

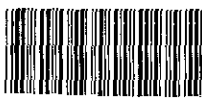
José Acacio de Barros

# Dois Exemplos de Indecidibilidade e Incompletude em Física

TESE DE  
DOUTORADO

CENTRO BRASILEIRO DE PESQUISAS FÍSICAS  
Rio de Janeiro  
- 1991 -

DOIS EXEMPLOS DE INDECIDIBILIDADE E  
INCOMPLETUDE EM FÍSICA



1991/43

B277

\*021401\*

Para Ana Lucia.

## Agradecimentos

Agradeço ao Prof. Francisco Antônio Doria, pela sua atenção e amizade durante a elaboração desta tese.

Ao Prof. Antonio Fernandes da F. Teixeira, pelo grande apoio no CBPF.

Ao Prof. Newton C. A. da Costa, pelo incentivo e paciência.

Ao Prof. Antonio F. F. do Amaral, pelas proveitosas discussões em Física.

Ao Dr. Marcelo Rebouças, pelas facilidades computacionais do Laboratório de Computação Algébrica (LCA/DRP) do CBPF.

Ao amigo Ary Ribeiro de Oliveira Jr., pelo grande apoio e confiança.

Aos amigos da CFC, em particular à Myriam S. Coutinho, pela eficiência e atenção.

Aos amigos, professores e funcionários do CBPF.

Aos meus pais.

À Ana Lucia.

## Resumo

Neste trabalho apresentamos algumas questões formalmente indecidíveis face aos Axiomas de Zermelo-Fraenkel (supondo estes consistentes). Primeiro demonstramos uma Proposição que nos impõe restrições à forma conexão para que tenhamos soluções não triviais da identidade diferencial de Bianchi. Feito isto, exibimos uma forma conexão sobre a qual é impossível demonstrarmos, em ZFC, que ela satisfaz às restrições mencionadas. Posteriormente, arguimos sobre a relação entre “genericidade” e “aleatoriedade” em espaços-tempo da Relatividade Geral; mostramos que a identificação de tais conjuntos é também indecidível em ZFC.

## Abstract

We show here a few formally undecidable questions with respect to the ZFC Axioms. We first prove that some restrictions are needed in the connection form in such that we can have nontrivial solutions for the Bianchi differential conditions. We then exhibit a connection form such that is impossible to prove from the ZFC axioms it satisfies the preceding restrictions. We also argue about the relations between set-theoretically genericity and randomness of spacetime supports of General Relativity; we prove that the identification of those sets is an undecidable question within ZFC.

# Índice

<b>1</b>	<b>Introdução</b>	<b>1</b>
1.1	Motivação . . . . .	1
1.2	Dos Capítulos . . . . .	2
<b>2</b>	<b>O Décimo Problema de Hilbert e Certas de Suas Consequências</b>	<b>4</b>
2.1	Introdução . . . . .	4
2.2	Equações e Conjuntos Diofantinos . . . . .	4
2.2.1	Algoritmos e Sistemas Formais . . . . .	10
2.2.2	Uma Equação Diofantina Exponencial . . . . .	12
2.2.3	Teorema do Quantificador Limitado . . . . .	15
2.2.4	Alguns Exemplos Envolvendo Problemas Famosos . . . . .	16
2.3	O Teorema de Richardson-da Costa-Doria . . . . .	17
<b>3</b>	<b>Algumas Questões sobre a Geometria dos Campos de Gauge</b>	<b>28</b>
3.1	Introdução . . . . .	28
3.2	Geometria dos Campos de Gauge . . . . .	30
3.3	Uma Degenerescência nas Identidades de Bianchi . . . . .	37
3.4	Soluções Não-Curvatura para as Identidades Diferenciais de Bianchi . . . . .	41
3.5	Uma Questão Indecidível sobre a Geometria dos Campos de Gauge . . . . .	46
<b>4</b>	<b>Indecibilidade na Relatividade Geral</b>	<b>49</b>
4.1	Introdução . . . . .	49
4.2	Genericidade, Aleatoriedade e uma Questão Indecidível . . . . .	50

4.3	Uma Topologia para $\mathcal{S}$ . . . . .	50
4.4	Computabilidade, Aleatoriedade e Indecidibilidade em $\mathcal{M}$ . . . . .	55
<b>5</b>	<b>Conclusões</b>	<b>60</b>
	<b>Apêndice A</b>	<b>61</b>
A.1	Programas “REDUCE” . . . . .	62
A.1.1	A Equação Exponencial Diofantina . . . . .	62
A.1.2	Uma Equação Diofantina para o Conjunto dos Primos . . . . .	63
A.2	Programas “MAPLE”: A Última Conjectura de Fermat e a Hipótese de Riemann . . . . .	65
A.2.1	A Última Conjectura de Fermat . . . . .	65
A.2.2	A Hipótese de Riemann (HR) . . . . .	72

# Capítulo 1

## Introdução

### 1.1 Motivação

Em 1931, um trabalho pioneiro de Kurt Gödel [44] apresentou um resultado estarrecedor na metamatemática: dada uma teoria formal, poderosa o suficiente para conter os teoremas da Aritmética Elementar, existem proposições que, nem ela nem sua negação, podem ser demonstradas nesta teoria. E mais, se todas as proposições forem demonstráveis, então a teoria é inconsistente. Tal fato ficou depois conhecido como “Teorema de Gödel”.

Resultados indecidíveis já eram conhecidos da matemática, mais precisamente na Geometria. No século XIX, com o surgimento de novas geometrias, ficou estabelecido que o quinto postulado de Euclides (o das paralelas) era de fato independente dos outros axiomas da geometria plana, pois não podia deles ser derivado. A demonstração da independência do quinto postulado foi feita mostrando-se que se a geometria euclidiana é consistente, então reinterpretando-se determinadas curvas geodésicas sobre esferas como retas, então os quatros postulados se verificavam mas o quinto era violado (segundo esta interpretação).

O trabalho de Gödel parecia estar bem distante dos trabalhos sobre a geometria não-euclidiana. O exemplo de sentença indecidível apresentada por Gödel fugia à intuição matemática usual, e muitos pensavam que, por este motivo, proposições indecidíveis não apareceriam usualmente na matemática do dia a dia.

Estas suposições foram desmistificadas em 1963 pelos trabalhos de P.

J. Cohen, que demonstrou que o Primeiro Problema de Hilbert, a Hipótese do Contínuo, era indecidível na Teoria dos Conjuntos de Zermelo-Fraenkel [19]. A partir de então, pipocaram inúmeros resultados de indecibilidade em diversas áreas da matemática, a saber: topologia, análise, teoria da medida, etc...

Em 1982 Chaitin [17] demonstrou que as questões indecidíveis são de se esperar em toda a parte. Na realidade, estas questões, como veremos, são extremamente comuns. Hoje em dia sabemos que se pode escrever expressões na linguagem da análise clássica, provavelmente iguais a 0 ou 1, mas sem que possamos decidir qual seu valor. [22]

Seguindo a idéia de que a indecibilidade está em toda a parte, podemos nos perguntar sobre sua existência em qualquer área do pensamento humano que envolva a matemática como base, como por exemplo a física. Trabalhos nesta direção são [2] [6] [9] [10] [17] [24] [22] [23] [36] [67]

Nesta tese, sequência de nossos trabalhos [6] [24] [39], apresentamos algumas proposições formalmente indecidíveis face ao sistema de axiomas de Zermelo-Fraenkel para a Teoria dos Conjuntos. Particularmente, mostramos questões deste tipo que aparecem na Teoria dos Campos de Gauge Clássicos [26] e na Relatividade Geral [25].

## 1.2 Dos Capítulos

Este trabalho se acha dividido em 5 capítulos, sendo o primeiro este intróito e o quinto as conclusões.

No capítulo 2 apresentamos uma breve pincelada sobre a teoria das funções e dos conjuntos diofantinos [28]. Um esboço da teoria dos algoritmos e dos sistemas formais é desenhado na seção 2.2.1, onde estabelecemos algumas definições necessárias ao que se segue [22] [56]. O Décimo problema de Hilbert é exposto, assim como sua solução [28] [30]. Para tal, aduzimos uma equação exponencial diofantina plena, tal qual [28], e em consonância com isto estabelecemos o Teorema do Quantificador Limitado [30]. Finalmente, na última seção, expomos uma extensão [22] dos resultados de Richardson [66] sobre indecibilidade nas funções reais.

A porção original da tese está nos Capítulos 3 e 4.

No Capítulo 3 tratamos sobre as indecibilidades nas Teorias de Gauge Clássicas [26]. Na seção 3.2 fixamos a notação usada e os objetos de estudo



em questão. Feito isto, apresentamos uma série de versões do Teorema de Frobenius que nos serão úteis nas seções seguintes. Posteriormente, uma degenerescência nas identidades diferenciais de Bianchi é obtida e mostramos algumas condições para a existência de soluções não-curvas para estas identidades. Finalmente, na última seção, obtemos nosso resultado de indecidibilidade.

No quarto Capítulo estudamos o caso da Relatividade Geral [25]. Na seção 4.3 construímos uma topologia razoável para o conjunto de todas as variedades que podem ser espaços-tempo. De posse desta topologia, arguimos o significado físico das variedades genéricas, comparando-as com “variedades aleatórias”. Mostra-se que em ZFC é impossível demonstrar que tais características (genericidade e aleatoriedade) coincidem (módulo um conjunto irrelevante).

# Capítulo 2

## O Décimo Problema de Hilbert e Certas de Suas Consequências

### 2.1 Introdução

Neste Capítulo apresentamos um esboço do que nos será essencial nesta tese sobre a teoria das equações e dos conjuntos diofantinos. O objetivo básico é expor o resultado de Richardson [66] sobre funções subelementares sobre os reais, que se mostrou um poderoso instrumento na obtenção de sentenças indecidíveis [26] [22].

### 2.2 Equações e Conjuntos Diofantinos

Consideremos um *Domínio de Integridade*  $D$  qualquer e seja  $a_0, a_1, \dots, a_m$  uma coleção de elementos de  $D$ , sendo  $a_m \neq 0$ . Uma forma polinomial de grau  $m$  sobre a variável  $x$  é toda a expressão em  $D$  do tipo

$$a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \tag{2.1}$$

**Definição 2.1** *Se  $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$  e  $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$  então  $p(x) = q(x)$  se e somente se para todo o inteiro  $i \geq 0$ ,  $a_i = b_i$ .*

**Definição 2.2** *Seja  $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m$ . A função  $p : D \rightarrow D$  que atribui a cada elemento  $x \in D$  um  $p(x) \in D$  é chamada função polinomial.*

A soma e a multiplicação de dois polinômios

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m$$

e

$$q(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$$

podem ser definidas “ponto a ponto” como

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n + \dots + a_mx^m \quad (2.2)$$

e

$$p(x)q(x) = \sum_{j=0}^k c_jx^j \quad (2.3)$$

respectivamente, onde  $c_i = a_ib_0 + a_{i-1}b_1 + \dots + a_{i-i}b_i + \dots + a_0b_i$  e  $m > n$ .

A coleção de todas as formas polinomiais (2.1) sobre  $D$  constituem, com a soma e a multiplicação definidas por (2.2) e (2.3), também um domínio de integridade, denotado  $D[x]$ .  $D$  é um subdomínio de integridade de  $D[x]$  (cf. [12] [47]).

Até agora lidamos com polinômios numa única variável  $x$ . Polinômios com mais de uma variável podem ser naturalmente definidos como se segue: seja  $p^i(x) = a_0^i + a_1^ix + a_2^ix^2 + \dots + a_m^ix^m$  uma coleção de  $m + 1$  polinômios em  $x$ , com  $i = 0 \dots m$ ; podemos definir um  $r(x, y)$  como

$$r(x, y) = p^0(x) + p^1(x)y + \dots + p^m(x)y^m.$$

Um exemplo de um polinômio em  $x$  e  $y$  seria

$$r(x, y) = x + 2x^2y + xy^2$$

De uma maneira geral, podemos definir por recursivamente um polinômio de  $n$  variáveis como um elemento de  $D[x_1, x_2, \dots, x_n]$  dado por

$$D[x_1, x_2, \dots, x_n] = D[x_1, x_2, \dots, x_{n-1}][x_n] \quad (2.4)$$

Por indução, é evidente que a coleção de todos os polinômios de  $n$  variáveis  $D[x_1, \dots, x_n]$  é um domínio de integridade.

De agora em diante, somente consideremos os polinômios  $p(x_1, \dots, x_n)$  contidos no anel polinomial  $Z[x_1, \dots, x_n]$ , onde  $Z = \{0, \pm 1, \pm 2, \pm 3, \dots\}$  é o conjunto dos inteiros.

**Definição 2.3** *Todo o polinômio  $p(x_1, \dots, x_n) \in Z[x_1, \dots, x_n]$  é chamado polinômio diofantino.*

O nome “diofantino” é uma homenagem ao grande matemático grego Diofanto de Alexandria (século III AC), cujo grande tratado *Arithmetica* aborda inúmeras equações polinomiais de inteiros em inteiros e suas soluções. Por exemplo, uma típica equação diofantina é

$$x^2 + y^2 = z^2 \quad (2.5)$$

que pode representar a relação entre os catetos  $x$  e  $y$  e a hipotenusa  $z$  de um dado triângulo retângulo com lados inteiros, dada pelo teorema de Pitágoras; as soluções de (2.5), amplamente estudadas por Diophantus, nos dão todos os triângulos retângulos de lados inteiros.

**Definição 2.4** *Seja  $p(x_1, \dots, x_n)$  um polinômio diofantino. A expressão  $p(x_1, \dots, x_n) = 0$  é chamada equação diofantina; e os valores de  $x_1, \dots, x_n$  que satisfazem esta igualdade são suas soluções.*

Como podemos ver pela Definição 2.4, uma dada equação diofantina pode ser associada a um conjunto de soluções, expresso por uma coleção de  $k$   $n$ -uplas  $\langle x_1, \dots, x_n \rangle$ , se esta equação admite  $k$  soluções. Estas soluções nos sugerem definir determinados conjuntos a partir de dadas equações diofantinas.

**Definição 2.5** *Seja  $p(x_1, \dots, x_n, y_1, \dots, y_m)$  um polinômio diofantino com  $n + m$  variáveis  $x_1, \dots, x_n$  e  $y_1, \dots, y_m$ . Um conjunto  $S$  de  $n$ -uplas dado por*

$$\langle x_1, \dots, x_n \rangle \in S \leftrightarrow \exists y_1, \dots, y_m (p(x_1, \dots, x_n, y_1, \dots, y_m) = 0) \quad (2.6)$$

*é chamado diofantino. Neste caso os  $x_1, \dots, x_n$  são chamados parâmetros e os  $y_1, \dots, y_m$  variáveis.*

Desta maneira,  $S$  é um conjunto (definido pelo polinômio diofantino  $p(x_1, \dots, x_n, y_1, \dots, y_m)$ ) cujos elementos são as soluções de  $p(x_1, \dots, x_n, y_1, \dots, y_m)$  quando permitimos aos parâmetros  $y_1, \dots, y_m$  variarem em  $\mathbb{Z}$ , isto é

$$S = \{(x_1, \dots, x_n) \mid \exists y_1, \dots, y_m (p(x_1, \dots, x_n, y_1, \dots, y_m) = 0)\}$$

Usando um artifício simples criado por Hilary Putnam [30], podemos trabalhar somente com as soluções em  $\mathbb{N} = \{1, 2, 3, 4, \dots\}$  de um polinômio diofantino. Isto é feito do seguinte modo: seja  $p(x, y_1, \dots, y_m)$  um polinômio diofantino com  $m$  parâmetros  $y_1, \dots, y_m$  e uma variável  $x$ ; definamos o polinômio  $Q(x, y_1, \dots, y_m) = (x + 1)[1 - p^2(x, y_1, \dots, y_m)] - 1$ . De imediato obtemos

**Proposição 2.6** *O conjunto  $S$  definido pelo polinômio  $Q(x, y_1, \dots, y_m)$  construído acima consiste dos valores não-negativos assumidos por  $Q(x, y_1, \dots, y_m)$  quando  $x, y_1, \dots, y_m$  assumem valores em  $\mathbb{N}$ .*

*Demonstração:*  $P(x, y_1, \dots, y_m) = 0$  implica  $Q(x, y_1, \dots, y_m) = x$ ; com isto  $Q(x, y_1, \dots, y_m) = x \geq 0$ , o que implica  $(1 - p^2(x, y_1, \dots, y_m))(x + 1) - 1 \geq 0$  e  $1 - p^2(x, y_1, \dots, y_m) > 0$ , nos dando  $p(x, y_1, \dots, y_m) = 0$  e  $x = Q$ .  $\square$

Daqui por diante, a menos que digamos explicitamente o contrário, trabalharemos somente com equações diofantinas sobre  $\mathbb{N}$ .

Como podemos observar, vários subconjuntos de  $\mathbb{N}$  podem ser expressos por equações diofantinas, como nos mostrarão os exemplos que se seguem.

**Exemplo 1 (o conjunto dos pares):** Fazendo-se  $p(x, y) = 2y - x$  este conjunto pode ser definido como

$$x \in P \leftrightarrow x \text{ é par} \leftrightarrow \exists y (x = 2y),$$

sendo  $P$  o conjunto de todos os números pares.

**Exemplo 2 (os números que não são potência de 2):** Com  $p(x, y, z) = y(2z + 1) - x$  temos

$$x \in S \leftrightarrow \exists y, z (p(x, y, z) = 0),$$

Ainda utilizando equações diofantinas, podemos definir relações binárias, ternárias ou  $n$ -árias sobre números naturais, uma vez que os elementos dos conjuntos gerados são  $n$ -uplas. Com isto, relações como  $x|y$ ,  $x < y$  ou  $x > y$  podem ser facilmente obtidas, como mostraremos nos exemplos 3 e 4.

**Exemplo 3 (Relação  $x|y$ ):** Construamos o conjunto diofantino

$$\langle x, y \rangle \in S \leftrightarrow \exists z(xz = y) \leftrightarrow \exists(p(x, y, z) = 0),$$

onde  $p(x, y, z) = xz - y$ . É óbvio que  $p(x, y, z)$  é zero somente se  $x$  divide  $y$ , para  $x, y, z \in \mathbb{N}$ .

**Exemplo 4 (Relação  $x < y$ ):** Podemos ver claramente que  $x$  é menor que  $y$  se existir um  $z \in \mathbb{N}$  tal que

$$x = y - z,$$

e o conjunto desejado pode ser expresso como

$$\langle x, y \rangle \in M \leftrightarrow \exists z(x - y + z = 0),$$

que é diofantino.

Nosso interesse é, frequentemente, combinar afirmações sobre determinados conjuntos, isto é, em geral desejamos obter um conjunto tendo simultaneamente duas propriedades distintas que em separado são diofantinas. Podemos nos perguntar: é este conjunto diofantino? Se é, como podemos escrever um polinômio que o represente? Para responder a estas questões, consideremos os conjuntos diofantinos dados por

$$x \in S \leftrightarrow \exists z_1, \dots, z_n p(x, z_1, \dots, z_n) = 0 \quad (2.7)$$

e

$$y \in T \leftrightarrow \exists w_1, \dots, w_n q(y, w_1, \dots, w_n) = 0 \quad (2.8)$$

que são conjuntos que obedecem as propriedades determinadas por  $p(x, z_1, \dots, z_n)$  e  $q(y, w_1, \dots, w_n)$ . Definamos

$$r(x, y, z_1, \dots, z_n, w_1, \dots, w_n) = p^2(x, z_1, \dots, z_n) + q^2(y, w_1, \dots, w_n) \quad (2.9)$$

Da definição anterior, segue-se  $r(x, y, z_1, \dots, z_n, w_1, \dots, w_n) = 0$  se e somente se  $p(x, z_1, \dots, z_n) = 0$  e  $q(y, w_1, \dots, w_n) = 0$ . Como vimos no início, pelo fato de ser  $Z[x_1, \dots, x_n]$  um domínio de integridade, então  $r(x, y, z_1, \dots, z_n, w_1, \dots, w_n)$  também é uma equação diofantina. Este procedimento pode imediatamente ser estendido para o caso de vários polinômios diofantinos cujas propriedades queremos fazer valer ao mesmo tempo e que pode ser representado pelo conjunto simultâneo de equações diofantinas

$$\begin{cases} p^{(1)}(z_1^{(1)}, \dots, z_n^{(1)}, w_1^{(1)}, \dots, w_m^{(1)}) = 0 \\ p^{(2)}(z_1^{(2)}, \dots, z_n^{(2)}, w_1^{(2)}, \dots, w_m^{(2)}) = 0 \\ \vdots \\ p^{(k)}(z_1^{(k)}, \dots, z_n^{(k)}, w_1^{(k)}, \dots, w_m^{(k)}) = 0 \end{cases}$$

Este sistema pode ser representado pela única equação

$$(p^{(1)}(z_1^{(1)}, \dots, z_n^{(1)}, w_1^{(1)}, \dots, w_m^{(1)}))^2 + (p^{(2)}(z_1^{(2)}, \dots, z_n^{(2)}, w_1^{(2)}, \dots, w_m^{(2)}))^2 + \dots + (p^{(k)}(z_1^{(k)}, \dots, z_n^{(k)}, w_1^{(k)}, \dots, w_m^{(k)}))^2 = 0$$

que, pelos motivos mencionados anteriormente, é diofantina.

Acabamos de apresentar uma maneira dada duas propriedades sobre elementos do conjunto dos inteiros, representadas por uma equação diofantina, juntá-las utilizando o conectivo lógico “e” (que representaremos por<sup>1</sup> “ $\wedge$ ”). Em outras palavras  $(p(x) = 0 \wedge q(y) = 0) \leftrightarrow (p^2(x) + q^2(y) = 0)$ . Isto implica

$$\langle x, y \rangle \in S \leftrightarrow (p(x) = 0 \wedge q(y) = 0) \leftrightarrow (p^2(x) + q^2(y) = 0).$$

De imediato, o conectivo “ou” pode ser introduzido como:

$$\langle x, y \rangle \in S \leftrightarrow (p(x) = 0 \wedge q(y) = 0) \leftrightarrow (p(x)q(y) = 0)$$

uma vez que  $p(x)q(y) \neq 0$  se e somente se  $p(x)$  e  $q(y)$  são ao mesmo tempo diferentes de zero, e  $p(x)q(y)$  se anula se *pelo menos um* dos polinômios  $p(x)$  ou  $q(y)$  é zero.

---

<sup>1</sup>Observemos que o símbolo utilizado para o conectivo lógico “ou” coincide com o utilizado para representar o produto exterior. Isto não apresentará nenhuma confusão, pois ficará claro no texto a que caso estaremos aludindo

A negação lógica também é naturalmente introduzida na linguagem das equações diofantinas, pois

$$x \in S \leftrightarrow (\neg p(x) = 0) \leftrightarrow \exists z(p(x) = z + 1 \wedge p(x) = -z - 1) \leftrightarrow$$

$$\leftrightarrow \exists z((p(x) - z - 1)(p(x) + z + 1) = 0) \leftrightarrow \exists z(p'(x, z) = 0)$$

onde  $p'(x, z) = (p(x) - z - 1)(p(x) + z + 1)$ .

Como vimos, usando-se equações diofantinas podemos traduzir os predicados  $P(x) \wedge Q(y)$  e  $P(x) \vee Q(y)$  sobre elementos de  $\mathbb{N}$  (sendo  $P(x)$  e  $Q(y)$  eles mesmo representáveis via equações diofantinas) nas equações  $p^2(x) + q^2(y) = 0$  e  $p(x)q(y) = 0$  respectivamente, onde  $p(x) = 0 \leftrightarrow P(x)$  e  $q(x) = 0 \leftrightarrow Q(x)$ .

Neste ponto é válido nos perguntarmos se podemos construir um “cálculo proposicional” utilizando as equações diofantinas, no sentido de obtermos, para cada subconjunto de  $\mathbb{N}$  descrito por um predicado  $P(x)$ , uma determinada equação diofantina. A resposta a isto é dada mostrando-se a existência de uma equação diofantina especial: a *exponencial diofantina*. De posse da função exponencial diofantina, demonstra-se o *Teorema do Quantificador Limitado*. Antes disto vejamos algumas definições *en passant* sobre a teoria dos algoritmos e suas aplicações sobre sistemas formais.

