A é uma k-álgebra simples central. Seja $\overline{k}$ (um) fecho algébrico de k, pelo lema 2.3.6 temos que $A \otimes_k \overline{k}$ é simples central e pelo corolário 2.3.1 $A \otimes_k \overline{k} \cong M_n(\overline{k})$ para algum n. Como $\overline{k}$ é um fecho algébrico temos $\overline{k} = \bigcup K_i$, onde os K_i são extensões finitas de k para todo i. Assim para cada dessas extensões finitas K_i temos que $K_i \subset \overline{k}$ e esta inclusão nos induz a uma aplicação injetiva $A \otimes_k K \longrightarrow A \otimes_k \overline{k}$, daí segue que $A \otimes_k \overline{k} = \bigcup A \otimes_k K_i$. Sejam $e_1, ..., e_{n^2} \in A \otimes_k \overline{k}$ as pré-imagens dos elementos da base padrão de $M_n(\overline{k})$ pelo isomorfismo $A \otimes_k \overline{k} \cong M_n(\overline{k})$. Para cada $i, j \in \{1, ..., n^2\}$ podemos escrever:

$$e_i e_j = \sum_{k=1}^{n^2} a_{ijk} e_k,$$

para certos $a_{ijk} \in \overline{k}$. Escolhemos agora uma extensão finita K de k, suficientemente grande, que contém todos os a_{ijk} e que é tal que $e_1, ..., e_{n^2} \in A \otimes_k K$. Então, obtemos um isomorfismo $A \otimes_k K \cong M_n(K)$.
$\Leftarrow$ Supomos $A \otimes_k K \cong M_n(K)$. Temos $Z(A \otimes_k K) = Z(M_n(K)) = K$ e assim $A \otimes_k K$ é simples central e portanto pelo lema anterior temos que A é simples central sobre k. ■

Obtemos logo:

Corolário 2.3.2. *Se A é uma k-álgebra simples central, a sua dimensão sobre k é um quadrado.*

Demonstração. Seja $\overline{k}$ um fecho algébrico de k, pelo teorema 2.3.2 $\overline{A} = A \otimes_k \overline{k}$ é uma álgebra simples central sobre $\overline{k}$. Como $\overline{k}$ é algebricamente fechado, segue que $\overline{A} \cong M_n(\overline{k})$, logo, $dim_k(A) = dim_{\overline{k}}(\overline{A}) = n^2$. ■

A partir desse corolário podemos definir o grau de uma álgebra simples central.

Definição 2.3.5. *Uma extensão de corpos K/k para a qual $A \otimes_k K \cong M_n(K)$ para n inteiro adequado é conhecida como* ***corpo de decomposição*** *de A. Também podemos dizer que A se cinde sobre K ou que K cinde A. O número inteiro $\sqrt{\dim_k A}$ é chamado de* ***grau*** *de A, e é denotado $deg(A)$.*

Agora iremos enunciar o seguinte teorema de Noether e Köthe que será de fundamental importância para o resultado a ser obtido neste trabalho.

Teorema 2.3.3. *(Noether, Köthe)*
Toda k-álgebra simples central tem um corpo de decomposição que é separável sobre k.

Demonstração. A demonstração desse teorema necessita de alguns argumentos da geometria algébrica, para mais detalhes ver [6] proposição 2.2.5. ■

Chegamos agora no resultado principal desta seção. Este resultado nos permitirá aplicar toda a teoria da cohomologia galoisiana do segundo capítulo ao estudo de álgebras simples centrais. Relembramos a definição do grupo de Galois de uma extensão de corpos:

Definição 2.3.6. *Seja K/k uma extensão finita, normal e separável de corpos, então o conjunto*

$$Aut_k(K) = \{\sigma : K \longrightarrow K; \sigma|_k(a) = a\},$$

onde σ é isomorfismo de corpos, é chamado de ***grupo de Galois*** *de K sobre k.*

Corolário 2.3.3. *Uma k-álgebra A de dimensão finita é uma álgebra simples central se, e somente se existir um inteiro $n > 0$ e uma extensão galoisiana finita de corpos K/k para a qual $A \otimes_k K \cong M_n(K)$.*

Demonstração. Como A é uma k-álgebra de dimensão finita que é simples central, temos pelo teorema 2.3.2 que existem $n \geq 1$ inteiro e uma extensão finita de corpo K/k onde

$$A \otimes_k K \cong M_n(K).$$

Agora pela proposição 2.3.3 nós podemos escolher uma tal extensão que é separável. Como esta extensão é finita e separável ela pode ser estendida a uma extensão galoisiana. ■

2.3.2 O índice de uma álgebra simples central

Para podermos chegar ao resultado desejado neste trabalho precisamos definir o índice de uma álgebra simples central e alguns resultados importantes obtidos à partir dela.

Definição 2.3.7. *Seja A uma k-álgebra. A* ***álgebra oposta*** *A^{op} de A é a k-álgebra, que tem A como k-espaço vetorial subjacente e onde o produto esta dado por $y \cdot x = x \cdot_A y$, onde $\cdot_A$ denota o produto em A.*

Quando uma álgebra A é central simples sobre um corpo k, então a sua álgebra oposta A^{op} também o será.

Observação 2.3.4. *Definimos uma aplicação k-linear $A \otimes_k A^{op} \longrightarrow End_k(A)$ não nula que associa o endomorfismo k-linear $x \longrightarrow \sum a_i \cdot x \cdot b_i$ a um elemento do tipo $\sum a_i \otimes_k b_i$. Temos pelo fato de $A \otimes_k A^{op}$ ser simples que esta aplicação é injetiva e observando suas dimensões também é sobrejetiva, logo $A \otimes_k A^{op} \cong End_k(A)$.*

Definição 2.3.8. *Seja A uma álgebra simples central sobre um corpo k e D uma álgebra com divisão sobre k tal que $A \cong M_n(D)$. Então, chamamos o* ***índice*** *de A o grau de D, assim:*

$$ind_k(A) = deg_k(D).$$

Proposição 2.3.1. *Seja D uma k-álgebra com divisão. Se D contém um subcorpo K cujo grau é o índice de D, ou seja, $deg(K) = ind(D)$, então, D é cindida sobre K.*

Demonstração. Seja D^{op} a k-álgebra oposta da k-álgebra com divisão D e usando a observação 2.3 temos que $D \otimes_k D^{op} \cong End_k(D)$. Sendo K como da nossa hipótese e o fato de ser comutativo temos que se $K \subset D \Rightarrow K \subset D^{op}$. Consequentemente como $D \otimes_k D^{op}$ é simples temos que $D \otimes_k K$ é simples também e assim a aplicação $f : D \otimes_k K \longrightarrow End_k(D)$ é injetiva. Sendo D um K-espaço vetorial à direita temos através da multiplicação por elementos de K que a imagem de f cai dentro de $End_K(D)$. Como D é um K-espaço vetorial, então temos que $End_K(D) \cong M_n(K)$, com $n = ind_k(D)$, em particular $End_K(D)$ tem dimensão n^2 sobre K. Por outro lado, temos $dim_K(D \otimes_k K) = dim_k(D) = n^2$, e sendo assim f é um isomorfismo e portanto K é um corpo de decomposição para D. ■

Provaremos agora uma proposição que nos será útil no capítulo em que falaremos sobre o Teorema de Brauer que é o objetivo deste nosso trabalho. Esta proposição pode ser considerada uma refinamento do teorema de 2.3.3, pois ela nos diz que, para uma k-álgebra simples central A, não só é possível encontrar uma extensão separável K/k que cinde A, mas é possível encontrar uma tal extensão K/k de grau $ind(A)$ e tal que $K \subset A$. O seguinte lema usa o noção de polinômio característico reduzido, para a definição deste polinômio veja a discussão depois de [6], prop. 4.5.4.

Lema 2.3.7. *Seja A uma k-álgebra simples central que é cindida pela extensão separável K/k de grau $ind_k(A)$. Podemos encontrar um $a \in A$ tal que seu polinômio característico reduzido $P_a(T) \in k[T]$ tenha raízes distintas.*

Demonstração. Assim como o teorema de 2.3.3, a demonstração deste lema necessita alguns fatos da geometria algébrica. A prova pode ser encontrada em [6], cap. 4, lema 4.5.5. ■

Proposição 2.3.2. *Toda k-álgebra simples central A é cindida por uma extensão separável K/k de grau $ind(A)$. Além disso, tal K pode ser encontrado entre as k-subálgebras de A.*

Demonstração. Usando o teorema de Wedderburn podemos assumir que A é uma álgebra com divisão e usando o lema 2.3.7 podemos encontrar um $a \in A$ de maneira que $P_a(T)$ tenha raízes distintas no fecho algébrico. Segue imediatamente que o anel $K = k[T]/(P_a(T))$ é uma extensão separável de k. Portanto, o homomorfismo $k[T] \longrightarrow A$ que associa $a \in A$ a um polinômio característico com raízes distintas faz com que K se torne um subcorpo em A que é de grau $degP_a(T) = deg_k(A) = ind_k(A)$ sobre k, pelo fato de A ser uma álgebra de divisão e usando a proposição 2.3.1 temos o nosso resultado. ■

2.4 O grupo de Brauer

Nesta seção definimos o grupo de Brauer, que nos ajudará a classificar álgebra centrais simples que é o objeto central deste trabalho.

Proposição 2.4.1. *Para um corpo k, todos os automorfismos de anéis de matrizes $M_n(k)$ são internos, isto é, são dados pela aplicação $M \longrightarrow CMC^{-1}$ para alguma matriz inversível $C \in M_n(k)$.*

Demonstração. Considere o ideal à esquerda minimal $I_1 = [m_{ij}]$ tal que $m_{ij} = 0$ se $j \neq 1$ e seja $\lambda \in Aut(M_n(k))$. Se necessário conjugamos λ por uma matriz adequada e podemos assumir que $\lambda(I_1) = I_1$. Temos um isomorfismo $I_1 \cong k^n$ de k-espaços vetoriais, assim λ induz um automorfismo de k^n. Esse automorfismo é dado por uma matriz inversível C. Nós temos que para toda matriz $M \in M_n(k)$, o endomorfismo de k^n definido na base canônica por $\lambda(M)$ é a matriz CMC^{-1}, e o lema segue. ■

Corolário 2.4.1. *O grupo de automorfismos de $M_n(k)$ é o grupo linear projetivo geral $PGL_n(k)$.*

Demonstração. Existe um homomorfismo natural $GL_n(k) \longrightarrow Aut(M_n(k))$ que leva $C \in GL_n(k)$ a um automorfismo $A \longmapsto CAC^{-1}$. Pelo lema anterior este automorfismo é sobrejetivo e seu núcleo é o centro de $GL_n(k)$, isto é, o subgrupo de matrizes escalares. ■

Antes de prosseguir lembramos um fato sobre anéis de matrizes.

Lema 2.4.1. *Sejam $M_n(k)$ e $M_m(k)$ duas álgebras de matrizes sobre k, temos que*

$$M_n(k) \otimes_k M_m(k) \cong M_{nm}(k).$$

Demonstração. Tomemos as bases E_{ij} e F_{rl} (onde $i, j = 1, ..., n$ e $r, l = 1, ..., m$) de matrizes elementares de $M_n(k)$ e $M_m(k)$ respectivamente. Claramente $E_{ij} \otimes F_{rl}$ é matriz elementar de $M_{nm}(k)$. Com isso obtemos o isomorfismo

$$\begin{aligned} f : M_n(k) \otimes_k M_m(k) &\xrightarrow{\sim} M_{nm}(K) \\ (E_{ij}, F_{rl}) &\longmapsto E_{ij} \otimes F_{rl}; \end{aligned}$$

e portanto temos $M_n(k) \otimes_k M_m(k) \cong M_{nm}(k)$. ■

Lema 2.4.2. *Se A e B são k-álgebras simples centrais que se cindem sobre K, então $A \otimes_k B$ também é uma k-álgebra simples central que se cinde sobre K.*

Demonstração. Como A e B se cindem sobre K, temos que existem n, m inteiros positivos tais que $A \otimes_k K \cong M_n(K)$ e $B \otimes_k K \cong M_m(K)$.
Agora:

$$(A \otimes_k K) \otimes_k (B \otimes_k K) \cong (A \otimes_k B) \otimes_k K \tag{2.1}$$

E por outro lado, temos:

$$(A \otimes_k K) \otimes_k (B \otimes_k K) \cong M_n(K) \otimes_k M_m(K) \cong M_{nm}(K) \tag{2.2}$$

Logo temos que

$$(A \otimes_k B) \otimes_k K \cong M_{nm}(K)$$

e assim temos que $A \otimes_k B$ se cinde sobre K. ■

Definição 2.4.1. *Sejam A e B duas álgebras simples centrais sobre k tais que $A \cong M_n(D)$ e $B \cong M_m(D')$. Dizemos que A e B são **similares**, quando D e D' são isomorfas, ou seja, $A \sim B \Leftrightarrow D \cong D'$. Isso é uma relação de equivalência.*

Definição 2.4.2. *O **conjunto de Brauer** de k, denotado por $Br(k)$, é o conjunto das classes de equivalência das álgebras simples centrais sobre k para a relação $\sim$. Denotaremos por $[A]$ a classe de equivalência de A.*

Definição 2.4.3. *Seja K/k uma extensão de corpos. O conjunto das classes de álgebras centrais sobre k que se cindem sobre K formam um subconjunto de $Br(k)$, denotado por $Br(K/k)$.*

