

Universidade Federal do Amazonas
Instituto de Ciências Exatas
Programa de Pós-Graduação em Matemática
Mestrado em Matemática

Álgebras de Loop e Cohomologia Galoisiana

Fernando Junior Soares dos Santos

Manaus – AM
Julho de 2017

Universidade Federal do Amazonas
Instituto de Ciências Exatas
Programa de Pós-Graduação em Matemática
Mestrado em Matemática

Álgebras de Loop e Cohomologia Galoisiana

por

Fernando Junior Soares dos Santos

sob a orientação do

Prof. Dr. Wilhelm Alexander Cardoso Steinmetz
Orientador

Prof. Dr. Vyacheslav Futorny
Co-orientador

Manaus – AM
Julho de 2017

Ficha Catalográfica

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

S237á Santos, Fernando Junior Soares dos
Álgebras de Loop e Cohomologia Galoisiana / Fernando Junior
Soares dos Santos. 2017
46 f.: il.; 31 cm.

Orientador: Wilhelm Alexander Cardoso Steinmetz
Coorientador: Vyacheslav Futorny
Dissertação (Mestrado em Matemática Pura e Aplicada) -
Universidade Federal do Amazonas.

1. Álgebras de Lie. 2. Álgebras de Loop (Álgebras de Lacetes). 3.
Cohomologia Galoisiana. 4. Cohomologia Não-Abeliana. 5.
Espaços Principais Homogêneos. I. Steinmetz, Wilhelm Alexander
Cardoso II. Universidade Federal do Amazonas III. Título

Álgebras de Loop e Cohomologia Galoisiana

por

Fernando Junior Soares dos Santos ¹

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 06 de Julho de 2017.

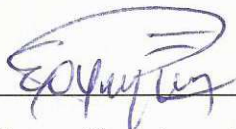
Banca Examinadora:



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



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



Prof. Dr. Elkin Oveimar Quintero Vanegas – (Membro Externo)
Universidade Federal do Ceará - UFC

¹O autor foi bolsista da Fundação de Amparo à Pesquisa do Estado do Amazonas - FAPEAM durante a elaboração desta dissertação.

*Dedico este trabalho a minha
mãe Raimunda dos Santos
Souza, ao meu pai Fernando
Soares de Souza que sempre
me incentivaram a dar conti-
nuidade aos meus estudos.*

Agradecimentos

Ao concluir este trabalho, agradeço:

A Deus em primeiro lugar, pelo dom da vida, pois sem ele não somos nada.

A minha mãe Raimunda dos Santos e ao meu padrasto Amaro Rodrigues, que sempre me incentivaram nos meus estudos, a meus irmãos, que sempre me apoiaram e me deram forças para vencer essa etapa.

Agradeço a minha companheira de todas as horas Elizangela de Souza Castro que me apoiou durante essa caminhada e também aos meus pequenos Stephanny e Jhonnata.

Agradeço a meu orientador Prof. Dr. Wilhelm Alexander Steinmetz e co-orientador Prof. Dr. Vyacheslav Futorny pela paciência na orientação e incentivo que tornaram possível a conclusão deste trabalho.

Aos professores do Departamento de Matemática, em especial, aos professores: Roberto Cristóvão Mesquita Silva, que incansavelmente nos ajudou em qualquer obstáculo e sempre nos incentivou dando força para prosseguir; Stefan Josef Ehbauer e Germán Alonso, pelas dúvidas sanadas e incentivos que tornarão possíveis a conclusão desse trabalho.

Aos amigos, pelos incentivos, contribuições e principalmente pelos momentos de diversões que tivemos juntos. Em especial, aos amigos do Mestrado em Matemática: Márcia Sarraf, Daniele Alencar, Ayana Santana, Alan Kardec, Bruno Lopes, Cristiano Silva, Edfram Pereira, Fábio Junior, João Raimundo, Osenildo Maciel, Rafael Arcos, Teo Felipe, Suellen Lima, Eduardo Bruno, Gariel Sousa, Matheus Hudson, Wanessa. Aos amigos do Doutorado em Matemática: Airton, Clebes, Abraão, Adrian e Andreia. Obrigado a todos por fazerem essa caminhada muito mais proveitosa.

Aos amigos secretários do PPGM, Aristocles Rannyeri Nascimento de Lima e ao Elclimar Alves Saraiva, muito obrigado pela paciência e pelos incentivos.

À FAPEAM, pelo apoio financeiro.

Resumo

Neste trabalho se estuda como certos tipos de álgebras de loop podem ser classificados com a ajuda da cohomologia galoisiana. Na primeira parte do trabalho é exposta a teoria de álgebras de Lie de dimensão finita e é introduzida a noção de álgebra de loop. Em seguida, é explicado a relação das álgebras de loop com as S/R formas de $\mathfrak{g}(R)$, para R o anel de polinômios de Laurent em uma variável sobre um corpo algebricamente fechado e S uma extensão deste anel. No capítulo seguinte será apresentado a teoria da cohomologia galoisiana. No final será mostrado como classes de isomorfismo de álgebras de loop podem ser representados por elementos de conjuntos da cohomologia galoisiana.

Palavras-chave: Álgebras de Lie; Álgebras de Loop (Álgebras de Lacetes); Cohomologia Galoisiana; Cohomologia Não-Abeliana; Espaços Principais Homogêneos.

Abstract

In this work we study how certain types of loop algebras can be classified with the help of Galois cohomology. In the first part of the paper we expose the theory of finite-dimensional Lie algebras and introduce the notion of a loop algebra. Subsequently we explain the relationship of loop algebras with the S/R -forms of $\mathfrak{g}(R)$, where R is the ring of Laurent polynomials in one variable over an algebraically closed field and S an extension of the ring. In the second chapter the theory of Galois cohomology will be developed. Finally we will show how isomorphism classes of loop algebras can be represented by elements of sets of Galois cohomology.

Keywords: Lie Algebras; Loop Algebras; Galois Cohomology; Non-Abelian Cohomology. Principal Homogeneous Spaces.

Sumário

Introdução	10
1 Álgebras de Lie e de Loop	12
1.1 Definições e exemplos de álgebras de Lie	12
1.2 Homomorfismo de álgebras de Lie	16
1.3 Soma direta e representações de álgebras de Lie	19
1.4 Álgebras de Lie solúveis e semi-simples	23
1.4.1 Série derivada	23
1.4.2 Álgebra semi-simples	24
1.5 Álgebras de loop	25
1.5.1 Definição e algumas propriedades	25
2 Cohomologia Galoisiana	28
2.1 O Grupo de Galois como grupo profinito	28
2.1.1 Grupos topológicos	29
2.1.2 Limite inverso	30
2.2 Cohomologia galoisiana	32
2.2.1 G -módulos discretos	32
2.2.2 Cocadeias, cociclos e cohomologia	32
2.3 Cohomologia não abeliana	36
2.3.1 Definições de H^0 e H^1	36
2.3.2 Espaços principais homogêneos	37
2.3.3 Torsão (Twisting)	39
2.4 Álgebras de loop e cohomologia galoisiana	40
Referências Bibliográficas	45

Introdução

Álgebras de loop, representam realizações concretas de álgebras de Kac-Moody: Uma álgebra de Kac-Moody afim sobre \mathbb{C} pode ser vista como uma extensão central de uma álgebra de loop sobre \mathbb{C} . Álgebras de Kac-Moody foram descobertas independentemente por Victor Kac e Robert Moody nos anos 1960s. Estas álgebras aparecem naturalmente na física teórica, Johnny T. Ottesen (1995) [15], Jurgen Fuchs (1992) [6] e foram amplamente pesquisadas. Por sua vez as técnicas de cohomologia galoisiana e não-abeliana foram desenvolvidas nos anos 1950 e 1960 por John Tate, Jean-Pierre Serre e Jean Giraud entre outros, a partir das necessidades da teoria dos números e da geometria algébrica, vide [21] e [11].

Esse trabalho está baseado nos artigos de A. Pianzola (2005) [16], (2002) [18], onde foram usadas pela primeira vez técnicas de cohomologia galoisiana e cohomologia não-abeliana para a classificação de álgebras de loop, como torsões sobre o anel de polinômios de Laurent em uma variável sobre um corpo de característica zero. Estes artigos foram os pontos de partida de vários outros trabalhos que em seguida utilizaram estas técnicas para classificar álgebras de multi-loop (uma generalização de álgebras de loop) nos anos seguintes, como Gille-Pianzola (2007) [8], (2008) [9], (2013) [10] e Steinmetz-Zikesch (2012) [25].

Nós ilustraremos a rica interação de duas áreas de álgebra, que parecem relativamente distintas: álgebras de Lie de dimensão infinita e cohomologia galoisiana. Uma álgebra de loop L (construída a partir de uma álgebra de Lie \mathfrak{g} de dimensão finita sobre \mathbb{C}) contém o anel $R = \mathbb{C}[t, t^{-1}]$ e é "trivializada" por uma extensão finita de R . Isto é, existe uma extensão finita (e galoisiana) de anéis S/R , tal que

$$L \otimes_R S \simeq \mathfrak{g}_R \otimes_R S,$$

onde $\mathfrak{g}_R = \mathfrak{g} \otimes_{\mathbb{C}} R$. Este fato permite aplicar técnicas de cohomologia a estas álgebras de loop. No nosso trabalho mostraremos como o problema da classificação de álgebras de loop sobre \mathbb{C} pode ser transformado essencialmente em um problema de cohomologia galoisiana.

A nossa teoria se aplica principalmente a álgebras de loop sobre o corpo \mathbb{C} . Porém a nossa teoria só utiliza propriedades algébricas e não analíticas do corpo \mathbb{C} , assim ela será desenvolvida, em maior generalidade, sobre um corpo algebricamente fechado de característica zero. Estruturamos o nosso trabalho em dois capítulos da seguinte forma:

No Capítulo 1, estudamos alguns conceitos relacionados a álgebras de Lie de dimensão finita, apresentamos exemplos e revisamos alguns resultados clássicos que serão de importância no decorrer deste trabalho, utilizando como principais referências, os textos [5], [12], [20] e [22]. Na última parte do capítulo 1 definiremos a noção de álgebra de loop $L(\mathfrak{g}, \sigma)$, para \mathfrak{g} uma álgebra de Lie de dimensão finita e σ um automorfismo de \mathfrak{g} de período finito e mostramos que toda álgebra de loop é uma S/R -forma de $\mathfrak{g} \otimes R$, para S

uma extensão finita de $\mathbb{C}[t, t^{-1}]$. Utilizamos como principais referências, [1], [17] e [24].

No Capítulo 2, apresentamos a teoria da cohomologia galoisiana. Começamos por introduzir as noções de grupo topológico, limite inverso e grupo profinito. Em seguida, desenvolvemos a teoria da cohomologia de grupos profinitos na medida que precisamos. Esta teoria pode ser aplicada ao grupo de Galois de uma extensão de corpos, sendo um grupo profinito. Apresentaremos as noções de espaços principais homogêneos (torsores) da cohomologia não-abeliana. No final do capítulo mostraremos que as álgebras de loop podem ser associadas a cociclos da cohomologia não-abeliana. Assim mostraremos que álgebras de loop $L(\mathfrak{g}, \sigma)$ podem ser classificados, a menos de R -isomorfismo, pelas classes do conjunto de cohomologia galoisiana $H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$, onde $\mathfrak{g}(S) = \mathfrak{g} \otimes_{\mathbb{C}} S$. Construimos explicitamente uma função injetiva:

$$\left\{ \begin{array}{l} \text{Classes de } R\text{-isomorfismos de álgebras de loop da forma} \\ L(\mathfrak{g}, \sigma), \text{ onde } \sigma \text{ é um automorfismo de } \mathfrak{g} \text{ de período } m. \end{array} \right\} \longrightarrow H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$$

Desta correspondência podemos rapidamente deduzir as classes de \mathbb{C} -isomorfismo de álgebras de loop. De fato as classes de \mathbb{C} -isomorfismo podem ser identificados com um quociente do conjunto de cohomologia acima. A importância disso é que nós conseguimos transformar um problema da teoria de álgebras de Lie de dimensão infinita (a classificação de álgebras de loop) em um problema de cohomologia galoisiana. Além disso classificação destas álgebras não depende diretamente da álgebra de Lie \mathfrak{g} , mas apenas do seu grupo de $\text{Aut}(\mathfrak{g})$, ou seja do grupo de automorfismos de S -álgebra $\mathfrak{g} \otimes S$.

Capítulo 1

Álgebras de Lie e de Loop

As álgebras de loop, que são o objeto principal do nosso trabalho e que serão introduzidas na última seção deste capítulo, são álgebras de Lie de dimensão infinita sobre o corpo \mathbb{C} . Portanto começamos por expor neste capítulo os conceitos básicos da teoria das álgebra e Lie sobre um corpo.

1.1 Definições e exemplos de álgebras de Lie

Definição 1.1.1. Seja k um corpo. Uma *Álgebra de Lie* consiste de um k -espaço vetorial \mathfrak{g} , munido de uma aplicação bilinear, (colchete ou comutador)

$$[,] : \mathfrak{g} \times \mathfrak{g} \longrightarrow \mathfrak{g}$$

satisfazendo as seguintes propriedades:

- (L1) $[x, x] = 0$ para todo $x \in \mathfrak{g}$,
- (L2) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ para todo $x, y, z \in \mathfrak{g}$.

A condição (L2) é conhecida como identidade de Jacobi. Neste trabalho, iremos por a condição de que o corpo k seja algebricamente fechado de característica zero.

Observação 1.1.1.

- A condição (L1) implica que $[x, y] = -[y, x]$ para todo $x, y \in \mathfrak{g}$ e é equivalente se o corpo de escalares k não é de característica dois.
- Em uma álgebra de Lie \mathfrak{g} , tem-se que $[x, 0] = 0 = [0, x]$ para todo $x \in \mathfrak{g}$, pois, $[x, 0] = [x, 0 + 0] = [x, 0] + [x, 0]$ o que implica que $[x, 0] = 0 = [0, x]$.
- Em geral uma álgebra de Lie \mathfrak{g} , não é uma álgebra associativa, pois podemos ter $[x, [x, y]] \neq [[x, x], y]$ quando $[x, [x, y]] \neq 0$.

Exemplo 1.1.1 (Álgebras de Lie proveniente de álgebras associativas). Seja \mathcal{A} uma álgebra associativa. Podemos definir sobre o espaço vetorial \mathcal{A} um colchete a partir do produto associativo da seguinte forma:

$$[x, y] := xy - yx \text{ para todo } x, y \in \mathcal{A}$$

onde xy indica a multiplicação k -bilinear associativa em \mathcal{A} . O colchete definido assim dá uma estrutura de álgebra de Lie em \mathcal{A} a qual denotamos por $\mathcal{A}^{(-)}$, para indicar que é uma álgebra de Lie proveniente de uma álgebra associativa.

Exemplo 1.1.2. $(\mathcal{M}(n, k), [,])$ onde $\mathcal{M}(n, k)$ é o k -espaço vetorial das matrizes de orden $n \times n$ com entradas em k , é uma álgebra de Lie. De fato, defina o colchete de Lie, pondo $[A, B] := AB - BA$ para todo $A, B \in \mathcal{M}(n, k)$, onde AB indica o produto usual de matrizes. É fácil ver, que $[,]$ é uma aplicação bilinear e cumpre as condições (L1) e (L2).

Essa álgebra de Lie será denotada por $\mathfrak{gl}(n, k)$. Muitas das vezes elas serão indicadas somente por $\mathfrak{gl}(n)$, sem especificar o corpo quando este não for relevante.

Exemplo 1.1.3. Seja V um k -espaço vetorial. Considere o k -espaço vetorial $\text{End}(V)$, isto é, o conjunto de todas as transformações lineares do k -espaço vetorial V . $\text{End}(V)$ é uma álgebra de Lie, onde o colchete é dado por $[T_1, T_2] = T_1 \circ T_2 - T_2 \circ T_1$ para todo $T_1, T_2 \in \text{End}(V)$, a qual $T_1 \circ T_2$ indica a composição de transformações lineares. Por definição, $[,]$ é bilinear, onde cumpre as condições (L1), (L2).