### 2.2.1 Algoritmos e Sistemas Formais

Um algoritmo é, intuitivamente, um procedimento “mecânico” que gera a partir de uma dada sequência finita de símbolos e utilizando um número finito de passos *determinísticos* uma nova sequência finita de símbolos [37] [56]. A teoria dos algoritmos é formalizada através da *Teoria das Funções Recursivas* ou das *Máquinas de Turing*, fundando-se na *Tese de Church* [56]. Na teoria das funções recursivas podemos definir várias espécies de subconjuntos dos naturais:

**Definição 2.7** *Um conjunto  $A \subseteq \omega_0$  é recursivamente enumerável se existe um algoritmo tal que, aplicado sobre o conjunto dos naturais  $0, 1, 2, 3, \dots$ , tem como imagem  $A$ .*

**Definição 2.8** *Um conjunto  $A \subseteq \omega_0$  é recursivo se existe um algoritmo que, aplicado a todo o  $n \in \omega_0$ , toma o valor 1 se  $n \in A$ , e 0 se  $n \notin A$ .*



Um dos resultados cruciais na teoria dos algoritmos é que todo o conjunto recursivo é recursivamente enumerável, mas nem todo o conjunto recursivamente enumerável é recursivo [56] [77].

Como *sistema formal* entendemos um conjunto de símbolos de um dado alfabeto  $A$ , dotado de regras específicas para a manipulação deste símbolos, e de um conjunto de axiomas apresentados como “fórmulas bem formadas” (abreviadamente wff) neste alfabeto [56] [46] [19]. A teoria de algoritmos é amplamente utilizada no trato com sistemas formais, uma vez que torna rigoroso o conceito de *demonstração* [77].

Nesta seção estaremos interessados em sistemas formais com linguagens de primeira ordem, como por exemplo  $L_{Ar}^1$  (a linguagem da aritmética elementar) ou  $L_{ZFC}^1$  (a linguagem da teoria dos conjuntos de Zermelo-Fraenkel mais o Axioma da Escolha) [56]. Note que  $L_{Ar}^1 \subset L_{ZFC}^1$ .

Seguindo [22], consideremos uma teoria  $T$  formalizada numa linguagem de primeira ordem tal que  $L_{Ar}^1 \subseteq L_T^1$  e suponhamos que existe uma função computável biunívoca  $\iota : \mathcal{S}_T \leftrightarrow \omega_0$  sobre o conjunto contável de sentenças de  $T$ , que chamaremos  $\mathcal{S}_T$ .

Seja  $\mathcal{T}_T \subset \mathcal{S}_T$  o conjunto de teoremas de  $T$ , que é recursivamente enumerável.

**Definição 2.9** *Para qualquer teoria  $T$  como estabelecido temos:*

1. *Se  $\mathcal{T}_T \subset \mathcal{S}_T$  é um conjunto recursivo, então  $T$  é uma teoria decidível.*
2. *Se  $\mathcal{T}_T \subset \mathcal{S}_T$  não é um conjunto recursivo, então  $T$  é uma teoria indecidível.*
3. *Se, para toda a sentença  $\xi \in \mathcal{S}_T$ , ou  $\xi \in \mathcal{T}_T$  ou  $\neg\xi \in \mathcal{T}_T$ , então dizemos que  $T$  é uma teoria completa.*
4. *Se existe um  $\xi_0 \in \mathcal{S}_T$  tal que tanto  $\xi_0 \notin \mathcal{T}_T$  quanto  $\neg\xi_0 \notin \mathcal{T}_T$ , então chamamos  $T$  uma teoria incompleta e  $\xi_0$  uma sentença indecidível de  $T$ .*

Denotaremos  $\mathbf{N}$  o modelo standard que satisfaz os axiomas da aritmética e  $\mathbf{V}$  o modelo bem fundado de Von Neumann para ZFC.

**Definição 2.10** *Dizemos que a teoria  $T$  é aritmeticamente consistente se e somente se  $\mathbf{N}$  é um modelo para todas as sentenças em  $\mathcal{S}_{Ar}$  que são*

demonstráveis em  $T$ , com  $L_T^1 \supset L_{Ar}^1$  e sendo  $S_{Ar}$  o conjunto de todas as sentenças da aritmética.

Após este breve passeio na teoria de sistemas formais, onde definimos o essencial para o que se segue, voltemos às equações diofantinas. Remetemos o leitor não familiarizado com o assunto que tratamos para as referências [19] [46] [54] [56] [77] e bibliografias lá citadas.

### 2.2.2 Uma Equação Diofantina Exponencial

Em 1961, Martin Davis, Hilary Putnam e Julia Robinson [31] demonstraram que todo o conjunto recursivamente enumerável pode ser definido existencialmente em termos de equações *exponenciais diofantinas*. Equações exponenciais diofantinas são obtidas quando permitimos que nossas equações polinomiais diofantinas contenham termos do tipo  $c\alpha_1^{\beta_1}\alpha_2^{\beta_2}\cdots\alpha_n^{\beta_n}$  onde os  $\alpha_i$  e os  $\beta_i$  podem ser tanto inteiros quanto variáveis [30]. Da afirmação “nem todo o conjunto recursivamente enumerável é recursivo” [19] [56] [37] [77], e do resultado de Davis, Putnam e Robinson estabeleceu-se a *não existência de um algoritmo que nos diga se uma dada equação diofantina exponencial tem soluções*.

O resultado que acabamos de exibir está intimamente relacionado com o décimo problema da famosa lista que o matemático alemão David Hilbert apresentou no “International Congress of Mathematics” em 1900 [28]. O Décimo Problema de Hilbert pode ser apresentado como:

**Décimo Problema de Hilbert:** Suponhamos dada uma equação diofantina com número arbitrário de variáveis e com coeficientes inteiros racionais. Apresentar um procedimento pelo qual seja possível determinarmos, após um número finito de operações, se esta equação é solúvel ou não nos inteiros racionais.

Em outras palavras: encontrar um algoritmo que teste as equações polinomiais diofantinas com coeficientes inteiros e nos diga se estas equações apresentam soluções nos inteiros ou não.

Como vimos, se pudermos encontrar um polinômio diofantino que represente a exponencial diofantina, então temos uma resposta negativa para o 10<sup>o</sup> problema de Hilbert.

A existência de tal polinômio foi demonstrada pela primeira vez por Y. Matijasevič em 1970 [30] usando as propriedades das sequências geradas pelos números de Fibonacci pares e mostrando ser esta sequência diofantina.

Uma equação diofantina explícita representando  $m = n^k$  foi posteriormente obtida por Martin Davis [29]. Apresentamos aqui esta versão de Martin Davis [28] para a função diofantina exponencial, obtida a partir de uma equação de Pell do tipo

$$x^2 - (a^2 - 1)y^2 = 1 \quad (2.10)$$

onde  $x, y \geq 0$  e  $a > 1$ . Pode-se numerar as soluções de (2.10), que formam um conjunto infinito bem conhecido [30], em ordem crescente

$$\begin{aligned} x &= \chi_a(0), & y &= \psi_a(0) \\ x &= \chi_a(1), & y &= \psi_a(1) \\ x &= \chi_a(2), & y &= \psi_a(2) \\ \vdots & & \vdots & \end{aligned} \quad (2.11)$$

onde os  $\psi_a$  são números que crescem exponencialmente. Davis demonstrou que  $y = \psi_a(k)$  é diofantina [28] tornando factível a definição de uma exponencial, pois

$$(2a - 1)^n \leq \psi_a(n + 1) \leq (2a)^n$$

Usando os resultados precedentes, demonstra-se que o conjunto simultâneo de eq. diofantinas

$$\begin{aligned} x^2 - (o^2 - 1)y^2 - 1 &= 0 \\ u^2 - (o^2 - 1)v^2 - 1 &= 0 \\ v - ry^2 &= 0 \\ b - 1 - 4py &= 0 \\ b - o - qu &= 0 \\ s - x - cu &= 0 \\ s^2 - (b^2 - 1)t^2 - 1 &= 0 \\ t - k - 4(d - 1)y &= 0 \end{aligned}$$

$$\begin{aligned}
y - k - e + 1 &= 0 \\
(x - y(o - n) - m)^2 - (f - 1)^2(2on - n^2 - 1)^2 &= 0 \\
m + g - 2on + n^2 + 1 &= 0 \\
n + h - w &= 0 \\
k + l - w &= 0 \\
o^2 - (w^2 - 1)(w - 1)^2 z^2 - 1 &= 0
\end{aligned}$$

tem soluções nos argumentos  $x, o, y, u, v, r, b, p, q, s, c, t, e, d, f, g, h, w, l, z$  se e somente se  $m = n^k$  [28].

Partindo-se deste conjunto de equações diofantinas, podemos construir uma única eq. diofantina  $A(m, n, k, w_1, \dots, w_{20})$  tal que  $\exists w_1, \dots, w_{20}(A(m, n, k, w_1, \dots, w_{20}) = 0) \leftrightarrow m = n^k$ , simplesmente fazendo com que  $A(m, n, k, w_1, \dots, w_{20})$  seja a soma dos quadrados de cada equação do sistema anterior. Tal construção é trabalhosa, mas pode facilmente ser obtida com o auxílio de um computador dotado de algum bom programa de Computação Algébrica<sup>2</sup>.

O sistema anterior não é o único que representa  $m = n^k$ . Na verdade equações com apenas 5 parâmetros foram obtidas para a exponencial. Isto se deve ao fato de sempre podermos reduzir o número de parâmetros de uma eq. diofantina para pelo menos 13 [58].

A existência de uma equação diofantina exponencial nos permite afirmar que o subconjunto dos números primos é diofantino.  $p$  é primo se e somente se o sistema de equações

$$\begin{aligned}
p &= s + 1 \\
p &= r + 2 \\
q &= s! \\
ap - bq &= 1
\end{aligned}$$

é satisfeito para algum valor de  $a, b, s, r, q \in \mathbb{N}$ . Como  $s!$  pode ser representado como uma exponencial diofantina (cf. [30]) o sistema de eq. anterior é diofantino. A característica de serem os primos diofantinos se a função exponencial for diofantina foi um argumento muito usado para se conjecturar que  $m = n^k$  não era diofantina.

---

<sup>2</sup>Alguns programas deste tipo usando as linguagens MAPLE e REDUCE estão listados no Apêndice A

De posse da equação  $m = n^k$  podemos agora apresentar uma representação dos quantificadores lógicos em termos de equações diofantinas.

### 2.2.3 Teorema do Quantificador Limitado

Os quantificadores  $\exists$  e  $\forall$  podem ser traduzidos em equações diofantinas de acordo com o teorema [30] [28] [56]

**Teorema 2.11** *Seja  $p(x, y, k, z_1, \dots, z_n)$  um polinômio diofantino com variáveis  $z_1, \dots, z_n$  e parâmetros  $x, y, k$ . Então*

$$\begin{aligned} (\forall k)_{k \leq x} (\exists z_1, \dots, z_n)_{z_1, \dots, z_n \leq y} [p(x, y, k, z_1, \dots, z_n) = 0] &\leftrightarrow \\ &\leftrightarrow \exists b_1, \dots, b_n [(b_{y+1}^1) \equiv (b_{y+1}^2) \equiv \dots \\ &\equiv (b_{y+1}^n) \equiv p(x, y, Q! - 1, b_1, \dots, b_n) \equiv 0 \pmod{(Q! - 1)}] \end{aligned}$$

onde  $Q$  é um polinômio diofantino tal que

$$Q = Q(x, y) > |p(x, y, k, z_1, \dots, z_n)| + 2x + y + 1$$

para todos os  $k \leq x$  e para todos os  $z_1 \leq y, \dots, z_n \leq y$ .  $b_1, \dots, b_n$  também são escolhidos tais que  $b_i < (b_{y+1}^n)$ ,  $i = 1 \dots n$ .

Note que uma vez em posse da exponencial diofantina imediatamente construímos expressões diofantinas que representem  $n!$  e  $\binom{n}{k}$ , se lembramos que estas funções são aproximadas por expressões do tipo  $x^y$  [30] [28].

**Corolário 2.12** *Seja  $R$  e  $S$  definidos como:*

$$\langle y, z_1, \dots, z_n \rangle \in S \leftrightarrow (\forall k)_{k \leq y} (\exists x_1, \dots, x_m) [p(y, k, z_1, \dots, z_n, x_1, \dots, x_m) = 0] \quad (2.12)$$

$$\langle y, z_1, \dots, z_n \rangle \in R \leftrightarrow (\exists k)_{k \leq y} (\exists x_1, \dots, x_m) [p(y, k, z_1, \dots, z_n, x_1, \dots, x_m) = 0] \quad (2.13)$$

onde  $p(y, k, z_1, \dots, z_n, x_1, \dots, x_m)$  é um polinômio diofantino. Então  $S$  e  $R$  são diofantinos.

Observamos que de fato temos uma sistemática poderosa para contruirmos definições diofantinas de variados conjuntos, aplicando para tal o teorema 2.11 em conjunção com as técnicas apresentadas para a introdução dos conectivos  $\wedge$  e  $\vee$ . Vejamos alguns exemplos de problemas famosos que podem ser escritos na linguagem das equações diofantinas.

## 2.2.4 Alguns Exemplos Envolvendo Problemas Famosos

**Exemplo 1:** A *última conjectura de Fermat*, também conhecida como último teorema de Fermat, é a seguinte afirmação: a equação

$$x^n + y^n = z^n$$

não tem soluções para  $x, y, z$  inteiros  $> 0$  se  $n$  for um inteiro maior que 2.

Seja  $A(m, n, k, x_1, \dots, x_{20})$  uma função que representa a exponencial, como anteriormente. A expressão anterior pode ser escrita como (omitindo-se as variáveis, por simplicidade):

$$\begin{aligned} A^2(a, x, n) + A^2(b, y, n) + A^2(a + b, z, n) = \\ = F(a, b, x, y, z, n, x_1, \dots, x_{60}) = 0 \end{aligned}$$

implicando ser o último teorema de Fermat falso se e somente se

$$\exists a, b, x, y, z, n, x_1, \dots, x_{60} [F(a, b, x, y, z, n + 2, x_1, \dots, x_{60}) = 0]$$

o que nos mostra poder este problema ser reduzido a uma questão sobre a existência ou não de soluções de uma dada equação diofantina.

**Exemplo 2:** A função zeta de Riemann é definida

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

Esta função tem um polo em  $s = 1$  e é analítica em todo o plano complexo, exceto neste polo.  $\zeta$  tem ainda zeros nos pontos  $-2, -4, -6, -8, \dots$ , chamados zeros *triviais*. Todos os outros zeros da função zeta de Riemann são chamados *não-triviais*.

A *Hipótese de Riemann* assera que todos os zeros não-triviais da função zeta se situam na linha  $\text{Re}(s) = 1/2$ , e mostra-se que esta hipótese é equivalente à afirmação de que  $\zeta(s)$  não tem zeros no intervalo  $\frac{1}{2} < \text{Re} < 1$ . Recentemente Y. Matiasевич demonstrou (computacionalmente) a Hipótese de Riemann, dando-lhe uma prova de que há uma demonstração analítica para ela.

Definindo

$$\delta(x) = \prod_{n=1}^{x-1} \prod_{j=1}^n \eta(j)$$

com

$$\begin{cases} \eta(j) = 1, & \text{se } j \text{ não é potência de um primo} \\ \eta(p^k) = p, & p \text{ primo} \end{cases}$$

a Hipótese de Riemann pode ser escrita como [30] [56]:

$$\left( \sum_{k \leq \delta(n)} \frac{1}{k} - \frac{n^2}{2} \right)^2 < 36n^3 \text{ para } n = 1, 2, 3, \dots \quad (2.14)$$

A equação anterior é diofantina, uma vez que o conjunto dos primos é diofantino e que o produto e o somatório limitados são diofantinos (em virtude do teorema 2.11).

Ambos os problemas apresentados acima podem ser abordados via equações diofantinas, de tal forma que demonstrar a existência de soluções para o polinômio correspondente seria equivalente a demonstrar estas hipótese ou a falsidade destas hipótese.

Embora seja trabalhoso, polinômios correspondentes aos problemas anteriores podem ser escritos explicitamente usando-se as técnicas apresentadas. A dificuldade que nos surge é a grande quantidade de variáveis envolvidas em tais problemas, que no caso da Hipótese de Riemann (usando-se a exponencial com 20 variáveis) pode chegar a mais de 300.000 [7]. Sabemos que qualquer eq. diofantina pode ser reduzida a pelo menos 13 variáveis [58] ou ainda a 9 [49], mas este procedimento de redução exige a construção de uma *equação diofantina universal* cujo grau pode chegar à ordem de  $5^{60}$ . No Apêndice A apresentamos alguns programas de computação algébrica usando as linguagens MAPLE e REDUCE que nos constroem explicitamente tais polinômios.

## 2.3 O Teorema de Richardson-da Costa-Doria

Nesta seção exibiremos os resultados de indecibilidade na análise real, advindos do Teorema de Gödel (mais diretamente, da resposta negativa

dada por Matijasevič ao Décimo Problema de Hilbert), expostos no artigo de Richardson [66]. A versão que apresentaremos, elaborada por N. C. A. da Costa e F. A. Doria [22], é uma expansão da encontrada em [66], que procura incompletudes na análise clássica.

Seja  $E$  um conjunto de expressões, numa dada linguagem  $L_T^1$  para a teoria formal  $T$  com  $L_T^1 \supset L_{Ar}^1$ , representando funções parcialmente definidas de uma só variável dos reais sobre os reais. Se este conjunto  $E$  de expressões se referir somente a uma álgebra específica de funções  $\mathcal{D}$ , explicitaremos isto por  $E(\mathcal{D})$ . Deste modo funções  $f \in \mathcal{D}$  são representadas em  $L_T^1$  como elementos  $E(f) \in E(\mathcal{D})$ . Observemos que não há uma correspondência biunívoca entre elementos de  $\mathcal{D}$  e  $E(\mathcal{D})$  posto que uma mesma função pode ser “escrita” de diversas maneiras.

Os seguinte resultados foram demonstrados por Richardson:

- Se a álgebra  $\mathcal{D}$  é fechada pela adição, subtração, multiplicação e composição de funções e contém  $\log 2$ ,  $\pi$ ,  $e^x$  e  $\sin x$ , então o problema *dada uma expressão  $E(f) \in E(\mathcal{D})$  decidir se existe um real  $x$  tal que  $f(x) < 0$*  será **algoritmicamente insolúvel**.
- Se incluímos à álgebra  $\mathcal{D}$  do item anterior a função módulo (valor absoluto) de  $x$ ,  $|x|$ , então o problema *dada uma expressão  $E(f) \in E(\mathcal{D})$  decidir se  $f(x) = 0$*  será **algoritmicamente insolúvel**.
- Se, além dessas condições, acrescentamos à  $\mathcal{D}$  uma função  $B(x)$  tal que para nenhuma função  $f(x)$  em  $\mathcal{D}$  e nenhum intervalo  $I \in \mathbb{R}$  temos  $\frac{df(x)}{dx} = B(x)$  em  $I$ , então o problema *dada uma  $E(f) \in E(\mathcal{D})$  decidir se existe uma função  $g \in \mathcal{D}$  tal que  $\frac{dg(x)}{dx} = f(x)$*  será **algoritmicamente insolúvel**.

Onde  $g(x)$  representa o valor de  $g \in \mathcal{D}$  no ponto  $x$  e  $g(x) = f(x)$  se e somente se  $g$  e  $f$  são definidos sobre os mesmos pontos e se seus valores são iguais nestes pontos.

A idéia por trás da demonstração de Richardson é a seguinte:

Primeiro suporemos  $\mathcal{D}$  como a álgebra das *funções subelementares*, ou seja,  $\mathcal{D}$  é fechada pela soma, subtração e multiplicação de funções.  $\mathcal{D}$  também contém polinômios, senos, co-senos, exponenciais e os números



reais  $\log 2$ ,  $\pi$  e todos os racionais. Observemos que esta álgebra é extremamente rica<sup>3</sup>, uma vez que grande parte dos objetos que trabalhamos em física pode ser representado por elementos de  $\mathcal{D}$ .

Consideremos um polinômio diofantino  $p(y, x_1, \dots, x_n)$  qualquer. Vimos alhures que Davis, Matijasevič e Robinson demonstraram não existir um algoritmo capaz de apontar se  $p$  tem zeros ou não. Permitamos agora que  $p$  assuma valores dos reais sobre os reais e construamos a seguinte função:

$$K(y, x_1, \dots, x_n)[p^2(y, x_1, \dots, x_n) + \sum_{j=1}^n \sin^2(\pi x_j)] \quad (2.15)$$

onde  $K(y, x_1, \dots, x_n)$  é uma função subelementar rápida e monótonamente crescente com  $K(0, 0, 0, \dots, 0)$  muito grande. A parte de (2.15) que contém os senos só se anula se os  $x_j$  são inteiros. Portanto, decidir se a expressão anterior tem zeros é equivalente a decidir se existem soluções para a equação diofantina  $p(y, x_1, \dots, x_n) = 0$ , o que é impossível no caso geral. Formalizemos isto, seguindo da Costa e Doria [22].

Começemos definindo de maneira rigorosa a álgebra  $\mathcal{A}[x_1, \dots, \mathbb{Q}]$  das funções subelementares com variáveis  $\{x_1 \dots\}$  definida sobre os racionais  $\mathbb{Q}$ .

**Definição 2.13** *A álgebra  $\mathcal{A}[x_1, \dots, \mathbb{Q}]$  é tal que:*

1.  $\pi$ ,  $q$ ,  $x_i$ ,  $\sin x_i$  e  $e^{x_i}$  pertencem a  $\mathcal{A}$ , com  $q \in \mathbb{Q}$ .
2. Se  $A$  e  $B$  são elementos de  $\mathcal{A}$ , então  $A + B$ ,  $A - B$  e  $A \cdot B$  também são elementos de  $\mathcal{A}$ .
3.  $\mathcal{A}$  é a menor álgebra fechada segundo as condições anteriores.

Chamaremos  $\mathcal{A}'$  a quase-álgebra definida como  $\mathcal{A}$  apenas acrescentando ao item 2 a condição de que  $A \circ B$  (o denota composição de funções) também seja elemento da álgebra.

Notemos que como  $\mathcal{A}$  é definida sobre os racionais,  $\mathcal{A}$  é um anel enumerável [12]. É natural estendermos  $\mathcal{A}[\mathbb{Q}]$  para os reais de tal forma que  $\mathcal{A}[\mathbb{Q}] \subset \mathcal{A}[\mathbb{R}]$ , onde  $\mathcal{A}[\mathbb{R}]$  é a extensão de  $\mathcal{A}[\mathbb{Q}]$ , e desta forma  $\mathcal{A}[\mathbb{R}]$  não é contável. Seguindo [22], quando for relevante o fato da álgebra  $\mathcal{A}$  ser contável ou não, explicitaremos no texto.

---

<sup>3</sup>É só nos lembrarmos, por exemplo, da importância dos osciladores harmônicos em física

**Lema 2.14**  $\mathcal{A}$  é fechada segundo a derivação parcial  $\partial_i = \partial/\partial x_i$ .

*Demonstração:* Por indução.  $\partial_i \pi = \partial_i q = \partial_i x_j = \partial_i(\sin x_j) = \partial_i(e^{x_j}) = 0 \in \mathbb{Q} \subset \mathcal{A}$ , para  $i \neq j$ . Ainda  $\partial_i x_i = 1 \in \mathcal{A}$ ,  $\partial_i(\sin x_i) = \cos x_i = \sin(x_i + \frac{\pi}{2}) \in \mathcal{A}$  e  $\partial_i(e^{x_i}) = e^{x_i} \in \mathcal{A}$ . Suponhamos que  $A$  e  $B \in \mathcal{A}$ , então é evidente por indução e pela linearidade do operador  $\partial_i$  que  $\partial_i C \in \mathcal{A}$ ,  $C$  obtido a partir de  $A$  e  $B$  por  $+$ ,  $-$ ,  $\circ$ ,  $\cdot$ .  $\square$

Apresentemos agora o primeiro dos resultados listados anteriormente. Como nesta proposição constroem-se uma função que leva elementos da álgebra das equações diofantinas em elementos da álgebra  $\mathcal{A}$  anteriormente definida, chamaremos a esta função *functor de Richardson I* [22].