Lema 2.4.3. *Sejam A e B álgebras simples centrais. Então $A \sim B$ se, e somente se, existirem inteiros positivos r e s tais que*

$$A \otimes_k M_r(k) \cong B \otimes_k M_s(k).$$

Demonstração. Sabemos pelo teorema de Wedderburn que existem inteiros positivos m, n tais $A \cong M_n(D)$ e $B \cong M_m(D')$ onde D e D' são álgebras centrais com divisão e sabemos também que $M_n(D) \cong D \otimes_k M_n(k)$ e $M_m(D') \cong D' \otimes_k M_m(k)$.
$\Rightarrow$ Supomos primeiro que $A \sim B$. Então $D \cong D'$. Logo $A \otimes_k M_m(k) \cong M_n(D) \otimes_k M_m(k) \cong D \otimes_k M_n(k) \otimes_k M_m(k) \cong D \otimes_k M_m(k) \otimes_k M_n(k) \cong D' \otimes_k M_m(k) \otimes_k M_n(k) \cong M_m(D') \otimes_k M_n(k) \cong B \otimes_k M_n(k)$.
$\Leftarrow$ Agora supomos que $A \otimes_k M_r(k) \cong B \otimes_k M_s(k) \Rightarrow M_n(D) \otimes_k M_r(k) \cong M_m(D') \otimes_k M_s(k) \Rightarrow D \otimes_k M_n(k) \otimes_k M_r(k) \cong D' \otimes_k M_m(k) \otimes_k M_s(k) \Rightarrow D \otimes_k M_{nr}(k) \cong D' \otimes_k M_{ms}(k) \Rightarrow M_{nr}(D) \cong M_{ms}(D')$ e pelo teorema de Wedderburn temos que $D \cong D'$ e por tanto $A \sim B$. ■

Corolário 2.4.2. *Se $A \sim A'$ e $B \sim B'$ então $A \otimes_k B \sim A' \otimes_k B'$.*

Demonstração. Se $A \sim A'$ e $B \sim B'$ então pelo lema 2.4.3 existem inteiros positivos r_1, s_1, r_2, s_2 tais que

$$A \otimes_k M_{r_1}(k) \cong A' \otimes_k M_{s_1}(k) \tag{2.3}$$

e

$$B \otimes_k M_{r_2}(k) \cong B' \otimes_k M_{s_2}(k) \tag{2.4}$$

onde então fazendo produtos tensorial entre (2.3) e (2.4) temos $A \otimes_k M_{r_1}(k) \otimes_k B \otimes_k M_{r_2}(k) \cong A' \otimes_k M_{s_1}(k) \otimes_k B' \otimes_k M_{s_2}(k) \Rightarrow (A \otimes_k B) \otimes_k M_{r_1}(k) M_{r_2}(k) \cong (A' \otimes_k B') \otimes_k M_{s_1}(k) M_{s_2}(k) \Rightarrow (A \otimes_k B) \otimes_k M_{r_1 r_2}(k) \cong (A' \otimes_k B') \otimes_k M_{s_1 s_2}(k)$ e com isso temos que $A \otimes_k B \sim A' \otimes_k B'$. ■

Graças a este corolário podemos definir uma operação em $Br(k)$ da seguinte forma:

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

Proposição 2.4.2. *O conjunto $Br(k)$ munido com a operação do produto acima é um grupo abeliano, chamada o grupo de Brauer.*

Demonstração. As propriedades associativa e comutativa seguem de imediato das propriedades do produto tensorial.
A classe de k é o elemento neutro e classe de A^{op} é o elemento simétrico de A. Com efeito, pela observação 2.3.4 temos um isomorfismo $A \otimes_k A^{op} \cong End_k(A)$ e $End_k(A) \cong M_n(k)$. Assim o conjunto $Br(k)$ é um grupo abeliano com o produto acima definido. ■

Corolário 2.4.3. *O conjunto $Br(K/k)$ é um subgrupo de $Br(k)$.*

Demonstração. (1) Sejam A e B álgebras que se cindem sobre K, então o lema 2.4.2 garante que $A \otimes_k B$ também se cinde sobre o corpo K, logo temos que $[A][B] = [A \otimes_k B]$ é fechado para operação em $Br(K/k)$.
(2) Como A se cinde sobre K, temos que A^{op} também se cinde sobre K. ■

Proposição 2.4.3. *Se $\varphi : k \longrightarrow K$ é um homomorfismo de corpos, então obtemos um homomorfismo $Br(\varphi) : Br(k) \longrightarrow Br(K)$ de grupos abelianos.*

Demonstração. Seja $\varphi : k \longrightarrow K$ um morfismo de corpos. Vamos definir uma aplicação $Br(\varphi) : Br(k) \longrightarrow Br(K)$ por $Br(\varphi)([A]) = [A \otimes_k K]$ onde a proposição 2.9 e corolário 2.6 garantem a boa definição. Agora, vamos mostrar que $Br(\varphi)$ é um homomorfismo de grupos abelianos,assim:

$$Br(\varphi)([A][B]) = Br(\varphi)([A \otimes_k B]) = [(A \otimes_k B) \otimes_k K] = [(A \otimes_k B) \otimes_k (K \otimes_K K)] =$$

$$= [A \otimes_k K \otimes_K K \otimes_k B] = [(A \otimes_k K) \otimes_K (B \otimes_k K)] = [A \otimes_k K][B \otimes_k K] = Br(\varphi)([A])Br(\varphi)([B]).$$

Portanto $Br(\varphi)$ é um homomorfismo de grupos abelianos como queríamos demonstrar. ■

Exemplo 2.4.1. *$Br(\mathbb{C}) = 0$, pois $\mathbb{C}$ é algebricamente fechado. De forma mais geral, para todo corpo algebricamente fechado $k = \bar{k}$, nós temos $Br(k) = 0$.*

Exemplo 2.4.2. *$Br(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}_2$, onde $\mathbb{H}$ é a álgebra de quatérnios de Hamilton da definição 2.2.1.*

Exemplo 2.4.3. *$Br(\mathbb{F}_p) = 0$, onde p é primo. De forma geral, se k é corpo finito então $Br(k) = 0$.*

Exemplo 2.4.4. *Seja k uma extensão finita de $\mathbb{Q}$, i.e. um corpo global. Pelo teorema de Brauer-Hasse-Noether temos uma sequência exata:*

$$0 \longrightarrow Br(k) \longrightarrow \bigoplus_v Br(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

onde v percorre todos os lugares (finitos e infinitos) de k. Se $k = \mathbb{Q}$, esta sequência tem a seguinte forma:

$$0 \longrightarrow Br(\mathbb{Q}) \longrightarrow \mathbb{Z}/2 \times \bigoplus_p \mathbb{Q}/\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

onde p percorre os primos de $\mathbb{Z}$.

Definição 2.4.4. *Chamamos de **período** de uma k-álgebra simples central A a ordem do elemento $[A]$ no grupo de Brauer:*

$$per_k(A) = o([A])$$

Nesse trabalho mostraremos, que este período é sempre finito e que para uma álgebra simples central o índice sempre divide o período. Para poder avançar precisamos algumas técnicas da cohomologia galoisiana que apresentaremos nos próximos capítulos.

Capítulo 3

Cohomologia de Grupos

Neste capítulo apresentaremos a teoria da cohomologia galoisiana. Assim poderemos identificar o grupo de Brauer com um grupo de cohomologia desta teoria. Observamos que o grupo de Galois de uma extensão K/k é completamente determinado pelos grupos de Galois das extensões finitas de L/k, onde $L \subset K$.
Como veremos, um grupo que é determinado desta maneira pelos seus quocientes finitos é chamado um grupo profinito. As referências principais para este capítulo são [6] e [9].

3.1 Grupos profinitos

Primeiro lembramos a definição de um grupo topológico:

Definição 3.1.1. *Seja G um grupo, cujo conjunto subjacente se encontra munido de um topologia. Dizemos que G é um* ***grupo topológico*** *quando as aplicações:*

$$\begin{array}{rcl} \varphi : G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & gh \end{array} \qquad e \qquad \begin{array}{rcl} \phi : G & \longrightarrow & G \\ h & \longmapsto & h^{-1} \end{array}$$

são contínuas. Um homomorfismos de grupos topológicos é um homomorfismo de grupos que é ao mesmo tempo um homeomorfismo de espaços topológicos.

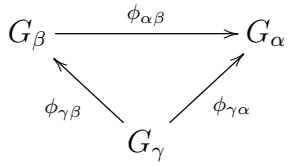
Antes de podermos definir o que é um grupo profinito precisamos definir as noções de

conjunto dirigido, de **sistema inverso** e **limite inverso**. Em algumas publicações, sistemas e limites inversos são chamados de sistemas e limites projetivos.

Definição 3.1.2. *Sejam Λ um conjunto não vazio e $\leq$ uma relação, então $(\Lambda, \leq)$ é um* ***conjunto dirigido****, quando:*
Para todo $\alpha \in \Lambda$, então $\alpha \leq \alpha$. (Reflexividade)
Para todos $\alpha, \beta \in \Lambda$ se $\alpha \leq \beta$ e $\beta \leq \alpha$ então $\alpha = \beta$. (Anti-simetria)
Para todos $\alpha, \beta, \sigma \in \Lambda$ se $\alpha \leq \beta$ e $\beta \leq \sigma$ então $\alpha \leq \sigma$. (Transitividade)
Para todos $\alpha, \beta \in \Lambda$ existe $\lambda \in \Lambda$ tal que $\alpha \leq \lambda$ e $\beta \leq \lambda$. (Existência de um limite superior)

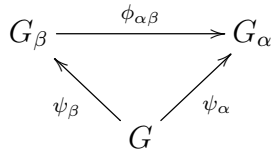
Seja $(G_\alpha)_{\alpha\in\Lambda}$ uma família de grupo topológicos indexada por um conjunto dirigido $(\Lambda, \leq)$ e $\{\phi_{\alpha\beta} : G_\beta \longrightarrow G_\alpha\}_{\alpha\leq\beta}$ uma família de homomorfismos contínuos, temos:

Definição 3.1.3. *Nós dizemos que $(G_\alpha, \phi_{\alpha\beta})_\Lambda$ é um* ***sistema inverso (ou projetivo)*** *quando para todo $\alpha, \beta, \gamma \in \Lambda$ o diagrama*



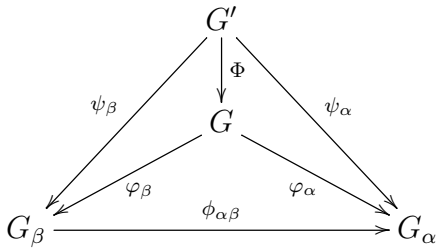
é comutativo, ou seja, $\phi_{\gamma\beta} \circ \phi_{\alpha\beta} = \phi_{\gamma\alpha}$ e $\phi_{\alpha\alpha} = id_{G_\alpha}$.

Seja G um grupo topológico e $\{\psi_\alpha : G \longrightarrow G_\alpha\}_{\alpha\in\Lambda}$ uma família de morfismos entre grupos topológicos. Esta é dita **compatível ao sistema inverso** $(G_\alpha, \phi_{\alpha\beta})_\Lambda$ de grupos topológicos quando



seja comutativo para todo $\alpha \leq \beta$.

Definição 3.1.4. *Um* ***limite inverso (ou projetivo)*** *(G, φ_α) de um sistema inverso (ou projetivo) $(G_\alpha, \phi_{\alpha\beta})_\Lambda$ de grupos topológicos é um grupo topológico G com uma família compatível $\{\varphi_\alpha : G \longrightarrow G_\alpha\}_{\alpha\in\Lambda}$ satisfazendo a seguinte propriedade universal: Para cada grupo topológico G' e para cada uma família compatível $\{\psi_\alpha : G' \longrightarrow G_\alpha\}_{\alpha\in\Lambda}$ existe uma única aplicação contínua $\Phi : G' \longrightarrow G$ tal que o diagrama a seguir comuta para todos $\alpha \leq \beta \in \Lambda$.*



Proposição 3.1.1. *O limite inverso de um sistema inverso existe e é único a menos de isomorfismo.*

Demonstração. Seja $(G_\alpha, \phi_{\alpha\beta})_\Lambda$ um sistema inverso de grupos topológicos. Provemos primeiro a existência de forma construtiva. Formamos o produto infinito $\prod_{\lambda\in\Lambda} G_\lambda$ e consideremos o subconjunto $G \subset \prod_{\lambda\in\Lambda} G_\lambda$ formado de elementos $(g_\lambda)_{\lambda\in\Lambda}$ tais que, se $\alpha \leq \beta$, então $\phi_{\alpha\beta}(g_\beta) = g_\alpha$, onde $\alpha, \beta \in \Lambda$. Para cada $\alpha \in \Lambda$ temos morfismos $\varphi_\alpha : G \hookrightarrow \prod_\lambda G_\lambda \to G_\alpha$, onde o primeiro é simplesmente a inclusão e o segundo a projeção para o fator G_α. Então é possível verificar que $(G, \varphi_\alpha)_\Lambda$ é um limite inverso. Mostremos agora a unicidade. Para isso tomemos $(G, \varphi_\alpha)_\Lambda$ e $(G', \psi_\alpha)_\Lambda$ dois limites inversos (ou projetivos) de $(G_\alpha, \phi_{\alpha\beta})_\Lambda$. Usando o fato que $(G, \varphi_\alpha)_\Lambda$ é um limite inverso e o fato que $(G', \psi_\alpha)_\Lambda$ uma família compatível, vemos que existe uma única aplicação $\Phi : G' \longrightarrow G$ tal que $\varphi_\alpha \circ \Phi = \psi_\alpha$ para todo $\alpha \in \Lambda$.