A essa álgebra de Lie, denotaremos por $\mathfrak{gl}(V)$. Quando o k -espaço vetorial V , tiver dimensão finita ($\dim_k V = n < \infty$), $\mathfrak{gl}(V)$ coincide com $\mathfrak{gl}(n)$. Essa álgebra de Lie é conhecido como álgebra linear geral.

Definição 1.1.2. Uma álgebra de Lie \mathfrak{g} é chamada de *abeliana*, se $[x, y] = 0$, para todo $x, y \in \mathfrak{g}$.

Exemplo 1.1.4.

- Seja \mathfrak{g} um espaço vetorial qualquer, em \mathfrak{g} definimos $[x, y] = 0$, para todo $x, y \in \mathfrak{g}$. Portanto \mathfrak{g} munido desse colchete é uma álgebra de Lie abeliana.
- Se dimensão de \mathfrak{g} é 1, então \mathfrak{g} é abeliana.
- Todo subespaço de dimensão 1 de uma álgebra de Lie é uma álgebra de Lie abeliana.

Alguns conceitos da teoria da álgebra e da álgebra linear podem ser introduzidas na teoria de álgebra de Lie, vejamos.

Definição 1.1.3. Sejam \mathfrak{g} uma álgebra de Lie e $\mathfrak{h} \subseteq \mathfrak{g}$. Dizemos que \mathfrak{h} é uma *subálgebra de Lie*, se \mathfrak{h} é um subespaço vetorial de \mathfrak{g} fechado para o colchete, isto é, para todo $x, y \in \mathfrak{h}$, $[x, y] \in \mathfrak{h}$.

Observação 1.1.2. Uma subálgebra de Lie \mathfrak{h} é um subespaço vetorial que herda as estruturas de álgebra de Lie de \mathfrak{g} .

Exemplo 1.1.5. O espaço $\mathfrak{b}(n, k)$ das matrizes triangulares superiores ($a_{ij} = 0 \forall i > j$) é uma subálgebra de Lie de $\mathfrak{gl}(n)$, pois a soma e a multiplicação de matrizes triangulares superiores ainda é uma matriz triangular superior. logo, $[A, B] \in \mathfrak{b}(n, k)$ para todo $A, B \in \mathfrak{b}(n, k)$.

Exemplo 1.1.6. O conjunto $\mathfrak{h} = \{A \in \mathfrak{gl}(n) \mid \text{Tr}(A) = 0\}$ é uma subálgebra de Lie de $\mathfrak{gl}(n)$, onde Tr indica o traço da matriz. Com efeito, \mathfrak{h} é subespaço vetorial de $\mathfrak{gl}(n)$, pois é não vazio ($0 \in \mathfrak{h}$) e para todo $A, B \in \mathfrak{h}$ e $\alpha \in k$, temos:

$$\text{Tr}(A + \alpha B) = \text{Tr}(A) + \alpha \text{Tr}(B) = 0$$

isto é, $A + \alpha B \in \mathfrak{h}$, provando assim que \mathfrak{h} é subespaço vetorial de \mathfrak{g} . Sejam agora $A, B \in \mathfrak{h}$, então

$$\text{Tr}([A, B]) = \text{Tr}(AB - BA) = \text{Tr}(AB) - \text{Tr}(BA) = 0.$$

Portanto, \mathfrak{h} é subálgebra de $\mathfrak{gl}(n)$.

Representaremos essa subálgebra de Lie por $\mathfrak{sl}(n, k)$ ou apenas $\mathfrak{sl}(n)$ quando não houver confusão em relação ao corpo.

As álgebra de Lie $\mathfrak{gl}(n)$ e $\mathfrak{sl}(n)$ aparecerão com bastante frequência no decorrer do trabalho, por isso, damos tal importância a elas para o desenvolvimento dessa teoria.

Definição 1.1.4. Sejam \mathfrak{g} uma álgebra de Lie, $\mathfrak{h} \subset \mathfrak{g}$ uma subálgebra. Definimos o *normalizador* de \mathfrak{h} em \mathfrak{g} como

$$N_{\mathfrak{g}}(\mathfrak{h}) = \{x \in \mathfrak{g} \mid [x, h] \in \mathfrak{h}, \forall h \in \mathfrak{h}\}.$$

Observação 1.1.3. É fácil verificar que $N_{\mathfrak{g}}(\mathfrak{h})$ é uma subálgebra de \mathfrak{g} , que contém \mathfrak{h} .

Definição 1.1.5. Sejam \mathfrak{g} uma álgebra de Lie e $\mathcal{I} \subseteq \mathfrak{g}$. Dizemos que \mathcal{I} é um *ideal* de \mathfrak{g} , se \mathcal{I} é um subespaço vetorial, tal que:

$$[x, y] \in \mathcal{I}, \forall x \in \mathfrak{g}, y \in \mathcal{I}.$$

Em outras palavras, $[\mathfrak{g}, \mathcal{I}] \subset \mathcal{I}$.

Observação 1.1.4.

- Em virtude da condição que $[x, y] = -[y, x] \forall x, y \in \mathfrak{g}$, não há uma distinção entre ideal a esquerda e a direita.
- Se \mathcal{I} é um ideal de \mathfrak{g} , então \mathcal{I} é uma subálgebra de \mathfrak{g} , mas a recíproca é falsa, um contra exemplo é a subálgebra $\mathfrak{b}(2, k)$ da álgebra de Lie $\mathfrak{gl}(2)$, onde considerando

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{b}(2, k), \quad \text{e} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \mathfrak{gl}(2).$$

podemos verificar que

$$\left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right] = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \notin \mathfrak{b}(2, k).$$

Exemplo 1.1.7. $\{0\}$, \mathfrak{g} são ideais de \mathfrak{g} chamados ideais triviais.

Exemplo 1.1.8. $\mathfrak{sl}(n)$ é um ideal de $\mathfrak{gl}(n)$, pois, para todo $A \in \mathfrak{sl}(n)$ e $B \in \mathfrak{gl}(n)$, $[A, B] = AB - BA \in \mathfrak{sl}(n)$.

Definição 1.1.6. Sejam \mathfrak{g} uma álgebra de Lie e $\mathcal{B} \subseteq \mathfrak{g}$. Chamamos de *centralizador* de \mathcal{B} em \mathfrak{g} ao conjunto

$$Z(\mathcal{B}) = \{x \in \mathfrak{g} \mid [x, y] = 0 \forall y \in \mathcal{B}\}.$$

Se $\mathcal{B} = \mathfrak{g}$ chamamos $Z(\mathfrak{g})$ de *centro* de \mathfrak{g} .

Observação 1.1.5. O centro $Z(\mathfrak{g})$ é um ideal da álgebra de Lie \mathfrak{g} . Isso é verificado através da identidade de Jacobi.

Mostraremos agora como propriedades de soma e interseção de ideais e subálgebras podem ser interpretadas. Vejamos isso na seguinte proposição.

Proposição 1.1.1. Sejam \mathfrak{g} uma álgebra de Lie e $\mathfrak{h}_1, \mathfrak{h}_2$ dois subespaços de \mathfrak{g} . Então:

$$\begin{array}{ccccccc} \mathfrak{h}_1 & \mathfrak{h}_2 & \implies & \mathfrak{h}_1 + \mathfrak{h}_2 & \mathfrak{h}_1 \cap \mathfrak{h}_2 & & \\ \text{Ideal} & \text{Ideal} & \implies & \text{Ideal} & \text{Ideal} & & \\ \text{Subálgebra} & \text{Ideal} & \implies & \text{Subálgebra} & \text{Subálgebra} & & \end{array}$$

Demonstração. Como \mathfrak{h}_1 e \mathfrak{h}_2 são subespaços de \mathfrak{g} , então claramente a soma e a interseção são subespaços de \mathfrak{g} . Suponhamos que $\mathfrak{h}_1, \mathfrak{h}_2$ são ideais, e sejam $x \in \mathfrak{h}_1 + \mathfrak{h}_2$ e $y \in \mathfrak{g}$, então existem $x_1 \in \mathfrak{h}_1$ e $x_2 \in \mathfrak{h}_2$, tal que $x = x_1 + x_2$, assim

$$[x, y] = [x_1 + x_2, y] = [x_1, y] + [x_2, y] \in \mathfrak{h}_1 + \mathfrak{h}_2.$$

Isso mostra que a soma de dois ideais é um ideal. Para a interseção de dois ideais, sejam $x \in \mathfrak{h}_1 \cap \mathfrak{h}_2$ e $y \in \mathfrak{g}$, por definição $[x, y] \in \mathfrak{h}_1 \cap \mathfrak{h}_2$, como queríamos.

No caso da soma de um ideal com uma subálgebra de Lie é fácil verificar que é uma subálgebra de Lie. □

Observação 1.1.6. A soma de duas subálgebras de Lie não é, em geral, uma subálgebra de Lie, um contra-exemplo é dado pelas subálgebras de Lie \mathfrak{h}_1 e \mathfrak{h}_2 de $\mathfrak{sl}(2, \mathbb{R})$ gerados por

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ e } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

respectivamente. Podemos verificar que

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}.$$

Suponhamos que

$$\begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} + \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix}$$

com $a, b \in \mathbb{R}$. Assim teremos, por igualdade em b , uma contradição. Portanto, $\mathfrak{h}_1 + \mathfrak{h}_2$ não é uma subálgebra de Lie.

Definição 1.1.7. Sejam \mathfrak{g} uma álgebra de Lie sobre k e \mathcal{A}, \mathcal{B} subconjuntos de \mathfrak{g} . Definimos o colchete de \mathcal{A}, \mathcal{B} como o k -subespaço vetorial gerado por $\{[x, y] : x \in \mathcal{A} \text{ e } y \in \mathcal{B}\}$, a qual denotamos por:

$$[\mathcal{A}, \mathcal{B}] = \text{Span}_k \{[x, y] \mid x \in \mathcal{A} \text{ e } y \in \mathcal{B}\}.$$

Proposição 1.1.2. Sejam \mathfrak{h}_1 e \mathfrak{h}_2 ideais de uma álgebra de Lie \mathfrak{g} . Então $[\mathfrak{h}_1, \mathfrak{h}_2]$ é um ideal de \mathfrak{g} .

Demonstração. Por definição $[\mathfrak{h}_1, \mathfrak{h}_2]$ é um subespaço vetorial de \mathfrak{g} . Sejam $z \in \mathfrak{g}$ e $w \in [\mathfrak{h}_1, \mathfrak{h}_2]$, então $w = \sum_i \alpha_i [x_i, y_i]$ com $x_i \in \mathfrak{h}_1$ e $y_i \in \mathfrak{h}_2$. Pela identidade de Jacobi, tem-se:

$$[z, w] = \left[z, \sum_i \alpha_i [x_i, y_i] \right] = \sum_i \alpha_i [z, [x_i, y_i]] = \sum_i \alpha_i ([x_i, [z, y_i]] + [[z, x_i], y_i]).$$

Portanto, $[z, w] \in [\mathfrak{h}_1, \mathfrak{h}_2]$, como queríamos. □

1.2 Homomorfismo de álgebras de Lie

Para procedermos no trabalho e assim definirmos as álgebras de loop, precisamos de alguns conceitos básicos sobre automorfismos de álgebras de Lie de período n , para isso, iniciaremos a expor sobre homomorfismo de álgebras de Lie, em que apresentaremos alguns exemplos e teoremas clássicos.

Definição 1.2.1. Sejam $\mathfrak{g}, \mathfrak{h}$ álgebras de Lie sobre um corpo k . Dizemos que a aplicação $\phi : \mathfrak{g} \longrightarrow \mathfrak{h}$ é um *homomorfismo* de álgebras de Lie, se cumpre as seguintes condições:

- (i) ϕ é uma transformação linear.
- (ii) ϕ preserva colchete de Lie, isto é, $\phi([x, y]) = [\phi(x), \phi(y)]$ para todo $x, y \in \mathfrak{g}$.

Observação 1.2.1.

- Notemos que no item (ii) o primeiro colchete é dado pela álgebra de Lie \mathfrak{g} e o segundo colchete é dado pela álgebra de Lie \mathfrak{h} .
- ϕ é chamado *monomorfismo*, se é injetora, *epimorfismo* se é sobrejetora e *isomorfismo* se é bijetora.
- Um *automorfismo* de uma álgebra de Lie \mathfrak{g} é um isomorfismo ϕ da forma $\phi : \mathfrak{g} \longrightarrow \mathfrak{g}$. Definimos um período de um automorfismo ϕ como um inteiro positivo n , tal que, $\phi^n = \text{Id}$, onde Id indica o homomorfismo identidade.
- $\text{Ker}(\phi) = \{x \in \mathfrak{g} \mid \phi(x) = 0\}$ é um ideal de \mathfrak{g} .
- $\text{Im}(\phi) = \{y \in \mathfrak{h} \mid y = \phi(x) \text{ para algum } x \in \mathfrak{g}\}$ é uma subálgebra de Lie de \mathfrak{h} .

Exemplo 1.2.1. A aplicação traço

$$\text{Tr} : \mathfrak{gl}(n) \longrightarrow k$$

é um homomorfismo de álgebras de Lie. De fato, Tr é uma transformação linear, tal que,

$$\begin{aligned}\text{Tr}([A, B]) &= \text{Tr}(AB - BA) \\ &= \text{Tr}(AB) - \text{Tr}(BA) \\ &= 0 \\ &= [\text{Tr}(A), \text{Tr}(B)]\end{aligned}$$

pois k é álgebra de Lie abeliana.

Exemplo 1.2.2. Consideremos as álgebras de Lie L e $\mathfrak{gl}(L)$, definimos o *homomorfismo adjunto*

$$\text{ad} : L \longrightarrow \mathfrak{gl}(L)$$

por $\text{ad}_x(y) := [x, y]$ para todo $x, y \in L$. Esta aplicação é um homomorfismo entre álgebras de Lie, pois,

$$\begin{aligned}\text{ad}_{\alpha x + \beta y}(z) &= [\alpha x + \beta y, z] \\ &= \alpha[x, z] + \beta[y, z] \\ &= \alpha \cdot \text{ad}_x(z) + \beta \cdot \text{ad}_y(z)\end{aligned}$$

para todo $x, y, z \in L$ e $\alpha, \beta \in k$ e da identidade de Jacobi, temos

$$\begin{aligned}\text{ad}_{[x, y]}(z) &= [[x, y], z] \\ &= [[x, z], y] + [x, [y, z]] \\ &= [x, [y, z]] - [y, [x, z]] \\ &= \text{ad}_x \circ \text{ad}_y(z) - \text{ad}_y \circ \text{ad}_x(z).\end{aligned}$$

Definição 1.2.2. Sejam \mathfrak{g} uma álgebra de Lie e \mathfrak{h} um ideal de \mathfrak{g} . O espaço vetorial quociente $\mathfrak{g}/\mathfrak{h} = \{x + \mathfrak{h} : x \in \mathfrak{g}\}$ tem estrutura de álgebra de Lie, definindo o colchete por

$$[x + \mathfrak{h}, y + \mathfrak{h}] := [x, y] + \mathfrak{h}.$$

É fácil verificar que a definição do colchete de acima independe dos representantes, no qual cumpre as condições (L1) e (L2). Com isso, podemos verificar que a projeção canônica $\pi : \mathfrak{g} \longrightarrow \mathfrak{g}/\mathfrak{h}$, dado por $\pi(x) = x + \mathfrak{h}$, $x \in \mathfrak{g}$, é um homomorfismo sobrejetor de álgebras de Lie, pois para todo $x, y \in \mathfrak{g}$, temos

$$\pi([x, y]) = [x, y] + \mathfrak{h} = [x + \mathfrak{h}, y + \mathfrak{h}] = [\pi(x), \pi(y)].$$

Teorema 1.2.1 (Teorema do Isomorfismo).