**Proposição 2.15 (Functor de Richardson I)** *Existe uma injeção  $\iota_P : P \rightarrow \mathcal{A}$ , onde  $P$  é a álgebra dos polinômios sobre  $\mathbb{Z}$  com número finito de variáveis e  $\mathcal{A}$  é a álgebra das funções subelementares, tal que:*

1. *Determinada uma expressão para  $p \in P$  em  $L_{\mathbb{A}^n}^1$ , existe um procedimento efetivo (algoritmo) para obtermos a expressão para  $F = \iota_P(p)$  em  $L_{\mathbb{Z}^n}^1$ .*
2.  *$\iota_P$  é biunívoca.*
3.  *$\exists \vec{x} \in \omega_0^n(p(m, \vec{x}) = 0)$  se e somente se  $\exists \vec{x} \in \mathbb{R}^n(F(m, \vec{x}) = 0)$  se e somente se  $\exists \vec{x} \in \mathbb{R}^n(F(m, \vec{x}) \leq 1)$ , para  $p \in P$  e  $F \in \mathcal{A}$ .*

Na proposição acima abreviamos  $\langle x_1, \dots, x_n \rangle$  por  $\vec{x} \in \mathbb{R}^n$ . Deste modo  $p(x_1, \dots, x_n)$  se escreve como  $p(\vec{x})$ .

*Demonstração:* É obtida a partir dos lemas seguintes [66] [22]:

**Lema 2.16** *Se  $f \in \mathcal{A}$ , então existe um  $g \in \mathcal{A}$  tal que:*

1.  $\forall \vec{x} \in \mathbb{R}^n g(\vec{x}) > 1$ .
2.  $\forall \vec{x}, \vec{\delta} \in \mathbb{R}^n (|\delta_1| \leq 1 \wedge \dots \wedge |\delta_n| \leq 1) \leftrightarrow (g(\vec{x}) > |f(\vec{x} + \vec{\delta})|)$ .

*Demonstração:* A demonstração é obtida por indução sobre o número de etapas que são necessárias para obtermos uma expressão para  $f(\vec{x})$ . As expressões fundamentais (etapa 0) são ou constantes ou variáveis. No estágio  $n + 1$  as expressões são da forma  $A \pm B$ ,  $A \cdot B$ ,  $e^A$  ou  $\sin$ , onde  $A$  e  $B$  são expressões obtidas em pelo menos  $n$  etapas. Pela construção de  $\mathcal{A}$  todas as funções subelementares são obtidas desta maneira.

Etapa 0: Ou  $f(\vec{x}) = c$  ou  $f(\vec{x}) = x_i$  ( $x_i$ , como antes, é a  $i$ -ésima componente de  $\vec{x}$ ). Se

$$f(\vec{x}) = c$$

definimos

$$g(\vec{x}) = |c| + 2$$

Se

$$f(\vec{x}) = x_i$$

definimos

$$g(\vec{x}) = x_i^2 + 2$$

Estas definições visivelmente satisfazem os itens 1 e 2 do Lema.

Etapa  $n + 1$ : Suponhamos que  $A$  e  $B$  tenham sido obtidas em ao menos  $n$  etapas e suponhamos ainda que  $k$  e  $h$  satisfazem os itens 1 e 2 do Lema para  $A$  e  $B$  respectivamente. Temos:

- Se  $f = A \pm B$  definimos  $g = k + h$ .
- Se  $f = A \cdot B$  definimos  $g = k \cdot h$ .
- Se  $f = e^A$  definimos  $g = e^k$
- Se  $f = \sin A$  definimos  $g = 2$

e  $g$  assim contruído satisfaz o Lema.  $\square$

**Lema 2.17** *Existe um procedimento construtivo tal que dada uma expressão para  $p \in P$  podemos obter expressões para funções  $k_i \in \mathcal{A}$  que satisfazem:*

$$k_i(m, \vec{x}) > |\partial_i(p^2(m, \vec{x} + \vec{\delta}))|$$

para  $\delta_i \in \mathbb{R}$  e  $|\delta_i| \leq 1$ .

*Demonstração:* Como  $\mathcal{A}$  é fechada por  $\partial_i$ , então aplicamos o procedimento do Lema anterior (que é algorítmico) ao argumento entre  $|\cdots|$ . Como a operação de derivação é algorítmica, resulta no Lema.  $\square$

**Definição 2.18** *Seja  $p \in P$  e  $k_i$  como no Lema 2.17, definimos:*

$$f(m, \vec{x}) = (n+1)^4 \left\{ p^2(m, \vec{x}) + \sum_{i=1}^n (\sin^2 \pi x_i) k_i^4(m, \vec{x}) \right\} \quad (2.16)$$

**Definição 2.19**  $F(m, \vec{x}) = f(m, x_1^2, \dots, x_n^2)$ .

Os dois primeiros itens da proposição 2.15 resultam de imediato destas definições, uma vez que  $(p_1 \neq p_2) \rightarrow (F_1 \neq F_2)$ .

Por contrução, é imediato no ítem 3 que [66]:

$$\begin{aligned} (\exists \vec{x} \in \omega_0^n (p(m, \vec{x}) = 0)) &\rightarrow (\exists \vec{x} \in \mathbb{R}^n (F(m, \vec{x}) = 0)) \rightarrow \\ &\rightarrow (\exists \vec{x} \in \mathbb{R}^n (F(m, \vec{x}) \leq 1)) \end{aligned}$$

O que precisamos demonstrar é  $(\exists \vec{x} \in \mathbb{R}^n (F(m, \vec{x}) \leq 1)) \rightarrow (\exists \vec{x} \in \omega_0^n (p(m, \vec{x}) = 0))$  supondo  $m \in \omega_0$ .

$$\begin{aligned} f(m, \vec{x}) \leq 1 &\rightarrow \\ \rightarrow p^2(m, \vec{x}) + \sum_{i=1}^n (\sin^2 \pi x_i) k_i^4(m, \vec{x}) &\leq \frac{1}{(n+1)^4} \end{aligned} \quad (2.17)$$

O lado esquerdo da equação (2.17) pode ser considerado em separado como sendo menor que o lado direito, resultando

$$p^2(m, \vec{x}) \leq \frac{1}{(n+1)^4} \quad (2.18)$$

e

$$(\sin \pi x_i)^{\frac{1}{4}} \cdot k_i(m, \vec{x}) \leq \frac{1}{(n+1)} \quad (2.19)$$

Seja  $\langle x \rangle$  o número natural mais próximo de  $x$ . Mostra-se que, para  $x \geq 0$ ,  $|\langle x \rangle - x| \leq (\sin^2 \pi x)^{1/4}$  [66].

De (2.19) obtemos

$$\sum_{i=1}^n |\langle x_i \rangle - x_i| k_i(m, \vec{x}) \leq \frac{n}{n+1}$$

De (2.18) e da eq. anterior obtemos

$$p^2(m, \vec{x}) + \sum_{i=1}^n |\langle x_i \rangle - x_i| k_i(m, \vec{x}) < 1 \quad (2.20)$$

Usando o teorema do valor médio,  $p^2(m, \langle \vec{x} \rangle) \leq p^2(m, \vec{x}) + \sum_{i=1}^n |\langle x_i \rangle - x_i| \cdot |\partial_i p^2(m, \bar{x}_1, \dots, \bar{x}_n)|$  onde  $\bar{x}$  situa-se no intervalo entre  $x$  e  $\langle x \rangle$ . Pelo Lema 2.17 temos  $k_i(m, \vec{x}) > |\partial_i(p^2(m, \bar{x}_1, \dots, \bar{x}_n))|$ . Pela eq. (2.20) obtemos

$$p^2(m, \langle \vec{x} \rangle) < 1$$

Por hipótes  $m$  é um número natural.  $p^2$  leva naturais nos inteiros. Portanto,  $p^2(m, \langle \vec{x} \rangle) = 0$  e  $p(m, \langle \vec{x} \rangle) = 0$ , o que completa a prova.  $\square$ .

A existência do functor apresentado nos mostra claramente como obter resultados de indecibilidade na Análise Real de uma função de várias variáveis. Richardson segue adiante e reduz esta função de várias variáveis a outra de somente uma variável. Esta redução é feita substituindo cada variável por uma função que oscila rapidamente em função de uma única variável  $x$ , como veremos no:

**Corolário 2.20 (Functor de Richardson II)** *Seja  $\mathcal{A}_1$  a álgebra das funções subelementares sobre uma única variável real  $x$ . Então existe uma aplicação  $\iota' : P \rightarrow \mathcal{A}_1$  tal que:*

1.  $\iota'$  é construtiva.
2.  $\iota'$  é biunívoca.
3.  $\exists \vec{x} \in \omega_0^n (p(m, \vec{x}) = 0)$  se e somente se  $\exists x \in \mathbb{R} (L(m, x) = 0)$  se e somente se  $\exists x \in \mathbb{R} (G(m, x) \leq 1)$ .

*Demonstração:* Definamos

$$h(x) = x \sin x$$

$$g(x) = x \sin x^3$$

Dada uma  $F(m, \vec{x})$  como definida anteriormente, fazemos as seguintes substituições:

$$\begin{aligned} x_1 &= h(x) \\ x_2 &= h \circ g(x) \\ x_3 &= h \circ g \circ g(x) \\ &\vdots \\ x_{n-1} &= h \circ \underbrace{g \circ \dots \circ g(x)}_{n-2 \text{ vezes}} \end{aligned}$$

e

$$x_n = \underbrace{g \circ g \circ \dots \circ g(x)}_n$$

Feitas as substituições obtemos  $G(m, x)$ . Definimos também

$$L(m, x) = G(m, x) - \frac{1}{2}$$

Se  $F$  é construtiva, é evidente que  $G$  e  $L$  são também construtivas, e com isto demonstramos os itens 1 e 3 (como consequência da Proposição 2.15).

O item 2 é imediato, pois  $p_1 \neq p_2$  implica  $G_1 \neq G_2$ .  $\square$

Como os funtores  $\iota$  e  $\iota'$  são construtíveis, existe um algoritmo que leva elementos de  $P$  em  $\mathcal{A}$ . No Apêndice A apresentamos um tal algoritmo escrito em linguagem MAPLE, aplicado a uma eq. diofantina particular.

**Lema 2.21** *Se*

$$B(m, x) = |G(m, x) - 1| - (G(m, x) - 1)$$

*então  $\forall x \in R(B(m, x) = 0)$  se e somente se  $\neg \exists x \in R(G(m, x) < 1)$ .*

*Demonstração:* Imediata.  $\square$

**Corolário 2.22** *Se*

$$\chi(m, x) = \min(1, 2 \overset{*}{-} 2G(m, x))$$

onde  $x \overset{*}{-} y = \frac{1}{2}(|x - y| + (x - y))$  e  $\min(x, y) = x - (x \overset{*}{-} y)$ , então

1.  $\neg \exists x \in \mathbb{R}(G(m, x) < 1)$  se e somente se  $\forall x \in \mathbb{R}(\chi(m, x) = 0)$ .
2.  $\exists x \in \mathbb{R}(G(m, x) < 1)$  se e somente se existe um intervalo  $I_m \subset \mathbb{R}$  tal que  $\forall x \in I_m(\chi(m, x) = 1)$ .

*Demonstração:* Veja [66].  $\square$

Estendamos a álgebra  $\mathcal{A}'_1$  para uma pseudo-álgebra  $\mathcal{Q}$  tal que (com  $f, g \in \mathcal{A}'_1$ ):

- $\frac{f}{g} \in \mathcal{Q}$ , no domínio onde a divisão é definida.
- Se  $r = \int_a^b f(x)dx$  (podendo a integral ser imprópria) então  $r \in \mathcal{Q}$ .
- $\eta(x) \in \mathcal{Q}$ , onde  $\eta$  é a função sinal, que é +1 para  $x$  positivo, -1 para  $x$  negativo e zero para  $x = 0$ .
- $d\eta(x)/dx \in \mathcal{Q}$ .
- $\mathcal{Q}$  é fechada segundo operações algébricas (finitas) e composição (finita) de funções, sempre que estes objetos forem bem definidos.

**Corolário 2.23** *Existe uma função  $\theta(m, x) \in \mathcal{Q}$  tal que:*

1.  $\neg \exists x \in \mathbb{R}(G(m, x) < 1)$  se e somente se  $\forall x \in \mathbb{R}(\theta(m, x) = 0)$ .
2.  $\exists x \in \mathbb{R}(G(m, x) < 1)$  se e somente se  $\forall x \in \mathbb{R}(\theta(m, x) = 1)$ .

*Demonstração:* Fazemos  $C(m, x) = (B(m, x))^2$  com  $B$  dado anteriormente. Definamos agora as integrais impróprias

$$K(m) = \int_{-\infty}^{+\infty} \frac{C(m, x)e^{-x^2}}{1 + C(m, x)} dx$$

$K(m)$  é finita. Fazemos agora

$$\theta(m, x) = \theta(m) = \eta\left(\frac{K(m)}{1 + K(m)}\right)$$

Podemos agora estabelecer o principal resultado de indecibilidade desta seção, consequência da solução negativa de Matijasevič ao Décimo Problema de Hilbert [66] [22]:

**Proposição 2.24** *Para um  $m \in \omega_0$  arbitrário, não existe um algoritmo geral que testa se:*

1. *Se existem reais  $\vec{x}$  tais que  $F(m, \vec{x}) = 0$ .*
2. *Existe um  $x \in \mathbb{R}$  tal que  $G(m, x) < 1$ .*
3.  *$\forall x \in \mathbb{R} B(m, x) = 0$ .*
4.  *$\forall x \in \mathbb{R} \chi(m, x) = 0$  ou  $\forall x \in \mathbb{R} \chi(m, x) = 1$  sobre um intervalo  $I_m \subset \mathbb{R}$ .*
5.  *$\forall x \in \mathbb{R} \theta(m, x) = 0$  ou  $\forall x \in \mathbb{R} \theta(m, x) = 1$  sobre os reais.*
6. *Para uma  $f(m, x)$  arbitrária temos  $f(m, x) \equiv \theta(m, x)$ .*

*Demonstração:* Advém dos resultados anteriores, junto com a solução negativa para o Décimo problema de Hilbert.  $\square$

Agora vejamos o resultado de incompletude deste Capítulo, que resulta das Proposições anteriores.

**Proposição 2.25** *Supondo-se ZFC aritmeticamente consistente, pode-se contruir uma equação diofantina*

$$p(x_1, \dots, x_n) = 0$$

*em ZFC, tal que não tenha soluções nos naturais, mas tal que*

$$\text{ZFC} \not\vdash \neg(\exists \vec{x} \in \omega_0^n p(\vec{x}) = 0),$$

*ainda que não possamos demonstrar que*

$$\text{ZFC} \vdash \neg(\exists \vec{x} \in \omega_0^n p(\vec{x}) = 0)$$



*Demonstração:* Veja [22].  $\square$

Para uma apresentação de outros resultados de incompletude na análise clássica, veja [22].

Como veremos no capítulo seguinte, o functor de Richardson se apresenta como uma poderosa ferramenta na demonstração de questões formalmente indecidíveis face a uma axiomática para a teoria dos conjuntos, como por exemplo ZFC.

## Capítulo 3

# Algumas Questões sobre a Geometria dos Campos de Gauge

### 3.1 Introdução

Desde os trabalhos iniciais de C. N. Yang e R. I. Mills [82], Schwinger [68] [69] [70] [71] e de R. Utiyama [78] que os *campos de gauge* adquiriram extrema importância no estudo das teorias de campos. Na verdade, os principais avanços na física de partículas elementares, nas últimas décadas, estão ligados a estas teorias [62] [52].

As teorias de gauge são, ao menos do ponto de vista clássico, puramente geométricas, resultado de uma mistura do espaço-tempo com grupos de simetria interna. Nestas geometrias, podemos definir com exatidão todos os elementos da análise tensorial clássica, como vetores ou formas tensoriais.

Uma das questões que surge naturalmente no decorrer do estudo de determinados campos é sobre a existência de um potencial que nos permita descreve-los. Isto se traduz, na linguagem das formas, como “é o dado campo representado por uma forma exata ?”

Formas diferenciais fechadas  $d\alpha = 0$  são, ao menos localmente, bem representadas via *Lema de Poincaré* como formas exatas, tal que  $\alpha = d\beta$ . Dependendo do grupo de cohomologia da variedade em questão estas formas podem ser representadas globalmente via derivada exterior de ou-

tras formas. Formas diferenciais *covariantes* fechadas aparecem em muitas situações em física. Tais formas são conhecidas como *condições diferenciais de Bianchi* e qualquer expressão do tipo

$$D\alpha = 0 \tag{3.1}$$

é chamada *identidade de Bianchi*, com  $D\alpha$  representando a derivada exterior covariante (que definiremos adiante) da forma  $\alpha$ .

As identidades de Bianchi aparecem em geral como condições geométricas que os campos de gauge - identificados na maioria das vezes com a forma curvatura - devem obedecer. Exemplifiquemos isto com alguns casos conhecidos da literatura temos:

**Eletromagnetismo Clássico:** O campo eletromagnético  $F_{\mu\nu}$  pode ser expresso através da derivada exterior de um potencial vetor  $A_\mu$ ,

$$F_{\mu\nu} = \partial_\mu A_\nu - \partial_\nu A_\mu.$$

Das equações de Maxwell na ausência de fontes,  $dF = 0$ , implicando  $F = dA$  (com  $F = \frac{1}{2}F_{\mu\nu}dx^\mu dx^\nu$  e  $A = A_\mu dx^\mu$ ). A identidade de Bianchi para o campo eletromagnético pode ser escrita como

$$\begin{aligned} DF &= \partial_{[\mu} F_{\nu\rho]} = \\ &= \partial_\mu F_{\nu\rho} + \partial_\rho F_{\mu\nu} + \partial_\nu F_{\rho\mu} = 0, \end{aligned}$$

onde  $[\dots]$  representa a antisimetrização com respeito aos índices entre colchetes.

**Relatividade Geral:** Consideremos o tensor de Riemann  $R^\alpha_{\beta\mu\nu}$  com relação à derivada covariante  $\nabla_\mu$ . A Identidade de Bianchi para  $R^\alpha_{\beta\mu\nu}$  fica como:

$$\nabla_{[\mu} R^\alpha_{\beta\rho\nu]} = \nabla_\mu R^\alpha_{\beta\rho\nu} + \nabla_\nu R^\alpha_{\mu\beta\rho} + \nabla_\rho R^\alpha_{\nu\mu\beta} = 0.$$

**Teorias Clássicas de Gauge :** Seja  $D_\mu = \partial_\mu + A_\mu$  a derivada covariante definida a partir da conexão de gauge  $A_\mu$ . O campo  $F_{\mu\nu}$  é dado pela curvatura

$$F_{\mu\nu} = [D_\mu, D_\nu] =$$

$$= \partial_\mu A_\nu - \partial_\nu A_\mu + [A_\mu, A_\nu],$$

onde  $A_\mu = A_\mu^a(x)\tau_a$ , sendo  $x$  um ponto na variedade base (o espaço-tempo, em geral) e  $\tau_a$  os geradores de um grupo de Lie compacto semi-simples. A identidade de Bianchi se escreve

$$D_{[\mu}F_{\nu\rho]} = 0$$

e resulta diretamente da Identidade de Jacobi para os comutadores de Lie  $[\dots, \dots]$ .

As soluções das Condições Diferenciais de Bianchi são de particular interesse nas teorias de gauge, por estarem associadas aos problemas das *cópias de campos de Gauge* [33] [34] [35] [3] [4] [38] [81] [13]. Recentemente, o estudo destas soluções tem apresentado especial relevância no problema das *anomalias chirais* [5] [60] [65], devido às violações de equações do tipo (3.1) no processo de quantização de determinados campos.

O que faremos neste capítulo é verificar as condições nas quais as identidades diferenciais de Bianchi apresentam soluções não-curvatura. Feito isto, mostraremos que dada uma forma conexão que admite soluções não-curvaturas, não podemos demonstrar que esta forma realmente se encaixa nas condições anteriormente obtidas [26]. Vejamos antes uma breve revisão das teorias de gauge sobre espaços fibrados.

## 3.2 Geometria dos Campos de Gauge

Um campo é, *grosso modo*, uma atribuição para cada ponto  $x$  do espaço-tempo de uma grandeza física, como por exemplo um vetor representando a velocidade de escoamento de um dado líquido, atribuição esta feita de maneira contínua. Campos de gauge são campos que se mantêm invariantes segundo determinadas transformações — ditas *de gauge* — que agem somente nestas atribuições.

Tendo estas idéias em mente, podemos observar que a maneira natural de representarmos uma teoria geral de campos de gauge seria ligarmos a cada ponto do espaço-tempo um *espaço interno* ou *espaço de gauge*; os campos, desta maneira, seriam mapeamentos lisos que levariam pontos do

espaço-tempo à elementos do espaço interno ligado a este ponto. As transformações de gauge se traduziriam como a ação de um grupo de transformações levando elementos do espaço interno sobre ele mesmo.

O instrumental matemático sobre o qual formalizamos todas as idéias expostas nos parágrafos acima é conhecido como *geometria diferencial* e o espaço contruído atribuindo-se a cada ponto um espaço interno como *espaço fibrado*.

Façamos isto de uma maneira mais rigorosa (seguindo [1] [18][27] [33] [52] [63]).

Nossos campos são contruídos sobre uma variedade base  $M$ ,  $n$ -dimensional,  $C^k$ -diferenciável,  $k > n$ , tipo Hausdorff (isto é, dados  $x, x' \in M$  existem abertos  $U, U' \subset M$  tal que  $x \neq x'$  implica que  $x \in U$ ,  $x' \in U'$  e  $U \cap U' = \emptyset$ ) dotada de um tensor métrico riemanniano (ou pseudo-riemanniano)  $g_{\mu\nu}$  nunca degenerado. Esta variedade  $M$  é combinada localmente com um grupo de simetria interna  $G$ , que será o gerador das transformações de gauge; com isto concluímos que  $M$  será intuitivamente o espaço-tempo.

Lembremos que um grupo de Lie  $G$  é uma variedade diferenciável dotada de uma estrutura de grupo, tal que a operação  $(a, g) \in G \times G \mapsto ag^{-1} \in G$  é diferenciável [74] [51]. Um grupo de Lie é *simples* se e somente se o único elemento que comuta com todos os outros for sua identidade. Um grupo semi-simples é a soma direta de grupos simples, isto é, dados dois grupos de Lie simples  $G$  e  $G'$ , o grupo  $S = G \oplus G'$  será semi-simples.

Tendo isto em mãos, contruímos o fibrado principal  $P(M, G)$  obedecendo às regras seguintes [18] [32] [51]:

1. Todo elemento  $\alpha$  do grupo de Lie  $G$  induz de uma maneira natural um mapa liso (por liso entendemos de classe  $C^k$ ,  $0 < k \leq +\infty$ )  $R_\alpha^*$  de  $P(M, G)$  sobre ele mesmo. Este mapa é definido como  $R_\alpha^* : (p, \alpha) \in P(M, G) \times G \rightarrow p\alpha \in P(M, G)$  dado por

$$p(\alpha\beta) = (p\alpha)\beta, \quad \forall \alpha, \beta \in G, p \in P(M, G)$$

2. O grupo  $G$  age livremente sobre  $P(M, G)$ . Isto significa que  $p\alpha = p$  para algum  $p \in P(M, G)$  implica  $\alpha = e$ , onde  $e$  representa o elemento identidade do grupo  $G$ .
3. A cada elemento  $p = (x, g) \in P(M, G)$ , com  $x \in M$  e  $g \in G$  definimos uma projeção canônica  $\pi : P(M, G) \rightarrow M$  dada por  $\pi(p) = \pi(x, g) = x \in M$ . Com isto  $M = P(M, G)/R_\alpha^*$ .

4. O fibrado  $P(M, G)$  é localmente trivial, ou seja, para todo  $x \in M$  existe um aberto  $U$  tal que  $x \in U$  e tal que  $\pi^{-1}(U)$  é isomorfo a  $U \times G$ , ou seja, existe um difeomorfismo que leva os elementos  $p \in \pi^{-1}(U)$  em  $(\pi(p), \phi(p)) \in U \times G$  tal que  $\phi(pa) = \phi(p)a, \forall a \in G$ .  $U$  é chamado domínio trivializante de  $P(M, G)$ .