Agora usando o fato que $(G', \psi_\alpha)_\Lambda$ é também limite inverso e que $(G, \varphi_\alpha)_\Lambda$ uma família compatível, existe também uma única aplicação $\Psi : G \longrightarrow G'$ tal que $\psi_\alpha \circ \Psi = \varphi_\alpha$ para todo $\alpha \in \Lambda$.

Logo $\Phi \circ \Psi : G \longrightarrow G$ e $\varphi_\alpha \circ \Phi \circ \Psi = \psi_\alpha \circ \Psi = \varphi_\alpha$ para todos $\alpha \in \Lambda$. Além disso $\varphi_\alpha \circ id_G = \varphi_\alpha$, para todo $\alpha \in \Lambda$. Assim $\Phi \circ \Psi = id_G$ graças à unicidade de Φ e Ψ. Analogamente $\Psi \circ \Phi = id_{G'}$ e assim mostramos a unicidade do limite inverso. ■

Observação 3.1.1. *A noção de limite inverso existe de forma mais geral em qualquer categoria. Por exemplo na categoria dos conjuntos podemos reencontrar a simples interseção entre conjuntos construída como limite inverso. Porém para os nossos fins nos limitamos à categoria dos espaços topológicos.*

Definição 3.1.5. *Dizemos que uma grupo G é um* ***grupo profinito*** *quando for isomorfo a um limite inverso, ou seja:*

$$G \cong \lim_{\leftarrow\Lambda} G_\alpha,$$

para um sistema inverso $(G_\alpha, \phi_(\alpha\beta))_\Lambda$*, onde* G_α *é finito para todo* $\alpha \in \Lambda$*.*

Lembramos a definição de topologia discreta:

Definição 3.1.6. *Seja* X *um conjunto munido de uma topologia. Dizemos esta topologia é* ***discreta*** *quando todos os subconjuntos de* X *são abertos.*

Exemplo 3.1.1. *Consideremos o conjunto dirigido* $(\mathbb{Z}, >)$*, com* $m > n$ *se, e somente se,* n *divide* m*, para cada* $m, n \in \mathbb{Z}$*. Nós definiremos* $G_m = \mathbb{Z}/m\mathbb{Z}$*, munido topologia discreta, e consideremos as projeções naturais*

$$\begin{aligned} f_{nm} : \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ r + m\mathbb{Z} &\longmapsto r + n\mathbb{Z}, \end{aligned}$$

que são bem definidos no caso em que $n \mid m$ *e observando o diagrama abaixo*

$$\begin{array}{ccc} G_m = \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\qquad f_{nm} \qquad} & G_n = \mathbb{Z}/n\mathbb{Z} \\ & {\scriptstyle f_{pm}} \nwarrow \quad \nearrow {\scriptstyle f_{pn}} & \\ & G_p = \mathbb{Z}/p\mathbb{Z} & \end{array}$$

verificamos que é comutativo para todos $m, n, p \in \mathbb{Z}$ *e* p *divide* n *e* n *divide* m*. Assim* $(G_m, f_{nm})_\mathbb{Z}$ *é um sistema inverso. O seu limite inverso é o grupo* $\widehat{\mathbb{Z}} = \varprojlim_{m \in \mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$*, munido pela topologia induzida pela topologia discreta de cada um dos* $\mathbb{Z}/m\mathbb{Z}$*.*

Exemplo 3.1.2. *Seja* p *um número primo. Consideremos agora* $I = \mathbb{N}$ *munido da ordem usual. Definimos* $G_n = \mathbb{Z}/p^n\mathbb{Z}$*,* $n \in \mathbb{N}$*, dotado da topologia discreta e consideremos as projeções naturais*

$$f_{mn} : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$$

que são bem definidas no caso $m \leq n$*. Portanto,* $(G_n, f_{mn})_\mathbb{N}$ *é um sistema inverso e o seu limite inverso é* $\mathbb{Z}_p = \varprojlim_{m \in \mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}$*.*

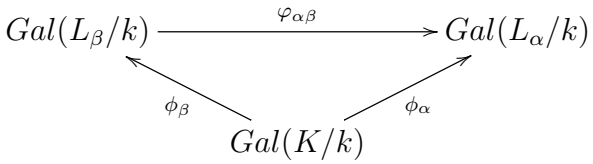
Agora seja $Gal(K/k)$ o grupo de Galois de uma extensão de corpos K/k. Chamaremos E o conjunto de todas as extensões intermediárias finitas L_α/k, $\alpha \in I$, então $(E, \subset)$ forma um conjunto dirigido. No mais, cada um dos grupos $Gal(L_\alpha/k)$ pode ser munido da topologia discreta. Para duas extensões L_α/k e L_β/k, consideremos os homomorfismos naturais:

$$\varphi_{\alpha\beta} : Gal(L_\beta/k) \longrightarrow Gal(L_\alpha/k)$$
$$\sigma \longmapsto \sigma|_{L_\alpha},$$

Obtemos um sistema inverso de grupos topológicos:

$$\{\varphi_{\alpha\beta} : Gal(L_\beta/k) \longrightarrow Gal(L_\alpha/k)\}_{L_\alpha \subset L_\beta}.$$

Além disso, verifica-se que a família dos homomorfismos contínuos canônicos de restrição $\{\phi_\alpha : Gal(K/k) \longrightarrow Gal(L_\alpha/k)\}_{L_\alpha \in E}$ é compatível com este sistema inverso, pois o seguinte digrama comuta para todo α, β tais que $L_\alpha \subset L_\beta$:



A partir das aplicações restrições acima, obtemos um homomorfismo de grupos

$$\theta : Gal(K/k) \longrightarrow \prod_{L_\alpha \in E} Gal(L_\alpha/k).$$

A imagem de θ está contida em $\lim\limits_{\leftarrow L_\alpha \in E} Gal(L_\alpha, k)$, pois:

$$\varphi_{\alpha\beta}(\pi_{L_\beta}(\theta(\sigma))) = \varphi_{\alpha\beta}(\sigma|_{L_\alpha}) = \sigma|_{L_\beta} = \pi_{L_\alpha}(\theta(\sigma)),$$

onde $\pi_{L_\beta} : \prod\limits_{L_\alpha \in E} Gal(L_\alpha/k) \longrightarrow Gal(L_\beta/k)$, para $\beta \in \Lambda$ é a aplicação projeção. Não é difícil verificar que θ é um isomorfismo e a partir disso concluímos que

$$Gal(K/k) \cong \lim_{\leftarrow E} Gal(L_\alpha/k),$$

logo $Gal(K/k)$ é um grupo profinito.

Observação 3.1.2. *É possível provar que todo grupo profinito é o grupo de Galois de alguma extensão de corpos, vide Waterhouse [10].*

3.2 Cohomologia Galoisiana

Neste seção desenvolveremos a teoria da Cohomologia Galoisiana, que é a cohomologia do grupo de Galois $Gal(K/k)$ sendo visto como um grupo profinito.

Definição 3.2.1. *Seja $(G, \cdot)$ um grupo profinito, dizemos que o par $(A, *)$ é um G-**módulo**, se A é um grupo abeliano, munido da topologia discreta e se $*$ é uma ação contínua, isto é:*

$$\begin{aligned} * : G \times A &\longrightarrow A \\ (g, a) &\longmapsto g * a \end{aligned}$$

é uma aplicação contínua e para todos, $g, g' \in G$ e $a, a' \in A$, que satisfaz as condições:
(1) $(g \cdot g') * a = g * (g' * a)$
(2) $g * (a + a') = g * a + g * a'$.
(3) $1 * a = a$.

Definição 3.2.2. *Uma aplicação $\varphi : A \longrightarrow B$ é um G-**homomorfismo** entre os G-módulos A e B, quando for um homomorfismo de grupos abelianos compatível com a G-ação, ou seja,*

$$\varphi(ga) = g\varphi(a) \,\forall\, g \in G; \,\forall\, a \in A.$$

*Dizemos que $\varphi : A \longrightarrow B$ é um **morfismo de G-módulos** se o mesmo for um G-homomorfismo continuo. Chamaremos de D_G a categoria de todos os G-módulos.*

Para todo $n > 0$, G^n será o produto de n cópias de G, munido da topologia produto e para cada $A \in D_G$, definiremos $C^n(G, A) := \{\varphi | \, \varphi : G^n \longrightarrow A\}$ o conjunto de todas as funções contínuas $\varphi : G^n \longrightarrow A$, e colocaremos uma soma em $C^n(G, A)$, tal que:

$$\begin{aligned} \oplus : C^n(G, A) \times C^n(G, A) &\longrightarrow C^n(G, A) \\ (\varphi, \varphi') &\longmapsto \varphi \oplus \varphi'. \end{aligned}$$

onde $\varphi \oplus \varphi'$ está definida como segue

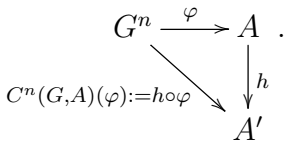
$$\begin{aligned} \varphi \oplus \varphi' : G^n &\longrightarrow A \\ x &\longmapsto \varphi(x) + \varphi'(x) \end{aligned}$$

O conjunto $(C^n(G,A),\oplus)$ formam um grupo abeliano.

Observação 3.2.1. *Se $h : A \longrightarrow A'$ for um morfismo em D_G, então ele determina homomorfismo de grupos abelianos da seguinte forma:*

$$C^n(G,h) : C^n(G,A) \longrightarrow C^n(G,A')$$
$$\varphi \longmapsto h \circ \varphi.$$

ou seja:



Através dessa definição é possível notar que $C^n(G,-)$ é um funtor que tem como domínio a categoria D_G e como contra-domínio a categoria Ab de grupos abelianos.

Proposição 3.2.1. *Se $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ é uma sequencia exata de G-módulos. Então, a sequencia $0 \longrightarrow C^n(G,A) \xrightarrow{f^*} C^n(G,B) \xrightarrow{g^*} C^n(G,C) \longrightarrow 0$ é exata, tal que $f^* := C^n(G,f)$ e $g^* := C^n(G,g)$.*

Demonstração. Injetividade de f^*:
Como $f \neq 0$ é injetiva temos que possui uma inversa pela esquerda, assim:
$f^*(\varphi) = f^*(\varphi') \Rightarrow f \circ \varphi = f \circ \varphi' \Rightarrow \varphi = \varphi' \ \therefore\ f^*$ é injetiva.
$Imf^* = Kerg^*$:
Seja $(g^* \circ f^*)(\varphi) = g^*(f^*(\varphi)) = g^*(\varphi \circ f) = (\varphi \circ f) \circ g = \varphi \circ (f \circ g) = \varphi \circ 0 = 0$, logo temos que $Imf^* \subset Kerg^*$. Agora, seja $\varphi \in Kerg^*$ então $\varphi(x) \in Kerg \Rightarrow \varphi(x) \in Imf$ pela exatidão da sequencia da nossa hipótese. Assim, tomemos $\varphi(x) = f(a_x)$ para um único $a_x \in A$ (pois f é injetiva). Assim, temos que $\varphi(x) \in Imf^*$, logo, $Kerg^* \subset Imf^*$ e portanto $Imf^* = Kerg^*$.
Sobrejetividade de g^*:
Seja $\varphi \in C^n(G,C)$, logo, temos que para todo $x \in G^n$ existe $b \in B$ tal que $\varphi(b) = g(x)$. A partir desta escolha podemos definir a seguinte aplicação $\widetilde{\varphi}^{-1} : G^n \longrightarrow B$, onde, $x \longmapsto b_x$, tal que $\widetilde{\varphi}(\{b_x\}) = \emptyset$ se $b \neq Im(\varphi)$ e sendo assim $\widetilde{\varphi}^{-1}(\{\widetilde{\varphi}(x)\}) = \widetilde{\varphi}^{-1}(\{g(b_x)\})$, logo temos que $\widetilde{\varphi} \in C^n(G,B)$ e portanto g^* é sobrejetiva. ■

Definição 3.2.3. *Definiremos a **aplicação de diferencial** para $n > 0$*

$$\partial^n : C^n(G,A) \longrightarrow C^{n+1}(G,A)$$

mediante a seguinte a fórmula

$$\partial^n\varphi(g_1, g_2, ..., g_n, g_{n+1}) =$$

$$= g_1\varphi(g_2, ..., g_n, g_{n+1}) + \sum_{r=1}^{n}(-1)^r\varphi(g_1, ..., g_r g_{r+1}, g_{r+2}, ..., g_{n+1}) + (-1)^{n+1}\varphi(g_1, ..., g_n).$$

Onde para $n = 0$ definiremos $\partial^0\varphi(g_1) = g_1\varphi - \varphi$.