(1) Se $\phi : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$ é um homomorfismo de álgebras de Lie, então

$$\mathfrak{g}_1/\text{Ker}(\phi) \simeq \text{Im}(\phi).$$

(2) Se \mathfrak{h}_1 e \mathfrak{h}_2 são ideais de \mathfrak{g} , então

$$(\mathfrak{h}_1 + \mathfrak{h}_2)/\mathfrak{h}_1 \simeq \mathfrak{h}_2/\mathfrak{h}_1 \cap \mathfrak{h}_2.$$

(3) Suponha que \mathfrak{h}_1 e \mathfrak{h}_2 são ideais de \mathfrak{g} , tal que $\mathfrak{h}_1 \subseteq \mathfrak{h}_2$. Então

$\mathfrak{h}_2/\mathfrak{h}_1$ é um ideal de $\mathfrak{g}/\mathfrak{h}_1$ e $(\mathfrak{g}/\mathfrak{h}_1)/(\mathfrak{h}_2/\mathfrak{h}_1) \simeq \mathfrak{g}/\mathfrak{h}_2$.

Demonstração. A demonstração é análogo as outras estruturas algébricas (Aneis, módulos, etc).

□

Exemplo 1.2.3. Sejam a aplicação traço $\text{Tr} : \mathfrak{gl}(n) \longrightarrow k$ e $\text{Ker}(\text{Tr}) = \mathfrak{sl}(n)$, assim, pelo Teorema do Isomorfismo $\mathfrak{gl}(n)/\mathfrak{sl}(n) \simeq k$.

Como caso particular de homomorfismo de álgebra de Lie temos as derivações:

Definição 1.2.3. Seja \mathfrak{g} uma álgebra de Lie sobre k . Uma *derivação* de \mathfrak{g} é uma aplicação k -linear

$$D : \mathfrak{g} \longrightarrow \mathfrak{g}$$

tal que

$$D([x, y]) = [D(x), y] + [x, D(y)] \text{ para todo } x, y \in \mathfrak{g}.$$

Podemos definir de forma mais geral, para uma álgebra \mathcal{A} , com um endomorfismo D de \mathcal{A} , onde cumpre a regra de Leibniz de derivada de produto $D(xy) = D(x)y + xD(y)$.

Exemplo 1.2.4. A adjunta dos elementos de uma álgebra de Lie \mathfrak{g} , é uma derivação. De fato, pela identidade de Jacobi,

$$\text{ad}_x([y, z]) = [x, [y, z]] = [[x, y], z] + [y, [x, z]].$$

Portanto, $\text{ad}_x([y, z]) = [\text{ad}_x(y), z] + [y, \text{ad}_x(z)]$ para todo $x, y, z \in \mathfrak{g}$.

O colchete de Lie de uma álgebra de Lie \mathfrak{g} de dimensão finita com base $\mathcal{B} = \{X_1, X_2, \dots, X_n\}$, está completamente determinado pelo colchetes dos elementos de

\mathcal{B} , pois $[X_i, X_j] = \sum_{k=1}^n c_{ij}^k X_k$, para alguns $c_{ij}^k \in k$ e para quaisquer $X, Y \in \mathfrak{g}$, temos,

$$X = \sum_{i=1}^n a_i X_i, Y = \sum_{j=1}^n b_j X_j \text{ e}$$

$$\begin{aligned} [X, Y] &= \left[\sum_{i=1}^n a_i X_i, \sum_{j=1}^n b_j X_j \right] \\ &= \sum_{i,j} a_i b_j [X_i, X_j] \\ &= \sum_{i,j,k} a_i b_j c_{ij}^k X_k \end{aligned}$$

A esses coeficientes c_{ij}^k , damos o nome de *constantes de estrutura* de \mathfrak{g} com respeito a base \mathcal{B} . Essas constantes de estruturas dependem da escolha da base de \mathfrak{g} , em geral, diferentes base implicam em diferentes constantes de estrutura.

Observação 1.2.2. Pela condição (L1) tem-se que $[X_i, X_i] = 0$, para todo i , a qual implica que $[X_i, X_j] = -[X_j, X_i] \forall i, j$. Então é suficiente conhecer as constantes de estrutura c_{ij}^k para $1 \leq i < j \leq n$.

Existe uma maneira de verificar que álgebras de Lie de dimensão finita são isomorfas através do colchete, onde analisamos as constantes de estrutura, esse é o resultado da proposição seguinte.

Proposição 1.2.1. Sejam \mathfrak{g} e \mathfrak{h} álgebras de Lie de dimensão finita. \mathfrak{g} é isomorfo a \mathfrak{h} se, e somente se, existe uma base \mathcal{B} de \mathfrak{g} e uma base \mathcal{C} de \mathfrak{h} , tal que, as constantes de estrutura de \mathfrak{g} com respeito a \mathcal{B} são iguais as constantes de estrutura de \mathfrak{h} com respeito a \mathcal{C} .

Demonstração. Sejam as bases $\mathcal{B}=\{X_1, X_2, \dots, X_n\}$ e $\mathcal{C}=\{Y_1, Y_2, \dots, Y_n\}$ de \mathfrak{g} e \mathfrak{h} respectivamente. Se \mathfrak{g} e \mathfrak{h} tem as mesmas constantes de estrutura c_{ij}^k e definirmos a transformação linear $\phi : \mathfrak{g} \longrightarrow \mathfrak{h}$, tal que $\phi(X_i) = Y_i$, então para todo $X = \sum_i a_i X_i$ e $Y = \sum_j b_j X_j$ em \mathfrak{g} , temos:

$$\begin{aligned} \phi([X, Y]) &= \sum_{i,j,k} a_i b_j c_{ij}^k Y_k \\ &= \sum_{i,j} a_i b_j [Y_i, Y_j] \\ &= [\phi(X), \phi(Y)] \end{aligned}$$

como consequência temos que as álgebras de Lie \mathfrak{g} e \mathfrak{h} são isomorfas.

Reciprocamente, se $\phi : \mathfrak{g} \longrightarrow \mathfrak{h}$ é um isomorfismo, então existem bases $\mathcal{B}=\{X_1, X_2, \dots, X_n\}$ e $\mathcal{C}=\{Y_1, Y_2, \dots, Y_n\}$ de \mathfrak{g} e \mathfrak{h} respectivamente, tal que, $\phi(X_i) = Y_i$. Consideremos as constantes de estrutura a_{ij}^k, b_{ij}^k de \mathfrak{g} e \mathfrak{h} com relação as bases \mathcal{B} e \mathcal{C} respectivamente, assim,

$$[Y_i, Y_j] = \phi([X_i, X_j]) = \sum_k a_{ij}^k \phi(X_k) = \sum_k a_{ij}^k Y_k.$$

Por outro lado, temos $[Y_i, Y_j] = \sum_k b_{ij}^k Y_k$, logo $\sum_k a_{ij}^k Y_k = \sum_k b_{ij}^k Y_k$, portanto, $a_{ij}^k = b_{ij}^k$. □

Exemplo 1.2.5. A menos de isomorfismo, existem apenas duas álgebras de Lie de dimensão dois. Uma delas é a abeliana e a outra é a que admite base $\{X, Y\}$, com $[X, Y] = Y$.

1.3 Soma direta e representações de álgebras de Lie

Definição 1.3.1. Sejam $\mathfrak{g}_1, \dots, \mathfrak{g}_n$ álgebras de Lie e

$$\mathfrak{g} = \mathfrak{g}_1 \oplus \dots \oplus \mathfrak{g}_n$$

sua soma direta como espaço vetoriais. Para $X = (X_1, \dots, X_n)$ e $Y = (Y_1, \dots, Y_n) \in \mathfrak{g}$, definimos o colchete

$$[X, Y] = ([X_1, Y_1], \dots, [X_n, Y_n]),$$

equipando \mathfrak{g} de uma estrutura de álgebra de Lie em que a i -ésima componente é um ideal isomorfo a \mathfrak{g}_i .

De forma semelhante, podemos definir o produto e a soma direta de uma família arbitrária de álgebras de Lie.

Definição 1.3.2. Uma *representação* de uma álgebra de Lie \mathfrak{g} sobre k , é um par (V, ρ) , em que V é um k -espaço vetorial e $\rho : \mathfrak{g} \rightarrow \mathfrak{gl}(V)$ é um homomorfismo de álgebras de Lie.

Dizemos que V é o *espaço da representação* e sua dimensão é a **dimensão da representação**. Dizemos ainda que a representação é fiel se $\text{Ker}(\rho) = \{0\}$.

Exemplo 1.3.1. Toda álgebra de Lie \mathfrak{g} tem uma representação trivial, $\rho : \mathfrak{g} \rightarrow \mathfrak{gl}(V)$, dada por $\rho(x) = 0$, para todo $x \in \mathfrak{g}$. Para toda álgebra de Lie $\mathfrak{g} \neq 0$, essa representação nunca é fiel.

Exemplo 1.3.2. Se $\mathfrak{g} \subseteq \mathfrak{gl}(V)$ é uma subálgebra de Lie, então a inclusão define uma representação de \mathfrak{g} em V , a qual chamamos de *representação canônica*.

Exemplo 1.3.3. Seja \mathfrak{g} uma álgebra de Lie. O homomorfismo adjunto

$$\text{ad} : \mathfrak{g} \rightarrow \mathfrak{gl}(\mathfrak{g})$$

é uma representação de \mathfrak{g} , chamada *representação adjunta*.

Definição 1.3.3. Dizemos que uma álgebra de Lie \mathfrak{g} é *simples* se

1. Os únicos ideais de \mathfrak{g} são 0 e \mathfrak{g} .
2. $\dim_k \mathfrak{g} \neq 1$.

Observação 1.3.1. O fato de $\dim_k \mathfrak{g} \neq 1$ é imposto para que simplesmente exista uma compatibilidade entre os conceitos de álgebra simple e semi-simples que veremos mais adiante.

Exemplo 1.3.4. A álgebra de Lie $\mathfrak{sl}(2, k)$ é simples.

$$\mathfrak{sl}(2, k) = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \mid a, b, c \in k \right\}.$$

Todo elemento $X \in \mathfrak{sl}(2, k)$ pode ser escrito como $X = \alpha e + \beta f + \delta h$, onde

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

é a base canônica para $\mathfrak{sl}(2, k)$ e o colchete entre eles cumprem a seguinte propriedade:

$$[e, f] = h \quad [h, e] = 2e \quad [h, f] = -2f.$$

Vamos provar que, se \mathfrak{h} um ideal não-nulo de $\mathfrak{sl}(2, k)$, então $\mathfrak{h} = \mathfrak{sl}(2, k)$. De fato, tomemos $Y = \alpha e + \beta f + \gamma h \in \mathfrak{h}$ não-nulo, notemos que,

$$\begin{aligned} [Y, e] &= -\beta h + 2\gamma e \in \mathfrak{h}, & [[Y, e], e] &= -2\beta e \in \mathfrak{h} \\ [Y, f] &= \alpha h - 2\gamma f \in \mathfrak{h}, & [[Y, f], f] &= -2\alpha f \in \mathfrak{h}. \end{aligned}$$

Portanto, se α ou β são não nulos, então \mathfrak{h} contém e ou f , assim $\mathfrak{h} = \mathfrak{sl}(n, k)$. Por outro lado, se $\alpha = \beta = 0$, então $\gamma \neq 0$ e portanto $h \in \mathfrak{h}$, logo $\mathfrak{h} = \mathfrak{sl}(n, k)$.

Podemos verificar que há uma relação entre representações de álgebras de Lie com módulos, eles podem nos fornecer informações importantes sobre a álgebra de Lie, como o Lema de Schur, que será mostrado em seguida.

Definição 1.3.4. Seja \mathfrak{g} uma álgebra de Lie sobre um corpo k . Um \mathfrak{g} -*módulo* é um par (M, \cdot) em que:

- (M1) M é um k -espaço vetorial,
- (M2) A aplicação $\cdot : \mathfrak{g} \times M \longrightarrow M$ é k -bilinear, em que associa $(x, m) \mapsto x \cdot m$, chamada **ação** de \mathfrak{g} sobre M
- (M3) $[x, y] \cdot m = x \cdot (y \cdot m) - y \cdot (x \cdot m) \forall x, y \in \mathfrak{g}$ e $m \in M$, compatibilidade com o colchete.

Notemos que, a condição (M2) implica que para cada $x \in \mathfrak{g}$, a aplicação $T_x : M \longrightarrow M$ onde $T_x(m) = x \cdot m$, é um endomorfismo linear de M , em outras palavras, os elementos de \mathfrak{g} agem sobre M por aplicações lineares

$$\begin{aligned} T : \mathfrak{g} &\longrightarrow \text{End}(M) \\ x &\mapsto T_x : M \longrightarrow M \\ & \quad m \mapsto T_x(m) = x \cdot m. \end{aligned}$$

Observação 1.3.2. Sejam \mathfrak{g} uma álgebra de Lie e (M, ρ) uma representação de \mathfrak{g} , então V é um \mathfrak{g} -módulo, pois, basta definir

$$\begin{aligned} \cdot : \mathfrak{g} \times M &\longrightarrow M \\ (x, m) &\mapsto x \cdot m = \rho_x(m). \end{aligned}$$

Reciprocamente, dado um \mathfrak{g} -módulo M , então (M, ρ) é uma representação de \mathfrak{g} , em que,

$$\begin{aligned} \rho : \mathfrak{g} &\longrightarrow \mathfrak{gl}(M) \\ x &\mapsto \rho_x : M \longrightarrow M \\ & \quad m \mapsto \rho_x(m) = x \cdot m. \end{aligned}$$

Portanto existe uma correspondência biunívoca,

$$\{\text{Representações de } \mathfrak{g}\} \xleftrightarrow{1-1} \{\mathfrak{g}\text{-módulos}\}.$$

Exemplo 1.3.5. Sejam M um k -espaço vetorial e \mathfrak{g} uma subálgebra de Lie de $\mathfrak{gl}(M)$, podemos verificar facilmente que M é um \mathfrak{g} -módulo, onde $x \cdot m$ é dado pela imagem de m pela aplicação linear x , isto é,

$$\begin{aligned} \cdot : \mathfrak{g} \times M &\longrightarrow M \\ (x, m) &\mapsto x \cdot m = x(m). \end{aligned}$$

Sejam \mathfrak{g} uma álgebra de Lie e V um \mathfrak{g} -módulo, dizemos que um subespaço W de V é um **submódulo** de V , se W é invariante pela ação de \mathfrak{g} , isto é, para cada $x \in \mathfrak{g}$ e $w \in W$, temos $x \cdot w \in W$.

Definição 1.3.5. Seja W um submódulo do \mathfrak{g} -módulo V . Como em outras estruturas, podemos também dar uma estrutura de \mathfrak{g} -módulo ao espaço quociente V/W . Essa estrutura é dada por:

$$x \cdot (v + W) := (x \cdot v) + W \text{ para todo } x \in \mathfrak{g} \text{ e } v \in V.$$

A este módulo chamamos de *quociente* ou *módulo de fator*. É fácil ver que essa ação de \mathfrak{g} em V/W independe dos representantes, ou seja, está bem definida.

Um homomorfismo de \mathfrak{g} -módulos é uma aplicação linear $\phi : V \longrightarrow W$, tal que, $\phi(x \cdot v) = x \cdot \phi(v) \quad \forall x \in \mathfrak{g} \text{ e } v \in V$. É fácil verificar que o *Teorema do Isomorfismo* é ainda válido para \mathfrak{g} -módulos.

Observação 1.3.3. As categorias de representações de \mathfrak{g} e de \mathfrak{g} -módulos são equivalentes.

Definição 1.3.6. Seja \mathfrak{g} uma álgebra de Lie. Dizemos que um \mathfrak{g} -módulo V é *irredutível* ou *simples*, se tem precisamente dois \mathfrak{g} -submódulos, o próprio e o $\{0\}$.

Observação 1.3.4. Usando a Observação 1.3.3, podemos dizer que no contexto de representações, uma representação ρ de \mathfrak{g} em V é irredutível se os únicos subespaços invariantes por ρ_x para todo $x \in \mathfrak{g}$, são os triviais, isto é, $\{0\}$ e V .

Exemplo 1.3.6. Sejam \mathfrak{g} uma álgebra de Lie simples e seja $(\mathfrak{g}, \text{ad})$ a representação adjunta, então \mathfrak{g} é um \mathfrak{g} -módulo irredutível.

