Universidade de Brasília

Grupos analíticos p-ádicos

de dimensões pequenas

Pedro Cusinato Loiola Lima

Orientador: Theo A. D. Zapata

Departamento de Matemática,
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestre em Matemática

Brasília, 5 de janeiro de 2026

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupos analíticos p-ádicos
de dimensões pequenas

Pedro Cusinato Loiola Lima[⋆]

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 5 de janeiro de 2026

Comissão Examinadora:

Prof. Dr. Theo Allan Darn Zapata – UnB (Orientador)

Prof[a]. Dr[a]. Cristina Acciarri – UniMoRe

Prof. Dr. Francesco Noseda – UFRJ

Prof. Dr. Jean Carlos de Aguiar Lelis – UnB (Suplente)

[⋆] O autor foi bolsista da CAPES durante a elaboração desta dissertação.

Agradecimentos

Primeiramente, agradeço à minha mãe, Ana, e ao meu pai, Jean, ao meu irmão, Lucas, e às minhas irmãs, Bibiana e Júlia, às minhas avós, Marta e Maria, à minha madrasta, Natiele, aos meus padrinhos, Renato e Denise, e a toda minha família por todo o suporte.

Agradeço ao meu orientador, Professor Theo, por me guiar nesta jornada desde minha graduação. Obrigado pela paciência e dedicação, por me mostrar a beleza da Teoria de Grupos e por alavancar meu gosto e maturidade pela Matemática.

Agradeço à Aryel, à Débora, ao Jorge, ao Matheus, ao Pedro, ao Rafael e a todos meus queridos amigos e colegas do mestrado e do doutorado. Sem eles não teria forças para finalizar este trabalho.

Agradeço aos meus amigos do PETMAT e do CAMAT, que me acompanharam durante minha graduação.

Agradeço ao Matheus Andrade, pela disponibilização e ajuda com o modelo desta dissertação.

Agradeço ao Eduardo, à Isabella, à Isabelle e ao Leonardo, amigos queridos que levo para vida.

Agradeço a todos os professores de Matemática que tive na escola, pela nobreza de seu trabalho e por despertarem a curiosidade matemática que havia dentro de mim.

Agradeço a todos os professores de graduação e pós-graduação que tive. Em especial, à Professora Luciana pela parceria durante minha graduação, ao Professor Martino pelas incontáveis aulas que me lecionou e por ter sido o primeiro a me mostrar a magia da Teoria de Grupos, aos professores Pavel Zalesskii e Pavel Shumyatsky pelas aulas memoráveis e importantes conselhos acadêmicos.

Agradeço à banca examinadora pela disposição.

Agradeço à CAPES pelas bolsas de fomento.

Resumo

Neste trabalho, investigamos a classe dos grupos analíticos p-ádicos. Apresentamos os resultados clássicos a respeito de suas relações com $\mathbb{Q}_p$-álgebras de Lie e $\mathbb{Z}_p$-reticulados de Lie, bem como resultados recentes sobre grupos analíticos pro-p livres-de-torção. Seguindo técnicas utilizadas por González-Sánchez e Klopsch (*Analytic pro-p groups of small dimensions*, 2009) e Noseda e Snopce (*On self-similarity of p-adic analytic pro-p groups of small dimension*, 2019), obtemos apresentações para todos os grupos analíticos pro-p livres-de-torção de dimensão quatro para $p > 3$.

Abstract

In this work, we investigate the class of p-adic analytic groups. We present the classical results concerning their relation with Lie $\mathbb{Q}_p$-algebras and with Lie $\mathbb{Z}_p$-lattices, as well as some recent results about torsion-free analytic pro-p groups. Following techniques used by González-Sánchez and Klopsch (*Analytic pro-p groups of small dimensions*, 2009) and Noseda and Snopce (*On self-similarity of p-adic analytic pro-p groups of small dimension*, 2019), we obtain exhibit group presentations for all four dimensional torsion-free analytic pro-p groups for $p > 3$.