Lema 3.2.1. *A aplicação diferencial $\partial^n : C^n(G, A) \longrightarrow C^{n+1}(G, A)$ é um homomorfismo de grupos.*

Demonstração. $\partial^n(\varphi \oplus \psi)(g_1, ..., g_{n+1})$

$= g_1(\varphi \oplus \psi)(g_2, ..., g_{n+1}) + \sum_{r=1}^{n}(-1)^r(\varphi \oplus \psi)(g_1, ..., g_r g_{r+1}, ..., g_{n+1}) + (-1)^{n+1}(\varphi \oplus \psi)(g_1, ..., g_n)$

$= g_1\varphi(g_2, ..., g_{n+1}) + g_1\psi(g_2, ..., g_{n+1}) + \sum_{r=1}^{n}(-1)^r(\varphi)(g_1, ..., g_r g_{r+1}, ..., g_{n+1})$

$+ \sum_{r=1}^{n}(-1)^r(\psi)(g_1, ..., g_r g_{r+1}, ..., g_{n+1}) + (-1)^{n+1}\varphi(g_1, ..., g_n) + (-1)^{n+1}\psi(g_1, ..., g_n)$

$= (\partial^n(\varphi) \oplus \partial^n(\psi))(g_1, ..., g_{n+1}).$

■

Proposição 3.2.2. *A sequência de homomorfismos de grupos*

$$C^0(G, A) \xrightarrow{\partial^0} C^1(G, A) \xrightarrow{\partial^1} C^2(G, A) \longrightarrow \cdots$$

$$\longrightarrow C^{n-1}(G, A) \xrightarrow{\partial^{n-1}} C^n(G, A) \xrightarrow{\partial^n} C^{n+1}(G, A) \longrightarrow \cdots$$

é um complexo de cadeias, isto é, $\partial^n \circ \partial^{n-1} = 0$, para todo $n \geq 1$.

Demonstração. Primeiro mostramos para $n = 1$, assim:

$$\begin{aligned}(\partial^1 \circ \partial^0\varphi)(g_1, g_2) &= g_1((\partial^0\varphi)(g_2)) - (\partial^0\varphi)(g_1g_2) + (\partial^0\varphi)(g_1)\\ &= g_1(g_2\varphi - \varphi) - (g_1g_2\varphi - \varphi) + (g_1\varphi - \varphi)\\ &= g_1g_2\varphi - g_1\varphi - g_1g_2\varphi + \varphi + g_1\varphi - \varphi\\ &= 0\end{aligned}$$

Logo $(\partial^1 \circ \partial^0\varphi)(g_1, g_2) = 0$.

Agora mostramos para $n > 1$:

$(\partial^n \circ \partial^{n-1}\varphi)(g_1, ..., g_{n+1})$

$$
\begin{aligned}
&= g_1((\partial^{n-1}\varphi)(g_2, ..., g_{n+1}) + \sum_{r=1}^{n}(\partial^{n-1}\varphi)(-1)^r(g_1, ..., g_r g_{r+1}, ..., g_{n+1}) + (-1)^{n+1}(\partial^{n-1}\varphi)(g_1, ..., g_n) \\
&= \ g_1 g_2(\varphi(g_3, ..., g_{n+1})) + \sum_{r=2}^{n}(-1)^{r-1} g_1(\varphi(g_2, ..., g_r g_{r+1}, ..., g_{n+1})) + (-1)^n g_1(\varphi)(g_2, ..., g_n) \\
&\quad -(\partial^{n-1})(g_1, g_2, g_3, ..., g_n) + \sum_{r=2}^{n}(-1)^r(\partial^{n-1}\varphi)(g_1, ..., g_r g_{r+1}, ..., g_{n+1}) + (-1)^{n+1} g_1(\varphi(g_2, ..., g_n))) \\
&\quad +(-1)^{n+1}(-1)\varphi(g_1 g_2, g_3, ..., g_n) + (-1)^{n+1}\sum_{r=2}^{n}(-1)^r\varphi(g_1, ..., g_r g_{r+1}, ..., g_n) \\
&\quad +(-1)^{n+1}(-1)^n\varphi(g_1, ..., g_{n-1}) \\
&= \ g_1 g_2(\varphi(g_3, ..., g_{n+1})) + \sum_{r=2}^{n}(-1)^{r-1} g_1(\varphi(g_2, ..., g_r g_{r+1}, ..., g_{n+1})) + (-1)^n g_1(\varphi(g_2, ..., g_n)) \\
&\quad -g_1 g_2(\varphi(g_3, ..., g_{n+1})) + \varphi(g_1 g_2 g_3, g_4, ..., g_{n+1}) - \sum_{r=3}^{n}(-1)^{r+1}\varphi(g_2 g_2, ..., g_r g_{r+1}, ..., g_{n+1}) \\
&\quad -(-1)^n\varphi(g_1 g_2, g_3, ..., g_{n+1}) + \sum_{r=2}^{n}(-1)^r g_1(\varphi(g_2, ..., g_r g_{r+1}, ..., g_{n+1})) \\
&\quad +(-1)^2(-1)\varphi(g_1 g_2 g_3, g_4, ..., g_{n+1}) + \sum_{r=3}^{n}(-1)^r(-1)\varphi(g_1 g_2, ..., g_r g_{r+1}, ..., g_{n+1}) \\
&\quad + \sum_{r=2}^{n}(-1)^r \sum_{l=2}^{r-2}(-1)^l\varphi(g_1, ..., g_l g_{l+1}, ..., g_r g_{r+1}, ..., g_{n+1}) \\
&\quad + \sum_{r=3}^{n}(-1)^r(-1)^{r-1}\varphi(g_1, ..., g_{r-1} g_r g_{r+1}, ..., g_{n+1}) + \sum_{r=2}^{n-1}(-1)^r(-1)^r\varphi(g_1, ..., g_r g_{r+1} g_{r+2}, ..., g_{n+1}) \\
&\quad + \sum_{r=2}^{n-2}(-1)^r \sum_{l=r+1}^{n}(-1)^{l-1}\varphi(g_1, ..., g_r g_{r+1}, ..., g_l g_{l+1}, ..., g_{n+1}) \\
&\quad + \sum_{r=2}^{n-1}(-1)^r(-1)^n\varphi(g_1, ..., g_r g_{r+1}, ..., g_n) + (-1)^n(-1)^n\varphi(g_1, ..., g_{n+1}) \\
&\quad +(-1)^{n+1} g_1(\varphi(g_2, ..., g_n)) + (-1)^{n+1}(-1)^n\varphi(g_1 g_2, g_3, ..., g_n) \\
&\quad +(-1)^{n+1}\sum_{r=2}^{n-1}(-1)^r\varphi(g_1, ..., g_r g_{r+1}, ..., g_n) + (-1)^{n+1}(-1)^n\varphi(g_1, ..., g_{n-1})
\end{aligned}
$$

Observando esta última igualdade temos que os termos dois a dois se anulam e com isso temos a anulação da igualdade e assim $(\partial^n \circ \partial^{n-1}\varphi)(g_1, ..., g_{n+1}) = 0$. ■

Corolário 3.2.1. *Para todo $n \geq 1$ tem-se $Im(\partial^{n-1}) \subset Ker(\partial^n)$.*

Demonstração. Seja $\partial^{n-1}(\varphi) \in Im(\partial^{n-1})$, logo $\partial^n(\partial^{n-1}(\varphi)) = \partial^n \circ \partial^{n-1}(\varphi) = 0(\varphi) = 0$. ■

Definição 3.2.4. *Seja G um grupo profinito e A um G-módulo. Então definimos os conjuntos*

$$Z^n(G, A) := Ker(\partial^n),$$

chamado de ***grupo de*** n***-cociclos*** *e*

$$B^n(G,A) := Im(\partial^{n-1})$$

chamado de ***grupo de*** n***-cobordos*** *para* $n > 0$ *e para* $n = 0$ *definimos* $B^n(G,A) = 0$. *O grupo o quociente*

$$H^n(G,A) := \frac{Z^n(G,A)}{B^n(G,A)},$$

chamamos de n*-ésimo grupo de cohomologia.*

Observação 3.2.2. *Estes grupos de cohomologia são bem-definidos, pois os grupos de cociclos e cobordos são ambos abelianos e pela proposição* 3.2 $B^n(G,A) \leq Z^n(G,A)$*, para todo* $n \in \mathbb{N}$.

Vamos agora dar a definição de aplicações compatíveis:

Definição 3.2.5. *Sejam* G, G' *grupos profinitos e* $A \in D_G$ *e* $A' \in D_{G'}$. *Sejam* $\psi : A' \longrightarrow A$ *um homomorfismo de grupos topológicos e* $\varphi : G \longrightarrow G'$ *um homomorfismo de grupos profinitos, respectivamente. Dizemos que estes homomorfismos são* ***compatíveis*** *quando*

$$\psi(\varphi(g) \cdot a') = g \cdot \psi(a')$$

para todo $g \in G$ *e todo* $a' \in A'$.
Isso é equivalente a dizer que ψ *é uma* G*-aplicação, se* A' *é considerado como um* G*-módulo com a ação*

$$g \cdot a' = \varphi(g) \cdot a'$$

para cada $a' \in A'$ *e* $g \in G$.

Exemplo 3.2.1. *Sejam* L *e* E *duas extensões de Galois de um corpo* k*, com* $k \subset E \subset L$. *E considerando a aplicação de restrição* $\pi : Gal(L/k) \longrightarrow Gal(E/k)$*, e a aplicação injetiva* $i : E^\times \hookrightarrow L^\times$. *Então estas aplicações são compatíveis.*

3.2.1 Lema de Shapiro, Restrição e Corestrição

Nesta seção mencionamos algumas propriedades funtoriais dos grupos de cohomologia que precisaremos mais tarde, vide [9], seção 2.5:

Lembremos que G é um grupo profinito, ou seja, limite inverso de grupos finitos. Assim possui uma topologia induzida pela topologia discreta para cada um destes grupos finitos.

Seja H um subgrupo fechado de G, para esta topologia e A um H-módulo. Definimos o módulo induzido $A^* := M_H^G(A)$ como sendo o conjunto de todas as aplicações contínuas a^* de G em A de tal modo que $a^*(hx) = h \cdot a^*(x)$ se $h \in H$ e $x \in G$, fazendo com que o grupo G aja em $M_H^G(A)$ da seguinte forma:

$$(ga^*)(x) = a^*(xg).$$

Lema 3.2.2. *(Lema de Shapiro) Existe um isomorfismo canônico*

$$\begin{aligned} f : H^i(G, M_G^H(A)) &\xrightarrow{\sim} H^i(H, A) \\ \varphi &\longmapsto f(\varphi); \end{aligned}$$

onde $f(\varphi) : h \longmapsto \varphi(i(h))(1)$ *para todo* $i \geq 0$.

Demonstração. Ver [9] capitulo I.2.5. ■

Podemos definir um homomorfismo injetivo:

$$\begin{aligned} i : A &\longrightarrow M_G^H(A) \\ a &\longmapsto (x \longmapsto xa); \end{aligned}$$

Passando para os grupos de cohomologia obtemos homomorfismos, ditos de restrição:

$$res : H^n(G, A) \longrightarrow H^n(G, M_G^H(A)) \cong H^n(H, A).$$

Agora supomos que H é um subgrupo aberto de G e que A um G-módulo, definimos um G-homomorfismo sobrejetivo:

$$\begin{aligned} p : M_G^H(A) &\longrightarrow A \\ a^* &\longmapsto p(a^*) = \sum_{x \in G/H} x \cdot a^*(x^{-1}); \end{aligned}$$

Isto é bem definido, pois $x \cdot a^*(x^{-1})$ depende só da classe de x módulo H. Como acima, obtemos homomorfismos, ditos de corestrição, de grupos de cohomologia:

$$cor : H^n(H, A) \cong H^n(G, M_G^H(A)) \longrightarrow H^n(G, A).$$

Através de algumas verificações deste obtemos:

Proposição 3.2.3. *Seja G um grupo profinito e H um subgrupo de índice finito n e seja A um G-módulo, então a aplicação composta*

$$cor \circ res : H^i(G, A) \longrightarrow H^i(G, A)$$

é dada por multiplicação por n para todos $i \geq 0$.

Demonstração. Basta olhar para a composição $i \circ p : A \longrightarrow M_G^H(A) \longrightarrow A$:

$$a \longmapsto \begin{pmatrix} a^* : G \longrightarrow A \\ x \longmapsto xa \end{pmatrix} \longmapsto \sum_{x \in G/H} x \cdot a^*(x^{-1}) =$$

$$= \sum_{x \in G/H} x \cdot (x^{-1} \cdot a) = \sum_{x \in G/H} (x \cdot x^{-1})a = \sum_{x \in G/H} a = n \cdot a.$$

■

No caso de $H = \{1\}$, da proposição 3.2.3 nos fornece de imediato o seguinte resultado:

Corolário 3.2.2. *Seja G um grupo finito de ordem n, então, os elementos de $H^i(G, A)$ possuem ordem finita que divide n para todos os G-módulos A e inteiros $i > 0$.*

3.3 O caso não abeliano

Nesta seção consideramos o caso onde A não é abeliano. Se A é um grupo topológico (para topologia discreta), então é possível definir o conjunto H^1, porém a construção de conjuntos de cohomologia de graus superiores é mais complicada e não será abordada no nosso trabalho.

Definição 3.3.1. *Seja G um grupo multiplicativo e A um conjunto não vazio. Supomos que G age (à esquerda) sobre A, ou seja, que existe uma aplicação*

$$\begin{aligned} \phi : G \times A &\longrightarrow A \\ (g, a) &\longmapsto g \cdot a =: {}^g a \end{aligned}$$

satisfazendo, para todo $a \in A$, as condições:
(1) ${}^1a = a$, *onde* 1 *é o elemento neutro de* G
(2) ${}^{g_1}({}^{g_2}a) = {}^{(g_1 \cdot g_2)}a$ *para todos* $g_1, g_2 \in G$,
ou equivalentemente que há um homomorfismo de grupos

$$\begin{aligned} \varphi : G &\longrightarrow S(A) \\ g &\longmapsto \varphi(g) := A \longrightarrow A \\ & \qquad a \longmapsto \varphi_g(x) := g \cdot a = {}^g a, \end{aligned}$$

onde $S(A)$ é o grupo das bijeções de A. Neste caso, dizemos que G age sobre A e que A é um ***G-conjunto***.
Quando A for um grupo e se G-ação φ acima satisfaz adicionalmente as condições (1) *e* (2) *então dizemos que A é um G-grupo*

Provemos agora uma proposição que nos será útil no próximo capítulo.