Definição 1.3.7. Seja \mathfrak{g} uma álgebra de Lie. Dizemos que um \mathfrak{g} -módulo V é *indecomponível* se não houver submódulos não-nulos U e W tal que $V = U \oplus W$.

Podemos verificar que um \mathfrak{g} -módulo V irredutível é indecomponível, mas a recíproca não é válida.

Definição 1.3.8. Seja V um \mathfrak{g} -módulo. V é dito *completamente redutível*, se pode ser escrito como soma direta finita de \mathfrak{g} -módulos irredutíveis, isto é, $V = \bigoplus V_i$ com V_i um \mathfrak{g} -módulo irredutível.

Exemplo 1.3.7. Seja $\mathfrak{g} = d(n)$ a subálgebra de $\mathfrak{gl}(n)$, consistindo de todas as matrizes diagonais. Seja o k -espaço vetorial $V = k^n$, defina $D \cdot v = D.v \forall D \in \mathfrak{g}$ e $v \in V$, em que $D.v$ indica o produto usual de matrizes. Assim, V torna-se um \mathfrak{g} -módulo completamente redutível. De fato, se $V_i = \text{Span}\{e_i\}$, então V_i é um \mathfrak{g} -submódulo de dimensão 1 e logo irredutível, no qual $V = \bigoplus V_i$.

Um dos resultados importantes na teoria de representações (ou módulos), no qual envolvem representações irredutíveis é o *Lema de Schur*, o qual diz:

Lema de Schur 1. Seja \mathfrak{g} uma álgebra de Lie sobre k e seja S um \mathfrak{g} -módulo irredutível de dimensão finita. A aplicação $\theta : S \rightarrow S$ é um homomorfismo de \mathfrak{g} -módulos se, e somente se, θ é um múltiplo por escalar da transformação identidade, isto é, $\theta = \lambda \text{Id}_S$, para algum $\lambda \in k$.

Demonstração. Suponhamos que $\theta : S \rightarrow S$ é um homomorfismo de \mathfrak{g} -módulos, como k é algebricamente fechado e θ é, em particular, uma transformação linear de espaços vetoriais, então θ possui um autovalor $\lambda \in k$. Agora $\theta - \lambda \text{Id}_S$ é um homomorfismo de \mathfrak{g} -módulos, o $\text{Ker}(\theta - \lambda \text{Id}_S)$ possui um λ -autovetor de θ , e assim $\text{Ker}(\theta - \lambda \text{Id}_S)$ é um submódulo não-nulo de S , como S é irredutível, $\text{Ker}(\theta - \lambda \text{Id}_S) = S$, portanto $\theta = \lambda \text{Id}_S$. A recíproca é claramente válida. \square

Com o Lema de Schur, temos muitas aplicações, como:

Lema 1.3.1. Seja \mathfrak{g} uma álgebra de Lie sobre um corpo algebricamente fechado e seja V um \mathfrak{g} -módulo irredutível. Se $z \in Z(\mathfrak{g})$, então z age por multiplicação escalar em V , isto é, existe $\lambda \in k$, tal que, $z \cdot v = \lambda v$, $\forall v \in V$.

Demonstração. Defina a aplicação $v \rightarrow z \cdot v$, $\forall v \in V$. Essa aplicação é um homomorfismo de \mathfrak{g} -módulo irredutível. De fato, seja $x \in \mathfrak{g}$, então:

$$z \cdot (x \cdot v) = x \cdot (z \cdot v) + [z, x] \cdot v = x \cdot (z \cdot v), \text{ onde } z \in Z(\mathfrak{g}).$$

Agora, aplicando Lema de Schur, tem-se que existe $\lambda \in k$, tal que, $z \cdot v = \lambda v$, para todo $v \in V$. \square

1.4 Álgebras de Lie solúveis e semi-simples

1.4.1 Série derivada

Seja \mathfrak{g} uma álgebra de Lie. Define-se por indução os seguintes subespaços de \mathfrak{g} :

$$\begin{aligned} \mathfrak{g}^{(0)} &= \mathfrak{g} \\ \mathfrak{g}^{(1)} &= [\mathfrak{g}, \mathfrak{g}] \\ &\vdots \\ \mathfrak{g}^{(j)} &= [\mathfrak{g}^{(j-1)}, \mathfrak{g}^{(j-1)}]. \end{aligned}$$

Esses subespaços são na verdade ideais de \mathfrak{g} (Proposição 1.1.2). Notemos que elas cumprem uma sequência de ideais, ou seja,

$$\mathfrak{g} = \mathfrak{g}^{(0)} \supseteq \mathfrak{g}^{(1)} \supseteq \dots \supseteq \mathfrak{g}^{(j)} \supset \dots$$

Essa sequência de ideais é conhecida por *série derivada* de \mathfrak{g} onde suas componentes são chamadas de *álgebras derivadas* de \mathfrak{g} .

Definição 1.4.1. Uma álgebra de Lie \mathfrak{g} é dita *solúvel*, se alguma de suas álgebras derivadas se anula, isto é,

$$\mathfrak{g}^{(n)} = 0$$

para algum $n \geq 1$ (e portanto, $\mathfrak{g}^{(j)} = 0$, para todo $j \geq n$).

Exemplo 1.4.1. As álgebras abelianas são solúveis, pois $\mathfrak{g}^{(1)} = 0$.

Exemplo 1.4.2. Toda álgebra de Lie \mathfrak{g} de dimensão 2 é solúvel. De fato, pelo Exemplo 1.2.5, \mathfrak{g} é abeliana ou existe uma base $\{X, Y\}$, tal que, $[X, Y] = Y$. Segue do Exemplo 1.4.1 que, se \mathfrak{g} é abeliana então \mathfrak{g} é solúvel. Se \mathfrak{g} não é abeliana, então, têm álgebra derivada de dimensão 1 e, portanto, a segunda derivada se anula.

Proposição 1.4.1. Seja \mathfrak{g} uma álgebra de Lie.

- (1) Se \mathfrak{g} é solúvel, então também são, todas subálgebra e imagens homomorficas de \mathfrak{g} .
- (2) Se \mathfrak{h} é um ideal solúvel de \mathfrak{g} , tal que, $\mathfrak{g}/\mathfrak{h}$ é solúvel, então \mathfrak{g} é solúvel.
- (3) Se \mathfrak{h}_1 e \mathfrak{h}_2 são ideais solúveis de \mathfrak{g} , então $\mathfrak{h}_1 + \mathfrak{h}_2$ é um ideal solúvel.

Demonstração. A demonstração pode ser encontrada em ([12], Cap. 1, p.11). □

Proposição 1.4.2. Seja \mathfrak{g} uma álgebra de Lie de dimensão finita. Então, existe em \mathfrak{g} um único ideal solúvel $\mathfrak{r} \subset \mathfrak{g}$ que contém todos os ideais solúveis de \mathfrak{g} .

Demonstração. Seja n o máximo das dimensões dos ideais solúveis de \mathfrak{g} e seja \mathfrak{r} um ideal solúvel com $\dim \mathfrak{r} = n$. Então, todo ideal solúvel de \mathfrak{g} está contido em \mathfrak{r} . De fato, seja \mathfrak{h} um ideal solúvel de \mathfrak{g} , então, $\mathfrak{r} + \mathfrak{h}$ também é solúvel. Pela maximalidade da dimensão, $\dim(\mathfrak{r} + \mathfrak{h}) = \dim \mathfrak{r}$, assim $\mathfrak{r} + \mathfrak{h} \subset \mathfrak{r}$, segue que, $\mathfrak{h} \subset \mathfrak{r}$. Portanto, \mathfrak{r} contém todos ideais solúveis de \mathfrak{g} e ele é evidente o único. □

O ideal \mathfrak{r} da Proposição 1.4.2 é chamado de **radical solúvel** de \mathfrak{g} , no qual denotaremos por $\mathfrak{r}(\mathfrak{g})$. Assim uma álgebra de Lie é solúvel se $\mathfrak{r}(\mathfrak{g}) = \mathfrak{g}$.

1.4.2 Álgebra semi-simples

Definição 1.4.2. Uma álgebra de Lie é dita *semi-simples* se

$$\mathfrak{r}(\mathfrak{g}) = 0$$

ou seja, \mathfrak{g} não contém ideais solúveis além do 0.

Para uma álgebra semi-simples \mathfrak{g} , o seu centro é um ideal necessariamente nulo. Como o centro de uma álgebra de Lie é o núcleo da representação adjunta, segue que, a representação adjunta de uma álgebra semi-simples é fiel, assim, toda álgebra semi-simples pode ser vista como uma subálgebra de $\mathfrak{gl}(\mathfrak{g})$.

Exemplo 1.4.3. As álgebras simples são semi-simples. De fato, \mathfrak{g} não contém ideais exceto \mathfrak{g} e 0 . Como $\mathfrak{r}(\mathfrak{g})$ é um ideal, ele deve ser 0 ou \mathfrak{g} . No primeiro caso, \mathfrak{g} é semi-simples como se pretende. O segundo caso, não pode ocorrer, pois $\mathfrak{r}(\mathfrak{g}) = \mathfrak{g}$ implica em \mathfrak{g} ser solúvel e, portanto $\mathfrak{g}' \neq \mathfrak{g}$. Como \mathfrak{g}' também é um ideal, $\mathfrak{g}' = 0$, isto é, \mathfrak{g} é abeliana, logo todo subespaço de uma álgebra abeliana é um ideal, o que não pode acontecer, pois, $\dim_k \mathfrak{g} \geq 2$.

Exemplo 1.4.4. A álgebra de Lie $\mathfrak{sl}(2, \mathbb{C})$ é semi-simples, pois não possui ideais próprios.

Proposição 1.4.3. Sejam \mathfrak{g} uma álgebra de Lie que não é solúvel e $\mathfrak{h} \subset \mathfrak{g}$ um ideal solúvel. Então, $\mathfrak{g}/\mathfrak{h}$ é semi-simples se, e somente se, $\mathfrak{h} = \mathfrak{r}(\mathfrak{g})$.

Demonstração. A demonstração pode ser consultada em ([20], Cap. 1, 51). □

1.5 Álgebras de loop

Nesta seção, fixaremos um corpo k algebricamente fechado de característica zero e $(\zeta_n)_{n \geq 1}$ uma família compatível de n -ésimas raízes primitivas da unidade em k .

Consideremos nesta seção uma álgebra de Lie \mathfrak{g} de dimensão finita sobre k e σ um automorfismo de \mathfrak{g} de período m . Usaremos o símbolo \otimes , para indicar o produto tensorial sobre o corpo k . As principais referências para esta seção são, [1], [17] e [24].

1.5.1 Definição e algumas propriedades

Consideremos o seguinte conjunto,

$$\mathfrak{g}_{\bar{i}} = \{x \in \mathfrak{g} \mid \sigma(x) = \zeta_m^i x\},$$

onde ζ_m é uma m -ésima raiz primitiva da unidade em k , $i \in \mathbb{Z}$ e $i \rightarrow \bar{i}$ é a projeção natural da aplicação $\mathbb{Z} \rightarrow \Gamma := \mathbb{Z}/m\mathbb{Z}$. A álgebra de Lie \mathfrak{g} pode ser decomposta em autoespaços

$$\mathfrak{g} = \bigoplus_{\bar{i} \in \Gamma} \mathfrak{g}_{\bar{i}}. \quad (1.1)$$

Podemos notar que $\mathfrak{g}_{\bar{0}} = \mathfrak{g}^\sigma$, isto é, o conjunto dos pontos fixos de σ em \mathfrak{g} .

Seja $R := k[t, t^{-1}]$ a k -álgebra dos polinômios de Laurent na variável t . Podemos identificar R com uma k -subálgebra do anel polinomial de Laurent na variável z de

$$S := k[z, z^{-1}]$$

via

$$t = z^m \text{ e } t^{-1} = z^{-m}.$$

Desta forma S é uma R -álgebra. Este anel pode também ser denotado por $S = k[t^{\frac{1}{m}}, t^{-\frac{1}{m}}]$. Consideremos a S -álgebra de Lie

$$\mathfrak{g}(S) := \mathfrak{g} \otimes S, \quad [x \otimes z^i, y \otimes z^j] = [x, y] \otimes z^{i+j}.$$

Podemos identificar essa álgebra de Lie $\mathfrak{g}(S)$ com $\mathfrak{g}[z, z^{-1}]$. Assim temos:

$$\mathfrak{g}(S) = \bigoplus_{i \in \mathbb{Z}} (\mathfrak{g} \otimes z^i).$$

Fixando a componente $\mathfrak{g} \otimes z^j$, por (1.1), temos,

$$\begin{aligned} \mathfrak{g} \otimes z^j &= \left(\bigoplus_{\bar{i} \in \Gamma} \mathfrak{g}_{\bar{i}} \right) \otimes z^j \\ &= \bigoplus_{\bar{i} \in \Gamma} (\mathfrak{g}_{\bar{i}} \otimes z^j) \\ &= \bigoplus_{\bar{i} \neq \bar{j} \in \Gamma} (\mathfrak{g}_{\bar{i}} \otimes z^j) \oplus (\mathfrak{g}_{\bar{j}} \otimes z^j) \end{aligned}$$

Observação 1.5.1. A noção de álgebra de Lie se estende de forma natural a um anel de base, isto é para A um anel comutativo com unidade é possível definir sem problemas a noção de A -álgebra de Lie, vide ([23], Cap.1, Parte 1).

Definição 1.5.1. A **álgebra de loop** de \mathfrak{g} relativo a σ é a subálgebra

$$L(\mathfrak{g}, \sigma) := \bigoplus_{j \in \mathbb{Z}} \mathfrak{g}_{\bar{j}} \otimes z^j$$

da álgebra $\mathfrak{g}(S)$, onde $\bar{j} \in \mathbb{Z}/m\mathbb{Z}$ é a imagem de $j \in \mathbb{Z}$ pelo homomorfismo canônico.

As álgebras de loop satisfazem as seguintes propriedades:

Propriedades 1.5.1.

- $L(\mathfrak{g}, \sigma)$ é uma R -subálgebra de $\mathfrak{g}(S)$, e portanto uma k -álgebra.
- Para todo $i \in \mathbb{Z}$, existe um único R -automorfismo de S , que denotamos por \underline{i} tal que

$$\underline{i}(z) = \zeta_m^i z.$$

Então a aplicação $\bar{i} \mapsto \underline{i}$ é um isomorfismo de Γ para o grupo de todos os R -automorfismo de S , que denotaremos por $Aut_R(S)$.

- $Aut_R(S)$ é gerado por $\underline{1}$, onde $\underline{1}(z) = \zeta_m z$.

Exemplo 1.5.1. Se $\sigma = \text{Id}$ e $m = 1$, então $L(\mathfrak{g}, \text{Id}) = \mathfrak{g} \otimes R$. Esta álgebra de loop é chamada de não-torcida ou untwisted e denotada por $L(\mathfrak{g})$. Dizemos que $L(\mathfrak{g}, \sigma)$ é **trivial**, se $L(\mathfrak{g}, \sigma) \simeq_k \mathfrak{g} \otimes R$.

Uma definição alternativa para uma álgebra de loop, pode ser dada da seguinte forma: Seja σ um automorfismo de \mathfrak{g} de período m , e ζ_m uma m -ésima raiz primitiva da unidade, estendendo o automorfismo σ , para um automorfismo $\tilde{\sigma}$ da álgebra de Lie $\mathfrak{g}(S)$, dado por

$$\begin{aligned} \tilde{\sigma} : \mathfrak{g}(S) &\longrightarrow \mathfrak{g}(S) \\ e_r \otimes z^k &\longmapsto \zeta_m^{-k} \sigma(e_r) \otimes z^k, \end{aligned}$$

onde $\{e_r\}$ e $\{z^k\}$ são bases de \mathfrak{g} e S , respectivamente. Definimos a **álgebra de loop** de \mathfrak{g} relativo a σ , por

$$L(\mathfrak{g}, \sigma) = (\mathfrak{g}(S))^{\tilde{\sigma}} = \{a \in \mathfrak{g}(S) \mid \tilde{\sigma}(a) = a\}. \quad (1.2)$$

Propriedades 1.5.2.