Sumário

Introdução **10**

1 Preliminares **12**
1.1 Limites projetivos . . . 12
1.2 Grupos profinitos e pro-p . . . 13
1.3 Corpos completos e os números p-ádicos . . . 15
1.4 Funções analíticas . . . 16
1.5 Álgebras de Lie . . . 16

2 Variedades Analíticas **20**
2.1 Noções básicas . . . 20
2.1.1 Espaço tangente . . . 21
2.1.2 Um pouco de topologia diferencial . . . 23
2.1.3 Formas diferenciais e integração . . . 27
2.2 Classificação das variedades p-ádicas . . . 28

3 Grupos analíticos **32**
3.1 Grupos formais e grupos padrão . . . 32
3.1.1 Fórmulas para leis formais . . . 35
3.1.2 Quocientes . . . 36
3.1.3 Outros exemplos de grupos . . . 37
3.2 Grupos p-saturáveis . . . 39
3.3 Caracterização dos grupos analíticos . . . 41

4 Teoria de Lie **45**
4.1 A álgebra de Lie de um grupo de Lie . . . 45
4.2 Propriedades básicas e exemplos . . . 46
4.3 Grupos e Álgebras de Lie . . . 49
4.4 Subgrupos de Lie . . . 53
4.5 A correspondência de Lazard . . . 54
4.5.1 A álgebra grupo de um grupo p-valorado . . . 54
4.5.2 exp e log . . . 55

5 Grupos analíticos de dimensões pequenas **59**
5.1 De grupos saturáveis a filtrações potentes 59
5.2 Isoladores 62
5.3 Grupos de dimensões pequenas 62
5.4 Dimensão 2 64
5.5 Dimensão 3 66
5.6 Dimensão 4 74
5.7 Propriedade CA 81

Bibliografia **85**

Índice Remissivo **87**

Introdução

Nesta dissertação de mestrado, investigamos a classe dos grupos analíticos p-ádicos. Grupos analíticos p-ádicos são análogos p-ádicos aos grupos de Lie reais ou complexos, possuindo uma estrutura de variedade analítica sobre $\mathbb{Q}_p$ compatível com suas operações. Essa classe de grupos foi estudada inicialmente por Robert Hooke em 1942 (vide [Hoo42]), mas o interesse nela se intensificou na década de 1960.

A coleção *Éléments de mathématique* de Bourbaki, em seus volumes sobre grupos e álgebras de Lie, constrói de forma unificada a teoria de Lie para grupos de Lie reais e p-ádicos; o fascículo de resultados *Variétés différentielles et analytiques*, publicado em 1967, também aborda variedades reais e p-ádicas de maneira simultânea. Em 1964, Jean-Pierre Serre leciona em Harvard sobre grupos e álgebras de Lie, sintetizando a abordagem dos Bourbaki. Tais aulas foram posteriormente publicadas (vide [Ser00]) e constituem referência padrão no assunto.

O primeiro avanço substancial, contudo, se dá com Michel Lazard em seu trabalho massivo *Groupes analytiques p-adiques*, publicado em 1965. Esse trabalho, além de caracterizar plenamente quais grupos topológicos são analíticos p-ádicos, desenvolve uma teoria de Lie particular aos grupos analíticos p-ádicos. Um grupo pro-p finitamente gerado G é dito p-saturável se existe uma função $\omega : G \to \mathbb{R} \cup \{\infty\}$ satisfazendo:

(i) $\omega(g) > \dfrac{1}{p-1}$ para todo $g \in G$;

(ii) $\omega(g) = \infty$ se, e somente se $g = 1$;

(iii) $\omega(gh^{-1}) \geq \min\{\omega(g), \omega(h)\}$;

(iv) $\omega([g,h]) \geq \omega(g) + \omega(h)$;

(v) $\omega(g^p) = \omega(g) + 1$;

(vi) se $\omega(g) > \dfrac{p}{p-1}$, então existe $h \in G$ tal que $h^p = g$.