Seja agora G um grupo e A um G-grupo. Uma aplicação $\phi : G \longrightarrow A$ contínua é dita um 1-cociclo de G com valores em A, quando para cada $g, h \in G$ temos que

$$\phi(gh) = \phi(g) \cdot {}^g\phi(h),$$

e chamaremos de $Z^1(G, A)$ o conjunto de todos os 1-cociclos de G com valores em A.

Agora sejam $\phi, \psi \in Z^1(G, A)$, dizemos que ϕ e ψ são cohomólogos, se existir $a \in A$ tal que

$$\phi(g) = a^{-1} \cdot \psi(g) \cdot {}^g a$$

para todo $g \in G$, então escrevemos que $\phi \sim \psi$.

Lema 3.3.1. *A relação de cohomologia descrita acima é uma relação de equivalência no conjunto $Z^1(G, A)$ de* 1*-cociclos.*

Demonstração. Temos que $\phi \sim \psi \Leftrightarrow \exists a \in A$ tal que $\phi(g) = a^{-1} \cdot \psi(g) \cdot {}^g a, \forall g, h \in G$.
Reflexividade:

Basta tomar $a = 1_A$, então $\phi(g) = (1_A)^{-1} \cdot \phi(g) \cdot {}^g(1_A) = 1_A \cdot \phi(g) \cdot 1_A = \phi(g) \therefore \phi \sim \phi$.
Simetria:
Se $\phi \sim \psi$ então existe $a \in A$ tal que $\phi(g) = a^{-1} \cdot \psi(g) \cdot {}^g a$, logo fazendo $b = a^{-1}$ temos

$$\psi(g) = b^{-1} \cdot \phi(g) \cdot {}^g b \therefore \psi \sim \phi.$$

Transitividade:
Se $\phi \sim \psi$ e $\psi \sim \omega$ então existem $a, b \in A$ tais que

$$\phi(g) = a^{-1} \cdot \psi(g) \cdot {}^g a \qquad (1)$$

$$\psi(g) = b^{-1} \cdot \omega(g) \cdot {}^g b \qquad (2)$$

Agora substituindo a (2) na (1) temos

$$\phi(g) = a^{-1} \cdot [b^{-1} \cdot \omega(g) \cdot {}^g b] \cdot {}^g a = (a^{-1}b^{-1}) \cdot \omega(g) \cdot ({}^g b \cdot {}^g a) = (ba)^{-1} \cdot \omega(g) \cdot {}^g(ba)$$

Agora tomando $c = ba$, temos que $\phi(g) = c^{-1} \cdot \omega(g) \cdot {}^g c \therefore \phi \sim \omega$. ■

Com a ajuda deste lema, podemos agora definir o primeiro grupo de cohomologia $H^1(G, A)$ como sendo o quociente do conjunto de todos os 1-cociclo $Z^1(G, A)$ por esta relação de equivalência, ou seja,

$$H^1(G, A) := Z^1(G, A)/\sim .$$

A função $\phi : G \longrightarrow A$ tal que $\phi(g) = 1_A$ para todo $g \in G$ é chamado de 1-cociclo trivial. Em particular $Z^1(G, A)$ não será vazio e como consequência $H^1(G, A)$ também não será.
Também não é difícil notar que o 1-cociclo $\phi : G \longrightarrow A$ é cohomologo ao 1-cociclo trivial se, e somente se, existir $a \in A$ tal que

$$\phi(g) = a^{-1} \cdot 1 \cdot {}^g a = a^{-1} \cdot {}^g a,$$

para todo $g \in G$. Todos os cociclos têm esta propriedade exatamente quando $H^1(G, A)$ for trivial. Este é um conjunto pontuado, isto é, um conjunto munido de um elemento distinguido, dito também ponto base. No caso de $H^1(G, A)$ este elemento é a classe do cociclo trivial.

Observação 3.3.1. *Seja G for um grupo de ordem n e se os elementos de $H^i(G, A)$ forem de ordem finita, temos que a ordem de cada elemento de $H^i(G, A)$ divide n para todos os G-módulos A e inteiros $i > 0$.*

Agora mostramos como podemos obter sequências exatas de conjuntos de cohomologia não abeliana a partir de sequências exatas curtas de grupos:

Proposição 3.3.1. *Seja G um grupo e supomos que temos uma sequência exata de G-grupos:*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

onde B e C não são necessariamente comutativos, mas A é comutativo e contido no centro de B. Então temos uma sequência exata de conjuntos pontuados

$$1 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta_0} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \xrightarrow{\delta_1} H^2(G, A)$$

Demonstração. Nós seguimos de perto aqui as provas das proposições 2.7.1. e 4.4.1 de [6]. A exatidão nos termos A^G, B^G e $H^1(G, B)$ é trivial. Precisamos construir o morfismo $\delta_0 : C^G \longrightarrow H^1(G, A)$, mostrar a exatidão em C^G e $H^1(G, A)$ e construir o morfismo $\delta_1 : H^1(G, C) \longrightarrow H^2(G, A)$ e mostrar a exatidão em $H^1(G, C)$. Seja $c \in C^G$, podemos definir δ_0, ao tomar uma pré-imagem $b \in B$ através da aplicação sobrejetiva $B \longrightarrow C$. Agora para todo $\sigma \in G$ o elemento $b\sigma(b^{-1})$ é enviado a 1 em C, pois $c = \sigma(c)$ que pertence a A por hipótese. Através de alguns cálculos verificamos que a aplicação $\sigma \longrightarrow b\sigma(b^{-1})$ é um 1-cociclo e que ao modificar b por um elemento de A produz um cociclo equivalente. Assim podemos afirmar que δ_0 é bem definida, e com isso podemos enviar elementos com origem em B^G para 1. A relação $\delta_0(c) = 1$ significa por definição que $b\sigma(b^{-1}) = a^{-1}\sigma(a)$ para algum $a \in A$, logo c possui como pré-imagem ab em B, que é um elemento G-invariante. Assim, temos a exatidão na sequência no termo C^G. A composição $C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B)$ é o morfismo trivial por construção. Finalmente um cociclo $\sigma \longrightarrow {}^\sigma a$ com valores em A sendo trivial em $H^1(G, B)$ significa que ${}^\sigma a = b^{-1}\sigma(b)$, para algum $b \in B$, e modificando $\sigma \longrightarrow {}^\sigma a$ por um A-cobordo podemos escolher um b de modo que sua imagem c em C seja fixa por G, e então $\delta_0(c) = [\sigma \longrightarrow {}^\sigma a]$. Observamos também que a classe de cohomologia $\sigma \longrightarrow {}^\sigma a$ depende apenas de c. Temos então a exatidão em $H^1(G, A)$.

Construiremos agora δ_1 e mostraremos a exatidão em $H^1(G, C)$. Seja $c : G \longrightarrow C$ um 1-

cociclo. Para cada $\sigma \in G$, escolha uma pré-imagem ${}^{\sigma}b \in B$ de ${}^{\sigma}c$ sob ψ. Seja c um cociclo, ${}^{\sigma}b \cdot ({}^{\sigma} \cdot {}^{\tau}b) \cdot {}^{\sigma\tau}b^{-1}$ está no núcleo de ψ para cada $\sigma, \tau \in G$. Portanto, existe um único ${}^{\sigma\tau}a \in A$ tal que ${}^{\sigma\tau}a = {}^{\sigma}b \cdot ({}^{\sigma} \cdot {}^{\tau}b) \cdot {}^{\sigma\tau}b^{-1}$. Assim, podemos definir uma aplicação

$$\begin{aligned} a = \delta_1(c) : G \times G &\longrightarrow A \\ (\sigma, \tau) &\longmapsto {}^{\sigma\tau}a. \end{aligned}$$

Para mostrar que a é um 2-cociclo, mostraremos que

$${}^{\sigma}({}^{\tau,\eta}a) \cdot {}^{\sigma\tau,\eta}a^{-1} = {}^{\sigma,\tau\eta}a \cdot {}^{\sigma,\eta}a^{-1} = 1.$$

Usando a definição de a e o fato de que A é abeliano temos a igualdade. Similarmente, podemos mostrar que δ_1 passa para o quociente de uma aplicação $\delta_1 : H^1(G, C) \longrightarrow H^2(G, A)$ e que sua definição não depende da pré-imagem ${}^{\sigma}b$ de ${}^{\sigma}c$.
Agora, se $c \in Im\psi_*$, então a aplicação $b : G \longrightarrow B$ é um 1-cociclo, isto implica que ${}^{\sigma,\tau}a = 1$ para cada $\sigma, \tau \in G$. E com isso podemos supor que $c \in Ker(\delta)$ o que nos fornece a existência de uma aplicação $g : G \longrightarrow A$ tal que

$${}^{\sigma}b \cdot ({}^{\sigma}. {}^{\tau}b) \cdot {}^{\sigma\tau}b^{-1} = \sigma(g(\tau)) \cdot g \cdot (\sigma\tau)^{-1} \cdot g(\sigma).$$

Agora vamos definir também $\widetilde{b} : G \longrightarrow B$ como sendo ${}^{\sigma}\widetilde{b} = {}^{\sigma}b \cdot g(\sigma)^{-1}$. E com isso temos de imediato que $\widetilde{b}$ é um 1-cociclo e que $\psi_*(\widetilde{b}) = b$. Portanto, temos que $Im\psi_* = Ker\delta$, logo temos a exatidão. ■

O Teorema 90 de Hilbert o qual iremos demonstrar descreve esse conjunto de cohomologia em uma situação muito especial. Iremos considerar uma extensão de corpos K/k finita Galoisiana, onde $G = Gal(K/k)$ é um grupo de Galois. Para cada $g \in G$ e cada $x \in K$ escrevemos $g \cdot x = g(x) = {}^{g}x$. Obtendo assim uma ação

$$\begin{aligned} G \times K^{\times} &\longrightarrow K^{\times} \\ (g, x) &\longmapsto g \cdot x = {}^{g}x. \end{aligned}$$

de G sobre o grupo multiplicativo $K^{\times}$.

Teorema 3.3.1. *(Teorema 90 de Hilbert)*

Seja K/k uma extensão finita Galoisiana de grupos de Galois $G = Gal(K/k)$, então temos que $H^1(G, K^\times) = 1$.

Demonstração. Seja $\phi : G \longrightarrow K^\times$ um 1-cociclo. Cada elemento de G define um caractere $K^\times \longrightarrow K^\times$. Do teorema de Dedekind sobre a independência linear de caracteres temos que G, visto como sendo um subconjunto do K-espaço vetorial de todas as funções $K^\times \longrightarrow K$, é linearmente independente. Em particular, uma combinação linear $\sigma = \sum_{g\in G} \phi(g)g$ é um elemento não nulo desse espaço vetorial, então existe $x \in K^\times$ tal que $\sigma(x) \neq 0$. Pondo $y = \sigma(x) \in K^\times$.
Agora seja $g \in G$, temos

$$^g y = {}^g(\sum_{h\in G} \phi(h) \cdot {}^h x) = \sum_{h\in G} {}^g\phi(h) \cdot {}^{gh}x$$

e, como ϕ é um 1-cociclo, temos

$$^g y = \sum_{h\in G} \phi(g)^{-1} \cdot \phi(gh) \cdot {}^{gh}x = \phi(g)^{-1} \cdot y$$

e assim $^g y = \phi(g)^{-1} \cdot y \Rightarrow \phi(g) = y \cdot {}^g y^{-1}$, e com isso temos que ϕ é cohomologo ao 1-cociclo trivial. ■

Olhando para o corolário 2.3.3 e 2.4.1 podemos enunciar teorema 90 de Hilbert da seguinte forma: Seja K/k uma extensão finita Galoisiana de grupos de Galois $G = Gal(K/k)$ e $n > 0$, então temos que $H^1(G, GL_n(K)) = 1$.

Capítulo 4

O Grupo de Brauer Cohomológico

Agora voltamos ao grupo de Brauer, munidos das técnicas cohomológicas do último capítulo. Fixamos neste capítulo um corpo k de característica arbitrária. A referência principal para este capítulo é [6].

4.1 As álgebras simples centrais classificadas por H^1

Fixamos nesta seção uma extensão galoisiana finita K/k e um fecho separável k_s de k que contém K e escrevemos $G = Gal(K/k)$ e $G_s = Gal(k_s/k)$. Denotamos $ASC_k(n)$ o conjunto das k-álgebras simples centrais de grau n a menos k-isomorfismo.

4.1.1 A Descida de Galois

Lema 4.1.1. *A aplicação*

$$\begin{aligned} \varphi : Hom_k(k, V) &\longrightarrow V \\ f &\longmapsto f(1); \end{aligned}$$

é um isomorfismo, onde k é corpo e V um espaço vetorial.

Demonstração. (I) Boa definição:

φ é claramente bem definida, pois f é bem definida.

(II) Homomorfismo:

Sejam $f, g \in Hom_k(k, V)$, temos que $\varphi(f) = f(1) = u$ e $\varphi(g) = g(1) = v$ para alguns $u, v \in V$.