- (a) $L(\mathfrak{g}, \sigma^{-1}) \simeq_k L(\mathfrak{g}, \sigma)$.
- (b) Se $\tau \in \text{Aut}_k(\mathfrak{g})$, então $L(\mathfrak{g}, \tau\sigma\tau^{-1}) \simeq_R L(\mathfrak{g}, \sigma)$.

Demonstração.

- (a) Seja $\kappa : S \longrightarrow S$ o automorfismo da k -álgebra S , tal que, $\kappa(z) := z^{-1}$, então a aplicação $\text{id} \otimes \kappa$ é um automorfismo da k -álgebra $\mathfrak{g}(S)$, que aplica $L(\mathfrak{g}, \sigma)$ em $L(\mathfrak{g}, \sigma^{-1})$.
- (b) Seja $\tau \in \text{Aut}_k(\mathfrak{g})$. Então a aplicação $\tau \otimes \text{id}$ é um automorfismo da R -álgebra $\mathfrak{g}(S)$, que aplica $L(\mathfrak{g}, \sigma)$ em $L(\mathfrak{g}, \tau\sigma\tau^{-1})$. □

Definimos agora a noção de S/R -forma de uma álgebra. Para isso observamos que:

$$\mathfrak{g}(S) = \mathfrak{g} \otimes S = \mathfrak{g} \otimes R \otimes_R S = \mathfrak{g}(R) \otimes_R S.$$

Definição 1.5.2. Uma S/R -forma de $\mathfrak{g}(R)$ é uma R -álgebra A , tal que

$$A \otimes_R S \simeq \mathfrak{g}(R) \otimes_R S$$

como S -álgebras.

Este conceito nos será útil no próximo capítulo. Pela identificação $t = z^m$ e $t^{-1} = z^{-m}$, podemos notar que S é um R -módulo livre com base $1, z, \dots, z^{m-1}$ e obtemos então a seguinte proposição.

Proposição 1. Se A é uma S/R forma de $\mathfrak{g}(R)$, então A pode ser identificado com uma R -subálgebra de $\mathfrak{g}(S)$, tal que cada elemento de $\mathfrak{g}(S)$, pode ser expresso unicamente na forma $\sum_{i=0}^{m-1} z^i y_i$, onde $y_i \in A$ para $i = 0, \dots, m-1$. Reciprocamente, qualquer R -subálgebra A de $\mathfrak{g}(S)$ com esta propriedade é uma S/R forma de $\mathfrak{g}(R)$.

Assim observamos que toda álgebra de loop $L(\mathfrak{g}, \sigma)$, é uma S/R -forma de $\mathfrak{g} \otimes R$.

Capítulo 2

Cohomologia Galoisiana

Neste capítulo começamos por expor a teoria da cohomologia galoisiana e a teoria da cohomologia não-abeliana. A teoria de cohomologia não-abeliana pode ser visto como uma generalização parcial da cohomologia galoisiana para grupos de coeficientes não-abelianos. Definiremos a noção de espaço principal homogêneo e mostraremos que as álgebras de loop podem ser identificados com espaços principais homogêneos sobre $R = k[t, t^{-1}]$. Assim mostraremos que as álgebras de loop podem ser classificadas (como R -álgebras) por um conjunto desta cohomologia não-abeliana.

2.1 O Grupo de Galois como grupo profinito

Começamos por lembrar algumas definições básicas sobre grupo de Galois. Observamos que o grupo de Galois, por definição, é completamente determinado por seus quocientes finitos. Ele é o que chamamos de um grupo profinito. Como veremos em seguida, um grupo profinito é um grupo que é limite inverso (ou projetivo) de grupos finitos e assim é naturalmente munido de uma topologia. Assim um grupo profinito é um grupo topológico. A cohomologia galoisiana então pode ser enxergado como a cohomologia do grupo de Galois (do ponto de vista da teoria de cohomologia de grupos), levando em conta a topologia da qual ele é munido, isto é, só serão considerados aplicações contínuas para a construção dos grupos de cohomologia. Aqui daremos uma definição explícita dos grupos de cohomologia com cocadeias, seguindo J.P. Serre [21].

A teoria da cohomologia galoisiana tem aplicações e sua motivação originou-se principalmente na teoria algébrica dos números, ilustraremos isso ao mostrarmos no caminho alguns teoremas clássicos como **Hilbert 90** e **Teoria de Kummer**. No final do capítulo mostraremos como a cohomologia galoisiana pode ter um papel na classificação de álgebras de loop.

Definição 2.1.1. Suponha que K é uma extensão do corpo k (denotada por K/k). Diz-se que um automorfismo de K é um K/k -automorfismo, ou um automorfismo de K/k , se ele fixa os elementos de k .

Em outras palavras, um automorfismo de K/k é um isomorfismo ϕ de K para K tal que $\phi(x) = x$ para todo $x \in k$. Podemos verificar que o conjunto de todos os automorfismos de K/k , forma um grupo com a operação composição de funções, o qual denotamos por $Aut(K/k)$.

Definição 2.1.2. Se K/k é uma extensão de Galois então $Aut(K/k)$ é chamado de grupo de Galois da extensão K/k e o denotamos por $Gal(K/k)$.

2.1.1 Grupos topológicos

Definição 2.1.3. Um conjunto G de elementos é chamado *grupo topológico*, se satisfaz as seguintes propriedades:

- (1) G é um grupo,
- (2) G é um espaço topológico,
- (3) A aplicação $m : G \times G \longrightarrow G$, definida por $m(a, b) = ab$ é contínua, onde $G \times G$ é equipada com a topologia produto,
- (4) A aplicação $i : G \longrightarrow G$, definida por $i(a) = a^{-1}$ é contínua.

Observação 2.1.1. As propriedades (3) e (4) podem ser reformuladas respectivamente da seguinte forma:

- Se $a, b \in G$, então para todo aberto $U \subseteq G$ tal que $m(a, b) = ab \in U$, existem abertos V_1 e V_2 , com $a \in V_1$ e $b \in V_2$, tal que $m(V_1 \times V_2) = V_1 V_2 \subseteq U$.
- Se $a \in G$, então para todo aberto $U \subseteq G$, com $i(a) = a^{-1} \in U$, existe um aberto V , tal que $a \in V$, de tal forma que $i(V) = V^{-1} \subseteq U$.

Exemplo 2.1.1.

- Todo grupo munido da topologia discreta, é um grupo topológico.
- O grupo aditivo dos números reais $(\mathbb{R}, +)$ munido da topologia usual de \mathbb{R} , é um grupo topológico.

Definição 2.1.4. Um homomorfismo de grupos topológicos é um homomorfismo de grupos contínuo.

A partir da definição acima, podemos ver que um isomorfismo de grupos topológicos é um homeomorfismo.

Proposição 2.1.1. Seja G um grupo topológico. Para cada $g \in G$, as seguintes aplicações, são homeomorfismos:

- Translação a esquerda: $f_g : G \longrightarrow G$, $f_g(h) = gh$,
- Translação a direita: $\phi_g : G \longrightarrow G$, $\phi_g(h) = hg$,
- Inversão: $i : G \longrightarrow G$, $i(h) = h^{-1}$,
- Conjugação: $\rho_g : G \longrightarrow G$, $\rho_g(h) = ghg^{-1}$.

Demonstração. Perceba que f_g é a restrição da aplicação m ao subconjunto $g \times G$. Como por definição m é contínua, sua restrição também será contínua. Considere a aplicação contínua $f_{g^{-1}}$ como foi definida acima, então:

$$\begin{aligned} (f_g \circ f_{g^{-1}})(h) &= f_g(f_{g^{-1}}(h)) = f_g(g^{-1}h) = gg^{-1}h = h \\ (f_{g^{-1}} \circ f_g)(h) &= f_{g^{-1}}(f_g(h)) = f_{g^{-1}}(gh) = g^{-1}gh = h \end{aligned}$$

Portanto, f_g é um homeomorfismo. Análogo para os demais itens. \square

Podemos verificar que o subgrupo de um grupo topológico também é um grupo topológico.

Proposição 2.1.2. Seja G um grupo topológico e $H \leq G$ subgrupo. Então H é um grupo topológico.

Demonstração. É fácil ver que H é um espaço topológico e um grupo. Basta mostrar que as aplicações m e i são contínuas, mas a restrição de uma aplicação contínua a um subconjunto é contínua. Portanto, H é um espaço topológico. \square

2.1.2 Limite inverso

Para procedermos precisamos de algumas definições técnicas. Como veremos nesta seção, o fato que o grupo de galois é determinado por seus quocientes finitos, em outras palavras pode ser expresso matematicamente como um limite inverso de grupos finitos.

Definição 2.1.5. Um conjunto não-vazio (I, \preceq) é chamado conjunto dirigido, se satisfaz a seguintes condições:

- (1) $i \preceq i$, para todo $i \in I$.
- (2) Se $i \preceq j$ e $j \preceq k$, então $i \preceq k$, para todo $i, j, k \in I$.
- (3) Se $i, j \in I$, então existe um $k \in I$, tal que, $i, j \preceq k$.

Exemplo 2.1.2. Seja I o conjunto formado por todos os subgrupos normais de índice finito de um grupo G . Em I defina a seguinte ordem: $U_\alpha \preceq U_\beta \iff U_\beta \subset U_\alpha$. Então I é um conjunto dirigido.

Definição 2.1.6. Seja I um conjunto dirigido. Um sistema inverso (ou projetivo) $(X_i, f_{ij})_I$ de espaços topológicos indexados por I , consiste de uma família $\{X_i \mid i \in I\}$ de espaços topológicos e de uma família $\{f_{ij} : X_j \rightarrow X_i \mid i, j \in I, i \preceq j\}$ de aplicações contínuas, tais que:

- (1) f_{ii} é a identidade sobre X_i , para todo $i \in I$.
- (2) $f_{ij} \circ f_{jk} = f_{ik}$, para todo $i \preceq j \preceq k \in I$.

Exemplo 2.1.3. Considere o seguinte conjunto dirigido (\mathbb{Z}, \preceq) , com $n \preceq m$ se, e somente se, n divide m , para todo $m, n \in \mathbb{Z}$. Considere $\mathbb{Z}/m\mathbb{Z}$ junto com a projeção natural

$$f_{nm} : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, \text{ com } f_{nm}(k + m\mathbb{Z}) = k + n\mathbb{Z}$$

A aplicação acima está bem definida pela relação dada no conjunto dirigido, e temos ainda que, $f_{nm} \circ f_{mj} = f_{nj}$, para todo $n \preceq m \preceq j \in \mathbb{Z}$. Então $(\mathbb{Z}/m\mathbb{Z}, f_{nm})_{\mathbb{Z}}$ é um sistema inverso.

Definição 2.1.7. Se Y é um espaço topológico, chamamos a família de aplicações contínuas $\{\psi_i : Y \rightarrow X_i\}_{i \in I}$ de compatível, se $f_{ij} \circ \psi_j = \psi_i$ para todo $i \preceq j \in I$. Em outras palavras o seguinte diagrama é comutativo.

$$\begin{array}{ccc} & Y & \\ \psi_j \swarrow & & \searrow \psi_i \\ X_j & \xrightarrow{f_{ij}} & X_i \end{array}$$

Definição 2.1.8. Um limite inverso (ou projetivo) (X, ψ_i) (denotado por $\lim_{\leftarrow I} X_i$) de um sistema inverso $(X_i, f_{ij})_I$ de espaços topológicos, é um espaço topológico X , equipado com uma família compatível $\{\psi_i : X \rightarrow X_i\}_{i \in I}$ satisfazendo a seguinte propriedade universal: Para todo espaço topológico Y e para toda família compatível $\{\phi_i : Y \rightarrow X_i\}_{i \in I}$, existe uma única aplicação contínua $\theta : Y \rightarrow X$, tal que o seguinte diagrama é comutativo para todo $i \preceq j \in I$.

$$\begin{array}{ccc} & Y & \\ \exists! \downarrow \theta & & \\ \phi_j \swarrow & X & \searrow \phi_i \\ \psi_j \swarrow & & \searrow \psi_i \\ X_j & \xrightarrow{f_{ij}} & X_i \end{array}$$

Podemos garantir a *existência e a unicidade*, a menos de um homeomorfismo, do limite inverso $\lim_{\leftarrow I} X_i$ de um sistema inverso $(X_i, f_{ij})_I$, o leitor interessado pode consultar a demonstração em ([19], Cap.1, p.2). Se considerarmos ainda, o caso de um sistema inverso $(G_i, f_{ij})_I$, onde cada G_i é um grupo topológico, então $\lim_{\leftarrow I} G_i$ é um subgrupo topológico de $\prod_{i \in I} G_i$, consistindo de seqüências (g_i) , tal que, $f_{ij}(g_j) = g_i$, $i \leq j$. Podemos agora definir o que é um *grupo profinito*.

Definição 2.1.9. Um *grupo profinito* G é um grupo topológico que é isomorfo a um limite inverso de um sistema inverso $(G_i, f_{ij})_I$ de grupos finitos, onde cada G_i é munido com a topologia discreta.

Exemplo 2.1.4. De acordo com o Exemplo 2.1.3, $(\mathbb{Z}/m\mathbb{Z}, f_{nm})_{\mathbb{Z}}$ é um sistema inverso, onde denotamos $\widehat{\mathbb{Z}} := \lim_{\leftarrow m \in \mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ como seu limite inverso. $\widehat{\mathbb{Z}}$ é chamado de *grupo de Prüfer*.

Teorema 2.1.1. Seja K/k uma extensão galoisiana e seja a coleção $\mathcal{F} = \{K' \mid k \subseteq K' \subseteq K, K'/k \text{ extensão galoisiana}\}$. Então, $\text{Gal}(K/k)$ é o limite inverso do grupo finito $\text{Gal}(K'/k)$ com $K' \in \mathcal{F}$; em particular, $\text{Gal}(K/k)$ é um grupo profinito.

Demonstração. A demonstração pode ser consultada em ([19], Cap. 2, p.68). □

2.2 Cohomologia galoisiana

Nesta seção introduziremos a cohomologia galoisiana. Faremos uma construção explícita aqui, baseada na abordagem de J.P. Serre em [21]. Esta construção, em particular a definição de cocadeias, é baseada na cohomologia de complexos simpliciais da topologia algébrica. Definiremos primeiro G -módulos discretos, eles podem ser vistos como os coeficientes desta teoria de cohomologia. Em seguida mostraremos como estas definições nos fornecem uma teoria cohomológica.

2.2.1 G -módulos discretos

Definição 2.2.1. Seja (G, \cdot) um grupo profinito. Um G -módulo discreto é um grupo abeliano $(A, +)$ equipado com a topologia discreta, em que G age continuamente em A . Em outras palavras, um G -módulo discreto é um grupo abeliano A , com uma aplicação contínua $G \times A \rightarrow A : (g, a) \mapsto g \cdot a$, em que para todo $a, b \in A$ e $g_1, g_2, g \in G$, cumprem as seguintes condições:

- (1) $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a)$,
- (2) $g \cdot (a + b) = g \cdot a + g \cdot b$,
- (3) $1_G \cdot a = a$.

Definição 2.2.2. Sejam G um grupo profinito e A e B dois G -módulos discretos. Dizemos que a aplicação $\phi : A \rightarrow B$ é um G -homomorfismo, se ϕ é um homomorfismo de grupos, tal que:

$$\phi(g \cdot a) = g \cdot \phi(a), \forall g \in G \text{ e } \forall a \in A.$$

2.2.2 Cocadeias, cociclos e cohomologia

Seja G um grupo profinito e A um G -módulo discreto. Consideremos o seguinte conjunto:

$$C^n(G, A) := \{f : G^n \rightarrow A \mid f \text{ contínua}\}.$$

Por A ser um grupo abeliano, $C^n(G, A)$ também é um grupo abeliano, o qual chamamos de grupo de n -cocadeia.