Lazard caracterizou os grupos analíticos p-ádicos como os grupos topológicos contendo um subgrupo aberto p-saturável. Além disso estabeleceu uma equivalência categórica entre a categoria dos grupos p-saturáveis e uma subcategoria adequada da categoria das álgebras de Lie de dimensão finita sobre $\mathbb{Z}_p$.

Outra caracterziação foi obtida na década de 1980 por Lubotzky e Mann, que, em [LuMa87b], mostraram que um grupo pro-p G é analítico p-ádico se, e somente se, tem posto finito, isto é, se existe

um inteiro positivo n tal que todo subgrupo fechado de G pode ser gerado topologicamente por n elementos.

O presente trabalho começa, em seu Capítulo 1, com alguns resultados preliminares para facilitar a leitura. No Capítulo 2 investigamos as variedades analíticas e apresentamos duas demonstrações de um teorema de estrutura para variedades p-ádicas, obtido originalmente por Serre.

No Capítulo 3 tratamos sobre a classe dos grupos analíticos p-ádicos, exibimos diversos exemplos e apresentamos alguns resultados iniciais, culminando na caracterização obtida por Lazard.

No Capítulo 4 abordamos a Teoria de Lie para grupos analíticos p-ádicos, a ferramenta central do método de investigação desta dissertação. Primeiramente tratamos da construção via grupos formais e posteriormente da correspondência de Lazard para grupos p-saturáveis.

No Capítulo 5 falamos sobre desenvolvimentos recentes, como a caracterização de grupos p-saturáveis como grupos admitindo filtrações potentes e a classificação de grupos analíticos pro-p livres-de-torção de dimensão 3. Finalizamos este trabalho com alguns resultados originais: construímos, para todo primo $p > 3$, apresentações para todos os grupos analíticos pro-p livres-de-torção de dimensão quatro e determinamos quais grupos analíticos pro-p livres-de-torção de dimensão até quatro possuem a propriedade CA (centralizadores abelianos).

Capítulo 1

Preliminares

Neste Capítulo colecionamos alguns conceitos e resultados importantes para leitura fluida do trabalho. É assumido que o leitor tenha alguma familiaridade com topologia, medida de Haar e teoria de grupos. Uma leitura dos capítulos 1 e 3 de [Bou71a], do capítulo 7 de [Bou63] e dos doze primeiros capítulos de [Hall59] é mais do que suficiente.

1.1 Limites projetivos

Apresentamos nesta seção o conceito de limite projetivo, que nos será fundamental. O leitor poderá consultar o Capítulo 1 de [RiZa10] para demonstrações dos resultados mencionados.

Seja I um conjunto parcialmente ordenado em que todo par de elementos tem cota superior. Um sistema projetivo de espaços topológicos é uma coleção $\{X_i\}_{i\in I}$ de espaços topológicos indexados por I e uma coleção de aplicações contínuas $\varphi_{ij} : X_i \to X_j$ definidas sempre que $i \geq j$ tais que o diagrama

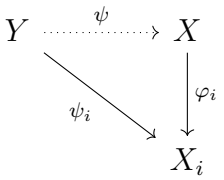
$$\begin{array}{ccc} X_i & \xrightarrow{\varphi_{ik}} & X_k \\ & \searrow^{\varphi_{ij}} & \uparrow{\scriptstyle \varphi_{jk}} \\ & & X_j \end{array}$$

comuta sempre que $i \geq j \geq k$. Denotaremos esse sistema projetivo por $\{X_i, \varphi_{ij}, I\}$. Se Y é um espaço topológico e $\psi_i : Y \to X_i$ são aplicações contínuas definidas para todo i em I tais que sempre que $i \geq j$, o diagrama

$$\begin{array}{ccc} Y & \xrightarrow{\psi_j} & X_j \\ & \searrow^{\psi_i} & \uparrow{\scriptstyle \varphi_{ij}} \\ & & X_i \end{array}$$