Teçamos alguns comentários sobre os itens anteriores:

- Dado um ponto  $x$  qualquer na variedade base  $M$ , a este ponto associamos um conjunto  $\pi^{-1}(x)$  definido consistentemente por  $\pi(\pi^{-1}(x)) = x$ . Por outro lado, se lembrarmos que  $\pi$  projeta um elemento do espaço interno do ponto  $x$  no mesmo  $x$ , então  $\pi^{-1}(x)$  pode ser visto como este mesmo espaço interno em  $x$ .  $\pi^{-1}(x)$  é chamada fibra sobre  $x$  e é isomorfa ao grupo  $G$ , sendo ela mesma uma variedade lisa (devido ao isomorfismo com  $G$ ).
- Transformações de gauge locais (ou de segunda espécie) podem ser vistas neste formalismo como ações de elementos de  $G$  sobre ele mesmo no fibrado, que vimos ser representada pelo mapeamento induzido  $R_\alpha^*$ .
- No item 2 estabelecemos ser o grupo de Lie livre. Isto significa não impormos nenhuma origem para as coordenadas em  $G$ , de acordo com o princípio de invariância de gauge.
- Em 3 um ponto no espaço-tempo determina unicamente um ponto no espaço fibrado *módulo transformações de gauge*.

Retornemos ao espaço fibrado  $P(M, G)$  como dado pelos itens anteriores. Partindo-se de  $P(M, G)$  podemos construir os chamados *fibrados associados* [51] [74]. Para tal, seja  $F$  uma variedade sobre a qual o grupo de Lie age pela esquerda. Definimos a ação do grupo  $G$  pela direita sobre  $P(M, G) \times F$  como  $R_\alpha^*(p, q) = (p\alpha, \alpha^{-1}q)$ ,  $\alpha \in G$  e  $(p, q) \in P(M, G) \times F$ . O espaço quociente  $E(P(M, G), F) = P(M, G) \times F / R_\alpha^*$  é chamado *fibrado  $F$  associado* ao espaço fibrado  $P(M, G)$ . Pode-se verificar que  $E(P(M, G), F)$  é uma variedade diferencial e que existe uma projeção canônica  $\pi_E(x)$  induzida por  $\pi : P(M, G) \leftrightarrow M$ ; o próprio espaço fibrado  $P(M, G)$  pode ser visto como um fibrado associado a ele mesmo, com a fibra  $F = G$ .

Uma seção de corte deste fibrado é um mapeamento liso  $\sigma : M \rightarrow E(P(M, G), F)$  que atribui a cada valor de  $x \in M$  um elemento do fibrado  $E(P(M, G), F)$  tal que  $\pi(\sigma(x)) = x$ . Definir uma seção num fibrado equivale a atribuir a cada ponto da variedade base um valor específico para a fibra neste ponto, ou seja, determinar um “campo” sobre  $M$  (no sentido que dissemos no início desta seção).

Como sabemos,  $\{\partial_\mu\}$ ,  $\mu = 1 \dots n$  forma uma base sobre  $M$ . Como as derivadas parciais obedecem às relações de comutação

$$[\partial_\mu, \partial_\nu] = 0$$

$\{\partial_\mu\}$  é uma base coordenada, pelo teorema de Frobenius.

Definamos a álgebra de Lie subjacente ao grupo de Lie  $G$  como a álgebra  $\mathcal{G}$  identificada com o espaço tangente de  $G$  no ponto  $e$  ( $e$  é o elemento identidade do grupo de Lie  $G$ )  $\mathcal{G} = T_e G$ . Se a dimensão do grupo de Lie  $G$  é  $m$  temos  $\dim \mathcal{G} = m$ . Escolhamos um conjunto de elementos  $\{\tau_a\}$ ,  $a = 1 \dots m$  que forma uma base para  $T_e G = \mathcal{G}$ .  $\{\tau_a\}$  é composto dos campos vetoriais invariantes por multiplicações pela esquerda de elementos de  $G$  dados por

$$R_\alpha \tau_a = \tau_a \quad \forall \alpha \in G$$

onde  $R_\alpha \tau_a$  é o mapa induzido pelo mapa de  $G$  sobre ele mesmo dado por  $R_\alpha : G \rightarrow G$  com  $R_\alpha \beta = \alpha \beta$ .  $\{\tau_a\}$  não forma uma base coordenada, e obedece as seguintes relações de comutação

$$[\tau_a, \tau_b] = C_{ab}^i \tau_i$$

onde  $C_{ab}^i$  são as constantes de estrutura do grupo de Lie  $G$ .

A ação de  $G$  sobre  $P(M, G)$  pela esquerda gera de uma maneira natural, para cada elemento  $\alpha \in \mathcal{G}$ , um campo vetorial  $\alpha^*$  dado pela ação do subgrupo uniparamétrico  $\phi_\alpha = e^{t\alpha}$ ,  $t \in \mathbb{R}$  sobre o fibrado.

O fibrado  $P(M, G)$  é, localmente, o produto cartesiano de  $U \times G$ , sendo  $U \subset M$ , e portanto também uma variedade diferencial. Definiremos agora sobre o fibrado tangente associado à  $P(M, G)$  um objeto fundamental para a teoria de campos de gauge, a *conexão*. Seja  $T_p P(M, G)$  o fibrado tangente associado de  $P(M, G)$  no ponto  $p \in P(M, G)$ .  $TP(M, G) = E(P(M, G), T)$ , onde  $T$ , a fibra, é o espaço tangente à  $P(M, G)$ . Definir uma conexão  $\Gamma$  para nosso fibrado significa apresentar uma decomposição lisa de  $T_p P(M, G)$  num

espaço vertical  $\mathcal{V}$  e num espaço horizontal  $\mathcal{H}$  tal que  $T_pP(M, G) = \mathcal{V}_p \oplus \mathcal{H}_p$ . Esta decomposição obedece:

1. O espaço tangente  $T_pP(M, G)$  se decompõe na soma direta (ou soma de Whitney) de um subespaço vertical  $\mathcal{V}_p$  e de um subespaço horizontal  $\mathcal{H}_p$  em todos os pontos  $p \in P(M, G)$ .
2.  $\mathcal{V}_p$  pertence somente ao espaço tangente da fibra  $G$  no ponto  $p$ .
3.  $\mathcal{H}_{p\alpha} = R_\alpha^* \mathcal{H}_p$ , para todo  $\alpha \in G$  e todo  $p \in P(M, G)$ .
4.  $\mathcal{H}_p$  varia de maneira contínua sobre  $p \in P(M, G)$ .

Definida a conexão  $\Gamma$ , podemos decompor todo vetor  $X \in T_pP(M, G)$  como a soma direta de dois vetores  $vX$  e  $hX$  tal que  $X = vX + hX$  com  $vX \in \mathcal{V}_p$  e  $hX \in \mathcal{H}_p$ .  $vX$  e  $hX$  são chamadas componentes *vertical* e *horizontal*, respectivamente.

A *forma conexão*  $\gamma$  pode agora ser definida tal como segue [41] [51] [63] [74]: seja  $T_p^*P(M, G)$  o dual do espaço tangente  $T_pP(M, G)$  no ponto  $p \in P(M, G)$ .  $T_p^*P(M, G)$  é o espaço de todas as 1-formas definidas sobre  $T_pP(M, G)$ . Note que estas formas, assim definidas, são valoradas sobre a álgebra de Lie  $\mathcal{G}$ . Construímos um subespaço  $\mathcal{V}_p^*$  de  $T_p^*P(M, G)$ , o subespaço de todas as formas que aniquilam os vetores horizontais, isto é,  $\gamma_p \in \mathcal{V}_p^*$  implica que  $\gamma(X) = 0$  para todo  $X \in \mathcal{H}_p$ . Seja agora o campo vetorial  $\alpha^*$  induzido pelo elemento  $\alpha$  da álgebra de Lie  $\mathcal{G}$ , como definido anteriormente. Conforme [51], definimos a forma conexão  $\gamma \in \mathcal{V}_p^*$  como sendo o único elemento  $\alpha \in \mathcal{G}$  tal que  $(\alpha^*)_p$  é igual à componente vertical de  $X$ , para todo  $X \in T_pP(M, G)$ . Uma das consequências desta definição é que [51]  $R_\alpha^* \gamma = \text{Ad}(\alpha^{-1})\gamma = \alpha\gamma\alpha^{-1}$  ( $\text{Ad}$  denota a representação adjunta de  $G$  em  $\mathcal{G}$ ).

Das definições anteriores é evidente que a dimensão de  $\mathcal{V}$  é igual à  $\dim \mathcal{G}$ , pois  $\mathcal{V}$  pertence somente ao espaço tangente da fibra, e  $\mathcal{G}$  é justamente  $T_eG$ . Como  $\dim TP(M, G) = \dim TU + \dim TG$ , com  $U$  sendo um domínio trivializante de  $P(M, G)$  (pois localmente o fibrado pode ser visto como o produto cartesiano de  $U \times G$ ), então  $\dim \mathcal{H} = \dim M$  (considerando  $TP(M, G) = \mathcal{V} \oplus \mathcal{H}$ ). Tendo isto em vista, podemos definir uma base local para  $TP(M, G)$  como  $\{(D_\mu, \partial/\partial z^a)\}$ , onde  $z\partial/\partial z = \tau$ , sendo  $z^a$  um



sistema de coordenadas para  $\mathcal{G}$ .  $\{D_\mu\}$  é, deste modo, uma base (nem sempre coordenada) para o espaço horizontal  $\mathcal{H}$ .

Uma vez que a forma conexão é Lie-valorada, podemos representá-la como  $\gamma = \gamma^a \tau_a = \gamma^a \partial / \partial z^a$  e obter as seguintes relações:

$$\begin{aligned} \gamma^a(hX) &= \gamma^a(x_h^\mu D_\mu) = \\ &= x_h^\mu \gamma^a(D_\mu) = 0 \end{aligned}$$

onde  $x_h^\mu$  é a componente horizontal de  $X$  na base  $\{D_\mu\}$ . Com isto temos

$$\gamma^a(D_\mu) = 0 \quad (3.2)$$

De maneira análoga obtemos

$$\gamma^a\left(\frac{\partial}{\partial z^b}\right) = \delta_{ab} \quad (3.3)$$

A única 1-forma que é uma solução não-trivial para as equações (3.2) e (3.3) é [41]

$$\omega^a = dz^a + \Gamma_{\mu b}^a dx^\mu z^b \quad (3.4)$$

Os  $\Gamma_{\mu b}^a$  são conhecidos como *símbolos de Christoffel generalizados* (herança da Relatividade Geral). Constroi-se, a partir da dada conexão, a base  $\{D_\mu\}$  em termos das coordenadas  $z^a$  e  $x^\mu$ , usando-se a eq. (3.4), obtendo

$$D_\mu = \frac{\partial}{\partial x^\mu} - \Gamma_{\mu b}^a z^b \frac{\partial}{\partial z^a} \quad (3.5)$$

A derivada covariante  $D_\mu$  pode ser vista como uma projeção da derivada exterior  $\partial_\mu = \partial / \partial x^\mu$  sobre o espaço horizontal  $\mathcal{H}$ .

Mostra-se que, para um fibrado principal, é possível escrevermos a forma conexão Lie-valorada como [51] [41] [63] [74]

$$\gamma = g^{-1}dg + g^{-1}Ag \quad (3.6)$$

onde  $A = A_\mu^a(x)\tau^a dx^\mu$ , com  $\tau^a \in \mathcal{G}$  satisfazendo as relações de comutação

$$[\tau^a, \tau^b] = C_{ab}^c \tau^c$$

onde os  $C_{bc}^a$  são as constantes de estrutura do grupo de Lie  $G$ .

Mantendo a forma conexão em (3.6) invariante segundo transformações que agem somente na fibra, ou seja, fazendo uma transformação  $R_\alpha^*$  no espaço fibrado, com  $(x, g) \in P(M, G) \mapsto (x, g') = (x, \alpha g) \in P(M, G)$ , tal que

$$g^{-1}dg + g^{-1}Ag = (g')^{-1}dg' + (g')^{-1}A'g' \quad (3.7)$$

A eq. (3.7) é satisfeita se

$$A' = \alpha d\alpha^{-1} + \alpha A \alpha^{-1} \quad (3.8)$$

Esta eq. (3.8) é conhecida como *Lei de Transformação de Gauge* e a conexão associada  $A_\mu^a(x)$  é chamada *potencial de gauge*.

Identificando  $(\lambda^a/2i)z(\partial/\partial z)$  com  $\tau_a$ , encontramos o comutador de  $D_\mu$

$$[D_\mu, D_\nu] = F_{\mu\nu}^a \tau_a \quad (3.9)$$

$F_{\mu\nu}^a$  é chamado *tensor curvatura* e é dado por

$$F_{\mu\nu}^a = \partial_\mu A_\nu^a - \partial_\nu A_\mu^a + C_{bc}^a A_\mu^b A_\nu^c$$

Em teoria de gauge,  $F_{\mu\nu}^a$  é chamado *Campo de Gauge*. Observemos que  $F$  se transforma como um tensor de 2ª ordem.

Aqui é importante e essencial para este trabalho ressaltarmos que tudo o que foi exposto nesta seção, e nas que se seguem, pode ser formalizado, via predicados de Suppes, dentro da teoria dos conjuntos de Zermelo-Fraenkel<sup>1</sup> [21].

Agora que já descrevemos, sucintamente, a geometria dos campos de gauge, vejamos alguns resultados. Aconselhamos, a quem não está familiarizado com o que descrevemos nesta seção, a leitura de uma das inúmeras referências sobre o assunto, como por exemplo [1] [18] [27] [33] [40] [41] [52] [63] [65].

---

<sup>1</sup>A menos que digamos explicitamente o contrário, quando nos referirmos a uma formalização de uma dada teoria, por simplicidade entenderemos como uma formalização dentro de ZFC; todavia alguns resultados posteriores não são necessariamente vinculados a uma dada forma de axiomatização da teoria [21]

### 3.3 Uma Degenerescência nas Identidades de Bianchi

Introduzimos aqui os já conhecidos, em geometria diferencial, operadores  $i_X$  (representando o produto interno com respeito a um campo de vetores  $X$ ) e  $\mathcal{L}_X$  (a derivada de Lie com respeito ao campo vetorial  $X$ ), com  $\mathcal{L}_X$  definida por

$$\mathcal{L}_X(\eta)_p = \lim_{t \rightarrow 0} \left( \frac{1}{t} \right) (\phi_t^*(\eta)_p - \eta_p)$$

onde  $\phi_t$  é um arraste de Lie, representado pelo grupo uniparamétrico gerado pelo campo vetorial  $X$ , e onde  $Y_p = Y|_p$  denota a restrição de  $Y$  a  $p$ . Em geral

$$\phi_t = e^{tX}$$

$t \in \mathbb{R}$ . O arraste  $\phi_t$  é um automorfismo sobre a variedade  $M$ .

Seja  $V$  um espaço vetorial real de dimensão finita; seja  $V^*$  seu dual, o espaço de todas as formas lineares sobre os reais em  $V$ . Seja  $\Lambda(V^*)$  a álgebra exterior de  $V$ . A partir da suposição de existência de um produto interno, podemos definir um mapeamento

$$\langle \dots | \dots \rangle : V \times V^* \rightarrow \mathbb{R}$$

linear em ambos os fatores, onde  $\mathbb{R}$  representa o conjunto dos reais. Para um dado subespaço linear  $U \subseteq V$  definimos  $U^0 \subseteq V^*$  como sendo o subespaço linear de todas as formas de  $\Lambda(V^*)$  que aniquilam  $U$ :

$$\langle U | U^0 \rangle = 0$$

Um *ideal*  $\mathcal{I} \subseteq \Lambda(V^*)$  é um subespaço linear tal que dado um  $\beta \in \Lambda(V^*)$  e um  $\alpha \in \mathcal{I}$  temos que  $\beta \wedge \alpha \in \mathcal{I}$ . Um ideal é um conjunto que incorpora novos objetos pela esquerda via produto exterior. Notemos que  $\alpha \wedge \beta = (-1)^{\deg \beta \deg \alpha} \beta \wedge \alpha$  e com isto o ideal incorpora também objetos pela direita via produto exterior. Um conjunto  $\Gamma \subset \mathcal{I}$  é um *gerador* para o ideal  $\mathcal{I}$  se para todo o elemento  $\beta$  de  $\mathcal{I}$  podemos escrever  $\beta$  como  $\beta = \alpha \wedge \gamma$ , onde  $\alpha \in \Lambda(V^*)$  e  $\gamma \in \Gamma$ . Um ideal  $\mathcal{I}$  é chamado *homogêneo* se seu geradore  $\Gamma$  tem como elementos somente  $r$ -formas, isto é, se existe um  $r$  tal que  $\Gamma \subseteq \Lambda^r(V^*)$ . De acordo com esta definição,  $\mathcal{I} = \sum_r \mathcal{I} \cap \Lambda^r(V^*)$  se e somente se  $\mathcal{I}$  é homogêneo.

**Proposição 3.1** *Seja  $\mathcal{I} \subseteq \Lambda(v^*)$  um ideal homogêneo e seja  $U \subset V$  um subespaço vetorial de  $V$ . Então  $\mathcal{I}$  tem geradores em  $\Lambda(U^0)$  se e somente se*

$$i_X \alpha \in \mathcal{I}, \forall \alpha \in \mathcal{I},$$

para todo o  $x \in U$ .

*Demonstração:* Se os geradores  $\{\alpha_a\}$  de  $\mathcal{I}$  pertencem a  $\Lambda(U^0)$ , então

$$i_X \alpha_a = 0, \forall X \in U.$$

Então

$$i_X(z \wedge \alpha_a) = (i_X z) \wedge \alpha_a \in \mathcal{I},$$

para uma forma arbitrária  $z$ .

Para a demonstração da recíproca, veja Sternberg [74], pag. 28.  $\square$

De agora em diante, seja  $M$  uma variedade  $n$ -dimensional real de classe  $C^k$ ,  $k > n$ ; seja  $TM$  e  $T^*M$  os fibrados tangente e cotangente, respectivamente, e seja ainda  $\Lambda(M)$  o fibrado exterior sobre  $M$ . As definições anteriores dadas nesta seção se estendem naturalmente para  $M$  e suas fibras. Dado um ideal homogêneo  $\mathcal{I} \subseteq \Lambda(M)$ , criamos

$$D^{\mathcal{I}} = \{X \in TM : i_X \alpha \in \mathcal{I}, \forall \alpha \in \mathcal{I}\} \quad (3.10)$$

Para nossos propósitos, dizemos que  $\mathcal{I}$  é *não-singular* se e somente se a dimensão de  $D^{\mathcal{I}}$  é constante num aberto regular  $A \subseteq M$  ( $A$  é um aberto regular se e somente se  $A = (\overline{A})^\circ$ , onde  $\overline{A}$  e  $A^\circ$  são o fecho e o interior de  $A$ , respectivamente).

Neste trabalho nossos resultados serão obtidos a partir das consequências de duas versões do Teorema de Frobenius. Seja  $D \subseteq TM$  um subfibrado  $p$ -dimensional,  $p \leq n$ . Dizemos que  $D$  é integrável se  $D = TN$ , o fibrado tangente de  $N$ , onde  $N \subseteq M$  é uma subvariedade imersa em  $M$ . Então:

**Proposição 3.2 (Teorema de Frobenius, primeira versão)**  *$D \subseteq TM$  é integrável se e somente se  $D$  é uma álgebra de Lie, isto é, se e somente se  $X, Y \in D$  implica  $[X, Y] \in D$ .*

*Demonstração:* Veja Sternberg [74].  $\square$

Formemos  $D^0 \subseteq T^*M$ , o conjunto de todas as formas diferenciais que se anulam em  $D$ , e peguemos o ideal  $\mathcal{I}(D^0)$  gerado por  $D^0$  em  $\Lambda(M)$ . Como o ideal incorpora objetos da álgebra exterior,  $D^0$  sempre gera um ideal. Se  $d$  é a derivada exterior em  $\Lambda(M)$ , dizemos que o ideal  $\mathcal{I}(D^0)$  é um ideal diferencial se e somente se  $d\mathcal{I}(D^0) \subseteq \mathcal{I}(D^0)$ . Então,

**Proposição 3.3 (Teorema de Frobenius, segunda versão)**  *$D$  é integrável se e somente se  $\mathcal{I}(D^0)$  é um ideal diferencial.*

*Demonstração:* Veja [74]  $\square$

Numa carta local, se as  $r = n - p$  formas linearmente independentes  $\omega^i \in D^0$  são os geradores do ideal, as condições diferenciais sobre o ideal são equivalentes á existência de 1-formas  $\theta_j^i$  tal que

$$d\omega^i = \theta_j^i \wedge \omega^j, \quad i, j = 1, \dots, r \quad (3.11)$$

**Corolário 3.4**  *$D$  é integrável sobre uma carta local  $U \subseteq M$  se e somente se existem funções  $u_j^i$  e  $\beta^j$ , com  $u = (u_j^i)$  inversível sobre  $U$ , tal que*

$$\omega^i = u_j^i d\beta^j \quad (3.12)$$

*Demonstração:* Veja Flanders [43]  $\square$

Notemos que a equação (3.11) é um tipo de condição diferencial covariante que se anula. Agora apresentaremos e provaremos um resultado de Cartan que estende o teorema de Frobenius a uma situação mais geral [74].

**Teorema 3.5 (de Cartan)** *Seja  $\mathcal{I} \subseteq \Lambda(M)$  não-singular, homogêneo e diferencial. Então  $D^{\mathcal{I}}$  é integrável.*

*Demonstração:* Antes precisamos de um lema:

**Lema 3.6** *Se  $\alpha \in \Lambda(M)$ ,*

$$i_{[X,Y]}\alpha = d([i_X, i_Y]\alpha) + i_X di_Y \alpha - i_Y di_X \alpha. \quad (3.13)$$

*Demonstração:* Temos

$$i_{[X,Y]}\alpha = i_{\mathcal{L}_X Y}\alpha = \mathcal{L}_X i_Y \alpha - i_Y \mathcal{L}_X \alpha$$

e também

$$\mathcal{L}_X \alpha = di_X \alpha + i_X d\alpha.$$

Então

$$i_{[X,Y]}\alpha = d([i_X, i_Y]\alpha) + i_X di_Y \alpha - i_Y di_X \alpha.$$

□.