Para cada $n \geq 1$ definimos a aplicação

$$d_n : C^n(G, A) \rightarrow C^{n+1}(G, A)$$

$$\begin{aligned} (d_n f)(g_1, \dots, g_{n+1}) &= g_1 \cdot f(g_2, \dots, g_{n+1}) \\ &+ \sum_{i=1}^n (-1)^i f(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \dots, g_n), \end{aligned}$$

para todo $f \in C^n(G, A)$ e todo $(g_1, \dots, g_{n+1}) \in G^{n+1}$. E para $n = 0$ definimos por

$$(d_0 a)(g) = g \cdot a - a$$

para todo $a \in A$ e todo $g \in G$. Essas aplicações são chamadas de *operadores cobordo*. Uma fácil verificação mostra que d_n é um homomorfismo de grupos, tal que,

$$d_{n+1} \circ d_n = 0 \quad (2.1)$$

para todo n . Assim obtemos um complexo de grupos abelianos:

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

Como de costume podemos agora definir os grupos de cociclos e grupos de cobordo deste complexo:

Definição 2.2.3. Sejam G um grupo profinito e A um G -módulo discreto.

- Chamamos de grupo de n -**cociclos** de G , ao grupo $Z^n(G, A) := \text{Ker}(d_n)$,
- Chamamos de grupo de n -**cobordos** de G , ao grupo $B^n(G, A) := \text{Im}(d_{n-1})$.

A equação (2.1), implica que $B^n(G, A) \subseteq Z^n(G, A)$, isto é, $B^n(G, A)$ é um subgrupo de $Z^n(G, A)$. Assim podemos definir os grupos de cohomologia deste complexo como de costume:

Definição 2.2.4. Sejam G um grupo profinito e A um G -módulo discreto. Chamamos de n -ésimo grupo de cohomologia de G com coeficientes em A , ao grupo

$$H^n(G, A) := Z^n(G, A)/B^n(G, A).$$

Exemplo 2.2.1. Consideremos $A = \mathbb{Z}$, a qual G age trivialmente em \mathbb{Z} , então $H^1(G, A) = \text{Hom}_c(G, \mathbb{Z})$. Onde Hom_c denota todos os homomorfismos contínuos.

Podemos verificar que essa construção dos grupos de cohomologia é funtorial em relação aos G -módulos discretos, isto é:

Para todo G -homomorfismo $A \longrightarrow B$ existem aplicações canônicas

$$H^i(G, A) \longrightarrow H^i(G, B)$$

para todo i . Além disso $H^0(G, A) = A^G$, onde A^G denota os elementos de A fixos pela ação de G . No mais, uma sequência exata curta de G -módulos discretos induz uma sequência exata longa de grupos de cohomologia:

Teorema 2.2.1. Seja $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$ uma sequência exata curta de G -módulos discretos. Então existe uma sequência exata longa de grupos abelianos

$$\dots \longrightarrow H^n(A') \longrightarrow H^n(A) \longrightarrow H^n(A'') \longrightarrow H^{n+1}(A') \longrightarrow \dots$$

Demonstração. A demonstração pode ser encontrada em ([7], Cap. 4, p.90)

□

Podemos verificar que a construção acima nos fornece uma teoria de cohomologia no sentido de Henry Cartan e Samuel Eilenberg [3], vide também Philippe Gille e Tamás Szamuely 3.1 [7]. O grupo de Galois de uma extensão de corpos K/k é um grupo profinito pelo Teorema 2.1.1. A teoria exposta acima então se aplica ao grupo de Galois. Podemos então definir:

Definição 2.2.5 (Cohomologia galoisiana). Seja $G = \text{Gal}(K/k)$ o grupo de Galois da extensão de corpos K/k e A um G -módulo discreto. Então chamamos o grupo $H^n(G, A)$ de *n -ésimo grupo de cohomologia galoisiana* da extensão K/k com valores em A . Se K é um fecho separável de k então denotamos esse grupo por $H^n(k, A)$.

Exemplo 2.2.2. Se $A = k_S^*$, então $H^0(k, A) = A^G = k^*$.

Observamos que é possível também obter estes grupos de cohomologia galoisiana como limites diretos dos grupos de cohomologia dos grupos de Galois das extensões finitas. Para isso precisamos da definição de limite direto que é dual à definição de limite inverso:

Definição 2.2.6. Sejam I um conjunto dirigido e \mathfrak{C} uma categoria. Um *sistema direto* $(X_i, f_{ij})_I$ de objetos da categoria \mathfrak{C} indexados por I , consiste de uma família $\{X_i \mid i \in I\}$ de objetos e de uma família $\{g_{ij} : X_i \rightarrow X_j \mid i, j \in I, i \preceq j\}$ de morfismos, tal que:

- (1) g_{ii} é a identidade sobre X_i , para todo $i \in I$.
- (2) $g_{jk} \circ g_{ij} = g_{ik}$, para todo $i \preceq j \preceq k \in I$.

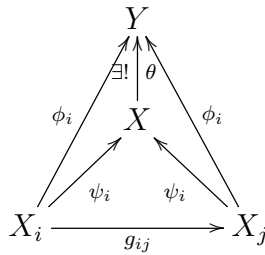
Exemplo 2.2.3. Sejam A um G -módulo discreto e I como no Exemplo 2.1.2. Seja ainda A^{U_α} o subconjunto dos pontos de A que são fixos pelos subgrupos normais de G de índice finito $U_\alpha \in I$. Consideremos $G_\alpha = G/U_\alpha$. Então:

- A^{U_α} é um G_α -módulo.
- $\phi_{\alpha\beta} : G_\beta \rightarrow G_\alpha$ induz $\text{Inf}_{\alpha\beta} : H^n(G_\alpha, A^{U_\alpha}) \rightarrow H^n(G_\beta, A^{U_\beta})$, para todo $n \geq 0$.
- $(H^n(G_\alpha, A^{U_\alpha}), \text{Inf}_{\alpha\beta})_I$ é um sistema direto.

Definição 2.2.7. Seja Y um objeto de \mathfrak{C} , chamamos a família de morfismos $\{\psi_i : X_i \rightarrow Y\}_{i \in I}$ de *compatível*, se $\psi_j \circ g_{ij} = \psi_i$ para todo $i \preceq j \in I$. Em outras palavras o seguinte diagrama é comutativo.

$$\begin{array}{ccc} & Y & \\ \psi_i \nearrow & & \nwarrow \psi_j \\ X_i & \xrightarrow{g_{ij}} & X_j \end{array}$$

Definição 2.2.8. Um *limite direto* (ou *indutivo*) (X, ψ_i) (denotado por $\lim_{\rightarrow I} X_i$) de um sistema direto $(X_i, g_{ij})_I$ de objetos de \mathfrak{C} , é um objeto X , equipado com uma família compatível $\{\psi_i : X_i \rightarrow X\}_{i \in I}$ satisfazendo a seguinte propriedade universal: Para todo objeto Y e para toda família compatível $\{\phi_i : X_i \rightarrow Y\}_{i \in I}$, existe um único morfismo de \mathfrak{C} , $\theta : X \rightarrow Y$, tal que o seguinte diagrama é comutativo para todo $i \preceq j \in I$.



Proposição 2.2.1. Sejam $(G_i, f_{ij})_I$ um sistema inverso de grupos profinito e (A_i, g_{ij}) um sistema direto de G_i -módulos discreto. Sejam ainda, $G = \varprojlim_I G_i$ e $A = \varinjlim_I A_i$. Então:

$$H^n(G, A) = \varinjlim_I H^n(G_i, A_i), \text{ para todo } n \geq 0.$$

Demonstração. [21], Cap. 1, seção 2.2 Proposição 8. □

Como corolário obtemos que os grupos de cohomologia galoisiana podem ser descritos como limite direto dos grupos de cohomologia galoisiana dos seus quocientes finitos:

Corolário 2.2.1. Consideremos $(H^n(G_\alpha, A^{U_\alpha}), \text{Inf}_{\alpha\beta})_I$, o sistema direto, Seja $G = \text{Gal}(k_S/k)$, para algum fecho separável k_S de k . Então obtemos $H^n(G, A) = \varinjlim_I H^n(G_\alpha, A^{U_\alpha})$.

Observação 2.2.1. Em alguns textos os grupos de cohomologia galoisiana são definidos desta maneira, como limites diretos dos grupos de cohomologia dos grupos de Galois das extensões finitas ([7], Cap. 4, p.86).

Para ilustrar as aplicações originais da teoria da cohomologia galoisiana, enunciemos alguns teoremas clássicos da teoria de números que podem ser formulados e provados em termos da cohomologia galoisiana.

A primeira afirmação do seguinte teorema é o Teorema **Hilbert 90**.

Teorema 2.2.2. Para toda extensão de Galois K/k , temos, $H^1(k, K^*) = 0$ e $H^n(k, K) = 0$, para todo $n \geq 1$.

Demonstração. Proposição 1 em ([21]), Cap. 2, p.72). □

Corolário 2.2.2 (Teoria de Kummer). Seja n um inteiro ≥ 1 , primo com a característica de k . Seja μ_n o grupo das n -ésima raízes da unidade em k_S . Temos:

$$H^1(k, \mu_n) = k^*/(k^*)^n.$$

Demonstração. Consideremos a seguinte sequência exata:

$$1 \longrightarrow \mu_n \longrightarrow^i k_S^* \longrightarrow^n k_S^* \longrightarrow 1$$

onde n denota o endomorfismo $x \mapsto x^n$. Pelo Teorema 2.2.1, esta sequência exata, induz uma sequência exata de cohomologia, dada por:

$$H^0(k, k_S^*) \longrightarrow H^0(k, k_S^*) \longrightarrow H^1(k, \mu_n) \longrightarrow H^1(k, k_S^*)$$

Pelo Exemplo 2.2.2 e o Teorema 2.2.2, $H^0(k, k_s^*) = k^*$ e $H^1(k, k_s^*) = 0$, logo a sequência é da forma:

$$k^* \longrightarrow k^* \longrightarrow H^1(k, \mu_n) \longrightarrow 0$$

Portanto, $H^1(k, \mu_n) = k^*/(k^*)^n$.

□

Observação 2.2.2. Se no corolário anterior, impormos a condição que $\mu_n \subset k^*$, então podemos identificar μ_n com $\mathbb{Z}/n\mathbb{Z}$ ao escolher uma n -ésima raiz primitiva da unidade. Logo, há um isomorfismo entre $k^*/(k^*)^n$ com $\text{Hom}_c(\text{Gal}(k_s/k), \mathbb{Z}/n\mathbb{Z}) = H^1(k, \mathbb{Z}/n\mathbb{Z})$. No caso em que $n = 2$, temos $H^1(k, \mathbb{Z}/2\mathbb{Z}) = k^*/(k^*)^2$.

2.3 Cohomologia não abeliana

Na seção anterior definimos a teoria da cohomologia galoisiana para A um G -módulo discreto - isto é, A sendo, em particular, um grupo abeliano.

Nesta seção estudaremos o caso quando A não é necessariamente abeliano. Como nós veremos é possível estender a teoria parcialmente a este caso. Os primeiros conjuntos de cohomologia (H^1) não possuem mais uma estrutura de grupo e não existe uma maneira fácil de definir conjuntos de cohomologia (H^n) se $n > 1$.

Nesta seção G denotará um grupo profinito.

2.3.1 Definições de H^0 e H^1

Dizemos que A é um G -conjunto, se A é um espaço topológico discreto, em que G age continuamente. Se $s \in G$ e $x \in A$, denotaremos por ${}^s x$ o resultado da ação de s sobre x . Se A e A' são dois G -conjuntos, um morfismo de A em A' é uma aplicação $f : A \longrightarrow A'$, que comuta com a ação de G , isto é, $f({}^s x) = {}^s f(x)$, para todo $s \in G$ e $x \in A$.

Se A é um grupo, o chamamos de G -grupo, e vale que ${}^s(xy) = {}^s x {}^s y$, para todo $s \in G$ e $x, y \in A$, e se A for ainda, comutativo, a definição de G -conjunto, coincide com a definição de G -módulos discretos.

Definição 2.3.1. Para qualquer G -conjunto A , definimos o seguinte conjunto

$$H^0(G, A) = A^G,$$

o conjunto dos elementos de A fixos pela ação de G . Se A é um G -grupo, $H^0(G, A)$ é um subgrupo de A .

Agora queremos definir o conjunto $H^1(G, A)$. Para isso, precisaremos da noção de um 1-cociclo de G com coeficientes em A .

Definição 2.3.2. Seja A um G -grupo. Um 1-cociclo de G (ou simplesmente cociclo) com coeficientes em A , é uma aplicação contínua $u : G \longrightarrow A$ que satisfaz a seguinte condição:

$$u_{st} = u_s {}^s u_t, \text{ para todo } s, t \in G,$$

onde $u(s) = u_s$ para $s \in G$. Denotamos por $Z^1(G, A)$ o conjunto de todos os 1-cociclos de G com coeficientes em A .

A aplicação $u : G \rightarrow A$, dada por $u_s = 1$ para todo $s \in G$, é um 1-cocilo, chamado de 1-cocilo trivial. É fácil ver que, para qualquer 1-cociclo $u \in Z^1(G, A)$, $u_1 = 1$.

Definição 2.3.3. Seja $u, v \in Z^1(G, A)$. Dizemos que u e v são *cohomólogos* (denotado por $u \sim v$), se existe um $b \in A$, tal que $v_s = b^{-1}u_s b$, para todo $s \in G$.

Podemos verificar facilmente que \sim define uma relação de equivalência em $Z^1(G, A)$.

Definição 2.3.4. Seja A um G -grupo. Definimos o *primeiro conjunto de cohomologia de G com coeficientes em A* , o qual denotamos por $H^1(G, A)$, ao conjunto quociente, dado por:

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

$H^1(G, A)$ tem um elemento especial, ou distinguido, que é a classe do cociclo trivial, pois através dele, $H^1(G, A)$ torna-se um **conjunto pontuado**. Na categoria de conjuntos pontuados, existe a noção de seqüências exatas.

Observação 2.3.1. No caso em que A é um grupo abeliano, a definição de $H^1(G, A)$ coincide com a definição de cohomologia no caso de G -módulos discretos.

2.3.2 Espaços principais homogêneos

Nesta seção daremos uma interpretação muito útil para o primeiro conjunto de cohomologia da cohomologia não-abeliana. Como veremos, os seus elementos podem ser identificados com classes de isomorfismos de espaços principais homogêneos.

Seja A um G -grupo e seja P um G -conjunto. Dizemos que A age a direita em P (\cdot), se A age no sentido natural

$$\begin{aligned} P \times A &\longrightarrow P \\ (x, a) &\mapsto x \cdot a \end{aligned}$$

e cumpre ${}^s(x \cdot a) = {}^s x \cdot {}^s a$, para todo $x \in P$ e $a \in A$. De maneira análoga, podemos definir a ação a esquerda.

Definição 2.3.5. Seja A um G -grupo. Um **espaço principal homogêneo**, ou **torsor** sobre A , é um G -conjunto P , tal que, A age a direita em P , de modo que para cada par $x, y \in P$, existe um único $a \in A$, tal que, $y = x \cdot a$, isto é, a ação de A em P é simples e transitiva ou que P é um "espaço afim" sobre A .

Um morfismo entre dois espaços principais homogêneos sobre A , é uma aplicação que é A -homomorfismo e G -homomorfismo. Um isomorfismo entre espaços principais homogêneos, é definido de modo natural. Podemos ainda, verificar que um morfismo entre espaços principais homogêneos é um isomorfismo.

Denotaremos o conjunto das classes de isomorfismo de espaços principais homogêneos sobre A , por $P(A)$.

Seja $P \in P(A)$, e escolhemos $x \in P$. Para cada $s \in G$, existe um único $a_s \in A$, tal que,

$${}^s x = x \cdot a_s.$$

Se definirmos a aplicação

$$\begin{aligned} a : G &\longrightarrow A \\ s &\longmapsto a_s \end{aligned}$$

podemos ver, que a , define um cociclo.

Por outro lado, se x' for outro elemento em P , pelo mesmo argumento dado acima, para todo $s \in G$ existe um único $a'_s \in A$, tal que, ${}^s x' = x' \cdot a'_s$, e a aplicação

$$\begin{aligned} a' : G &\longrightarrow A \\ s &\longmapsto a'_s \end{aligned}$$

é um cociclo.