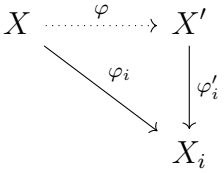
comuta, dizemos que a família de aplicações contínuas $\{\psi_i\}_{i\in I}$ é compatível com o sistema projetivo $\{X_i, \varphi_{ij}, I\}$. Um **limite projetivo** (ou limite inverso) do sistema $\{X_i, \varphi_{ij}, I\}$ é um espaço topológico X munido de aplicações contínuas $\varphi_i : X \to X_i$ possuindo a seguinte propriedade universal: para

todo espaço Y munido de aplicações compatíveis $\{\psi_i\}_{i\in I}$ com $\{X_i, \varphi_{ij}, I\}$, existe uma única aplicação contínua $\psi : Y \to X$ tal que o diagrama



comuta para todo $i \in I$.

Todo sistema projetivo de espaços topológicos possui um único limite no seguinte sentido: se $\{X, \varphi_i\}$ e $\{X', \varphi_i'\}$ são dois limites de $\{X_i, \varphi_{ij}, I\}$, então existe um único homeomorfismo $\varphi : X \to X'$ tal que, para todo $i \in I$, o diagrama



comuta. Costumamos denotar o limite projetivo (ou inverso) de $\{X_i, \varphi_{ij}, I\}$ por $\varprojlim_i X_i$. O espaço

$$X := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i : \varphi_{ij}(x_i) = x_j, \forall\ i \geq j \right\}$$

é o limite projetivo de $\{X_i, \varphi_{ij}, I\}$. Se cada X_i é Hausdorff, então X é fechado em $\prod_{i\in I} X_i$. Em particular, segue-se do teorema de Tychonoff que se cada X_i é compacto e Hausdorff, então X é compacto. Se, além disso, impormos que cada X_i é totalmente desconexo, então X é totalmente desconexo.

Na seção seguinte trataremos de grupos topológicos (mais especificamente de grupos profinitos e pro-p) e observamos de imediato que toda a discussão acima pode ser aplicada para grupos topológicos substituindo "aplicação contínua" por "homomorfismo contínuo" e "homeomorfismo" por "isomorfismo de grupos topológicos".

1.2 Grupos profinitos e pro-p

Um **grupo topológico** é um grupo G munido de uma estrutura de espaço topológico de forma que a multiplicação $m : G \times G \to G$ (em que $G \times G$ tem a topologia produto) e a inversão $i : G \to G$ sejam aplicações contínuas. Um **grupo profinito** é um grupo topológico compacto, Hausdorff e totalmente desconexo. É fácil ver que se G é um grupo profinito, então um subgrupo de G é aberto se, e somente se, é fechado e tem índice finito e que se N é um subgrupo normal fechado de G, então G/N é um grupo profinito com a topologia quociente.

Grupos profinitos aparecem naturalmente como grupos de Galois de extensões galoisianas infinitas munidos da topologia de Krull. Ocorre que se G é um grupo profinito e $\mathcal{U}$ é a coleção dos seus subgrupos normais abertos, então

$$G \cong \varprojlim_{U\in\mathcal{U}} G/U$$

(vide [DDMS99] 1.3). Assim, vemos que todo grupo profinito é um limite projetivo de grupos finitos. Reciprocamente, todo limite projetivo de grupos finitos discretos é um grupo profinito, já que é um subgrupo fechado do produto cartesiano, que, pelo teorema de Tychonoff, é compacto (além de ser Hausdorff e totalmente desconexo).

Um **grupo pro-p** é um limite projetivo de p-grupos finitos discretos, isto é, um grupo profinito tal que todo quociente por um grupo normal aberto é um p-grupo finito. Com um argumento padrão para construções com limite inverso, prova-se que para todo grupo profinito G e para todo primo p, G possui subgrupos pro-p maximais e que quaisquer subgrupos pro-p maximais são conjugados (cf. [RiZa10] 2.3.6).