Voltando à prova do teorema, notemos que  $D^{\mathcal{I}}$  é um espaço linear (como consequência da linearidade de  $i_X$ ). Sejam agora  $X_1, \dots, X_p$  geradores de  $D^{\mathcal{I}}$ . Então, da definição de  $D^{\mathcal{I}}$ ,  $i_{X_k} \mathcal{I} \subset \mathcal{I}$ ,  $k = 1, \dots, p$ . Para  $\alpha \in \mathcal{I}$ ,

$$i_{[X_i, X_j]}\alpha = d([i_{X_i}, i_{X_j}]\alpha) + i_{X_i} di_{X_j} \alpha - i_{X_j} di_{X_i} \alpha.$$

Claramente o produto de Lie  $[X_i, X_j] \in D^{\mathcal{I}}$ , posto que cada termo em separado na soma acima pertence a  $D^{\mathcal{I}}$ . Tendo isto mais as proposições anteriores fica completa a prova. □

Seja agora  $G \subseteq \Lambda^r(M)$ ,  $r$  fixo, um conjunto de geradores para  $\mathcal{I}(G)$  e sejam as  $r$ -formas  $\omega_i$ ,  $i = 1, \dots, p$  gerando  $G$ . Então,

**Lema 3.7** *O ideal não-singular homogêneo  $\mathcal{I}(G)$  é diferencial se e somente se existem 1-formas diferenciáveis  $\theta_j^i$  tais que*

$$d\omega^i = \theta_j^i \wedge \omega^j. \quad (3.14)$$

*Demonstração:* Suficiência: Para  $\alpha \in \Lambda(M)$ , escrevamos  $\xi = \alpha \wedge \omega^i$ . Então

$$d\xi = d\alpha \wedge \omega^i + (-1)^{\deg \alpha} \alpha \wedge d\omega^i.$$

Como temos, por hipótese,

$$d\omega = \theta \wedge \omega,$$

obtemos

$$d\xi = d\alpha \wedge \omega^i + (-1)^{\deg \alpha} \alpha \wedge \theta_j^i \wedge \omega^j \in \mathcal{I}.$$

Para mostrarmos a necessidade, como  $d\mathcal{I} \subset \mathcal{I}$ , dado  $\xi = \alpha \wedge \omega^i$ ,  $d\xi = d\alpha \wedge \omega^i + (-1)^{\deg \alpha} \alpha \wedge d\omega^i$ . Como  $d\xi \in \mathcal{I}$ , necessariamente  $\alpha \wedge d\omega^i \in \mathcal{I}$ . Aqui temos duas alternativas: ou  $\alpha \in \mathcal{I}$  ou  $\alpha \notin \mathcal{I}$ . Se  $\alpha \in \mathcal{I}$ ,  $d\xi \in \mathcal{I}$  trivialmente. Se não  $d\omega^i \in \mathcal{I}$ . Então  $d\omega^i$  tem que ser uma combinação linear dos produtos de 1-formas com os geradores do ideal, isto é,

$$d\omega^i = \theta_j^i \wedge \omega^j.$$

□

### 3.4 Soluções Não-Curvatura para as Identidades Diferenciais de Bianchi

Apresentamos o seguinte quadro geométrico para nosso problema: seja  $M$  uma variedade diferenciável real de dimensão  $n$ , com uma estrutura diferenciável de classe  $C^k$ ,  $k > n$ .  $M$  será nossa variedade base. Seja  $G$  um grupo de Lie semi-simples de dimensão finita. Formamos o fibrado principal  $P(M, G)$ , com  $G$  sendo a fibra e o grupo que age sobre os elementos da fibra ao mesmo tempo (conforme seção 3.2). Iremos supor também, além de  $P(M, G)$ , vários fibrados associados sobre  $M$ . Dotamos  $P(M, G)$  com uma conexão; isto significa que definimos uma decomposição  $C^k$  do fibrado tangente de  $P(M, G)$ ,  $TP$ , dividindo-o num espaço horizontal  $\mathcal{H}$  e num espaço vertical  $\mathcal{V}$ , tal que  $TP = \mathcal{V} \oplus \mathcal{H}$ . A forma conexão  $\gamma$  é definida de tal maneira que aniquile o espaço horizontal,  $\gamma(\mathcal{H}) = 0$ .

Consideraremos formas tensoriais sobre  $P(M, G)$  (i.e., formas que não têm componentes em  $\mathcal{V}$ ). No nosso caso uma forma tensorial  $L(G)$ -valorada sobre  $M$ , onde  $L(G)$  é a álgebra de Lie correspondente ao grupo  $G$ , é uma  $r$ -forma  $\alpha$  sobre  $P(M, G)$ ,  $r \leq n$ , com valores em  $L(G)$ , e tal que dados *quaisquer* campos vetoriais  $X, Y, Z, \dots$  sobre o fibrado,

$$\alpha(X, Y, Z, \dots) = \alpha(hX, hY, hZ, \dots), \quad (3.15)$$

onde  $hX$  denota a componente de  $X$  com relação ao espaço horizontal  $\mathcal{H}$ .

Temos o seguinte: uma *condição diferencial de Bianchi* sobre uma  $r$ -forma  $\alpha$  é dada por

$$d\alpha(hX, hY, \dots) = 0, \quad (3.16)$$

onde  $d$  é a derivada exterior sobre  $P(M, G)$ . Note que esta definição está perfeitamente de acordo com o que anteriormente chamamos identidade de Bianchi, pois a derivada covariante exterior é definida como a projeção da derivada exterior no espaço horizontal, uma vez definida a conexão. O que procuramos são soluções não curvas para (3.16). Dada uma base  $\tau_a$  para a álgebra de Lie  $L(G)$ , qualquer forma  $L(G)$ -valorada pode ser escrita como  $\alpha(X, \dots) = \alpha^a(X, \dots)\tau_a$ , e a condição (3.16) se torna

$$d\alpha^a = -\gamma_b^a \wedge \alpha^b. \quad (3.17)$$

Nossa principal questão pode agora ser formulada como se segue:

1. Existem formas conexões  $\gamma$  tal que podemos encontrar pelo menos uma forma tensorial  $\alpha$  que não pode ser obtida das formas curvatura de  $\gamma$  sobre  $P(M, G)$  e que, contudo, ainda satisfazem as condições diferenciais tipo Bianchi para  $\gamma$ , como a expressa em (3.17) ?
2. Se existem tais forma, quais propriedades caracterizam estes  $\gamma$ 's e  $\alpha$ 's ?

Como

$$\Omega(X, Y) = d\gamma(X, Y) + \frac{1}{2}[\gamma(X), \gamma(Y)], \quad (3.18)$$

temos que  $\Omega$  satisfaz trivialmente a identidade de Bianchi

$$D\Omega = 0.$$

Assim, se  $\alpha$  for obtido de combinações lineares de  $\Omega$ , então  $\alpha$  deve obedecer à (3.17). Por exemplo: coloquemos

$$\alpha = \Omega \wedge \Omega.$$

Temos

$$D\alpha = D\Omega \wedge \Omega + (-1)^{\deg \Omega} \Omega \wedge D\Omega,$$

e ainda  $\alpha \neq \Omega$ . Este exemplo nos impele a definir um conjunto cujos objetos, por construção derivados de  $\Omega$ , obedecem a (3.17).

Seja  $\mathcal{M}$  o espaço de todas as forma curvaturas sobre  $P(M, G)$  e  $\alpha(---)$  um funcional linear definido sobre  $\mathcal{M}$  com valores no espaço das formas tensoriais  $L(G)$ -valoradas sobre o espaço fibrado. O operador derivada exterior covariante com respeito à forma conexão  $\gamma$  é denotado  $D(\gamma)$ .



**Definição 3.8** Dizemos que  $\alpha(\Omega)$  é curvatura-relacionado se e somente se  $\Omega \in \mathcal{M}$  implica identicamente que  $D(\gamma)\alpha(\Omega) \equiv 0$ .

Seja  $\Omega(\gamma)$  uma forma curvatura sobre  $P(M, G)$ , derivada da forma conexão  $\gamma$ , e seja  $B(\Omega)$  a álgebra linear sobre  $\mathbb{R}$  gerado por  $\Omega$  e suas contrações, produtos, produtos de Lie e equivalentes. Seja  $K(\Omega) \subset B(\Omega)$  a restrição de  $B$  à álgebra linear das formas tensoriais  $\mathcal{G}$ -valoradas sobre  $P(M, G)$ . Então, um elemento arbitrário  $\alpha$  de  $K$  é dado por algum funcional linear  $\alpha(\Omega)$ . Fazemos  $K^0 = \{\alpha \in K : D(\gamma)\alpha = 0\}$ . Seja  $\gamma'$  uma outra forma conexão sobre  $P(M, G)$ , e seja  $\Omega'$  a forma curvatura correspondente. Em geral, mesmo se  $D(\gamma)\alpha(\Omega)$ , podemos ter  $D(\gamma')\alpha(\Omega')$ . Contudo, existirão alguns funcionais  $\alpha$  tal que a derivada exterior covariante  $D\alpha \equiv 0$ , para qualquer  $\gamma$  e  $\Omega$ . Escrevamos

$$A(\Omega) = \{\alpha \in K^0(\Omega) : D(\gamma')\alpha(\Omega') \equiv 0, \text{ qualquer } \gamma'\}.$$

Mostra-se que  $A(\Omega) = \{k\Omega : k \in \mathbb{R}\}$ .

**Definição 3.9** Um forma  $\mathcal{G}$ -valorada  $\alpha$  sobre  $P(M, G)$  é não-trivial se e somente se  $\alpha \neq 0$  e  $\alpha$  é não curvatura-relacionada.

Responderemos agora às duas questões anteriores simultaneamente.

**Definição 3.10** Uma conexão genérica é uma distribuição contínua que atribui a cada ponto  $y \in P(M, G)$  uma direção privilegiada tangente a  $P(M, G)$  de dimensão  $n = \dim M$  que é perpendicular à fibra passando por  $y$ .

**Definição 3.11** Uma  $G$ -conexão é uma família de direções horizontais em  $P(M, G)$  tal que todos os arraste de Lie  $\phi_t$  pertencem a  $G$ .

Suponhamos a existência de uma  $r$ -forma tensorial  $\alpha$  sobre o fibrado  $P(M, G)$  dotado de uma forma conexão  $\gamma$  tal que

$$h(d\alpha(X, Y, \dots)) = 0 \tag{3.19}$$

sobre um domínio aberto trivializante  $\pi^{-1}(U) = U \times G \subset P(M, G)$ ,  $U \subset M$ . Seja  $\mathcal{I}(\alpha)$  o ideal em  $\Lambda(P)$  gerado pelos  $\alpha^a$ . Suponhamos ainda que o grupo fibrado coincide com o grupo de holonomia da conexão de Ambrose-Singer, gerado pela forma curvatura  $\Omega$  associada a  $\gamma$  [51]. Notemos que  $\gamma$  assim definida não é uma  $G$ -conexão, necessariamente, sendo em geral genérica [40].

**Lema 3.12** *Se existem tais  $\alpha^a$ , então  $\mathcal{I}(\alpha)$  é um ideal diferencial não-singular homogêneo em  $\Lambda(P)$ .*

*Demonstração :* Imediata, como consequência da eq. (3.17) junto com o Lema 3.7.  $\square$

**Lema 3.13** *Se existem tais  $\alpha^a$ , então para  $\mathcal{I}(\alpha)$ ,  $\mathcal{V} \subseteq D^{\mathcal{I}}$ .*

*Demonstração:* Se  $\beta$  é uma forma qualquer sobre  $P(M, G)$ , dado um gerador  $\alpha^a$  para  $\mathcal{I}(\alpha)$ , se  $X$  é um vetor vertical sobre  $P(M, G)$ , isto é,  $hX = 0$ , temos

$$i_X(\beta \wedge \alpha^a) = i_X\beta \wedge \alpha^a + (-1)^{\deg\beta} \beta \wedge i_X\alpha^a.$$

Como, por definição  $\alpha^a(hX, hY, \dots)\tau_a = \alpha^a(X, Y, \dots)\tau_a$  temos

$$i_X(\beta \wedge \alpha^a) = i_X\beta \wedge \alpha^a$$

para  $hX = 0$ . Isto implica, junto com a construção de  $D^{\mathcal{I}}$ , que qualquer vetor vertical  $X$  pertence a  $D^{\mathcal{I}}$ , o que completa a demonstração.  $\square$

Observemos que o lema anterior pode naturalmente ser estendido para  $\alpha^a = 0$ , o que nos mostra que um  $D^{\mathcal{I}}$  construído da maneira dada anteriormente sempre conteria ao menos o espaço vertical  $\mathcal{V}$ .

Lembremos agora que a forma conexão  $\gamma$  divide o fibrado em dois espaços: o espaço horizontal  $\mathcal{H}$  e o vertical  $\mathcal{V}$ , tal que localmente  $TP = \mathcal{V} \oplus \mathcal{H}$ . Como  $\mathcal{V} \subseteq D^{\mathcal{I}}$ , é imediato que  $D^{\mathcal{I}} = \mathcal{V} \oplus \mathcal{K}$ , onde  $\mathcal{K} \subseteq \mathcal{H}$ ,  $\mathcal{K} = D^{\mathcal{I}} - \mathcal{V}$ .

**Definição 3.14**  *$\mathcal{I}(\alpha)$  é trivial se e somente se  $\mathcal{K} = 0$ .  $\mathcal{I}(\alpha)$  é não-trivial se e somente se  $\mathcal{K}$ .*

Podemos provar agora que existem  $\mathcal{I}(\alpha)$  não triviais, e relaciona-los com nossos objetivos:

**Proposição 3.15** *As seguintes condições são equivalentes:*

1.  $\mathcal{I}(\alpha)$  é não-trivial.

2.  $\mathcal{K}$  é horizontal, integrável e  $\gamma$  restrito à variedade integral de  $\mathcal{K}$  é plana.
3. Existe uma  $r$ -forma tensorial  $L(G)$ -valorados  $\alpha$  sobre  $P(M, G)$  que é não-trivial não relacionada à curvatura que satisfaz as identidades diferenciais de Bianchi com respeito a  $\gamma$ .

*Demonstração:* Que 3 implica 1 é imediato. Mostraremos que  $1 \rightarrow 2 \rightarrow 3$ .

(1  $\rightarrow$  2) Suponhamos que  $\mathcal{K}$  seja diferente de zero. Por definição,  $\mathcal{K}$  é horizontal. Se  $\mathcal{I}(\alpha)$  é um ideal diferencial, homogêneo e não-singular, então  $\mathcal{K}$  é integrável, como resultado do Teorema de Frobenius. Seja  $K$  sua subvariedade integral em  $P(M, G)$ . Então, a restrição de  $\gamma$  a  $K$ , denotada  $\gamma_K$ , é uma conexão parcial plana [50].

(2  $\rightarrow$  3) Suponhamos que, por hipótese,  $\gamma_K$  é plana. Suponhamos ainda que estejamos sobre um domínio aberto trivializante de  $P(M, G)$ . Podemos escrever, via Teorema de Frobenius, para uma dada base da Álgebra de Lie e para 1-formas  $\theta^a$  que determinam  $K$

$$d\theta^a = -\gamma_b^a \wedge \theta^b \quad (3.20)$$

Como  $\gamma_K$  é plana, existe uma transformação de gauge que leva  $\gamma_K$  em 0 e os  $\theta^a$  em  $\bar{\theta}^b = g_a^b \theta^a$  tal que temos  $d\bar{\theta}^b = 0$ . Chamamos este gauge de *gauge zero* para  $\gamma_K$ . Seja  $\Lambda(\bar{\theta})$  a álgebra exterior gerada pelos  $\bar{\theta}^b$ . Devido à linearidade da álgebra, no gauge zero se  $\eta \in \Lambda(\bar{\theta})$ , então  $d\eta = 0$ . Então, se  $\bar{\alpha}^a \in \Lambda(\bar{\theta})$  for um conjunto de  $r$ -formas,  $r < \dim(K)$ , homogêneas linearmente independentes, temos, no gauge zero,  $d\bar{\alpha} = 0$ .

Voltando ao gauge original da equação (3.20), temos:

$$d\alpha^a = -\gamma_b^a \wedge \alpha^b$$

O que completa a demonstração.  $\square$

Com isto respondemos positivamente à questão 1 apresentada anteriormente: existem soluções não-curvas de grau arbitrário para as Condições Diferenciais de Bianchi exatamente quando  $\mathcal{I}(\alpha)$  é não trivial, ou quando a conexão  $\gamma$  se divide em  $\gamma = \gamma^1 \oplus \gamma^0$ , onde  $\gamma^0$  é uma forma conexão parcial plana que determina um  $\mathcal{K}$  integrável, no sentido de Kamber e Toundeur [50].

Para respondermos à segunda questão, consideremos o seguinte: Se  $\alpha$  é uma 1-forma tensorial, o espaço gerado pelos  $\alpha^a$  aniquila  $\mathcal{V} \oplus \mathcal{H}$ . Contudo, a Proposição 3.15 nos permite afirmar que, num domínio trivializante  $U$  de  $P(M, G)$ , existe uma transformação de gauge que leva cada  $\alpha^a$  numa forma exata, isto é, existe, ao menos neste domínio, um mapeamento de gauge  $g : P(M, G)|U \longrightarrow P(M, G)|U$  tal que

$$d\beta = g^{-1}\alpha g, \beta \text{ uma função} \quad (3.21)$$

onde  $g = (g_b^a)$  na representação adjunta.

O mesmo se aplica a  $r$ -formas,  $r > 1$ , que satisfazem a eq. (3.16). Todas elas serão expressas como formas (localmente) exatas  $L(G)$ -valoradas no mesmo gauge, que é aquele no qual a parte plana da conexão vai para zero.

Isto pode ser enfatizado no

**Corolário 3.16** *Se  $\mathcal{I}(\alpha)$  é não-trivial, então existe um gauge onde, ao menos localmente, podemos escrever  $\alpha^a = d\beta^a$ , para todos os índices  $a$ .*

podendo ser complementado por

**Corolário 3.17** *Se  $\mathcal{I}(\alpha)$  é trivial, então  $\mathcal{I}(\alpha) = \mathcal{I}(\Omega)$ .*

Neste ponto, vejamos um resultado de indecibilidade.

### 3.5 Uma Questão Indecidível sobre a Geometria dos Campos de Gauge

Nas duas seções anteriores mostramos que, dadas algumas condições bem definidas sobre a forma conexão, existem  $r$ -formas Lie-valoradas não triviais sobre o fibrado que satisfazem as identidades de Bianchi com respeito à conexão  $\gamma$ . Uma questão que podemos nos colocar é: dada a forma conexão, podemos saber se ela obedece ou não estas condições? De outra maneira: dada uma propriedade sobre um determinado campo de gauge, podemos determinar se um dado campo específico a satisfaz? A resposta a estas perguntas é *não*, como mostraremos a seguir.

**Proposição 3.18** *Se ZFC é aritmeticamente consistente então:*

1. Dado um fibrado principal  $P(M, G)$ , existe uma forma conexão  $\gamma$  para a qual é verdadeiro, num dado modelo  $\mathbf{M}$  de ZFC (onde  $\mathbf{M}$  contém o modelo standard  $\mathbf{N}$ ), que o ideal associado  $\mathcal{I}(\alpha)$  é trivial, mas isto não pode ser demonstrado dos axiomas de ZFC.
2. Dado um fibrado principal  $P(M, G)$ , existe uma forma conexão  $\lambda$  para a qual é verdadeiro, num dado modelo  $\mathbf{M}$  de ZFC (onde  $\mathbf{M}$  contém o modelo standard  $\mathbf{N}$ ), que o ideal associado  $\mathcal{I}(\alpha)$  é não-trivial, mas isto não pode ser demonstrado dos axiomas de ZFC.
3. Existe uma família enumerável de formas conexão  $\gamma_m$ ,  $m \in \mathbf{N}$  ( $\mathbf{N}$  representando os naturais), tal que, para um  $m$  qualquer, não existe nenhum algoritmo que possa decidir se o ideal correspondente  $\mathcal{I}_m(\alpha)$  é trivial ou não.

*Demonstração:* O nosso resultado vem do Teorema de Richardson, apresentado na seção 2.3, em conjunto com os seguintes lemas:

**Lema 3.19** *Se ZFC é aritmeticamente consistente, então podemos explicitamente e algoritmicamente construir a expressão para uma função  $\theta_m(x) \in \mathcal{Q}$  tal que:*

1. Para todo o real  $x$ ,  $\theta_m(x) = 0$  se e somente se não existem reais  $y$  tal que  $B_m(y) > 0$
2. Para todo o real  $x$ ,  $\theta_m(x) = 1$  se e somente se existe um real  $y$  tal que  $B_m(x) > 0$

onde  $B_m(x)$  é o mesmo da seção 2.3

*Demonstração:* Veja Seção 2.3  $\square$

**Lema 3.20** *Se ZFC é aritmeticamente consistente, então não existe nenhum algoritmo geral que decide, para um  $m$  arbitrário e para um conjunto dado  $\zeta_m(x) \in \mathcal{B}^1$ , se*

$$\zeta_m(x) = \theta_m(x)$$

para todos os reais  $x$ .

*Demonstração:* Fazendo-se

$$\zeta_m = \theta_m + B_m$$

□

Voltando à proposição. Seja  $U \subset M$  um domínio trivializante do fibrado  $P(M, G)$  tal que  $U \times G$  seja uma trivialização local. Fixemos para esta trivialização um sistema de coordenadas local, e seja ainda  $\gamma^0$  neste sistema a forma conexão tal que o ideal  $\mathcal{I}(\alpha)$  é trivial e  $\lambda^0$  a forma conexão tal que  $\mathcal{I}(\alpha)$  é não trivial. Formemos localmente as formas

$$\gamma = (1 - B(x^1))\gamma^0 + B(x^1)\lambda^0$$

$$\lambda = B(x^1)\gamma^0 + (1 - B(x^1))\lambda^0$$

onde  $x^1$  é uma das componentes das coordenadas locais sobre  $M$ , e onde  $B(x)$  é a função definida na seção 2.3. Das equações acima, podemos ver que  $\gamma$  satisfaz o item 1 e  $\lambda$  o 2, uma vez que  $B(x) = 0$  mas que em ZFC não podemos demonstrar isto.

Definamos agora

$$\gamma_m = (1 - \theta_m)\gamma^0 + \theta_m\lambda^0$$

e o item 3 resulta como consequência do lema 3.20.

# Capítulo 4

## Indecibilidade na Relatividade Geral

### 4.1 Introdução

No capítulo precedente, obtivemos um resultado de indecibilidade face aos axiomas de ZFC na teoria dos campos clássicos de gauge. Percorrendo a idéia de que proposições indecidíveis estão por todo o lado, vejamos aqui um exemplo na Relatividade Geral.

Em trabalhos anteriores, mostramos que a existência de espaços-tempo genéricos estava ligada à compacticidade das variedades em questão: não existem variedades compactas genéricas, mas existem variedade não compactas genéricas [6] [25]. Dando sequência a estes trabalhos, discutiremos uma possível interpretação para variedades genéricas como objetos aleatórios.

Neste Capítulo, nosso principal interesse se assenta no comportamentos das 4-variedade diferenciáveis  $M$  que admitem uma estrutura espaço-temporal  $(M, g)$  ( $g$  é um tensor métrico de Riemann, nunca degenerado). Estas variedades serão soluções particulares das equações de Einstein com determinadas distribuições de matéria. Para tal, seja  $TM$  o fibrado tangente de  $M$ . A imposição de um tensor métrico é feita especificando-se um mergulho particular de  $P(M, O(3, 1)) \subset P(M, GL(4, \mathbb{R}))$  em  $P(M, GL(4, \mathbb{R}))$ , sendo  $O(3, 1)$  o grupo de Lorentz e  $GL(4, \mathbb{R})$  o grupo de

transformações lineares reais de dimensão 4.  $TM$  será um fibrado associado à  $P(M, O(3, 1))$  [41]. A formalização da Relatividade Geral na teoria de Zermelo-Fraenkel, com a utilização dos Predicados de Suppes pode ser encontrada em [6] [21] [25].

## 4.2 Genericidade, Aleatoriedade e uma Questão Indecidível

Suponhamos dada uma formalização para a Relatividade Geral numa teoria como, por exemplo, ZFC. Nesta teoria, podemos nos questionar sobre a propriedade do conjunto  $\mathcal{S}$  de todos os espaços-tempo, que existe como consequência do Axioma do Conjunto Potência e do Axioma da Especialização [56] [25].

É bem conhecido que existe um mergulho liso que leva uma variedade riemanniana qualquer de dimensão  $n$  em  $\mathbb{R}^{2n+1}$  [15] [55]. Como resultado, é sempre possível mergulhar um elemento qualquer de  $\mathcal{S}$  em  $\mathbb{R}^9$  (isto pode ser refinado para que o mergulho seja feito em  $\mathbb{R}^8$ , conforme [15], mas para nossos propósitos isto será irrelevante). Entretanto, apesar da existência deste mergulho, não nos surge nenhuma estrutura topológica induzida para  $\mathcal{S}$  que seja “espontânea”. Isto se reflete pela dificuldade que temos em imaginar quando uma sequência de espaços-tempo é contínua, isto é, “aproximar” um dado espaço-tempo por uma sequência contínua de espaços-tempo.

Apesar destas dificuldades, podemos dotar  $\mathcal{S}$  de diversas topologias diferentes que são bastante razoáveis. Descreveremos neste capítulo uma estrutura topológica simples para o conjunto das 4-variedades reais lisas e não-compactas. Esta estrutura servirá como topologia para  $\mathcal{S}$ , uma vez que excluiríamos do conjunto de espaços-tempo as variedades compactas. Variedades compactas podem ser excluídas de  $\mathcal{S}$ , uma vez que o conjunto de tais variedades tem cardinalidade  $\aleph_0$  e o conjunto das variedades não-compactas tem cardinalidade  $2^{\aleph_0}$  [25]. Com isto, a *probabilidade informal* de ser nosso universo compacto parece inclusive ser nula.