Como $x, x' \in P$, existe um único $b \in A$, tal que, $x' = x \cdot b$. Portanto, $a'_s = b^{-1} a_s b$, o que implica que a e a' , são cohomólogos, isto é, não depende da escolha dos representantes.

Desta maneira, obtemos uma aplicação

$$\begin{aligned} \lambda : P(A) &\longrightarrow H^1(G, A) \\ [P] &\longmapsto [a] \end{aligned}$$

onde a é o cociclo construído acima, que é bem definida.

A aplicação λ também possui uma aplicação inversa:

Seja $a \in Z^1(G, A)$. Podemos então definir um G -grupo P_a , que como grupo é igual a A , porém equipado com uma G -ação diferente ("torcida"):

$$\begin{aligned} G \times P_a &\longrightarrow P_a \\ (s, y) &\longmapsto {}^s y := a_s \cdot y \end{aligned}$$

Além disso, ao considerar a operação de A sobre P_a por translações:

$$\begin{aligned} P_a \times A &\longrightarrow P_a \\ (y, b) &\longmapsto y \cdot b \end{aligned}$$

observamos que, se $y \cdot b = yb$, P_a é um espaço principal homogêneo sobre A . Ora, para todo $a, a' \in Z^1(G, A)$, temos,

$$a \sim a' \implies P_a \simeq P_{a'}.$$

Para isso, basta considerar, o seguinte morfismo

$$\begin{aligned} P_a &\longrightarrow P_{a'} \\ y &\longmapsto b^{-1} \cdot y \end{aligned}$$

onde $b \in A$, tal que $a'_s = b^{-1}a_s^s b$, para todo $s \in G$.
Obtemos assim uma aplicação

$$\begin{aligned} \mu : H^1(G, A) &\longrightarrow P(A) \\ [a] &\longmapsto [P_a] \end{aligned}$$

que é bem definida.

Verificaremos finalmente que as aplicações λ e μ são inversas uma da outra. Para isso seja $P \in P(A)$, tal que $\lambda(P) = [a]$. Mostraremos que $[P_a] = [P]$. De fato, basta considerarmos que, para cada $x \in P$ fixo, a seguinte aplicação é um morfismo entre espaços principais homogêneos.

$$\begin{aligned} P_a &\longrightarrow P \\ y &\longmapsto x \cdot y \end{aligned}$$

Deste modo provamos a seguinte proposição:

Proposição 2.3.1. Seja A um G -grupo. Existe uma bijeção entre o conjunto $P(A)$ e o conjunto $H^1(G, A)$.

2.3.3 Torsão (Twisting)

Sejam A um G -grupo e P um espaço principal homogêneo sobre A . Seja F um G -conjunto em que A age a esquerda. Considere em $P \times F$ a seguinte relação:

$$(p, f) \sim (q, g) \iff \exists a \in A, \text{ tal que, } (q, g) = (p \cdot a, a^{-1}f).$$

Podemos ver que \sim define uma relação de equivalência em $P \times F$, a qual é compatível com a ação de G . Denotamos o G -conjunto quociente de $P \times F$ por essa relação de equivalência por:

$${}_P F = (P \times F) / \sim.$$

Denotaremos os elementos de ${}_P F$ por pf , e podemos ver que esses elementos cumprem a seguinte condição $(pa)f = p(af)$, e mais ainda, para todo $p \in P$, a aplicação abaixo é uma bijeção:

$$\Phi_p : F \longrightarrow {}_P F, \text{ dada por } f \mapsto \Phi_p(f) := pf.$$

Através disso, dizemos que ${}_P F$ é obtido de F , por *torsão* (ou um *twisting*) usando P . Vejamos essa noção de torsão, através de um cociclo.

Sejam $a \in Z^1(G, A)$ e ${}_a F$ o conjunto F em que G age da seguinte forma:

$$s'f = a_s \cdot s f.$$

Nesse caso, dizemos que ${}_aF$ é obtido de F , por *torsão* (ou por um *twisting*) usando o cociclo a .

A aplicação Φ_p definida acima induz um isomorfismo entre o G -conjunto ${}_aF$ e o G -conjunto ${}_pF$, para $a \in Z^1(G, A)$. De fato, basta mostrar que $\Phi_p({}'f) = \Phi_p(f)$. Se $p \in P$, vimos que p define um cociclo $a \in Z^1(G, A)$, tal que, ${}^sp = p \cdot a_s$.

$$\Phi_p({}'f) = p \cdot ({}'f) = p \cdot (a_s \cdot {}^sf) = {}^sp \cdot {}^sf = {}^s(p \cdot f) = {}^s\Phi_p(f).$$

Proposição 2.3.2. Sejam A um G -grupo, e F um G -conjunto em que A age a esquerda sobre F . Seja ainda $a \in Z^1(G, A)$. Então o grupo torcido (ou "twisted") ${}_aA$, age sobre ${}_aF$, de forma compatível com a ação de G .

Demonstração. A demonstração pode ser encontrada em ([21], Cap. 1, p. 48). \square

2.4 Álgebras de loop e cohomologia galoisiana

Seja a partir de agora k um corpo algebricamente fechado de característica zero e fixamos uma família de raízes compatíveis da unidade (ζ_n) , $n \in \mathbb{Z}$.

Mostraremos que as k -álgebras de loop podem ser classificadas por um conjunto de cohomologia galoisiana. Em primeiro lugar observamos que a teoria da cohomologia galoisiana, que foi desenvolvida no capítulo anterior para grupo de Galois de um corpo, pode ser estendida sem problemas para o anel $R = k[t, t^{-1}]$ no seguinte sentido:

Existe uma noção de extensão separável de anéis, vide ([14], I,7.3.3)], assim como uma noção de extensão galoisiana de anéis, vide ([14], III.1.1.3).

É possível verificar que as extensões $R_n = k[t^{\frac{1}{n}}, t^{-\frac{1}{n}}]$ já introduzidas na seção 1.5, para $n \in \mathbb{N}$, são extensões galoisianas, vide ([18], Remark 6) de R . Obtemos um grupo de Galois G_n para cada extensão R_n/R . Com a escolha da família de raízes da unidade acima podemos identificar o grupo de Galois G_n com o grupo finito cíclico $\mathbb{Z}/n\mathbb{Z}$, vide ([18], Remark 6).

Fixamos então um $m \in \mathbb{N}$, uma extensão galoisiana $S = k[t^{\frac{1}{m}}, t^{-\frac{1}{m}}] = k[z, z^{-1}]$ onde $z^m = t$ e $z^{-m} = t^{-1}$, como na seção 1.5. Notamos o grupo de Galois desta extensão por Γ e fazemos identificação $\Gamma = \mathbb{Z}/m\mathbb{Z}$. Lembramos também que $\mathfrak{g}(S) = \mathfrak{g} \otimes_k R \otimes_R S$. Retomando as demais notações da seção 1.5, obtemos a seguinte proposição, que mostra que $\text{Aut}_S(\mathfrak{g}(S))$ é um Γ -grupo:

Proposição 2.4.1. Para todo $\bar{i} \in \Gamma$ e $\tau \in \text{Aut}_S(\mathfrak{g}(S))$, a aplicação

$$\begin{aligned} \Gamma \times \text{Aut}_S(\mathfrak{g}(S)) &\longrightarrow \text{Aut}_S(\mathfrak{g}(S)) \\ (\bar{i}, \tau) &\longmapsto \bar{i}\tau := (\text{id} \otimes \underline{i})\tau(\text{id} \otimes \underline{i})^{-1} \end{aligned}$$

é bem definida e é uma ação de Γ em $\text{Aut}_S(\mathfrak{g}(S))$.

Demonstração. De fato, para todo $\bar{i}, \bar{j} \in \Gamma$ e $\tau, \sigma \in \text{Aut}_S(\mathfrak{g}(S))$, temos

- $\bar{0}\tau = (\text{id} \otimes \underline{0})\tau(\text{id} \otimes \underline{0})^{-1} = \tau$, pois $\underline{0}(z) = \zeta_m^0 z = z$.
- $\bar{i+\bar{j}}\tau = \overline{i+j}\tau = (\text{id} \otimes \underline{(i+j)})\tau(\text{id} \otimes \underline{(i+j)})^{-1}$

$$= (\text{id} \otimes \underline{i})(\text{id} \otimes \underline{j})\tau(\text{id} \otimes \underline{j})^{-1}(\text{id} \otimes \underline{i})^{-1} = \bar{i}(\bar{j}\tau)$$

$$\bullet \bar{i}(\tau\sigma) = (\text{id} \otimes \underline{i}) \tau \sigma (\text{id} \otimes \underline{i})^{-1} = (\text{id} \otimes \underline{i}) \tau (\text{id} \otimes \underline{i})^{-1} (\text{id} \otimes \underline{i}) \sigma (\text{id} \otimes \underline{i})^{-1} = \bar{i}\tau\bar{i}\sigma. \quad \square$$

Como veremos na próximas proposições, S/R -formas, a menos R -isomorfismo, correspondem bijectivamente a classes de $H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$, que por sua vez são representados por cociclos. Veremos primeiro como podemos construir uma S/R -forma de $\mathfrak{g}(R)$ através de um cociclo

$$u \in Z^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S))) :$$

Proposição 2.4.2. Seja um cociclo $u \in Z^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$, e consideremos o seguinte conjunto

$$\mathfrak{g}(S)_u = \{x \in \mathfrak{g}(S) \mid u_{\bar{i}}(\text{id} \otimes \underline{i})(x) = x, \forall \bar{i} \in \Gamma\}.$$

Então $\mathfrak{g}(S)_u$ é uma S/R -forma de $\mathfrak{g}(R)$.

Demonstração. Consideremos a aplicação $w_{\bar{i}} = u_{\bar{i}}(\text{id} \otimes \underline{i})$. Podemos ver que $w_{\bar{i}}$ é um R -automorfismo de $\mathfrak{g}(S)$ e para todo $\bar{i} \in \Gamma$, temos que $w_{\bar{i}}(z^k(x \otimes z^j)) = \underline{i}(z^k)w_{\bar{i}}(x \otimes z^j)$, isto é, $w_{\bar{i}}$ é \underline{i} -semilinear, e mais ainda, pela condição de u ser um cociclo, temos que para todo $\bar{i}, \bar{j} \in \Gamma$, $w_{\bar{i}\bar{j}} = w_{\bar{i}}w_{\bar{j}}$, ou seja, o conjunto $\{w_{\bar{i}} \mid \bar{i} \in \Gamma\}$ é um grupo cíclico gerado por $w_{\bar{1}}$.

Afirmamos que $\mathfrak{g}(S)_u = \text{Fix}(w_{\bar{1}})$ onde $\text{Fix}(w_{\bar{1}})$ é o conjunto dos pontos fixos de $w_{\bar{1}}$ em $\mathfrak{g}(S)$. De fato, se $x \in \text{Fix}(w_{\bar{1}})$, então $w_{\bar{1}}(x) = x$, portanto para todo $n \in \mathbb{N}$, temos $w_{\bar{1}}^n(x) = x$, e devido ao fato que $w_{\bar{1}}$ gera $\{w_{\bar{i}} \mid \bar{i} \in \Gamma\}$, então para todo $\bar{i} \in \Gamma$, existe um $n \in \mathbb{N}$, tal que, $w_{\bar{i}} = w_{\bar{1}}^n$, assim $w_{\bar{i}}(x) = w_{\bar{1}}^n(x) = x$. A outra inclusão é evidente.

Para todo $\bar{i} \in \Gamma$, consideremos o ζ_m^i -autoespaço $(\mathfrak{g}(S))_{\bar{i}}$ de $w_{\bar{1}}$ em $\mathfrak{g}(S)$, como temos, $w_{\bar{1}}^m = w_{\bar{0}} = \text{id}$, logo $\mathfrak{g}(S) = \bigoplus_{\bar{i} \in \Gamma} (\mathfrak{g}(S))_{\bar{i}}$, e pelo fato de $w_{\bar{1}}$ ser $\underline{1}$ -semilinear, obtemos

$$t^i(\mathfrak{g}(S))_{\bar{0}} \subseteq (\mathfrak{g}(S))_{\bar{i}} \quad \text{e} \quad t^{-i}(\mathfrak{g}(S))_{\bar{i}} \subseteq (\mathfrak{g}(S))_{\bar{0}}$$

para todo $0 \leq i \leq m-1$. Como t^i é invertível em S , temos $t^i(\mathfrak{g}(S))_{\bar{0}} = (\mathfrak{g}(S))_{\bar{i}}$, logo

$$\mathfrak{g}(S) = \bigoplus_{\bar{i} \in \Gamma} t^i(\mathfrak{g}(S))_{\bar{0}} = \bigoplus_{\bar{i} \in \Gamma} t^i(\mathfrak{g}(S)_u),$$

portanto $\mathfrak{g}(S)_u$ é uma S/R forma de $\mathfrak{g}(R)$ □

O próximo lema mostra que cociclos cohomólogos nos fornecem S/R -formas que são isomorfas como R -álgebras.

Lema 2.4.1. Sejam $u, v \in Z^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$. Então:

$$u \sim v \quad \Leftrightarrow \quad \mathfrak{g}(S)_u \simeq_R \mathfrak{g}(S)_v.$$

Demonstração. Se $u \sim v$, então existe um $f \in \text{Aut}_S(\mathfrak{g}(S))$, tal que, $v_{\bar{i}} = f^{-1}u_{\bar{i}}\bar{i}f$, para todo $\bar{i} \in \Gamma$, então:

$$v_{\bar{i}}(\text{id} \otimes \underline{i}) = f^{-1}u_{\bar{i}}(\text{id} \otimes \underline{i})f. \quad (2.2)$$

Afirmamos que f aplica $\mathfrak{g}(S)_v$ em $\mathfrak{g}(S)_u$. Com efeito, se $x \in \mathfrak{g}(S)_v$, temos por definição, $v_{\bar{i}}(\text{id} \otimes \underline{i})(x) = x$ e por (2.2), obtemos

$$\begin{aligned} f^{-1}u_{\bar{i}}(\text{id} \otimes \underline{i})f(x) &= v_{\bar{i}}(\text{id} \otimes \underline{i})(x) = x \\ u_{\bar{i}}(\text{id} \otimes \underline{i})f(x) &= f(x) \end{aligned}$$

portanto, $f(x) \in \mathfrak{g}(S)_u$, para todo $x \in \mathfrak{g}(S)_v$.

Por outro lado, se $y \in \mathfrak{g}(S)_u$, temos por definição, $u_{\bar{i}}(\text{id} \otimes \underline{i})(y) = y$ e por $f \in \text{Aut}_S(\mathfrak{g}(S))$ existe um $x \in \mathfrak{g}(S)$, tal que, $f(x) = y$, logo

$$\begin{aligned} u_{\bar{i}}(\text{id} \otimes \underline{i})f(x) &= f(x) \\ f^{-1}u_{\bar{i}}(\text{id} \otimes \underline{i})f(x) &= x \\ v_{\bar{i}}(\text{id} \otimes \underline{i})(x) &= x \end{aligned}$$

onde na última igualdade foi usado (2.2), portanto $x \in \mathfrak{g}(S)_u$. Assim $\mathfrak{g}(S)_v \simeq_R \mathfrak{g}(S)_u$.

Reciprocamente, seja $f : \mathfrak{g}(S)_v \rightarrow \mathfrak{g}(S)_u$ o R -isomorfismo. Como $\mathfrak{g}(S)_u$ e $\mathfrak{g}(S)_v$ são S/R -formas de $\mathfrak{g}(R)$, temos:

$$\mathfrak{g}(S)_v \otimes_R S \simeq_S \mathfrak{g}(S) \quad \text{e} \quad \mathfrak{g}(S)_u \otimes_R S \simeq_S \mathfrak{g}(S)$$

podemos assim estender f unicamente a um elemento $f \in \text{Aut}_S(\mathfrak{g}(S))$. Como $\text{id} \otimes \underline{i}$ é R -automorfismo \underline{i} -semilinear, então podemos considerar $f^{-1}u_{\bar{i}}(\text{id} \otimes \underline{i})f$ e $v_{\bar{i}}(\text{id} \otimes \underline{i})$ R -automorfismo de $\mathfrak{g}(S)$ que são \underline{i} -semilinear e fixam elementos de $\mathfrak{g}(S)_v$, com isso, $f^{-1}u_{\bar{i}}(\text{id} \otimes \underline{i})f = v_{\bar{i}}(\text{id} \otimes \underline{i})$, assim $v_{\bar{i}} = f^{-1}u_{\bar{i}} \bar{i} f$ para todo $\bar{i} \in \Gamma$, portanto $u \sim v$. \square

Obtemos então o seguinte resultado:

Proposição 2.4.3. As classes de R -isomorfismo de S/R formas de $\mathfrak{g}(R)$ estão em bijeção com as classes de cohomologia em $H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$.