Um número supernatural é um produto formal $n = \prod_{p \text{ primo}} p^{n_p}$, em que $n \in \mathbb{N} \cup \{\infty\}$. O mínimo múltiplo comum de uma família $(n_i)_{i \in I}$ de números supernaturais é o número supernatural $N = \text{mmc}\{n_i, i \in I\} := \prod_{p \text{ primo}} p^{n_{p,I}}$, em que $n_{p,I} = \max_{i \in I} n_{p,i}$. A **ordem** de um grupo profinito G é definida como

$$|G| := \text{mmc}\{|G/U|, U \in \mathcal{U}\},$$

em que $\mathcal{U}$ é o conjunto de todos os subgrupos normais abertos de G. Notamos que um grupo profinito G é pro-p se, e somente se, sua ordem é igual a p^n, com $n \in \mathbb{N} \cup \{\infty\}$.

Se X é um subconjunto de um grupo profinito G, denotamos por $\langle X \rangle$ a interseção de todos os subgrupos fechados de G contendo X. Equivalentemente, $\langle X \rangle$ é o fecho do subgrupo abstrato gerado por X em G. Dizemos que $\langle X \rangle$ é o subgrupo de G gerado por X.

Um grupo pro-p G é **finitamente gerado** se existe um subconjunto finito X de G que gera G. Uma **apresentação** de um grupo pro-p finitamente gerado é uma sequência exata curta

$$1 \to \langle R^G \rangle \to F(S) \to G \to 1,$$

em que, $F(S)$ é o grupo pro-p livre sobre o conjunto finito S (vide o capítulo 3 de [RiZa10]), R é um subconjunto de $F(S)$ e $R^G = \{g^{-1}rg, r \in R, g \in G\}$ (de forma que $\langle R^G \rangle$ é a interseção de todos os subgrupos normais fechados de $F(S)$ contendo R). Denotamos a apresentação acima por $\langle S \mid R \rangle$ e escrevemos $G = \langle S \mid R \rangle$. Dizemos que a apresentação é finita se R é finito.

O **subgrupo de Frattini** de um grupo profinito G é a interseção de todos os seus subgrupos fechados maximais. Se w é uma palavra (isto é, um elemento de um grupo livre abstrato de posto finito), então o **subgrupo verbal** $w(G)$ de um grupo profinito G é o subgrupo de G gerado (como grupo profinito) por todos os valores que w assume em G. Por exemplo, se $n \in \mathbb{N}$ e $w = x^n$, então $G^n := w(G) = \langle g^n, g \in G \rangle$. Já se $w = [\dots[x_1, x_2], \dots x_n]$, então $\gamma_n(G) := w(G) = \langle [\dots[x_1, x_2], \dots, x_n], x_i \in G \rangle$. Chamamos os subgrupos $\gamma_n(G)$ de termos da **série central inferior** de G. Observamos que os subgrupos verbais de G como grupo profinito diferem dos subgrupos verbais de G como grupo abstrato (o primeiro é o fecho do segundo). O leitor deverá sempre assumir que todos os subgrupos mencionados de um grupo profinito são fechados, bem como que todo homomorfismo entre grupos profinitos é contínuo. Se H e N são subgrupos normais fechados de um grupo profinito G e j é um inteiro positivo, denotamos por $[H,_j N]$ o subgrupo fechado gerado por elementos da forma $[\dots[h, n_1], \dots, n_j]$, em que $h \in H$ e $n_i \in N$ para $i = 1, \dots, j$. No caso em que $j = 1$, denotamos $[H,_1 N]$ simplesmente por $[H, N]$.

1.3 Corpos completos e os números p-ádicos

Seja k um corpo. Um **valor absoluto** em k é uma função $|\cdot| : k \to [0, \infty)$ tal que

(i) $|x| = 0$ se, e somente se $x = 0$;

(ii) $|xy| = |x||y|$;

(iii) $|x + y| \leq |x| + |y|$.

Um exemplo conhecido de valor absoluto é o módulo em $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. Se k é um corpo qualquer, podemos definir um valor absoluto em k por $|0| = 0$ e $|x| = 1$ se $x \neq 0$. Esse valor absoluto é dito discreto.