## 4.3 Uma Topologia para $\mathcal{S}$

Começaremos esta seção enunciando o seguinte:



**Proposição 4.1**  $ZFC \vdash$  “Se  $M$  é uma variedade real lisa de dimensão  $n$ , então  $M$  é triangulizável”.

*Demonstração:* Veja [14] [79].  $\square$

Como dissemos, o foco de nosso interesse são os espaços de dimensão 4 que podem ser espaços-tempo. Necessitamos nesse caso da Proposição:

**Proposição 4.2**  $ZFC \vdash$  “Se  $M$  é uma variedade topológica não-compacta real de dimensão 4, então  $M$  é alisável, isto é, pode ser dado um mapa liso que é compatível com a estrutura topológica da variedade.”

*Demonstração:* Veja [64].  $\square$

**Corolário 4.3** “ $ZFC \vdash$  Se  $M$  é um complexo simplicial com uma estrutura de variedade topológica 4-dimensional real, então  $M$  é alisável.”

*Demonstração:* Imediata, a partir da Proposição 4.2.  $\square$

Além deste resultados, necessitamos de algumas propriedades adicionais no que se refere aos atlas da nossa variedade. Seja  $A = \{(B_i, \varphi_i)\}$  um atlas para a variedade  $M$  onde os domínios das coordenadas locais são  $\{B_i : i \in \omega_0\}$ , com  $\bigcup_{i \in \omega_0} B_i = M$ . As propriedades exigidas para as cartas e seus domínios são:

- [i ] Os domínios  $B_i$  das coordenadas  $\varphi_i$ ,  $i \in \omega_0$ , pertencentes ao atlas da variedade  $n$ -dimensional  $M$  devem ser difeomorfos a uma bola aberta  $n$ -dimensional.
- [ii ] O atlas satisfaz a propriedade de interseção finita, ou seja, dado um domínio  $B_k$  da coordenada  $\varphi_k$  existirá no máximo um número *finito* de coordenadas  $\varphi_i$  tal que  $B_k \cap B_i \neq \emptyset$ ,  $k \neq i$ .
- [iii ]  $B_i \not\subseteq B_j$ , para todo  $i, j \in \omega_0$  tal que  $i \neq j$ .

onde entendemos por “bola aberta  $n$ -dimensional” um aberto que é difeomorfo a  $\mathbb{R}^n$  com sua estrutura diferenciável usual.

Estas condições impõem que qualquer variedade real  $n$ -dimensional lisa seja obtida a partir de duas sequências enumeráveis (ou até mesmo finitas) de mapas

$$\varphi_1 : B_1 \rightarrow \mathbb{R}^n, \dots, \varphi_i : B_i \rightarrow \mathbb{R}^n, \dots \quad (4.1)$$

$$\dots \varphi_{ij} : \varphi_j(B_i \cap B_j) \rightarrow \varphi_i(B_i \cap B_j) \dots \quad (4.2)$$

onde  $\varphi_{ij} = \varphi_i \circ \varphi_j^{-1}|_{\varphi_j(B_i \cap B_j)}$ , pois um atlas determina completamente a variedade em questão.

Abreviemos

$$B_i \cap B_j \cap \dots \cap B_k = B_{ij\dots k} \quad (4.3)$$

Com isto

**Definição 4.4** *Se  $M$  é uma variedade real lisa de dimensão  $n$ , então a cobertura  $\{B_i\}$  é chamada boa cobertura se e somente se todos os  $B_{ij\dots k}$  são difeomorfos a bolas abertas  $n$ -dimensionais*

e podemos formular a seguinte Proposição, com  $M$  dado como anteriormente:

**Proposição 4.5** *ZFC  $\vdash$  “ $M$  tem uma boa cobertura, homomorfa às estrelas abertas numa triangulação de  $M$ , que satisfaz as condições [i]–[iii]”.*

*Demonstração:* A demonstração encontra-se em [11]. Em [11] mostra-se também que, dada uma cobertura que satisfaz às condições [ii] e [iii], sempre podemos refiná-la para uma boa cobertura.  $\square$

Como dissemos, o conjunto de todas as variedades não-compactas tem a cardinalidade do contínuo. Isto significa que existe um mapa  $\iota$  que leva elementos de  $\mathcal{S}$  em  $(\omega_0)^{\omega_0}$ , o que equivale a dizer que podemos associar a cada elemento de  $\mathcal{S}$  uma sequência infinita de inteiros. Desejamos obter explicitamente um tal mapeamento. Com isto em mente, consideremos o conjunto  $\mathcal{C}$ , o conjunto de todos os conjuntos possíveis  $\{B_{ij\dots k}\}$ .

**Lema 4.6** *ZFC  $\vdash$  “Existe um mapeamento biunívoco e sobrejetor  $\lambda : \mathcal{C} \rightarrow \omega_0$  que é computável.”*

*Demonstração:* Formemos uma enumeração efetiva para os elementos de  $\mathcal{C}$ , da maneira seguinte:

- Para qualquer  $B_{ij\dots k} \in \mathcal{C}$  temos  $i < j < \dots < k$ .
- $B_{ij\dots k}$  é ordenado pelas regras:
  1. Primeiro ordenamos pela ordem crescente da soma  $s$  dos índices,  $s = i + j + \dots + k$ ;
  2. Dado um valor  $s_0$  para a soma, ordenamos “alfabeticamente” a coleção *finita* de conjuntos  $B_{ij\dots k}$  tais que  $i + j + \dots + k = s_0$ .

Esta ordenação nos resulta em algo como:

$$\mathcal{C} = \{B_{01}, B_{02}, B_{03}, B_{12}, B_{04}, B_{13}, B_{013}, \dots\}$$

que é o desejado.  $\square$

Seja  $\text{Fin}(\mathcal{C})$  o conjunto de todos os subconjuntos *finitos* de  $\mathcal{C}$ .

**Corolário 4.7**  $ZFC \vdash$  “ $\lambda$  induz um mapa  $\lambda^* : \text{Fin}(\mathcal{C}) \rightarrow \omega_0$  que é biunívoco e computável.”

*Demonstração:* Imediata, como escólio da demonstração anterior.  $\square$

Indicaremos  $(\omega_0)_{\mathcal{C}}$  a codificação de todos os subconjuntos finitos de  $\mathcal{C}$  sobre os naturais, como dada. Para um  $\mathcal{C}_i \subset \mathcal{C}$ , uma codificação efetiva (ie., computável) também pode ser encontrada, como consequência da original, e será denotada  $(\omega_0)_{\mathcal{C}_i}$ .

Construamos uma mapa biunívoco e sobrejetor de  $\mathcal{S}$  sobre  $(\omega_0)^{\omega_0}$  seguindo as seguintes etapas, feitas de uma maneira recursiva:

1. Seja  $\mathcal{B} = \{B_i : i \in \omega_0\}$  uma boa cobertura. Mapeamos todos os domínios de coordenadas  $B_i$  biunívoca e sobrejetivamente sobre  $\omega_0$ .  $(\omega_0)_{\mathcal{B}}$  denotará tal codificação.
2. Seleccionemos um subconjunto contável  $\mathcal{K} = \{\varphi_i : i \in \omega_0\}$ , denso no espaço de todos os difeomorfismos de  $B_i$  sobre  $\mathbb{R}^4$ , e formemos  $\mathcal{K}^{\omega_0}$ . Então uma coordenação para a cobertura  $\mathcal{B}$  é um par ordenado  $\langle \mathcal{B}, \varphi \rangle$ ,  $\varphi \in \mathcal{K}^{\omega_0}$ , dado pelas sequências  $\langle n, \varphi(n) \rangle$ ,  $n \in (\omega_0)_{\mathcal{B}}$ .

3. Agora descrevamos a boa cobertura através de seus elementos em  $\mathcal{C}$ . Começemos com  $B_0$ .  $B_0$  intersecta um número finito de elementos na boa cobertura  $\mathcal{B}$ , isto é, intersecta um conjunto finito  $\mathcal{C}_0 \subset \mathcal{C}$ , onde todos os elementos de  $\mathcal{C}_0$  são da forma  $B_{0ijk\dots l}$ . Como  $\mathcal{C}_0$  é um conjunto *finito*, de posse da codificação para  $(\omega_0)_{\mathcal{C}_0}$ , onde  $\mathcal{C}_0 = \{\dots B_{0ijk\dots m} \dots\}$ , determinamos um inteiro positivo  $n_0$ . Feito isto definimos  $F_M(0) = n_0$ .
4. Feito isto, escolhamos o menor índice depois de 0 em  $B_{0ijk\dots}$ , digamos  $j$ , e coloquemos  $j = 1$ . Renumeramos tudo de novo, de acordo com a codificação anterior, e seguimos para a etapa posterior, com o novo  $B_1$ .
5. Suponhamos dadas as construções para todos os  $B_i$ ,  $i < k$ , e que estamos entrando neste momento na  $k$ -ésima etapa. Excluimos de  $\mathcal{C}$  todos os conjunto que já foram utilizados em etapas anteriores e que já não são mais necessários, obtendo  $\mathcal{C}_k$  e sua respectiva codificação  $(\omega_0)_{\mathcal{C}_k}$ . Escolhemos, como no item 3, a parte da boa cobertura que tem índice  $k$  e obtemos o correspondente  $n_k$ . Definimos  $F_M(k) = n_k$ . Escolhemos então o menor índice em  $B_{kij\dots}$ , digamos  $i$ , e renumeramos tudo de novo com  $i = k + 1$ . Feito isto seguimos para uma nova etapa.

Notemos que associamos um mapa de cada cobertura para uma dada variedade  $M$  sobre  $\omega_0$ . Como no item 2 selecionamos somente subconjuntos densos  $\mathcal{K}$ , é imediato que duas variedades  $M$  que diferem por um conjunto magro tem o mesmo mapa que mencionamos. Construamos o conjunto  $\mathcal{M}$  de elementos de  $\mathcal{S}$  módulo conjuntos de primeira classe (magros) em  $\mathcal{S}$ . Com isto, como qualquer  $F \in (\omega_0)^{\omega_0}$  será associado a uma boa cobertura para uma variedade em  $\mathcal{M}$ , ou seja, para cada  $F \in (\omega_0)^{\omega_0}$  temos associado um  $F_M$  dado pela construção anterior, onde cada elemento de  $\mathcal{M}$  é denotado por uma única sequência  $\langle F_M(n), \varphi(n) \rangle$ , é fácil obter o mapeamento biunívoco e sobrejetor desejado  $\iota : \mathcal{M} \rightarrow (\omega_0)^{\omega_0}$ .

Demonstramos o:

**Proposição 4.8**  $ZFC \vdash$  “*Existe um mapeamento sobrejetivo e biunívoco  $\iota : \mathcal{M} \rightarrow (\omega_0)^{\omega_0}$ .*”

**Corolário 4.9**  $ZFC \vdash$  “*Existe uma correspondência biunívoca e sobrejetora  $\kappa : \text{Ir} \rightarrow \mathcal{M}$ , onde  $\text{Ir}$  é o conjunto de todos os irracionais,  $\text{Ir} \subset \mathbb{R}$ .*”

*Demonstração:* Veja [48].  $\square$

**Corolário 4.10**  $ZFC \vdash$  “Existe uma correspondência biunívoca  $\rho : B \cdot \text{Ir} \rightarrow \mathcal{M}$ ”, onde  $B \cdot \text{Ir} \subset [0, 1] \subset \mathbb{R}$  denota o conjunto dos binários irracionais.

*Demonstração:* Seguindo a linha do Corolário anterior, uma vez que binários irracionais podem ser vistos como expansões binárias de reais contidos em  $[0, 1]$  que não terminam numa sucessão infinita de zeros ou uns.  $\square$

Estes corolários nos permitem que definamos uma topologia para  $\mathcal{M}$ .

**Definição 4.11** A topologia de  $\mathcal{M}$  é a topologia induzida (ou co-induzida) de  $\iota, \kappa$  ou  $\rho$ , como dados anteriormente.

Da definição 4.11 obtemos que  $\mathcal{M}$  é um espaço métrico completo e separável, isto é, um *Espaço Polonês* [76]. Mais ainda:  $\mathcal{M}$  é completamente desconexo.

Obtida uma topologia para  $\mathcal{M}$ , vejamos algumas propriedades deste espaço.

## 4.4 Computabilidade, Aleatoriedade e Indecidibilidade em $\mathcal{M}$

Primeiro comecemos dizendo o que entendemos por um espaço-tempo computável:

**Definição 4.12**  $M \in \mathcal{M}$  é computável se e somente se  $F_M$  é computável.

o que resulta na

**Proposição 4.13**  $ZFC \vdash$  “O mapa  $\iota$  leva objetos computáveis sobre objetos computáveis”.

*Demonstração:* Imediata, a partir da construção de  $\iota$ .  $\square$

Nosso interesse é comparar aleatoriedade com genericidade (no sentido da teoria dos conjuntos [19] [8] [54]). Necessitamos então de uma definição

adequada, para nossos propósitos, de aleatoriedade. Usaremos o conceito de aleatoriedade estabelecido por Kolmogorov e Chaitin, que pode-se demonstrar ser equivalente à definição de aleatoriedade de Martin-Löf [16].

**Definição 4.14**  $M \in \mathcal{M}$  é K[olmogorov]C[haitin]-randômico se e somente se  $M = \rho(\sigma)$  e  $\sigma \in B \cdot \mathbb{I}r$  é uma sequência binária infinita KC-randômica.

Para uma caracterização do que vem a ser uma sequência KC-randômica veja o artigo de Chaitin [16].

De 4.14 obtemos:

**Proposição 4.15**  $ZFC \vdash$  “O conjunto de todos os espaços-tempo KC-randômicos de  $\mathcal{M}$  é de medida 1 (tem por complemento um conjunto de medida zero) na medida induzida”.

*Demonstração:* Imediata, através do homomorfismo  $\rho$ .  $\square$

Intuitivamente, “aleatoriedade” e “genericidade” são conceitos que devem estar intimamente ligados, se lembrarmos que genericidade é o conceito complementar a construtibilidade (no sentido de Gödel [56]) e que elementos construtíveis são justamente aqueles que obtemos de uma maneira “determinística”. Esta intuição é corroborada pelos modelos booleanos de Scott-Solovay [72], que originalmente eram construídos sobre funções aleatórias e álgebras de Borel. Imediatamente segue-se a questão: podemos relacionar formalmente “aleatoriedade” e “genericidade”? A resposta a isto será dada na Proposição 4.17. Entretanto, antes de enunciarmos o resultado principal deste capítulo, estabeleçamos uma relação de equivalência entre diferentes elementos de  $\mathcal{M}$ .

Seja  $M$  um elemento de  $\mathcal{M}$ . Como já asseveramos, toda a variedade diferenciável lisa  $M$  de dimensão 4 pode ser mergulhada num espaço euclidiano  $\mathbb{R}^9$ . Desejamos identificar espaços-tempo que diferem apenas pela ação de um grupo de difeomorfismos, e que portanto são “indistinguíveis” do ponto de vista da física. Isto é feito considerando o grupo de difeomorfismos  $\mathcal{D}$  de  $\mathbb{R}^9$ ; fazemos com que este grupo atue sobre o mergulho de  $M$  e colapsamos seus elementos pela ação do grupo. De outra maneira, obtemos o espaço quociente  $\mathcal{M}/\mathcal{D}$ .

**Definição 4.16**  $\mathcal{N} = \mathcal{M}/\mathcal{D}$  é o conjunto dos espaços-tempo fisicamente distintos.

Se dotamos  $\mathcal{N}$  de uma topologia projetada de  $\mathcal{M}$ , então  $\mathcal{N} = \mathcal{M}/\mathcal{D}$  também é um espaço polonês, e a sequência de espaços KC-randômicos em  $\mathcal{M}$  é novamente mapeada sobre um conjunto de medida 1.

Neste ponto podemos estabelecer o resultado principal deste capítulo:

**Proposição 4.17** *A sentença “O conjunto dos espaços-tempo fisicamente distintos e KC-randômicos é igual ao conjunto dos espaços-tempo genéricos fisicamente distintos módulo um conjunto de medida zero” é indecidível em ZFC.*

*Demonstração:* Primeiro exibimos um modelo no qual  $\psi$  ( $\psi$  representa a sentença entre aspas na Proposição acima) é verdade para depois exibirmos um modelo no qual  $\neg\psi$  é verdade. Para isto precisamos do Lema:

**Lema 4.18**  $V = L \models \neg\psi$

*Demonstração:* Imediata, uma vez que

$V = L \models$  “O conjunto de todos os objetos genéricos é vazio”.

□

Para um modelo em que valha  $\psi$  consideremos o seguinte: seja  $L$  o universo construtível de Gödel, e  $L^B$  sua extensão booleana tal que  $L^B \models$  “ZFC +  $2^{\aleph_0} > \aleph_1$  + Axioma de Martin” [54]. Com  $|X|$  denotando a cardinalidade do conjunto  $X$ , é sabido que

**Proposição 4.19**  $L^B \models$  “Se  $X$  é um espaço polonês e se  $U \subset X$  é tal que  $|U| < 2^{\aleph_0}$ , então  $U$  é um conjunto magro em  $X$ ”.

*Demonstração:* Veja Kunen [54]. □

e também

**Lema 4.20**  $L^B \models “|\hat{\mathcal{M}}| = \aleph_1”$

*Demonstração:* Resulta da conservação da cardinalidade [8] [25].  $\square$

**Lema 4.21**  $\mathbf{L}^B \models$  “O conjunto de todos os espaços-tempo fisicamente distintos  $\mathcal{M} - \hat{\mathcal{M}}$  é de medida 0 em  $\mathcal{M}$ ”.

*Demonstração:* Segue de imediato dos Lemas 4.20 e 4.19, pois subtraímos de um conjunto de medida 1 um conjunto de medida 0.  $\square$

Como  $\mathcal{M}$  obedece à propriedade da interseção finita,  $\mathcal{M}$  forma um filtro, e com isto

**Proposição 4.22**  $\mathcal{L}^B \models$  “O conjunto dos espaços-tempo fisicamente distintos KC-randômicos é igual ao conjunto dos espaços-tempo genéricos fisicamente distintos módulo um conjunto de medida 0”.

*Demonstração:* Imediata, indo-se para o espaço quociente com a topologia descrita anteriormente, em virtude dos lemas.  $\square$

Acabamos de deduzir que não podemos demonstrar usando-se os axiomas de ZFC que os conjuntos genéricos são iguais aos conjuntos KC-randômicos (módulo algum outro conjunto irrelevante). De uma maneira geral, estes os conjuntos KC-randômicos e os conjunto genéricos não coincidem. Isto pode ser enfatizado lembrando que existem sequências construtíveis (no sentido de Gödel) nos  $\mathbf{B} \cdot \text{Ir} \in \mathbf{L}^B$  e que, se  $u \in \mathbf{B} \cdot \text{Ir} \in \mathbf{L}^B$  é uma sequência genérico, podemos facilmente obter uma outra sequência  $f(u)$  que não satisfaz à Lei dos Grandes Números, e que ainda assim não será contrutível.

O que nos resta perguntar é se os dois conjuntos podem coincidir módulo um conjunto irrelevante menor que o conjunto de medida 0 da Proposição 4.17. Para que possamos entender melhor isto, consideremos os argumento seguintes.

Suponhamos que acreditemos existir uma classe não contável *própria*  $\mathbf{V} \models \text{ZFC}$ . Usamos o Teorema de Löwenheim-Skolem [19] [54] para passarmos de  $\mathbf{V}$  para um modelo contável  $\mathbf{M}$ , que posteriormente restringiremos para o universo contável construtível  $\mathbf{L}$ . Tudo isto pode ser feito transitivo pelo colapso de Mostowski [54]. Então temos que todos os binários  $(\mathbf{B} \cdot \text{Ir})^{\mathbf{L}} \subset$



$B \cdot \text{Ir} \in \mathbf{V}$ , devido à transitividade. Quando fazemos uma extensão por *forcing*  $\mathbf{L}(g)$ , necessitamos de um filtro genérico  $g$ , que no nosso caso pode ser obtido de  $2^{\omega_0}$ . Como  $g$  é genérico,  $g \notin \mathbf{L}$ , e sim  $g \in (B \cdot \text{Ir} - (B \cdot \text{Ir})^{\mathbf{L}})$ . Pode-se mostrar que o conjunto (com respeito a  $\mathbf{V}$ ) de todos os  $g$  genéricos assim obtidos é residual e tem medida 1 em  $B \cdot \text{Ir}$ . Além do mais, este conjunto não coincide com o conjunto de todas as sequências binárias KC-randômicas em  $B \cdot \text{Ir}$ , uma vez que existem sequências KC-randômicas que não são genéricas, na construção usual de  $g$ , e que existem filtros genéricos que não são randômicos (violam, digamos, a Lei dos Grandes Números) [39] [42] [48].

# Capítulo 5

## Conclusões

No Capítulo 3 resolvemos dois problemas diferentes. O primeiro é uma questão geométrica sobre os campos de gauge, e pode ser formulada como segue: quais as condições de existência para soluções não-curvatura da Identidade de Bianchi ? Como resposta, obtivemos que tais soluções existem se a forma conexão tem uma parte *flat*. Isto é equivalente à existência de uma distribuição integrável não-trivial no fibrado horizontal sobre  $P(M, G)$  [50]. Tais conexões existem e podem ser escrita explicitamente, se necessário for [35] [38].

A segunda questão tem uma resposta diferente. Suponhamos que nos seja apresentado um campo de gauge qualquer, representado por uma forma conexão escrita em termos de funções subelementares. Uma pergunta imediata que surge, em virtude da resposta anterior, é: dada esta forma conexão, podemos determinar se ela satisfaz as condições estabelecidas na Proposição 3.18 ? Não, ao menos algorítmicamente.

No Capítulo 4 sugerimos que, intuitivamente, objetos genéricos deveriam se assemelhar a objetos aleatórios. Apesar disto, não podemos provar em ZFC tal semelhança. Isto nos leva a crer que a procura de objetos indecidíveis na natureza é a procura de aleatoriedade, em virtude da sugestão anterior.

Finalmente, o que vimos no geral é que, longe de estar ausente, indecidibilidades existem em praticamente todas as áreas da física matemática. A questão que nos resta é: fazer física (teórica) é *computar* novos resultado a partir de determinadas leis; o que acontece quando tal computação não pode ser feita ?

# Apêndice A

Neste apêndice apresentamos uma série de programas em computação algébrica elaborados nas linguagens “MAPLE” e “REDUCE”. Estes programas basicamente manipulam algébricamente polinômios com número muito grande de variáveis.

Na manipulação de polinômios “gigantes” (mais de 1000 variáveis) a linguagem “MAPLE” se tornou mais adequada, pois os produtos entre polinômios e seus quadrados só são expandidos quando pedimos ao computador que o faça, ao contrário do “REDUCE”, que sempre os expande internamente [80]. Por este motivo, apresentaremos um programa “MAPLE” que calcula explicitamente uma equação diofantina que representa a hipótese de Riemann, ficando os programas “REDUCE” restritos somente a poucos exemplos.

Devemos ressaltar que nestes programas nosso objetivo principal é calcular uma equação diofantina que represente a “Hipótese de Riemann” e outra que represente a “Última Conjectura de Fermat”, junto com suas transformações de Richardson I e II. Como é grande o número de resultados intermediários necessários, foi mister decompor o processo de cálculo em vários subprogramas, de tal modo que pudéssemos esvaziar a memória do computador com resultados espúrios, aumentando a eficiência do processo de cálculo e também permitindo que não excedêssemos a capacidade da máquina.

Os programas menores que apresentaremos foram executados nos microcomputadores *Atari Mega ST-2* do Laboratório de Computação Algébrica (LCA) do CBPF. Os programas exigindo maior capacidade de memória foram executados na *Vax-Station* do LCA e no sistema MTS do LNCC (Laboratório Nacional de Computação Científica). Por este motivo, pequenas variações podem ser observadas entre os programas, mas estas são

irrelevantes.