Então:

$$\varphi(f+g) = (f+g)(1) = f(1) + g(1) = u + v = \varphi(f) + \varphi(g) \therefore \varphi(f+g) = \varphi(f) + \varphi(g)$$

$$\varphi(\lambda f) = (\lambda f)(1) = \lambda f(1) = \lambda u = \lambda\varphi(f) \therefore \varphi(\lambda f) = \lambda\varphi(f)$$

onde $\lambda \in k$.

Assim, φ é um homomorfismo.

(III) Injetividade:

Sejam $f, g \in Hom_k(k, V)$ tais que $f(1) = g(1)$, então:

$$f(x) = f(1 \cdot x) = xf(1) = xg(1) = g(1 \cdot x) = g(x)$$

logo,$f(x) = g(x), \forall x \in k$ por tanto φ é injetiva.

(IV) Sobrejetividade:

Seja $v \in V$, podemos definir uma aplicação linear

$$\begin{aligned} f : k &\longrightarrow V \\ 1 &\longmapsto v; \end{aligned}$$

que implica em $\varphi(f) = f(1) = v$.

Logo φ é sobrejetiva.

Assim provamos que φ é um isomorfismo ■

Teorema 4.1.1. *$Hom_k(V, k) \otimes_k W \cong Hom_k(V, W)$ para todos k-espaços vetoriais V, W.*

Demonstração. Usando o lema anterior temos que $Hom_k(V,k) \otimes_k W \cong Hom_k(V,k) \otimes_k Hom_k(k,W)$, assim: $Hom_k(V,k) \otimes_k W \cong Hom_k(V,k) \otimes_k Hom_k(k,W) \cong Hom_k(V \otimes_k k, k \otimes_k W) \cong Hom_k(V \otimes_k k, W \otimes_k k) \cong Hom_k(V,W)$. ■

Definição 4.1.1. *Seja V um espaço vetorial munido de um tensor do tipo (p,q), definimos esse tensor como um elemento do produto tensorial $V^{\otimes_p} \otimes_k (V^*)^{\otimes q}$, onde $p, q \geq 0$ são números*

inteiros e que $V^{\otimes_p} \otimes_k (V^*)^{\otimes q} \cong Hom_k(V^{\otimes_q}, V^{\otimes_p})$ *provém do teorema anterior e* V^* *é o espaço dual* $Hom_k(V, k)$.

O par ordenado (V, Φ) de k-espaços vetoriais munido com o produto definido acima é chamado de k-objeto.
Sejam (V, Φ) e (W, Ψ) dois tensores do tipo (p, q) e seja $f : V \longrightarrow W$ uma transformação linear. Então se considerarmos Φ e Ψ como aplicações multi-lineares, podemos definir as aplicações $f \circ \Phi$ e $\Psi \circ f$ por composições por f em cada fator V.

Definição 4.1.2. *Sejam* (V, Φ) *e* (W, Ψ) *dois tensores do tipo* (p, q). *Um morfismo que leva* (V, Φ) *para* (W, Ψ) *é uma aplicação* k*-linear* $f : V \longrightarrow W$ *tal que* $f \circ \Phi = \Psi \circ f$.

Se $f : V \xrightarrow{\sim} W$ é um isomorfismo, e $(f^*)^{-1} : V^* \xrightarrow{\sim} W^*$ um isomorfismo canônico induzido por f. Então, a condição $f \circ \Phi = \Psi \circ f$ nos faz obter

$$f^{\otimes_p} \otimes_k [(f^*)^{-1}]^{\otimes_q} : V^{\otimes_p} \otimes_k (V^*)^{\otimes_q} \xrightarrow{\sim} W^{\otimes_p} \otimes_k (W^*)^{\otimes_q} \tag{4.1}$$

tal que $f^{\otimes_p} \otimes_k [(f^*)^{-1}]^{\otimes_q}(\Phi) = \Psi$. Onde Φ é visto como elemento de $Hom_k(V^{\otimes_q}, V^{\otimes_p})$ e Ψ como elemento de $Hom_k(W^{\otimes_q}, W^{\otimes_p})$.

Exemplo 4.1.1. *Agora daremos alguns exemplos deste tipo de tensor.*

(a) O caso trivial $\Phi = 0$ *para todos* p, q, *assim* $\Phi \in V^{\otimes_0} \otimes_k (V^*)^{\otimes_0} \cong Hom_k(V^{\otimes_0}, V^{\otimes_0})$ *que implica* $\Phi \in k \otimes_k k \cong Hom_k(k, k)$ *e neste caso temos que* Φ *não possui nenhuma estrutura adicional.*

(b) $p = 1, q = 1$ *e neste caso* $\Phi \in V^{\otimes_1} \otimes_k (V^*)^{\otimes_1} \cong Hom_k(V^{\otimes_1}, V^{\otimes_1})$ *no qual implica que* $\Phi \in V \otimes_k (V^*) \cong Hom_k(V, V)$ *logo* Φ *é do tipo* $V \longrightarrow V$, *ou seja um endomorfismo linear de* V.

(c) $p = 0, q = 2$. *temos* $\Phi \in V^{\otimes_0} \otimes_k (V^*)^{\otimes_2} \cong Hom_k(V^{\otimes_2}, V^{\otimes_0})$ *que implica que o tensor* $\Phi \in k \otimes_k (V^* \otimes_k V^*) \cong Hom_k(V \otimes_k V, k)$, *e assim* Φ *é do tipo* $V \otimes_k V \longrightarrow k$.

(d) $p = 1, q = 2$. *Temos* $\Phi \in V^{\otimes_1} \otimes_k (V^*)^{\otimes_2} \cong Hom_k(V^{\otimes_2}, V^{\otimes_1})$ *que implica que o tensor* $\Phi \in V \otimes_k (V^*)^{\otimes_2} \cong Hom_k(V \otimes_k V, V)$ *e com isso* Φ *é do tipo* $V \otimes_k V \longrightarrow V$ *linear.*

Seja K/k uma extensão finita e G o grupo de Galois. Denotaremos por V_K o K-espaço vetorial $V \otimes_k K$ e por Φ_K o tensor $\Phi \otimes_k id_K$ induzido sobre V_K por Φ. Desta forma podemos associar (V, Φ) com o K-objeto (V_K, Φ_K). Além disso, denotaremos por $Aut_K(\Phi)$ o conjunto de automorfismos de (V_K, Φ_K).

Definição 4.1.3. *Seja (W, Ψ) um tensor do tipo (p, q). Nós dizemos que o tensor (W, Ψ) é uma K/k-forma torcida de (V, Φ) se $(V_K, \Phi_K) \cong (W_K, \Psi_K)$, ou seja, quando existir $f : V \xrightarrow{\sim} W$ tal que a aplicação 4.1 é induzida por este isomorfismo. Denotamos por $TF_K(V, \Phi)$, o conjunto de todas as formas torcidas de (V, Φ). Este é um conjunto pontuado com o seu ponto de base sendo as classes de (V, Φ).*

Como antes, consideremos uma extensão de Galois K/k com o grupo G de Galois, ela também nos permite classificar os k-isomorfismos das classes torcidas. Dado o k-automorfismo $\sigma : K \longrightarrow K$ que leva $\sigma(\lambda)$ em $\lambda \in K$, e fazendo o produto de tensor por V, através da aplicação $id_V : V \longrightarrow V$, obtemos assim $id_V \otimes_K \sigma : V \otimes_k K \longrightarrow V \otimes_k K$ que é um k-automorfismo $V_K \longrightarrow V_K$ que por abuso de notação chamaremos novamente por σ, consideremos agora um k-espaço vetorial de dimensão finita V e um tensor Φ em V. Iremos mostrar que existe uma bijeção de conjunto pontuados entre $TF_K(V, \Phi)$ e $H^1(G, Aut_K(\Phi))$. Cada aplicação K-linear $f : V_K \longrightarrow W_K$ induz a aplicação $\sigma(f) : V_K \longrightarrow V_K$ em $Aut_K(\Phi)$ através da G-ação:

$$\begin{aligned} G \times Aut_K(\Phi) &\longrightarrow Aut_K(\Phi) \\ (\sigma, f) &\longmapsto \sigma(f) = (id_V \otimes \sigma) \circ f \circ (id_V \times \sigma^{-1}) = \sigma \circ f \circ \sigma^{-1}; \end{aligned}$$

onde esta ação é compatível com a estrutura de grupo em $Aut_K(\Phi)$.

Observação 4.1.1. *Se f é um isomorfismo então $\sigma(f)$ também será.*

Seja (W, Ψ) uma K/k-forma torcida de (V, Φ), sabemos que existe um K-isomorfismo $f : V_K \longrightarrow W_K$ que envia Φ para Ψ. Associamos a esta K/k-forma torcida (W, Ψ) e o K-isomorfismo $g : (V_K, \Phi_K) \longrightarrow (W_K, \Psi_K)$ o seguinte 1-cociclo:

$$\begin{aligned} a : G &\longrightarrow Aut_K(\Phi) \\ \sigma &\longmapsto {}^{\sigma}a = g^{-1} \circ \sigma(g); \end{aligned}$$

Não é difícil ver que as classes do cociclo a em $H^1(G, Aut_K(\Phi))$ não depende da escolha do isomorfismo f. Esta aplicação satisfaz a relação fundamental ${}^{\sigma\tau}a = {}^{\sigma}a \cdot \sigma({}^{\tau}a)$ para todos $\sigma, \tau \in G$. Observando os cálculos temos ${}^{\sigma\tau}a = g^{-1} \circ \sigma(\tau(g)) = g^{-1} \circ \sigma(g) \circ \sigma(g^{-1}) \circ \sigma(\tau(g)) = {}^{\sigma}a \cdot \sigma({}^{\tau}a)$, onde assim nos fornece esta relação fundamental.

Agora seja outro K-isomorfismo $h : (V_K, \Phi_K) \tilde{\longrightarrow} (W_K, \Psi_K)$ definido por ${}^{\sigma}b := h^{-1} \circ \sigma(h)$ onde $\sigma \in G$. Então ${}^{\sigma}a$ e ${}^{\sigma}b$ estão relacionados por ${}^{\sigma}a = c^{-1} \cdot {}^{\sigma}b \cdot (\sigma(c))$, em que c é o K-automorfismo $h^{-1} \circ g$. Neste caso temos uma representação de um grupo de cohomologia que estudamos no final capitulo anterior e assim observamos que temos um caso de conjunto pontuado.

Para este caso em que estamos estudando, veremos que a classe $[{}^{\sigma}a]$ de $H^1(G, Aut_K(\Phi))$ de 1-cociclo ${}^{\sigma}a$ associado ao K-isomorfismo $g : (V_k, \Phi_K) \tilde{\longrightarrow} (W_K, \Psi_K)$ depende somente de (W_K, Ψ_K) e não da aplicação g.

Teorema 4.1.2. *Para um k-objeto (V, Φ) vamos considerar o conjunto pontuado $TF_K(V, \Phi)$ da (K/k)-forma torcida de (V, Φ) , com ponto de base dado por (V, Φ). Assim, a aplicação $(W, \Psi) \longrightarrow [a_\sigma]$ produz uma bijeção $\theta : TF_K(V, \Phi) \leftrightarrow H^1(G, Aut_K\Phi)$ que preserva ponto de base.*

Demonstração. Vamos provar que θ é uma bijeção, assim:

Injetiva:

Tomemos (W_1, Ψ_1) e (W_2, Ψ_2) duas formas torcidas com a mesma imagem por θ, e sejam $g_i : V \otimes_K K \longrightarrow W_i \otimes_k K$ os isomorfismos correspondentes. Poemos supor sem perda de generalidade que g_1 e g_2 geram o mesmo cociclo, ou seja

$$g_1^{-1}\sigma(g_1) = g_2^{-1}\sigma(g_2) \Rightarrow \sigma(g_2 g_1^{-1}) = g_2 g_1^{-1}$$

para todo $\sigma \in G$. Assim $g = g_2 g_1^{-1}$ é um K-isomorfismo entre (W_1, Ψ_1) e (W_2, Ψ_2), logo θ é injetora.

Sobrejetiva:

Seja $\phi : G \longrightarrow Aut_K(\Phi)$ um 1-cociclo, pelo teorema 90 de Hilbert (na sua observação, posta no capitulo anterior), temos que $Aut_K(\Phi) \subset GL_n(K)$, assim existe $f \in GL_n(K)$ tal que ${}^{\sigma}\phi = f^{-1} \cdot {}^{\sigma}\phi(f)$.

Definamos agora $\Psi = f(\Phi)$, cujo tal tensor pode sem problemas ser definido sobre K da

seguinte forma: para todo $\sigma \in G$ temos

$$\sigma(\Psi) = \sigma(f(\Phi)) = \sigma(f)\sigma(\Phi) = \sigma(g)\Phi = f\,{}^{\sigma}\phi(\Phi) = f(\Phi) = \Psi$$

(note que Φ está definido sobre K e que ${}^{\sigma}\phi(\Phi) = \Phi$ pois, ${}^{\sigma}\phi \in Aut_K(\Phi)$).
Assim (V, Φ) tem uma imagem dado pelo cociclo ϕ_σ.
Logo, $\theta(TF_K(V,\Phi)) \supset H^1(G, Aut_K(\Phi))$, assim, θ é sobrejetiva. Logo $TF_K(V,\Phi)) \cong H^1(G, Aut_K(\Phi))$.