Demonstração. Vamos denotar por $\mathcal{C}(R)$ o conjunto das classes de R -isomorfismo de S/R formas de $\mathfrak{g}(R)$. Seja $u \in Z^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$ e considere $[u] \in H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$. Pelo Lema 2.4.1, a aplicação

$$\begin{aligned} \Phi : H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S))) &\longrightarrow \mathcal{C}(R) \\ [u] &\longmapsto [\mathfrak{g}(S)_u] \end{aligned}$$

é bem definida, e ainda mais, ela é injetora. Resta mostrarmos que Φ é sobrejetora.

Seja A uma S/R forma de $\mathfrak{g}(R)$, para cada $\bar{i} \in \Gamma$ existe um único $\underline{i} \in \text{Aut}_R(S)$, assim consideremos $w_{\bar{i}}$ a única aplicação R -linear e \bar{i} -semilinear de $\mathfrak{g}(S)$ para $\mathfrak{g}(S)$ que fixa os elementos de A . Então $w_{\bar{i}}$ é um R -automorfismo de $\mathfrak{g}(S)$ e $w_{\bar{i}}w_{\bar{j}} = w_{\bar{i}+\bar{j}}$ para cada $\bar{i}, \bar{j} \in \Gamma$. A aplicação

$$\begin{aligned} u : \Gamma &\longrightarrow \text{Aut}_S(\mathfrak{g}(S)) \\ \bar{i} &\longmapsto u_{\bar{i}} := w_{\bar{i}}(\text{id} \otimes \underline{i})^{-1} \end{aligned}$$

define um cociclo de Γ em $\text{Aut}_S(\mathfrak{g}(S))$. De fato, para todo $\bar{i}, \bar{j} \in \Gamma$, temos

$$\begin{aligned} u_{\bar{i}+\bar{j}} &= w_{\bar{i}+\bar{j}}(\text{id} \otimes (\underline{i} + \underline{j}))^{-1} \\ &= w_{\bar{i}}w_{\bar{j}}((\text{id} \otimes \underline{i})(\text{id} \otimes \underline{j}))^{-1} \\ &= w_{\bar{i}}w_{\bar{j}}(\text{id} \otimes \underline{j})^{-1}(\text{id} \otimes \underline{i})^{-1} \\ &= w_{\bar{i}}u_{\bar{j}}(\text{id} \otimes \underline{i})^{-1} \\ &= u_{\bar{i}}(\text{id} \otimes \underline{i})u_{\bar{j}}(\text{id} \otimes \underline{i})^{-1} \\ &= u_{\bar{i}} \bar{i} u_{\bar{j}}. \end{aligned}$$

Assim, $u \in Z^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$ e verifica-se que $A = \mathfrak{g}(S)_u$, portanto Φ é sobrejetora. \square

A seguinte proposição mostra como toda álgebra de loop define um cociclo em $Z^1(\Gamma, Aut_S(\mathfrak{g}(S)))$.

Proposição 2.4.4. Sejam \mathfrak{g} uma álgebra de Lie e $L(\mathfrak{g}, \sigma)$ a álgebra de loop associada ao automorfismo σ de \mathfrak{g} de período m . A aplicação

$$\begin{aligned} \mathcal{L}(\mathfrak{g}, \sigma) : \Gamma &\longrightarrow Aut_S(\mathfrak{g}(S)) \\ \bar{i} &\longmapsto \sigma^{-i} \otimes \text{id} \end{aligned}$$

define um cociclo de $\Gamma = \mathbb{Z}/m\mathbb{Z}$ com coeficientes em $Aut_S(\mathfrak{g}(S))$.

Demonstração. Queremos mostrar que, para todo $\bar{i}, \bar{j} \in \Gamma$, temos $\mathcal{L}(\mathfrak{g}, \sigma)_{\bar{i}+\bar{j}} = \mathcal{L}(\mathfrak{g}, \sigma)_{\bar{i}} \bar{i} \mathcal{L}(\mathfrak{g}, \sigma)_{\bar{j}}$. Em outras palavras, queremos mostrar que:

$$(\sigma^{-(i+j)} \otimes \text{id})(\text{id} \otimes \underline{i}) = (\sigma^{-i} \otimes \text{id})(\text{id} \otimes \underline{i})(\sigma^{-j} \otimes \text{id}).$$

De fato, seja $\sum \lambda_{rk}(e_r \otimes z^k) \in \mathfrak{g}(S)$ onde a soma é finita e onde $\{e_r\}_{r \in I}$ e $\{z^k\}_{k \in J}$ são bases de \mathfrak{g} e S respectivamente e $\lambda_{rk} \in k$. Então

$$\begin{aligned} (\sigma^{-(i+j)} \otimes \text{id})(\text{id} \otimes \underline{i}) \left(\sum \lambda_{rk}(e_r \otimes z^k) \right) &= (\sigma^{-(i+j)} \otimes \text{id}) \left(\sum \lambda_{rk}(e_r \otimes \zeta_m^{ki} z^k) \right) \\ &= \sum \lambda_{rk}(\sigma^{-(i+j)}(e_r) \otimes \zeta_m^{ki} z^k). \end{aligned}$$

Por outro lado,

$$\begin{aligned} (\sigma^{-i} \otimes \text{id})(\text{id} \otimes \underline{i})(\sigma^{-j} \otimes \text{id}) \left(\sum \lambda_{rk}(e_r \otimes z^k) \right) &= (\sigma^{-i} \otimes \text{id})(\text{id} \otimes \underline{i}) \left(\sum \lambda_{rk}(\sigma^{-j}(e_r) \otimes z^k) \right) \\ &= (\sigma^{-i} \otimes \text{id}) \left(\sum \lambda_{rk}(\sigma^{-j}(e_r) \otimes \zeta_m^{ki} z^k) \right) \\ &= \sum \lambda_{rk}(\sigma^{-(i+j)}(e_r) \otimes \zeta_m^{ki} z^k) \end{aligned}$$

portanto, para todo $\bar{i}, \bar{j} \in \Gamma$, temos $\mathcal{L}(\mathfrak{g}, \sigma)_{\bar{i}+\bar{j}} = \mathcal{L}(\mathfrak{g}, \sigma)_{\bar{i}} \bar{i} \mathcal{L}(\mathfrak{g}, \sigma)_{\bar{j}}$. □

Observamos que nós podemos definir uma relação de equivalência no conjunto $H^1(\Gamma, Aut_S(\mathfrak{g}(S)))$, da seguinte maneira:

Sejam $[\mathcal{L}(\mathfrak{g}, \sigma)]$ e $[\mathcal{L}(\mathfrak{g}, \tau)] \in H^1(\Gamma, Aut_S(\mathfrak{g}(S)))$. Então definimos:

$$[\mathcal{L}(\mathfrak{g}, \sigma)] \sim [\mathcal{L}(\mathfrak{g}, \tau)] \quad \Leftrightarrow \quad [\mathcal{L}(\mathfrak{g}, \sigma)] = [\mathcal{L}(\mathfrak{g}, \tau)] \quad \text{ou} \quad [\mathcal{L}(\mathfrak{g}, \sigma^{-1})] = [\mathcal{L}(\mathfrak{g}, \tau)].$$

Enunciemos então os nossos resultados principais:

Teorema 2.4.1. Sejam \mathfrak{g} uma álgebra de Lie de dimensão finita e σ, τ dois k -automorfismos de mesmo período m , então:

$$\begin{aligned} L(\mathfrak{g}, \sigma) \simeq_R L(\mathfrak{g}, \tau) &\Leftrightarrow [\mathcal{L}(\mathfrak{g}, \sigma)] = [\mathcal{L}(\mathfrak{g}, \tau)]. \\ L(\mathfrak{g}, \sigma) \simeq_k L(\mathfrak{g}, \tau) &\Leftrightarrow [\mathcal{L}(\mathfrak{g}, \sigma)] \sim [\mathcal{L}(\mathfrak{g}, \tau)]. \end{aligned}$$

Demonstração. Verificamos anteriormente que $\mathcal{L}(\mathfrak{g}, \sigma)$ e $\mathcal{L}(\mathfrak{g}, \tau)$ são cociclos de $\Gamma = \mathbb{Z}/m\mathbb{Z}$ em $\text{Aut}_S(\mathfrak{g}(S))$. Usando a Proposição 2.4.3, basta mostrarmos que a S/R forma de $\mathfrak{g}(R)$ associados a esses cociclos são as álgebras de loop $L(\mathfrak{g}, \sigma)$ e $L(\mathfrak{g}, \tau)$.

Consideremos $w_{\bar{1}}$ como na Proposição 2.4.2, mostramos que $\mathfrak{g}(S)_{\mathcal{L}(\mathfrak{g}, \sigma)} = \text{Fix}(w_{\bar{1}})$, onde $w_{\bar{1}} = \mathcal{L}(\mathfrak{g}, \sigma)_{\bar{1}}(\text{id} \otimes \underline{1})$, assim,

$$\mathfrak{g}(S)_{\mathcal{L}(\mathfrak{g}, \sigma)} = \{x \in \mathfrak{g}(S) \mid w_{\bar{1}}(x) = x\}.$$

Podemos verificar que $\mathfrak{g}(S)_{\mathcal{L}(\mathfrak{g}, \sigma)}$ coincide com a definição dada na equação (1.2), ou seja, $\mathfrak{g}(S)_{\mathcal{L}(\mathfrak{g}, \sigma)} = L(\mathfrak{g}, \sigma)$. Portanto, pela Proposição 2.4.3, temos

$$L(\mathfrak{g}, \sigma) \simeq_R L(\mathfrak{g}, \tau) \Leftrightarrow [\mathcal{L}(\mathfrak{g}, \sigma)] = [\mathcal{L}(\mathfrak{g}, \tau)].$$

A segunda afirmação é uma consequência direta de ([8], Corollary 5.4). □

Corolário 2.4.1. Seja \mathfrak{g} uma k -álgebra de Lie de dimensão finita. Então obtemos uma correspondência injetiva:

$$\left\{ \begin{array}{l} \text{Classes de } R\text{-isomorfismos de álgebras de loop da forma} \\ L(\mathfrak{g}, \sigma), \text{ onde } \sigma \text{ é um automorfismo de } \mathfrak{g} \text{ de período } m. \end{array} \right\} \hookrightarrow H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S)))$$

$$\left\{ \begin{array}{l} \text{Classes de } k\text{-isomorfismos de álgebras de loop da forma} \\ L(\mathfrak{g}, \sigma), \text{ onde } \sigma \text{ é um automorfismo de } \mathfrak{g} \text{ de período } m. \end{array} \right\} \hookrightarrow H^1(\Gamma, \text{Aut}_S(\mathfrak{g}(S))) / \sim$$

Observação 2.4.1.

- Observamos a significância deste resultado: A classificação de álgebras de loop como k -álgebras depende somente da cohomologia galoisiana do grupo $\text{Aut}_S(\mathfrak{g}(S))$. Logo nós mostramos que o problema de classificar estas álgebras de Lie de dimensão infinita sobre k , pode ser essencialmente reduzido a um problema de cohomologia galoisiana.
- É possível mostrar que as injeções acima são de fato bijeções, vide ([8], Theorem 5.13) - isto é, toda classe do conjunto de cohomologia provém de uma álgebra de loop.

Referências Bibliográficas

- [1] ALLISON, BRUCE, STEPHEN BERMAN, AND ARTURO PIANZOLA. *Covering algebras II: Isomorphism of loop algebras*, J. Reine Angew. Math. 571 39 - 71, 2004.
- [2] BERHUY, GRÉGORIE, *An Introduction to Galois Cohomology and its Applications*, Vol. 377. Cambridge University Press, 2010.
- [3] CARTAN, HENRY, AND SAMUEL EILENBERG, *Homological Algebra*, (PMS-19). Vol. 19. Princeton University Press, 2016.
- [4] CORNELL, GARY, JOSEPH H. SILVERMAN, AND GLENN STEVENS, *Modular Forms and Fermat's Last Theorem*, Springer Science & Business Media, 2013.
- [5] ERDMANN, KARIN & WILDON, MARK, *Introduction to Lie Algebras*, Springer Science & Business Media, 2006.
- [6] FUCHS, JURGEN, *Affine Lie algebras and quantum groups: An Introduction, with applications in conformal field theory*, Cambridge university press, 1995.
- [7] GILLE, PHILIPPE, AND TAMÁS SZAMUELY. *Central simple algebras and Galois cohomology*, Vol. 101 of Cambridge Studies in Advanced Mathematics, 2006.
- [8] GILLE, PHILIPPE, AND ARTURO PIANZOLA. *Galois cohomology and forms of algebras over Laurent polynomial rings*, Mathematische Annalen 338.2 : 497-543, 2007.
- [9] GILLE, PHILIPPE, AND ARTURO PIANZOLA. *Isotriviality and étale cohomology of Laurent polynomial rings*, Journal of Pure and Applied Algebra 212.4 : 780-800, 2008.
- [10] GILLE, PHILIPPE, AND ARTURO PIANZOLA. *Torsors, reductive group schemes and extended affine Lie algebras*, Vol. 226. No. 1063. American mathematical society, 2013.
- [11] GIRAUD, JEAN, *Cohomologie Non Abélienne*, Springer-Verlag, 1971.
- [12] HUMPHREYS, JAMES. *Introduction to Lie Algebras and Representation Theory*, Vol. 9. Springer Science & Business Media, 2012.
- [13] JACOBSON, NATHAN. *Lie Algebras*, Jonh Wiley & Sons, INC. 1962.
- [14] KNUS, MAX-ALBERT, *Quadratic and Hermitian Forms over Rings*, Vol. 294. Springer Science & Business Media, 2012.
- [15] OTTESEN, JOHNNY T., *Infinite Dimensional Groups and Algebras in Quantum Physics*, Vol. 27. Springer Science & Business Media, 2008.

- [16] PIANZOLA, ARTURO. *Vanishing of H_1 for Dedekind rings and applications to loop algebras*, C. R. Acad. Sci. Paris, Ser. I 340 , 633-638, 2005.
- [17] PIANZOLA, ARTURO. *Twisted loop algebra and Galois cohomology*, Lecture Notes in Pure and Applied Mathematics, volume 248 , 292-304, 2006.
- [18] PIANZOLA, ARTURO. *Affine Kac–Moody Lie algebras as torsors over the punctured line*, Indag. Math. 13 249–257, 2002.
- [19] RIBES, LUIS, AND PAVEL ZALESSKII, *Profinite Groups* , 2st edition, Springer Berlin Heidelberg, . ISBN 978-3-642-01641-7, 2000.
- [20] SAN MARTIN, L. A. B. *Álgebras de Lie*, Editora da Unicamp, Campinas, 1999.
- [21] SERRE, JEAN-PIERRE. *Galois cohomology*, Springer Science & Business Media, 2013.
- [22] SERRE, JEAN-PIERRE, *Algèbres de Lie semi-simples complexes*, Benjamin Inc., New York, 1966.
- [23] SERRE, JEAN-PIERRE, *Lie Algebras and Lie Groups*, Benjamin, New York, 1965; Lect. Notes in Math. 1500, Springer-Verlag, 1992.
- [24] SENESI, PRASAD. *Finite-dimensional representation theory of loop algebras: a survey*, Quantum affine algebras, extended affine Lie algebras, and their applications, 506 : 263-283, 2010.
- [25] STEINMETZ ZIKESCH, WILHELM ALEXANDER. *Algèbres de Lie de dimension infinie et théorie de la descente*, Mémoires de la Société mathématique de France 129 : 1-99, 2012.