## A.1 Programas “REDUCE”

### A.1.1 A Equação Exponencial Diofantina

Este programa gera, a partir das equações apresentadas por [28], uma única equação tal que  $\exists a_1, \dots, a_{20} (p(m, n, k, a_1, \dots, a_{20}) = 0) \leftrightarrow m = n^k$ . Esta é depois gravada no arquivo “a:expo.dof”. As chaves *exp* e *nat* do “REDUCE” são desligadas para que o resultado se apresente de maneira mais compacta e seja reaproveitado em outro programa, simplesmente lendo-se o arquivo no qual ele é gravado.

```
%
%
% Construindo uma Eq. Diofantina que representa  $m=n^k$ 
%
% Variaveis: a(1),...,a(20)
% Parametros: m,n,k
% Equacao Final: expo
%
%
off exp;
operator a;
equ1:= x**2-(o**2-1)*y**2-1$
equ2:= u**2-(o**2-1)*v**2-1$
equ4:= v-r*y**2$
equ5:= b-1-4*p*y$
equ6:= b-o-q*u$
equ7:= s-x-c*u$
equ3:= s**2-(b**2-1)*tt**2-1$
equ8:= tt-k-4*(d-1)*y$
equ9:= y-k-ee+1$
equ10:= (x-y*(o-n)-m)**2-(f-1)**2*(2*o*n-n**2-1)**2$
equ11:= m+g-2*o*n+n**2+1$
equ12:= n+h-w$
equ13:= k+l-w$
```

```

equ14:= o**2-(w**2-1)*(w-1)**2*z**2-1$
%
% Somando os quadrados das equacoes
%
equ15:= equ1**2+equ2**2+equ3**2+equ4**2
+equ5**2+equ6**2+equ7**2+equ8**2+equ9**2$
equ16:= equ10**2+equ11**2+equ12**2+equ13**2+equ14**2$
equ17:= equ15+equ16$
sub(x=a(1),o=a(2),y=a(3),u=a(4),v=a(5),s=a(6),equ17)$
sub(b=a(7),tt=a(8),r=a(9),p=a(10),q=a(11),ws)$
sub(c=a(12),d=a(13),ee=a(14),f=a(15),g=a(16),
w=a(17),h=a(18),l=a(19),z=a(20),ws)$
off nat, echo$
%
% Gravando em disco
%
out "a:expo.dof"$
expo:=ws;
write ";end;"$
shut "a:expo.dof"$
end$
%      Fim de programa

```

## A.1.2 Uma Equação Diofantina para o Conjunto dos Primos

Usamos o polinômio de Jones [30] para obter uma equação representando o conjunto dos números primos. A equação é gravada na *file* "a:primos.dof".

```

%
%
% Construindo uma equacao diofantina para p, p sendo
% um primo.
%
% Variaveis: b(1),...,b(26)
% Parametros: p

```

```

% Equacao Final: primos
%
%
off exp$
operator b;
%
% Entrando com o polinomio de Jones
%
equ1:= (w*z+h+j-q)**2$
equ2:= ((g*k+2*g+k+1)*(h+j)+h-z)**2$
equ3:= (16*(k+1)**3*(k+2)*(n+1)**2+1-f**2)**2$
equ4:= (2*n+p+q+z-ee)**2$
equ5:= (ee**3*(ee+2)*(a+1)**2+1-o**2)**2$
equ6:= ((a**2-1)*y**2+1-x**2)**2$
equ7:= (16*r**2*y**4*(a**2-1)+1-u**2)**2$
equ8:= (((a+u**2*(u**2-a))**2-1)*(n+4*d*y)**2+1
        -(x+c*u)**2)**2$
equ9:= ((a**2-1)*l**2+1-m**2)**2$
equ10:= (a*ii+k+1-l-ii)**2$
equ11:= (n+l+v-y)**2$
equ12:= (p+l*(a-n-1)+b*(2*a*n+2*a-n**2-2*n-2)-m)**2$
equ13:= (q+y*(a-p-1)+s*(2*a*p+2*a-p**2-2*p-2)-x)**2$
equ14:= (z+p*l*(a-p)+tt*(2*a*p-p**2-1)-p*m)**2$
equ15:= equ1+equ2+equ3+equ4+equ5+equ6+equ7+equ8
        +equ9+equ10+equ11+equ12+equ13+equ14$
equ16:= (k+2)*(1-equ15)$
sub(a=b(1),b=b(2),c=b(3),d=b(4),ee=b(5),f=b(6),equ16)$
sub(g=b(7),h=b(8),ii=b(9),j=b(10),k=b(11),ws)$
sub(l=b(12),m=b(13),n=b(14),o=b(15),p=b(16),ws)$
sub(q=b(17),r=b(18),s=b(19),u=b(20),v=b(21),ws)$
sub(x=b(22),y=b(23),z=b(24),w=b(25),tt=b(26),ws)$
ws-p$
%
% Escrevendo polinomio para o arquivo "a:primos.dof";
%
off nat, echo$
out "a:primos.dof"$

```

```

primos:=ws;
write "end"$
shut "a:primos.dof";
end$
%      Fim de Programa

```

## A.2 Programas “MAPLE”: A Última Conjectura de Fermat e a Hipótese de Riemann

A lógica dos primeiros programas segue a de seus equivalentes em REDUCE. A equação obtida para a Exponencial Diofantina é posteriormente utilizada para obtermos a Última Conjectura de Fermat. A Hipótese de Riemann foi contruída na forma exponencial para evitarmos um número de variáveis exageradamente longo, tornando o tempo de execução do programa inviável para o sistema MTS.

### A.2.1 A Última Conjectura de Fermat

Geramos uma série de programas que produzem a Transformada de Richardson para um polinômio diofantino representando a Última Conjectura de Fermat.

#### Exponencial Diofantina

Este programa gera a mesma eq. que o “REDUCE”. A saída é feita na formatação interna do “MAPLE” e gravada na file “a:\maple\expo.m”, podendo ser utilizada posteriormente por outros programas.

```

#
#
#
# Calculo da eq Diof. para  $m=n^k$ :
#

```

```

# Variaveis: a1,...,a20
# Parametros: m,n,k
# Saida: expo
#
#
equ1:= x^2-(o^2-1)*y^2-1:
equ2:= u^2-(o^2-1)*v^2-1:
equ4:= v-r*y^2:
equ5:= b-1-4*p*y:
equ6:= b-o-q*u:
equ7:= s-x-c*u:
equ3:= s^2-(b^2-1)*tt^2-1:
equ8:= tt-k-4*(d-1)*y:
equ9:= y-k-ee+1:
equ10:= (x-y*(o-n)-m)^2-(f-1)^2*(2*o*n-n^2-1)^2:
equ11:= m+g-2*o*n+n^2+1:
equ12:= n+h-w:
equ13:= k+l-w:
equ14:= o^2-(w^2-1)*(w-1)^2*z^2-1:
#
# Somando Quadrados
equ15:= equ1^2+equ2^2+equ3^2+equ4^2
+equ5^2+equ6^2+equ7^2+equ8^2+equ9^2:
equ16:= equ10^2+equ11^2+equ12^2+equ13^2+equ14^2:
equ17:= equ15+equ16:
#
# Fazendo Substituicoes
subs(x=a1,o=a2,y=a3,u=a4,v=a5,s=a6,
b=a7,tt=a8,r=a9,p=a10,q=a11,equ17):
expo:= subs(c=a12,d=a13,ee=a14,f=a15,
g=a16,w=a17,h=a18,l=a19,z=a20,"):
save expo,'a:/maple/expo.m';
#     Fim de Programa

```

## A Última Conjectura

```
#
```



```

#
#
#   Calculo da eq. Diofantina representando a
#   ultima conjectura de Fermat.
#
# Variaveis: a1,...,a60
# Parametros: p, q, j, z, y, x
# Equacao de Saida: fermat
# Arquivo de Saida: "fermat.m"
#
#
#
# Lendo a Exponencial Diofantina
read 'expo.m':
# inicio da primeira substituicao
e1:= subs(m=p,n=x+1,k=j+3,expo):
e2:= expo:
# inicio da segunda substituicao
for i from 1 to 20 do
    e2:= subs(a.i=a.(i+20),e2)
od:
e2:= subs(m=q,n=y+1,k=j+3,e2):
# inicio da ultima substituicao
for i from 1 to 20 do
    expo:= subs(a.i=a.(i+40),expo)
od:
expo:= subs(m=p+q,n=z,k=j+3,expo):
fermat:= e1**2 + e2**2+ expo**2;
#
# Gravando Polinomio em Disco
save fermat,'fermat.m':
#   Fim de Programa

```

## Majorando as Funções

Nesta etapa, majoramos as funções que entram no procedimento para o cálculo do polinômio representando Fermat (como chamaremos abreviadamente sua Última Conjectura). Esta é uma etapa preliminar para o cálculo da Transformação de Richardson.

## Exponencial

```
#
#
#
# Calculo da eq que majora a eq Diof. para  $m=n**k$ :
#
# Variaveis: a(1),...,a(20)
# Parametros: m,n,k
# Saida: expog
#
#
equ1:= x**2+(o**2+3)*y**2+3:
equ2:= u**2+(o**2+3)*v**2+3:
equ4:= v+r*y**2:
equ5:= b+3+6*p*y:
equ6:= b+o+q*u:
equ7:= s+x+c*u:
equ3:= s**2+(b**2+3)*tt**2+3:
equ8:= tt+k+6*(d+3)*y:
equ9:= y+k+ee+3:
equ10:= (x+y*(o+n)+m)**2+(f+3)**2*(4*o*n+n**2+3)**2:
equ11:= m+g+2*o*n+n**2+3:
equ12:= n+h+w:
equ13:= k+l+w:
equ14:= o**2+(w**2+3)*(w+3)**2*z**2+3:
equ15:= equ1**2+equ2**2+equ3**2+equ4**2+equ5**2
      +equ6**2+equ7**2+equ8**2+equ9**2:
equ16:= equ10**2+equ11**2+equ12**2+equ13**2+equ14**2:
equ17:= equ15+equ16:
```

```

subs(x=a1,o=a2,y=a3,u=a4,v=a5,s=a6,b=a7,
      tt=a8,r=a9,p=a10,q=a11,equ17):
expog:= subs(c=a12,d=a13,ee=a14,f=a15,
            g=a16,w=a17,h=a18,l=a19,z=a20,"):
for i from 1 to 20 do
  expog:= subs(a.i=(a.i)**2+2,expog)
od:
# Gravando equacao
save expog,'expog.m';
#   Fim de Programa

```

## Fermat

```

#
#
#
#   Calculo da eq. Diofantina representando a
#   ultima conjectura de Fermat majorada.
#
#
#
#
#
read 'expog.m':
# inicio da primeira substituicao
e1:= subs(m=p,n=x+1,k=j+3,expog):
e2:= expog:
# inicio da segunda substituicao
for i from 1 to 20 do
  e2:= subs(a.i=a.(i+20),e2)
od:
e2:= subs(m=q,n=y+1,k=j+3,e2):
# inicio da ultima substituicao
for i from 1 to 20 do
  expog:= subs(a.i=a.(i+40),expog)
od:
expog:= subs(m=p+q,n=z,k=j+3,expog):

```

```

fermatg:= e1**2 + e2**2+ expog**2;
# Gravando em Disco
save fermatg,'fermatg.m':
#     Fim de Programa

```

## A Primeira Transformação de Richardson

```

#
#
#
# Programa que aplica a transformacao
# de Richardson do primeiro tipo
# 'a eq. Diof. que representa a
# u'ltima conjectura de Fermat.
#
#
# Lendo a eq. Diof. que representa Fermat
read 'fermatg.m':
read 'fermat.m':
fermatg:= subs(z=a65,x=a61,y=a62,q=a63,p=a64,j=a66,fermatg):
fermat:= subs(z=a65,x=a61,y=a62,q=a63,p=a64,j=a66,fermat):
# Inicio do primeiro for
for i from 1 to 66 do
    k.i:= diff(fermatg**2,a.i)
od:
# Fim do primeiro for
# Calculo de f(m,x1,...,xn)
# Inicio do calculo do somatorio
sum:= 0:
for i from 1 to 66 do
    sum:= (sin(Pi*a.i))**2*(k.i)**4 + sum
od:
# Fim do calculo do somatorio
f:= (66+1)**4*(fermat**2 + sum):
# Ultima etapa da transformac,ao de Richardson
for i from 1 to 66 do

```

```

        subs(a.1=(a.i)**2,")
od:
richferm:= ":
# Fim do calculo
# Escrevendo funcao em disco
save richferm,'richferm.m':
writeto('*print*'):
richferm;
writeto(terminal):
#      Fim de Programa

```

## A Segunda Transformação

```

#
#
#
# Faz a segunda transformacao de Richardson para Fermat
#
#
h:= proc(x) x*sin(x) end:
g:= proc(x) x*sin(x**3) end:
sum:= {a66 = h(x)} union {a1 = g@@66(x)}:
# Inicio do for
for i from 2 to 65 do
    sum:= {a.i = h@g@@(i-1)(x)} union sum:
od:
#Fazendo
read 'richferm.m':
# Substituindo
rich2:= subs(sum,richferm):
#Gravando
save rich2,'rich2.m':
#      Fim de Programa

```

## A.2.2 A Hipótese de Riemann (HR)

A HR é contruída executando-se os programas na ordem dada pela tabela abaixo:

Programa	Funcao	Saida	Variaveis
ORDEM	$c = S(a,b)$	ordem	$c_1, \dots, c_4$
COMFAT	$u = (t,s)$ $q = s!$	comb fator	$c_1, \dots, c_6$ $d_1, \dots, d_{10}$
PRIMOS	$P(p,d_1, \dots, d_{15}) = 0$ se e so se "p e' primo"	primos	$d_1, \dots, d_{15}$
MODULO	$k =  n $	modulo	$h_1, h_2$
ETA	$z = \text{eta}(j)$	etaj	$f_1, \dots, f_{19}$
RANGE1	$P(k,u,g_1, \dots, g_{30})$	range1	$g_1, \dots, g_{30}$
QUANT1	Para todo $k$ ( $k \leq j$ ) $P(k,u,g_1,g_{30}) = 0$	quant1	$b_1, \dots, b_{349}$
PRODUTO1	$z = \text{prod}_{\{k=1..j\}} \text{eta}(j)$	prod1	$w_1, \dots, w_{379}$
RANGE2	$P(k,u,g_1, \dots, g_{390})$	range2	$g_1, \dots, g_{390}$
QUANT2	Para todo $k$ ( $k \leq j$ ) $P(k,u,g_1, \dots, g_{390})$	quant2	$b_1, \dots, b_{4509}$
PRODUTO2	$z = \text{prod}_{\{k=1..x-1\}} \text{eta}(n)$ $\text{prod}_{\{n=1..k\}} \text{eta}(n)$ $= \text{delta}(x)$	produto2	$b_1, \dots, b_{4899}$
RANGE3	$P(k,u,g_1, \dots, g_{11})$	range3	$g_1, \dots, g_{11}$
QUANT3	Para todo $k$ ( $k \leq j$ ) $P(k,u,g_1, \dots, g_{11})$	quant3	$b_1, \dots, b_{140}$
SOMA	$z = \text{SUM}_{\{k=1..j\}} 1/k$	soma	$w_1, \dots, w_{151}$
RIEMANN	$P(n,g_1, \dots, g_{5056}) = 0$ se e somente se HR e' falsa	riemann	$g_1, \dots, g_{5056}$

### A Função Ordenadora

#

```

#
# Construindo a eq. Diof. para a funcao ordenadora S(a,b)=c;
#
# Variaveis: c1,...,c4
# Parametros: a,b,c
# Equacao de Saida: ordem
# Arquivo de Saida: "ordem.m"
#
#
a1:= (c1+c2-2)*(c1+c2-1)+2*c2-2*b;
a2:= c3*(1+a*c2)+c-c1;
a3:= c+c4-2-a*c2;
ordem:= a1**2+a2**2+a3**2;
# Gravando ordem
save ordem,'ordem.m';
#     Fim de Programa

```

## O Fatorial e a Combinação

```

#
#
# Construindo uma Eq. Diof. para u=(t,s) e q=s!
#
# Combinação de t elementos s a s, u=(t,s):
#     Variaveis: c1,...,c6
#     Parametros: u,t,s
#     Equacao de Saida: comb
#     Arquivo de Saida: "comb.m"
#
# q=s!:
#     Variaveis: d1,...,d10
#     Parametros: q,s
#     Equacao de Saida: fator
#     Arquivo de Saida: "fator.m"
#
#
a1 := y - 2**t -1;

```

```

a2 := z - y - 1;
a3 := z**t - (1*y**(s+1) + u*y**s + m);
a4 := u + v - 2**t;
a5 := m + n + 1 - y**s;
comb0:=0;
for i from 1 to 5 do comb.i := (a.i)**2 + comb.(i-1) od;
comb := subs(y=c1,l=c2,m=c3,v=c4,z=c5,n=c6,comb5);
#
# Gravando comb
save comb,'comb.m';
a6:= t-2*s**(s+2);
a7:= t**s-q*u-w;
a8:= u-w-x-1;
a9:= comb + a6**2 + a7**2 + a8**2;
a10:= subs(u=d1,t=d2,w=d3,x=d4,a9);
for i from 1 to 6 do a.(i+10):= subs(c.i=d.(i+4),a.(i+9)) od;
fator:=a16;
#
# Gravando fator
save fator,'fator.m';
#      Fim de Programa

```

## Uma Equação para os Primos

```

#
#
# Construindo uma Eq. Exp. Diof. para "p eh um numero primo"
#
# Variaveis: d1,...,d15
# Parametros: p
# Equacao de Saida: primos
# Arquivo de Saida: "primos.m"
#
#
read 'fator.m':
# Lendo fator; Calculando polinomio
a1:= p-s-1;

```



```

a2:= p-r-2;
a3:= a*p-b*q-1;
a4:= a1**2 + a2**2 + a3**2 + fator;
primos:= subs(a=d11,b=d12,q=d13,s=d14,r=d15,a4);
# Gravando primos
save primos,'primos.m';
#           Fim de Programa

```

### A Função Módulo

```

#
#
# Construindo um polinomio que representa  $k = \text{modulo}(n)$ 
#
# Variaveis: h1,h2
# Parametros: k,n
# Equacao de Saida: modulo
# Arquivo de Saida: "modulo.m"
#
#
a1:= (k-n)**2+(n-h1-1)**2;
a2:= (k+n)**2+(n+h2+1)**2;
modulo:= a2*a1;
# Gravando modulo
save modulo,'modulo.m';
#           Fim de Programa

```

### A Função $\eta$

```

#
#
# Construindo a Exp Dioph. Eq. representando  $z=\eta(j)$ 
#
# Variaveis: f1,...,f19
# Parametros: z, j
# Equacao de Saida: etaj
# Arquivo de Saida: "etaj.m"

```

```

#
#
a1:= (z-1)**2:
a2:= (j-f1**f2-f3-1)**2:
a3:= (z-f1)**2:
a4:= (j-f1**f2)**2:
a5:= (a1+a2)*(a3+a4):
read 'primos.m':
# Lendo primos; Comecando Substituicoes
b0:= subs(p=f1, primos):
for i from 1 to 15 do b.i:= subs(d.i=f.(i+3),b.(i-1)) od:
etaj:= a5+b15**2:
# Fim de Calculo; Escrevendo etaj no arquivo "etaj.m"
save etaj, 'etaj.m':
#      Fim de Programa

```

### Abrangência do Primeiro Quantificador

Para calcularmos os produtórios que necessitamos na HR (veja capítulo 2), decompomo-los em sua abrangência, para depois calculá-los.

```

#
#
#
# Calculus of the Dioph. Exp. Polinomial
# in the range of the 1st quantifier
# < k=1 or S(k,u)=eta(k)*S(k-1,u) >
#
# Variables: g1,...,g30
# Parameters: k,u
# Output equation: range1
# Output file: "range1.m"
#
#
#
# Reading ordem
read 'ordem.m':

```

```

# Begining substitution in ordem: <g5=S(k,u); g6=S(k-1,u)>
ordem1:= subs(a=k,b=u,c=g5,c1=g1,c2=g2,c3=g3,c4=g4,ordem):
ordem2:= subs(a=k-1,b=u,c=g6,c1=g7,c2=g8,c3=g9,c4=g10,ordem):
# Reading etaj
read 'etaj.m':
# Begining substitution in etaj
etaj:= subs(j=k,etaj):
for i from 1 to 19
  do
    etaj:= subs(f.i=g.(i + 10),etaj)
  od:
# Calculing polinomial
a1:= ((k-1)*(g5-z*g6))**2:
a2:= a1 + ordem1**2:
a1:= a2 + ordem2**2:
a2:= a1 + etaj**2:
range1:= subs(z=g30,a2):
# Saving range1
save range1,'range1.m':
# End of program

```

### Cálculo do Primeiro Quantificador

```

#
#
#
# Programa que controí o polinomio
# representando o 1o quantificador
#
# Variaveis: b1,...,b349
# Parametros: j,u
# Equacao de Saida: quanti
# Arquivo de Saida: "quant1.m"
#
#
#

```

```

read 'comb.m':
read 'fator.m':
read 'range1.m':
read 'modulo.m':
# Lendo modulo, fator, range1, comb
poli:=0:
# Definindo procedure f(i) = (b.(i+30) - (b.i, b61) )**2
f:= proc(i)
a0:= comb:
  for j from 1 to 6 do
    a.j := subs(c.j=b.(63+j+i*6),
                u=b.(i+30), t=b.i, s=b61, a.(j-1)):
  od:
a6:
end:
# Fazendo b31=(b1,b61) ... b60=(b30,b61)
for i from 1 to 30 do
  poli:= f(i)**2 + poli:
od:
# Fim do 1o for
a0:=0:
# Comecando substituicoes em range1
for i from 1 to 30 do
  range1:= subs(g.i=b.(i+249),range1)
od:
# Fim do 2o for
# Fazendo b63 = b64! ( = Q! )
a1:= subs(q=b63,s=b64,fator):
# Fazendo b61=x+1; b62=b63-1 (=b64!-1=Q!-1); b66=range1
poli:= (b61-x-1)**2 + (b62-b63-1)**2
      + (b66 - range1)**2 + a1**2 + poli:
# Fazendo b65=modulo(b66) (=modulo(range1))
a1:= subs(h1=b280, h2=b281, k=b65, n=b66, modulo):
modulo:= 0:
poli:= a1**2 + poli:
# Fazendo b64=Q
poli:= (b64-b65-2*y-x-b67+2)**2 + poli:

```

```

lixo:= 0:
# Adicionando as congruencias ao polinomio
for j from 1 to 30 do
    lixo:= (b68*b.(i+281)-b.(i+30))**2 + lixo
od:
# Terminado 3o for
poli:= lixo + poli:
a0:= comb:
for i from 1 to 6 do
    a0:= subs(c.i = b.(i+311),a0):
od:
# Terminado 4o for
# Fazendo b69=(b68,b62) e b69=y+1
poli:= (subs(u=b68,t=b62,s=b69,a0))**2
        + (b69-y-1)**2 + poli:
#1
a0:=0:
lixo:= 0:
# Fazendo b68 > b1,...,b30
for i from 1 to 30 do
    (b68 - b.i - b.(i+311) - 1)**2 + ":
od:
# Fim do 5o for
lixo:=":
quant1:= (subs(k=b62,range1) - b68*b348)**2 + lixo + poli:
quant1:= subs(x=b349,y=j, quant1):
# Fim do Calculo
# Gravando quant1 para o arquivo quant1.m
save quant1,'quant1.m';
#      Fim de Programa

```

## O Primeiro Produtório

Este programa gera a equação que representa o primeiro produtório na função  $\delta(x)$  (Capítulo 2).