■

Agora iremos mostrar que as álgebras simples centrais podem ser classificadas por um conjunto de cohomologia. Para isso vamos demonstrar o teorema de Skolem-Noether, que é uma generalização da Proposição 2.4.1 do capitulo 2:

Teorema 4.1.3. *Todos os automorfismos de uma k-álgebra simples central são internos, ou seja, são dados por conjugação por um elemento inversível.*

Demonstração. Seja A uma k-álgebra simples central de grau n, K uma extensão finita de Galois que cinde A e seja $A^\times$ o subgrupo dos elementos inversíveis de A. Usando a Proposição 2.4.1 obtemos uma sequência exata curta

$$1 \longrightarrow K^\times \longrightarrow (A \otimes_k K)^\times \longrightarrow Aut_K(A \otimes_k K) \longrightarrow 1$$

de grupos munidos com uma G-ação, onde a segunda aplicação leva um elemento inversível para o automorfismo interno. A Proposição 3.3.1 produz então uma sequência exata

$$1 \longrightarrow H^0(G, K^\times) \longrightarrow H^0(G, (A \otimes_k K)^\times) \longrightarrow H^0(G, Aut_K(A \otimes_k K)) \longrightarrow H^1(G, K^\times),$$

isto é

$$1 \longrightarrow (K^\times)^G \longrightarrow ((A \otimes_k K)^\times)^G \longrightarrow (Aut_K(A \otimes_k K))^G \longrightarrow H^1(G, K^\times),$$

e assim,

$$1 \longrightarrow k^\times \longrightarrow A^\times \longrightarrow Aut_k(A) \longrightarrow H^1(G, K^\times),$$

pois nós temos $(K^\times)^G = k^\times$ ($k^\times$ é o grupo invariante de $K^\times$ pela ação do grupo de Galois G sobre K), de modo análogo temos $((A \otimes_k K)^\times)^G = A^\times$ e $(Aut_K(A \otimes_k K))^G = Aut_k(A)$.

Pelo teorema 90 de Hilbert $H^1(G, K^\times)$ é trivial, e com isso obtemos uma sequência exata

$$1 \longrightarrow k^\times \longrightarrow A^\times \longrightarrow Aut_k(A) \longrightarrow 1,$$

e verificamos que temos um homomorfismo de grupos sobrejetivo $A^\times \longrightarrow Aut_k(A)$, isto é, todo k-automorfismo de A é um automorfismo interno. ■

Exemplo 4.1.2. *Da descida de Galois temos que $ASC_k(n) \leftrightarrow H^1(G_s, PGL_n(k_s))$ é uma bijeção de conjuntos pontuados.*

Demonstração. Seja A uma álgebra simples central de grau n sobre k. Temos um isomorfismo

$$\beta : A \otimes_k k_s \longrightarrow M_n(k) \otimes_k k_s,$$

e com isso podemos definir um cociclo

$$u : G_s \longrightarrow PGL_n(k_s) = Aut(M_n(k_s)) = Aut(M_n(k) \otimes_k k_s)$$

$$t \longmapsto {}^t u$$

pela equação:

$${}^t u = \beta \circ (id_A \otimes t) \circ \beta^{-1} \circ (id_{M_n(k)} \otimes t^{-1}),$$

Verificamos que est cociclo não depende da escolha do isomorfismo β. Assim obtemos uma função

$$\varphi : ASC_k(n) \longrightarrow H^1(G_s, PGL_n(k_s))$$

$$[A] \mapsto (t \mapsto {}^t u),$$

onde $[A]$ representa a classe de equivalência de A, módulo k-isomorfismo.
Inversamente, seja $(t \mapsto {}^t v) \in Z^1(G_s, PGL_n(k_s))$. Definimos

$$A' = \{x \in M_n(k) \otimes_k k_s \mid {}^t v \circ (id_{M_n(k)} \otimes t)(x) = x, \forall t \in G_s\},$$

e obtemos assim uma função

$$\psi : H^1(G_s, PGL_n(k_s)) \longrightarrow ASC_k(n)$$

$$(t \mapsto {}^t v) \mapsto [A'].$$

Para verificar que $\psi \circ \varphi = id$, supomos que $\psi(\varphi([A])) = \psi({}^t u) = [A']$. Então, por construção:

$$A' = \{x \in M_n(k) \otimes_k k_s \mid {}^t u(x) = x, \forall t \in G_s\}.$$

Logo, claramente $A \simeq A'$. A verificação que $\varphi \circ \psi = id$ é análoga. ■

Para recuperar agora o grupo de Brauer como grupo de cohomologia, teremos que nos livrar da dependência de n. Lembramos que K/k é uma extensão galoisiana finita e denotamos por $ASC_{K/k}(n)$ o conjunto das álgebras simples centrais trivializados pela extensão K/k, a menos k-isomorfismo. Nós gostaríamos de compreender a união $\bigcup_{n\in\mathbb{N}} ASC_{K/k}(n)$ e identificar ela com um conjunto de cohomologia. Sejam então n, m inteiros positivos, e definimos primeiro

$$\begin{aligned} \mu_{nm} : ASC_{K/k}(n) &\longrightarrow ASC_{K/k}(nm) \\ A &\longmapsto A \otimes_k M_m(k). \end{aligned}$$

Agora, suponha que $a : G \longrightarrow PGL_n(K)$ seja um 1-cociclo. Para cada $\sigma \in G$, obtemos uma matriz ${}^\sigma a$ e podemos definir uma matriz ${}^\sigma b \in M_{nm}(K)$ (módulo $K^\times$), colocando n vezes ${}^\sigma a$ ao longo da diagonal e zeros nas posições que estão fora desta diagonal, ou seja

$${}^\sigma b = \begin{pmatrix} {}^\sigma a & 0 & \cdots & 0 & 0 \\ 0 & {}^\sigma a & \cdots & 0 & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & {}^\sigma a & 0 \\ 0 & 0 & \cdots & 0 & {}^\sigma a \end{pmatrix}.$$

Pode-se verificar que isso dá origem a uma aplicação de conjuntos pontuados

$$\begin{aligned} \lambda_{nm} : H^1(G, PGL_n(K)) &\longrightarrow H^1(G, PGL_{nm}(K)) \\ [{}^\sigma a] &\longmapsto [{}^\sigma b]. \end{aligned}$$

Agora, consideremos as aplicações $\theta_m : ASC_{K/k}(m) \longrightarrow H^1(G, PGL_m(K))$ definidas de maneira análoga à aplicação da prova da proposição 4.1.2. Consideremos para todos inteiros positivos n e m, o diagrama:

$$\begin{array}{ccc} ASC_{K/k}(m) & \xrightarrow{\theta_m} & H^1(G, PGL_m(K)) \\ \downarrow{\scriptstyle \mu_{nm}} & & \downarrow{\scriptstyle \lambda_{nm}} \\ ASC_{K/k}(nm) & \xrightarrow{\theta_{nm}} & H^1(G, PGL_{nm}(K)) \end{array} .$$

Não é difícil verificar que este diagrama é comutativo, ou seja: $\theta_{nm} \circ \mu_{nm}(A) = \lambda_{nm} \circ \theta_m(A)$ para alguma k-álgebra simples central cindida pela extensão K/k. Portanto, obtemos uma aplicação

$$\theta : \bigcup_{m\in\mathbb{N}} ASC_{K/k}(m) \longrightarrow \bigcup_{m\in\mathbb{N}} H^1(G, PGL_m(K)).$$

onde as reuniões são construídas baseadas nas inclusões μ_{mn} e λ_{mn}. Definimos:

$$H^1(G, PGL_\infty(K)) := \bigcup_{m\in\mathbb{N}} H^1(G, PGL_m(K)).$$

Agora, gostaríamos de dotar $H^1(G, PGL_\infty(K))$ com uma estrutura de grupo. Sejam $n, m \in \mathbb{N}$, definimos a aplicação:

$$\begin{aligned} End(K^n) \times End(K^m) &\longrightarrow End(K^n \otimes K^m) \\ (\varphi, \psi) &\longmapsto \varphi \otimes \psi. \end{aligned}$$

Através da escolha de uma base, esta aplicação restringe e circunscreve uma aplicação de

$$GL_n(K) \times GL_m(K) \longrightarrow GL_{nm}(K).$$

Além disso, uma vez que um par de matrizes escalares é enviada para uma matriz escalar, temos $PGL_n(K) \times PGL_m(K) \longrightarrow PGL_{nm}(K)$. Finalmente, obtemos uma aplicação bem definida

$$\begin{aligned} H^1(G, PGL_n(K)) \times H^1(G, PGL_m(K)) &\longrightarrow H^1(G, PGL_{nm}(K)) \\ ([{}^\sigma a], [{}^\sigma b]) &\longmapsto [{}^\sigma a \otimes {}^\sigma b]. \end{aligned}$$

Por outro lado, temos uma operação binária

$$\begin{aligned} ASC_{K/k}(n) \times ASC_{K/k}(m) &\longrightarrow ASC_{K/k}(nm) \\ (A, B) &\longmapsto A \otimes_k B. \end{aligned}$$

É fácil verificar se essas duas leis são compatíveis com as aplicações $\lambda_{nm}, \lambda_{mn}, \mu_{mn}, \mu_{mn}$. Portanto temos o seguinte resultado:

Proposição 4.1.1. *Temos os seguintes isomorfismos de grupos:*

$$Br(K/k) \cong \bigcup_{m\in\mathbb{N}} H^1(G, PGL_n(K)) = H^1(G, PGL_\infty(K)).$$

e

$$Br(k) \cong \bigcup_{m\in\mathbb{N}} H^1(G_s, PGL_n(k_s)) = H^1(G_s, PGL_\infty(k_s)).$$

4.2 O Grupo de Brauer como um H^2

Agora vamos identificar o grupo de Brauer com um segundo grupo de cohomologia. Fixamos nesta seção também uma extensão galoisiana finita K/k e um fecho separável k_s de k que contém K. Escrevemos $G = Gal(K/k)$ e $G_s = Gal(k_s/k)$.

Teorema 4.2.1. *$Br(K/k) \cong H^2(G, K^\times)$ e $Br(k) \cong H^2(G_s, k_s^\times)$.*

Demonstração. Primeiro, consideremos a sequência exata

$$1 \longrightarrow K^\times \longrightarrow GL_n(K) \longrightarrow PGL_n(K) \longrightarrow 1$$

Agora usando o teorema 90 de Hilbert e a proposição 3.3.1, temos uma sequência exata:

$$1 \longrightarrow H^1(G, PGL_n(K)) \xrightarrow{\delta_n} H^2(G, K^\times) \tag{4.2}$$

que dá origem ao seguinte diagrama:

$$\begin{array}{ccccc} ASC_K(n) & \xrightarrow{\theta_m} & H^1(G, PGL_m(K)) & \xrightarrow{\delta_m} & H^2(G, K^\times) \\ \downarrow{\scriptstyle \mu_{nm}} & & \downarrow{\scriptstyle \lambda_{mn}} & \nearrow{\scriptstyle \delta_{mn}} & \\ ASC_K(nm) & \xrightarrow{\theta_{mn}} & H^1(G, PGL_{nm}(K)) & & \end{array}$$

Para ver que $\delta_{mn} \circ \lambda_{mn} = \partial_m$, consideremos um representante de

$$\begin{aligned} c : G &\longrightarrow PGL_m(K) \\ x &\longmapsto c_x \end{aligned}$$

de uma classe em $H^1(G, PGL_m(K))$. Lembre-se que um representante a do elemento $\delta_m(c)$ pode ser escrito como ${}^{\sigma,\tau}a = {}^{\sigma}b \cdot \sigma({}^{\tau}b) \cdot {}^{\sigma\tau}b^{-1}$, onde b_x é a pré-imagem de c_x sob a projeção canônica $\pi : GL_m(K) \longrightarrow PGL_m(K)$. Agora seja $c' = \lambda_{mn}(c)$. Um representa a' do elemento $\delta_{mn}(c')$ então é ${}^{\sigma,\tau}a' = {}^{\sigma}b' \cdot \sigma({}^{\tau}b') \cdot {}^{\sigma\tau}(b')^{-1}$, onde ${}^{\sigma}b'$ é simplesmente n cópias de ${}^{\sigma}b$ ao longo da diagonal pois ${}^{\sigma}c'$ é n cópias de ${}^{\sigma}c$ ao longo da diagonal. Portanto, temos $\delta_m(c) = \delta_{nm} \circ \delta_{mn}(c)$. E sendo assim, podemos passar para o limite e obter um morfismo de grupos

$$\delta : H^1(G, PGL_\infty(K)) \longrightarrow H^2(G, K^\times).$$

Agora falta provar que este morfismo é um isomorfismo. Passando a equação (4.2) para o limite vai nos mostrar que δ é injetivo. Para ver que δ é sobrejetivo, mostraremos que δ_n é sobrejetivo, onde $n = [K : k]$. Seja $a : G \times G \longrightarrow K^\times$ o representante de uma classe em $H^2(G, K^\times)$ e seja V o K-espaço vetorial de dimensão n de base $\{e_\sigma | \sigma \in G\}$. Definimos n automorfismos de V da forma seguinte:

$$\begin{aligned} b_\sigma : V &\longrightarrow V \\ e_\tau &\longmapsto a_{\sigma,\tau} \cdot e_{\sigma\tau}. \end{aligned}$$

queremos mostrar que $a_{\sigma,\tau} = b_\sigma \cdot \sigma(b_\tau) \cdot b_{\sigma\tau}^{-1}$. (Isto também mostrará que b é um 1-cociclo). Assim, podemos calcular,

$$b_{\sigma\tau}(e_\eta) = a_{\sigma\tau,\eta} e_{\sigma\tau\eta}$$

$$b_\sigma \circ \sigma(\tau)(e_\eta) = b_\sigma(\sigma(a_{\tau,\eta})) \cdot e_{\tau\eta} = \sigma(a_{\tau,\eta}) \cdot a_{\sigma,\tau\eta} e_{\sigma\tau\eta}.$$

Usando o fato que a é um 2-cociclo temos a igualdade requerida. ■

Ao identificar o grupo de Brauer com este grupo de cohomologia, podemos mostrar com facilidade que o grupo de Brauer é um grupo de torção:

Corolário 4.2.1. *Supomos que a extensão é de ordem n. Então cada elemento do grupo de Brauer $Br(K/k)$ possui uma ordem que divide n. Consequentemente, o grupo de Brauer $Br(k)$ é um grupo abeliano de torção.*

Demonstração. Pelo teorema 4.2.1 temos que $Br(K/k) \cong H^2(G, K^\times)$ e pelo corolário 3.2.2 obtemos que a ordem de todo elemento de $Br(K/k)$ divide n. Logo $Br(k)$ é de torção. ■

4.3 O teorema de Brauer de 1929

Nesta seção chegamos no objetivo deste trabalho que é o teorema de Brauer de 1929. Ele nos assegura que o período de uma k-álgebra simples central divide o índice e que ambos invariantes possuem os mesmos fatores primos. Em toda esta seção K/k denotará uma extensão separável finita e como acima k_s um fecho separável de k que contém K. Escrevemos $G_s = Gal(k_s/k)$.

Na sequência precisaremos da seguinte proposição:

Proposição 4.3.1. *Seja K/k um extensão separável de corpos de grau n, $\widetilde{K}$ seu fecho galoisiano e $G = Gal(\widetilde{K}/k)$. Então a aplicação de cobordo $\delta_n : H^1(G_s, PGL_n(k_s)) \longrightarrow Br(k)$ induz uma bijeção*

$$ker(f) \tilde{\longrightarrow} Br(K/k),$$

onde

$$\begin{aligned} f : H^1(G_s, PGL_n(k_s)) &\longrightarrow H^1(Gal(k_s/K), PGL_n(k_s)) \\ [A] &\longmapsto [A \otimes_k K]. \end{aligned}$$

Demonstração. Para esta demonstração são necessários alguns resultados técnicos. Remetemos o leitor para [6, proposição 4.5.6]. ■

Proposição 4.3.2. *Seja A uma k-álgebra simples central. O índice $ind(A)$ é o maior divisor comum dos graus das extensões de corpos separáveis e finitas K/k que decompõem A.*

Demonstração. Pela proposição 2.3.1, só precisamos mostrar que, se uma extensão finita K/k de grau n que é decomposição para A, então $ind(A)$ divide n. Para cada K, a classe de A em $Br(K/k)$ vem de uma classe em $H^1(G_s, PGL_n(k))$ de acordo com a proposição anterior. Sabemos que $H^1(G_s, PGL_n(k)) \leftrightarrow ASC_k(n)$ e com isso temos que essa classe também é representada por alguma k-álgebra simples central B de grau n, assim, o índice divide n, e como $ind(A) = ind(B)$ temos o nosso resultado. ■

Uma consequência importante dessa proposição é que $ind(A)$ é o menor entre os graus das extensões finitas e separáveis que decompõem A.

Corolário 4.3.1. *Sejam A e B duas k-álgebras simples centrais que geram o mesmo subgrupo em $Br(k)$. Então, $ind(A) = ind(B)$.*

Demonstração. Pela proposição 4.3.2 temos que para todo i temos que $ind(A^{\otimes_i})$ divide $ind(A)$. E tomando i, j adequados temos $[A^{\otimes_i}] = [B]$ e $[B^{\otimes_i}] = [A]$ em $Br(k)$ por suposição. Agora pelo teorema de Wedderburn as suas respectivas álgebras com divisão são isomorfas e portanto temos que $ind(A) = ind(B)$. ■

Corolário 4.3.2. *Seja K/k uma extensão finita e separável de corpos.*
(i) Temos as relações de divisibilidade

$$ind_K(A \otimes_k K) \mid ind_k(A) \mid [K : k] \cdot ind_K(A \otimes_k K).$$

(ii) Se o índice $ind_k(A)$ for primo a $[K : k]$, então $ind_k(A) = ind_K(A \otimes_k K)$. Em particular, se A é uma álgebra com divisão, então $A \otimes_k K$ também é.

Demonstração. *(i)* Usando a proposição 4.3.2 temos que $ind_K(A \otimes_k K) \,|\, ind_k(A)$ é imediato, e usando a proposição 2.3.1 é possível encontrar uma extensão de corpos finita e separável K'/K que é de decomposição para $A \otimes_k K$ com $[K' : K] = ind_K(A \otimes_k K')$. Então K' é também corpo de decomposição para A, e por isso usando a proposição 4.3.2 mostramos que $ind_k(A) \mid [K' : k] = ind_K(A \otimes_k K)[K : k]$.

(ii) Seja $ind_k(A) = p_1^{m_1} \cdot ... \cdot p_r^{m_r}$ a sua decomposição p-primária. Fixa um i. Temos que p_i não divide $[K : k]$, logo $p_i^{m_i}$ divide $ind_K(A \otimes_k K)$. Logo $ind_k(A)$ divide $ind_K(A \otimes_k K)$ e então eles são iguais. ■

Outro lema importante:

Lema 4.3.1. *Seja p um número primo que não divide $per(A)$. Então A é cindida por uma extensão finita e separável K/k de grau primo a p.*

Demonstração. Seja L/k uma extensão finita de Galois que é de decomposição para A, e seja também P um p-grupo de Sylow de $Gal(L/k)$ e K um corpo fixo. Usando o corolário 4.3.2 e o fato que $Br(L/k) \cong H^2(P, L^\times)$ temos que $Br(L/k)$ é um p-grupo de torção, p primo e com isso obtemos que a aplicação restrição $res : Br(L/k) \longrightarrow Br(L/K)$ é trivial, ou seja, A se cinde sobre K. ■

Agora chegamos ao centro do nosso trabalho, o resultado principal:

Teorema 4.3.1. *(Brauer 1929)*
Seja A uma k-álgebra simples central:
(i) *O período $per(A)$ divide o índice $ind(A)$.*
(ii) *O período $per(A)$ e o índice $ind(A)$ tem os mesmos fatores primos.*

Demonstração. Demonstração (i):
Como A é uma k-álgebra simples central, temos pela proposição 2.3.1 que existe uma extensão separável finita K/k cujo grau é $ind(A)$ e que é de decomposição para A, ou seja temos que $A \otimes_k K \cong M_n(K)$. Agora para o subgrupo fechado $Gal(k_s/K) \hookrightarrow Gal(k_s/k)$, de índice $n = [K : k]$ obtemos a restrição

$$res : H^2(Gal(k_s/k), k_s^\times) \longrightarrow H^2(Gal(k_s/K), k_s^\times),$$

ver 3.2.3, e como sabemos $H^2(Gal(k_s/k), k_s^\times) \cong Br(k)$ e $H^2(Gal(k_s/K), k_s^\times) \cong Br(K)$ pelo teorema 4.2.1. Então obtemos uma aplicação de restrição

$$res : Br(k) \longrightarrow Br(K)$$

$$[A] \longmapsto [A \otimes_k K]$$

que aniquila o representante $[A]$ da classe de A no grupo de Brauer $Br(k)$. Usando a proposição 3.2.3, temos que a composição $cor \circ res : Br(k) \longrightarrow Br(k)$ aniquila o elemento $[A]$ por uma multiplicação por $n = [K : k]$, ou seja, $[K : k] \cdot [A] = [k]$. Logo o período da classe da álgebra A no grupo de Brauer divide $n = [K : k]$. Então $per(A) = m \cdot [K : k]$, algum $m \in \mathbb{N}$. Portanto, $per(A) = m \cdot ind(A)$ com isso o período divide o índice da álgebra A.

Demonstração (ii):

Agora tomemos um p primo que não divide o período de A. Usando o lema 4.3.1, existe uma extensão finita K/k e separável que é decomposição para A, com índice $[K : k]$ co-primo a p, ou seja, o $m.d.c.(p, [K : k]) = 1$. Pela proposição 4.3.2, $ind(A)$ é o máximo divisor comum dos graus das extensões de corpos separáveis e finitas K/k que decompõem A. Logo $ind(A)$ não possui p como fator, isto é, p não divide $ind(A)$. ■

Observação 4.3.1. *Para um dado corpo k sabemos que $per(A)$ divide $ind(A)$. Porém a questão, para quais corpos estes dois invariantes de uma álgebra simples central coincidem ou, senão, quais valores são possíveis para a razão $ind(A)/per(A)$, é aberta em geral. Foi mostrado por de Jong, [4], que para corpos de funções de superfícies complexas, nós sempre temos $ind(A) = per(A)$. Para uma álgebra simples central sobre o corpo de funções de uma curva sobre o corpo p-ádico $\mathbb{Q}_p$, Saltman provou que a razão $ind(A)/per(A)$ é no máximo 2, se $per(A)$ é primo relativo a p, vide Saltman [8].*

Podemos agora falar sobre um corolário importante do Teorema de Brauer 1929 acima, que nos fornece um resultado sobre a estrutura de álgebras de divisão:

Proposição 4.3.3. *Seja D uma k-álgebra central com divisão e considere a decomposição primária*

$$ind(D) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}.$$

Então podemos encontrar álgebras simples centrais com divisão $D_i \, (i = 1, ..., r)$ tais que

$$D \cong D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$$

e $ind(D_i) = p_i^{m_i}$ *para cada* $i = 1, ..., r$. *Além disso, cada* D_i *é determinado unicamente por isomorfismo.*

Demonstração. Pelo corolário 4.2.1 temos que o grupo de Brauer é de torção, e devido a este fato é possível fazer uma decomposição p-primaria da seguinte forma

$$Br(k) = \bigoplus_p Br(k)\{p\}.$$

Usando a decomposição acima podemos escrever a classe $[D]$ da seguinte forma:

$$[D] = [D_1] + [D_2] + \cdots + [D_r].$$

Cada D_i é uma álgebra com divisão e $[D_i]$ é sua classe em $Br(k)\{p_i\}$, onde $i = 1, ..., r$ e p_i são primos. Agora usando o teorema 4.3.1 de Brauer na sua segunda parte podemos escrever o índice de cada D_i como uma potência de p_i. Tomamos o produto tensorial $A = D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$. Gostaríamos de provar que $A \cong D$. Nós temos:

$$deg(A) = deg(D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r) = deg(D_1) \cdot deg(D_2) \cdot ... \cdot deg(D_r) =$$

$$= ind(D_1) \cdot ind(D_2) \cdot ... \cdot ind(D_r) = \prod_i ind(D_i).$$

Temos $[A] = [D]$, então $ind(A) = ind(D)$. Como $ind(A)$ divide $deg(A)$, logo $ind(D)$ divide $\prod_i ind(D_i)$. Fazendo uma aplicação análoga a proposição 2.3.1 é possível mostrar que para cada i fixo obtemos uma extensão finita e separável K_i/k de grau primo a p_i, que cinde todos os D_j para $j \neq i$. A partir disso $D \otimes_k K_i$ e $D_i \otimes_k K_i$ possuem classes idênticas no grupo de Brauer $Br(K_i)$, e através destes fatos temos pelo corolário 4.3.2 na sua primeira parte obtemos o resultado que $ind_{K_i}(D_i \otimes_k K_i) | ind(D)$. Agora usando a segunda parte do corolário 4.3.2 as álgebras $D_i \otimes_k K_i$ ainda são com divisão com $ind(D_i)$ sobre K_i e com isso conseguimos provar que $ind(D_i)$ divide $ind(D)$ para todo i e sendo assim temos que $ind(D) = \prod_i ind(D_i)$. Logo $ind(A) = deg(A)$ e então A é divisão. Como $[A] = [D]$, nós temos $A \cong D$.

Para a unicidade observamos o seguinte: Supomos que

$$D \cong D_1 \otimes D_2 \otimes ... \otimes D_r$$

e

$$D \cong D'_1 \otimes D'_2 \otimes ... \otimes D'_r$$

duas tais composições. Logo $[D_i] = [D'_i]$ para todo $i = 1, ..., r$. Logo $D_i \cong D'_i$. ■

Referências Bibliográficas

[1] Brauer, Richard Über Systeme hyperkomplexer Zahlen. Math. Zeitschr. 30 (1929), 79-107.

[2] Bourbaki, Nicolas, *Algèbre*, Springer (2011).

[3] B. Felzenszwalb, *Álgebras de Dimensão Finitas*, IMPA - Instituto de Matemática Pura e Aplicada , (1979).

[4] de Jong, Aise Johan, *The period-index problem for the Brauer group of an algebraic surface*, Duke Math (2004).

[5] Elon Lages Lima, *Cálculo tensorial*, Coleção Publicações Universitárias - IMPA (2012).

[6] Gille, Philippe and Szamuely, Tamás, *Central simple algebras and Galois cohomology*, Cambridge, (2006).

[7] Knus, Max-Albert; Merkurjev, Alexander; Rost, Markus; Tignol, Jean-Pierre, *The book of involutions*, American Mathematical Society, Colloquion Publicatores (1998).

[8] Saltman, David J., *Division algebras over p-adic curves*, J. Ramanujan Math. Soc. (1997).

[9] Serre, Jean-Pierre, *Cohomologia Galoisienne*, Lecture Notes in Mathematics, volume 5, 5a edição, Springer Verlag (1997).

[10] Waterhouse, William C., *Profinite groups are Galois group*, volume 42, number 2 Proceeding of the American Mathematical Society (1974).