#

```

#
# Construindo a eq. Diof. para  $z=\text{prod}_{\{k=1..j\}} \text{etak}$ 
#
# Variaveis: w1,...,w379
# Parametros: j,z
# Equacao de Saida: produto1
# Arquivo de Saida: prod1.m
#
#
read 'ordem.m':
read 'etaj.m':
# Lendo ordem e etaj
delta1:= 3: # Variavel de Controle
# Fazendo w2=eta(1)
a1:= subs(z=w2,j=1,etaj):
for i from 1 to 19 do
    a1:= subs(f.i=w.(i+delta1),a1)
od:
# Fim do 1o for e das substituicoes em etaj
# Fazendo w1=S(1,w3)
a2:= subs(a=1,b=w3,c=w1,ordem):
for i from 1 to 4 do
    a2:= subs(c.i=w.(i+delta1+19),a2)
od:
# Fim do 2o for
# Fazendo z=S(j,w3)
a3:= subs(a=j,b=w3,c=z,ordem):
for i from 1 to 4 do
    a3:= subs(c.i=w.(i+delta1+23),a3)
od:
# Fim do 3o for
poli:= a1**2 + a2**2 + a3**2 + (w1-w2)**2:
# Lendo quant1
read 'quant1.m':
# Comcando ultimo for
for i from 1 to 349 do
    quant1:= subs(b.i=w.(i+delta1+27),u=w3,quant1):

```

```

od:
# Fim do ultimo for
produto1:= quant1**2 + poli;
# Fim do Calculo; escrevendo polinomio em prod1.m
save produto1,'prod1.m';
#      Fim de Programa

```

### Abrangência do Segundo Quantificador

```

#
#
#
# Calculo da eq. exp. Diof. na abrangencia
# do segundo quantificador
#
# Variaveis: g1,...,g390
# Parametros: k,u
# Equacao de Saida: range2
# Arquivo de Saida: "range2.m"
#
#
#
# Lendo ordem
read 'ordem.m':
# Comecando as substituicoes em ordem;
# Fazendo  $g_5=S(k,u)$  e  $g_6=S(k-1,u)$ 
ordem1:= subs(a=k,b=u,c=g5,c1=g1,c2=g2,c3=g3,c4=g4,ordem):
ordem2:= subs(a=k-1,b=u,c=g6,c1=g7,c2=g8,c3=g9,c4=g10,ordem):
# Lendo produto1
read 'prod1.m':
# Comecando substituicoes em produto1
etaj:= subs(j=k,produto1):
for i from 1 to 379
  do
    produto1:= subs(f.i=g.(i + 10),produto1)
  od:
# Calculando Polinomio

```

```

# Fazendo (k=1 or S(k,u) = produto1(k) * S(k-1,u)
a1:= ((k-1)*(g5-z*g6))**2:
a2:= a1 + ordem1**2:
a1:= a2 + ordem2**2:
a2:= a1 + produto1**2:
# Calculo Final
range2:= subs(z=g390,a2):
# Gravando polinomio
save range2,'range2.m':
#      Fim de Programa

```

## O Segundo Quantificador

```

#
#
#
#
# Programa que controli um polinomio representando
# o 2o quantificador
#
# Variaveis: b1,...,b4509
# Parametros: j,u
# Equacao de Saida: quant2
# Arquivo de Saida: "quant2.m"
#
#
#
read 'comb.m':
read 'fator.m':
read 'range2.m':
read 'modulo.m':
# Lendo modulo, fator, range2, comb
poli:=0:
# Definindo procedure f(i) = b.(i+390) - (b.i, b781)
f:= proc(i)
a0:= comb:
  for j from 1 to 6 do

```



```

        a.j := subs(c.j=b.(783+j+i*6),
                  u=b.(i+390), t=b.i, s=b781, a.(j-1)):
    od:
    a6:
end:
# Fazendo b391=(b1,b781) ... b780=(b390,b781)
for i from 1 to 390 do
    poli:= f(i)**2 + poli:
od:
# Fim do 1o for
a0:=0:
# Comecando substituicao em range1
for i from 1 to 390 do
    range1:= subs(g.i=b.(i+3129),range1)
od:
# Fim do 2o for
# Fazendo b63 = b64! ( = Q! )
a1:= subs(q=b63,s=b64,fator):
# Fazendo b61=x+1; b62=b63-1 (=b64!-1=Q!-1); b66=range1
poli:= (b61-x-1)**2 + (b62-b63-1)**2
        + (b66 - range1)**2 + a1**2 + poli:
# Fazendo b65=modulo(b66) (=modulo(range1))
a1:= subs(h1=b3720, h2=b3721, k=b65, n=b66, modulo):
modulo:= 0:
poli:= a1**2 + poli:
# Fazendo b64=Q
poli:= (b64-b65-2*y-x-b67+2)**2 + poli:
lixo:= 0:
# Inserindo congruencias no polinomio
for j from 1 to 390 do
    lixo:= (b68*b.(i+3721)-b.(i+390))**2 + lixo
od:
# Terminado 3o for
poli:= lixo + poli:
a0:= comb:
for i from 1 to 6 do
    a0:= subs(c.i = b.(i+4111),a0):

```

```

od:
# Terminado 4o for
# Fazendo b69=(b68,b62) e b69=y+1
poli:= (subs(u=b68,t=b62,s=b69,a0))**2 + (b69-y-1)**2 + poli:
#1
a0:=0:
lixo:= 0:
# Fazendo b68 > b1,...,b30
for i from 1 to 390 do
    (b68 - b.i - b.(i+4117) - 1)**2 + ":
od:
# Fim do 5o for
lixo:=":
quant2:= (subs(k=b62,range2) - b68*b4508)**2 + lixo + poli:
quant2:= subs(x=b4509,k=j, quant2):
# Fim do calculo
# Escrevendo quant2 no arquivo quant2.m
save quant2,'quant2.m';
#      Fim de Programa

```

## O Segundo Produtório

```

#
#
# Building the Diophantine eq. for
# z=prod_{k=1..x-1} produto1(k)
#
# Variables: w1,...,w4899
# Parameters: x,z
# Output equation: produto2
# Output file: prod2.m
#
#
read 'ordem.m':
read 'prod1.m':
# Read ordem and produto1
# Doing w2=produto1(1)

```

```

a1:= subs(z=w2,j=1,produto1):
for i from 1 to 379 do
  subs(f.i=w.(i+3),"")
od:
a1:= "":
# End of the 1st for and substitutions in produto1
# Doing w1=S(1,w3)
a2:= subs(a=1,b=w3,c=w1,ordem):
for i from 1 to 4 do
  subs(c.i=w.(i+382),"")
od:
a2:= "":
# End of the 2nd for
# Doing z=S(j,w3)
a3:= subs(a=j,b=w3,c=z,ordem):
for i from 1 to 4 do
  subs(c.i=w.(i+386),"")
od:
a3:= "":
# End of the 3rd for
poli:= a1**2 + a2**2 + a3**2 + (w1-w2)**2:
read 'lixo.m':
# Begining last for
for i from 1 to 4509 do
  sum:= {b.i=w.(i+390)}:
od:
# End of last for
# Reading quant2
read 'quant2.m':
# Making substitutions
subs(u=w3,sum,quant2):
# Final calculus
produto2:= ""**2 + poli:
# Last substitution
produto2:= subs(j=x-1,produto2):
# End of Calculus; writing polinomial to prod2.m
save produto2,'prod2.m';

```

```
# End of program
```

## Abrangencia do Último Quantificador

```
#  
#  
#  
# Building the 3rd quantifier's range  
#  
# Variables: g1,...,g11  
# Parameters: k,u  
# Output equation: range3  
# Output file: "range3.m"  
#  
#  
#  
read 'ordem.m':  
# Read ordem  
# Doing g1=S(k,u); g2=S(k-1,u)  
# So quant3=(k-1)((g1-g2-g3)^2 + kg3^2)  
ordem1:= subs(a=k,b=u,c=g1,c1=g4,c2=g5,c3=g6,c4=g7,ordem):  
#1  
ordem2:= subs(a=k-1,b=u,c=g2,c1=g8,c2=g9,c3=g10,c4=g11,ordem):  
#2  
range3:=((k-1)*((g1-g2-g3)**2 + (k*g3)**2)**2):  
range3:= ordem1**2 + ordem2**2 + range3:  
# End of calculus  
# Writing polinomial  
save range3, 'range3.m':  
# End of program
```

## O Somatório

```
#  
#  
# Building the Diophantine eq. for  $z=\sum_{k=1..j} 1/k$   
# iff  $P(j,z,w1,\dots,w151) = 0$ 
```

```

#
# Variables: w1,...,w151
# Parameters: j,z
# Output equation: soma
# Output file: "soma.m"
#
#
read 'ordem.m':
# Read ordem
# Doing w2=1
a1:= w2 - 1:
# Doing w1=S(1,w3)
a2:= subs(a=1,b=w3,c=w1,ordem):
for i from 1 to 4 do
    a2:= subs(c.i=w.(i+3),a2)
od:
# End of the 1st for
# Doing z=S(j,w3)
a3:= subs(a=j,b=w3,c=z,ordem):
for i from 1 to 4 do
    a3:= subs(c.i=w.(i+7),a3)
od:
# End of the 2nd for
poli:= a1**2 + a2**2 + a3**2 + (w1-w2)**2:
# Reading quant3
read 'quant3.m':
subs(u=w3,quant3):
# Begining last for
for i from 1 to 140 do
    subs(b.i=w.(i+11),u=w3,"):
od:
quant3:=":
# End of last for
soma:= quant3**2 + poli:
# End of Calculus; writing polinomial to soma.m
save soma,'soma.m':
# End of program

```

## A Hipótese de Riemann

```
#
#
#
# Program to build the Exp. Dioph. Eq. representing Riemann's
# Hypothesis.
#
# RH iff  $P(n, g_1, \dots, g) = 0$  has no solutions
#
#
# Variables:  $g_1, \dots, g_{5056}$ 
# Parameters:  $n$ 
# Output equation: riemann
# Output file: "riemann"
#
#
#
read 'prod2.m':
read 'soma.m':
#
#  $((\sum_{k=1 \dots \delta(n)} 1/k) - n^2/2)^2 = 36n^3 + g_1 - 1$ 
#  $\delta(n) = g_2$ 
#  $\sum_{k=1 \dots g_2} = g_3$ 
#  $n^2/2 = g_4$ 
#  $(g_3 - g_4)^2 = g_5$ 
#  $36n^3 = g_6$ 
#  $(g_5 - g_6 - g_1 + 1)^2 = 0$ 
#
soma:= subs(z=g3, j=g2, soma):
for i from 1 to 151 do
    subs(w.1=g.(i+6),")
od:
soma:= "":
# End of substitution in soma
produto2:= subs(z=g2, x=n, produto2):
for i from 1 to 4899 do
```

```

        subs(b.i=g.(i+157),")
od:
produto2:= ":
a1:= (2*g4 - n**2)**2:
a2:= ((g3 - g4)**2 - g5)**2 + (36*n**3 - g6)**2:
a3:= (g5 - g6 - g1 + 1)**2:
riemann:= produto2**2 + soma**2 + a1 + a2 + a3;
# Writing polinomial in a readable style
writeto(riemann.s):
riemann:= riemann;
writeto(terminal):
# End of program

```

# Bibliografia

- [1] R. Aldrovandi, *Teorias Clássicas de Gauge e Gravitação*, Escola de Física de Partículas e Campos Jorge André Swieca 1979.
- [2] B. W. Augerstein, “Hadron Physics and Transfinite Set Theory”, Intern. J. Theoretical Physics **23**(1984), 1197.
- [3] A. F. Furtado do Amaral, *Formalismo de Teitler e suas Interações*, Tese de Doutorado, IF/UFRJ, Rio de Janeiro 1983.
- [4] A. F. Furtado do Amaral, F. A. Doria e M. Gleiser, “Higgs Fields as Bargmann-Wigner Fields and Classical Symmetry Breaking”, J. Math. Phys. **24**(1983), 1888.
- [5] R. D. Ball, “Chiral Gauge Theories”, Phys. Rep. **182**(1989), 1.
- [6] J. A. de Barros, *Conjunto Genéricos Segundo Cohen e suas Aplicações à Física*, Tese de Mestrado, CBPF, Rio de Janeiro 1989.
- [7] J. A. de Barros, não publicado.
- [8] J. L. Bell, *Boolean-Valued Models and Independence Proofs in Set Theory*, 2nd, Clarendon Press 1985.
- [9] P. A. Benioff, “Models of Zermelo Fraenkel Set Theory as Carriers for the Mathematics of Physics. I”, J. Math. Phys. **17**(1976), 618.
- [10] P. A. Benioff, “Models of Zermelo Fraenkel Set Theory as Carriers for the Mathematics of Physics. II”, J. Math. Phys. **17**(1976), 629.
- [11] R. Bott e L. W. Tu, *Differential Forms in Algebraic Topology*, Springer 1982.



- [12] G. Birkhoff e S. MacLane, *Álgebra Moderna Básica*, Guanabara Dois 1980.
- [13] C. G. Bollini, J. J. Giambiagi e J. Tiomno, “Gauge Field Copies”, *Phys. Lett.* **83B**(1979), 185.
- [14] S. S. Cairns, “Homeomorphisms Between Topological Manifolds and Analytic Manifolds”, *Ann. Math.* **41**(1940), 796.
- [15] M. P. do Carmo, *Geometria Riemanniana*, IMPA (Projeto Euclides) 1979.
- [16] G. J. Chaitin, “Incompleteness Theorems for Random Reals”, *Advances in Applied Mathematics* **8**(1987), 119.
- [17] G. J. Chaitin, “Gödel’s Theorem and Information”, *Inter. J. Theoretical Physics* **21**(1982), 941.
- [18] Y. M. Cho, “Higher-Dimensional Unification of Gravitation and Gauge Theories”, *J. Math. Phys.* **16**(1975), 2029.
- [19] P. J. Cohen, *A Teoria dos Conjuntos e a Hipótese do Contínuo*, in M. Lourenço, ed., *Kurt Gödel: O Teorema de Gödel e a Hipótese do Contínuo*, Ed. Calouste Gulbenkian 1979.
- [20] N. C. A. da Costa e F. A. Doria, “Structures, Suppes Predicates and Boolean-Valued Models in Physics”, in J. Hintikka, ed., *Festschrift in Honor of V. I. Smirnov on His 60th Birthday*, 1991.
- [21] N. C. A. da Costa e F. A. Doria, “Suppes Predicates for Classical Physics”, a aparecer nos *Proceedings of the San Sebastián Congress on Scientific Structures* (1990).
- [22] N. C. A. da Costa e F. A. Doria, “Undecidability and Incompleteness in Classical Mechanics”, *Int. J. Theor. Phys.* **30**(1991), 1041.
- [23] N. C. A. da Costa e F. A. Doria, “Classical Physics and Penrose’s Thesis”, *Found. Phys. Lett.*, a sair.

- [24] N. C. A. da Costa, F. A. Doria e J. A. de Barros, “A Formally Undecidable Statement in Classical Electromagnetic Theory”, in C. A. Bertulani e J. Lopes Neto eds., *Encontro de Física Teórica do Rio de Janeiro; Homenagem Póstuma ao Prof. Carlos Márcio do Amaral*, UFRJ 1990.
- [25] N. C. A. da Costa, F. A. Doria e J. A. de Barros, “A Suppes Predicate for General Relativity and Set-Theoretically Generic Space-Times”, *Int. J. Theor. Phys.* **29**(1990), 935.
- [26] N. C. A. da Costa, F. A. Doria, A. F. Furtado do Amaral e J. A. de Barros, “Two Questions on the Geometry of Gauge Fields”, submetido à publicação.
- [27] M. Daniel e C. M. Viallet, “The Geometrical Setting of Gauge Theories of the Yang-Mills Type”, *Rev. Mod. Phys.* **52**(1980), 175.
- [28] M. Davis, “Hilbert’s Tenth Problem is Unsolvable”, *Amer. Math. Monthly*, **80**(1973), 233.
- [29] M. Davis, “An Explicit Diophantine Definition of the Exponential Function”, *Comm. Pure App. Math.* **24**(1971), 137.
- [30] M. Davis, Y. Matijasevič e J. Robinson, “Hilbert’s Tenth Problem. Diophantine Equations: Positive Aspects of a Negative Solution”, *Proc. of Symposia in Pure Mathematics*, **28**(1976), 323.
- [31] M. Davis, H. Putnam e J. Robinson, *Ann. of Math.*, “The Decision Problem for Exponential Diophantine Equations”, **74**(1961), 425.
- [32] P. Dolbeault, “On Connections”, in *Global Analysis and Its Applications* vol. II, Lectures Presented at an International Seminar Course at Trieste from 4 July to 25 August 1972, Organized by the ICTP/Trieste, International Atomic Energy Agency 1974.
- [33] F. A. Doria, “The Geometry of Gauge Field Copies”, *Comm. Math. Phys.* **79**(1981), 435.
- [34] F. A. Doria, “On the Existence of the Wu-Yang Ambiguity”, *An. Acad. brasil. Ciênc.* **53**(1981), 657.

- [35] F. A. Doria, “A Bifurcation Set Associated to the Copy Phenomenon in the Space of Gauge Fields”, in G. I. Zapata, ed. *Functional Analysis, Holomorphy and Approximation Theory II*, North Holland 1984, pg. 69.
- [36] F. A. Doria, “Chaos Cannot Always be Proved to Exist”, preprint 1991.
- [37] F. A. Doria, E. Carneiro Leão, M. Tavares D’Amaral e Muniz Sodré, *A Máquina e seu Averso*, Francisco Alves 1987.
- [38] F. A. Doria, M. Ribeiro da Silva e A. F. Furtado do Amaral, “A Generalization of Einstein’s  $\lambda$ -Transformation and Gravitational Copies”, *Lett. Nuovo Cimento* 40(1984), 509.
- [39] F. A. Doria, J. A. de Barros e M. Ribeiro da Silva, “Non-Computable Functions, Generic Functions and Random Sequences”, *Bol. Soc. Paran. de Matemática*, série 2<sup>a</sup>, 8(1987), 197.
- [40] B. Doubrovine, S. Novikov e A. Fomenko, *Géométrie Contemporaine*, tomes 1 et 2, Éditions Mir 1982.
- [41] T. Eguchi, P. B. Gilkey e A. J. Hanson, “Gravitation, Gauge Theories and Differential Geometry”, *Physics Reports* 66(1980), 213.
- [42] S. Feferman, “Some Applications of the Notion of Forcing and Generic Sets”, *Fundamenta Mathematicæ* 56(1965), 23.
- [43] H. Flanders, *Differential Forms with Applications to the Physical Sciences*, Academic Press 1963.
- [44] K. Gödel, “Acerca das Proposições Indecidíveis de Sistemas Matemáticos Formais”, in M. Lourenço, ed., *Kurt Gödel: O Teorema de Gödel e a Hipótese do Contínuo*, Editora Calouste Gulbenkian 1979.
- [45] P. R. Halmos, *Lectures on Boolean Algebras*, Van Nostrand Reinhold Co. 1963.
- [46] W. S. Hatcher, *The Logical Foundations of Mathematics*, Pergamon Press 1982.

- [47] I. N. Herstein, *Topics in Algebra*, 2nd edition, John Willey & Sons 1975.
- [48] P. G. Hinman, *Recursion-Theoretic Hierarchies*, Springer-Verlag 1978.
- [49] J. P. Jones, "Universal Diophantine Equation", *J. of Symbolic Logic*, bf 47(1982), 549.
- [50] F. W. Kamber e P. Tondeur, *Foliated Bundles and Characteristic Classes*, Lectures Notes In Math. 493, Springer-Verlag 1975.
- [51] S. Kobayashi e K. Nomizu, *Foundations of Differential Geometry*, Interscience Pub. 1963.
- [52] N. P. Konopleva e V. N. Popov, *Gauge Fields*, traduzido da segunda edição russa, Harwood Academic Publishers 1981.
- [53] C. Kosniowski, *A First Course in Algebraic Topology*, Cambridge University Press 1980.
- [54] K. Kunen, *Set Theory, An Introduction to Independence Proofs*, Elsevier Science Pub. Co. 1983.
- [55] E. L. Lima, *Variedades Diferenciáveis*, Monografias de Matemática do IMPA 15, 1973.
- [56] Yu. I. Manin, *A Course in Mathematical Logic*, Springer-Verlag 1984.
- [57] W. S. Massey, *Algebraic Topology: An Introduction*, Harcourt-Brace & World 1967.
- [58] Y. Matijasevič e J. Robinson, "Reduction of an Arbitrary Diophantine Equation to one in 13 unknowns", *Acta Arithmetica*, 27(1975), 521.
- [59] C. R. F. Maunder, *Algebraic Topology*, Van Nostrand Reinhold Co., 1972.
- [60] J. Thierry-Mieg, "Classical Geometrical Interpretations of Ghost Fields and Anomalies in Yang-Mills Theory and Quantum Gravity," in W. A. Bardeen e R. A. White, eds., *Symposium on Anomalies, Geometry, Topology*, World Scientific 1985.

- [61] E. E. Moise, "Affine Structure in 3-Manifolds. V. The Triangulation Theorem and Hauptvermutung", *Ann. Math.* **56**(1952), 96.
- [62] H. Muirhead, *The Physics of Elementary Particles*, Pergamon Press 1968.
- [63] C. Nash e S. Sen, *Topology and Geometry for Physicists*, Academic Press 1983.
- [64] F. Quinn, "Ends of Maps. III: Dimensions 4 and 5", *J. Diff. Geom.* **17**(1982), 503.
- [65] R. Rennie, "Geometry and Topology of Chiral Anomalies in Gauge Theories", *Advances in Phys.* **a39**(1990), 617.
- [66] D. Richardson, "Some Undecidable Problems Involving Elementary Functions of a Real Variable", *J. of Symbol. Logic* **33**(1968), 514.
- [67] D. K. Ross, "Alternative Models of the Real Number Line in Physics", *Intern. J. Theoretical Physics* **23**(1984), 1207.
- [68] J. Schwinger, "The Theory of Quantized Fields. I", *Phys. Rev.* **82**(1951), 914.
- [69] J. Schwinger, "The Theory of Quantized Fields. II and III", *Phys. Rev.* **91**(1953), 713.
- [70] J. Schwinger, "Non-Abelian Gauge Fields. Commutation Relations", *Phys. Rev.* **125**(1962), 1043.
- [71] J. Schwinger, "Non-Abelian Gauge Fields. Relativistic Invariance", *Phys. Rev.* **127**(1962), 324.
- [72] D. Scott, "A Proff of the Independence of the Continuum Hypothesis", *Mathematical Systems Theory* **1**(1967), 89.
- [73] I. M. Singer, "Some Remarks on the Gribov Ambiguity" *Comm. Math. Phys.* **60**(1978), 7.
- [74] S. Sternberg, *Lectures on Differential Geometry*, Chelsea Pub. Co. 1983.

- [75] C. H. Taubes, "Gauge Theory on Asymptotically Periodic 4-manifold", *J. Diff. Geometry* **25**(1987), 363.
- [76] F. Trèves, *Topological Vector Spaces, Distributions and Kernels*, Academic Press 1967.
- [77] Y. Uspenski, Gödel's Undecidability Theorem, Mir Publishers 1987.
- [78] R. Utiyama, "Invariant Theoretical Interpretation of Interaction", *Phys. Rev.* **101** (1956), 1597.
- [79] J. H. C. Whitehead, "On  $C^1$  Complexes", *Ann. Math.* **41**(1940), 809.
- [80] F. Wright, comunicação pessoal.
- [81] T. T. Wu e C. N. Yang, "Some Remarks about Unquantized non-Abelian Gauge Fields", *Phys. Rev.* **D12**(1975), 3843.
- [82] C. N. Yang and R. L. Mills, "Conservation of Isotopic Spin and Isotopic Gauge Invariance", *Phys. Rev.* **96**(1954), 191.

"DOIS EXEMPLOS DE INDECIDIBILIDADE E INCOMPLETUDE EM FÍSICA"

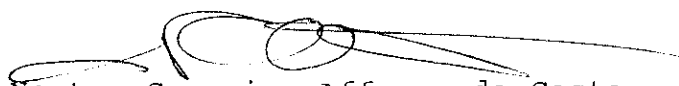
JOSÉ ACÁCIO DE BARROS


Tese de Doutorado apresentada no Centro Brasileiro de Pesquisas Físicas do Conselho Nacional de Desenvolvimento Científico e Tecnológico fazendo parte da banca examinadora os seguintes professores:

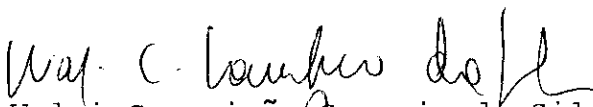
1 -

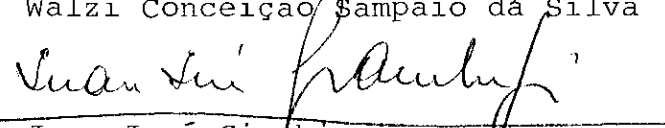
Francisco Antonio de Moraes Accioli Doria - Presidente

  
Antonio Fernandes da Fonseca Teixeira - Co-orientador

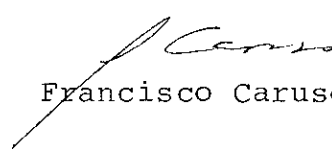
  
Newton Carneiro Affonso da Costa

  
Décio Krause

  
Walzi Conceição Sampaio da Silva

  
Juan José Gianbiagi

  
José Abdalla Helayél-Neto

  
Francisco Caruso Neto - Suplente