Observe que definindo $d : k \times k \to [0, \infty)$ por $d(x, y) = |x - y|$, vemos que (k, d) é um espaço métrico, possuindo, assim, uma topologia natural. Nesta topologia, as operações de soma e multiplicação em k são contínuas. Note que um valor absoluto discreto induz a topologia discreta, justificando a nomenclatura.

Um valor absoluto em um corpo k é dito **ultramétrico** se satisfaz

(iii') $|x - y| \leq \max\{|x|, |y|\}$.

É claro que (iii') implica (iii). Note que se $\{x_n\}_{n\in\mathbb{N}}$ é uma sequência de elementos em um corpo ultramétrico, então a série $\sum x_n$ converge se, e somente se, x_n converge para 0.

Fixe um primo p e considere o seguinte valor absoluto em $\mathbb{Q}$: se $x = 0$, tome $|x| = 0$ e se $x \neq 0$, escreva $x = p^m \dfrac{a}{b}$ com $(a, p) = (b, p) = 1$ e defina $|x| = p^{-m}$ (definimos também, de maneira auxiliar, a **valoração p-ádica** de x como $v_p(x) = m$). É fácil verificar que isso é de fato um valor absoluto e, além disso, é ultramétrico.

Então $\mathbb{Q}$ é um espaço métrico em relação a esse valor absoluto e, portanto, podemos tomar seu completamento, que denotamos por $\mathbb{Q}_p$ para exibir a dependência do primo p. As operações de soma e multiplicação em $\mathbb{Q}$ estendem-se por continuidade para $\mathbb{Q}_p$ e tornam este um corpo, o qual, assim como $\mathbb{R}$, é completo como espaço métrico e possui $\mathbb{Q}$ como subconjunto denso. O corpo $\mathbb{Q}_p$ é chamado corpo dos **números p-ádicos**.

Se k é um corpo ultramétrico, então definimos $\mathcal{O}_k$ como o conjunto dos elementos de valor absoluto menor do que ou igual a 1, que, devido à desigualdade ultramétrica, é um subanel de k. O conjunto $\mathfrak{m}$ dos elementos de k com valor absoluto estritamente menor do que 1 é, por sua vez, um ideal maximal de $\mathcal{O}_k$. O corpo $\mathcal{O}_k/\mathfrak{m}$ é dito corpo residual de k.

Se $k = \mathbb{Q}_p$, denotamos $\mathcal{O}_k$ por $\mathbb{Z}_p$. Formalmente, $\mathbb{Z}_p$ consiste em classes de equivalência de sequências de Cauchy em $\mathbb{Z}$ em relação ao valor absoluto p-ádico. Como o valor absoluto p-ádico é ultramétrico, os conjuntos $p^n\mathbb{Z}_p = \{p^n x, x \in \mathbb{Z}_p\}$ são subgrupos abertos e fechados do grupo aditivo $\mathbb{Q}_p$ que possuem interseção igual a 0. Isso mostra que $\mathbb{Q}_p$ é totalmente desconexo. Mais do que isso, $p^n\mathbb{Z}_p$ é um sistema fundamental de vizinhanças de 0 em $\mathbb{Z}_p$ e, assim, segue-se que $\mathbb{Z}_p$ é compacto. Portanto o grupo aditivo do anel $\mathbb{Z}_p$ é profinito. Podemos ver que $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ e, portanto, obtemos outra caracterização de $\mathbb{Z}_p$:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

Notemos que o corpo residual de $\mathbb{Q}_p$ é o corpo finito $\mathbb{F}_p$ de p elementos. Chamamos $\mathbb{Z}_p$ de grupo (ou anel) dos **inteiros p-ádicos**

1.4 Funções analíticas

Fixemos um corpo k completo com relação a um valor absoluto não discreto e consideramos o anel $k[[X_1, \ldots, X_n]]$ das séries de potências formais nas indeterminadas $X_1, \ldots, X_n$. Sejam $r = (r_1, \ldots, r_n) \in \mathbb{R}^n, r_i > 0$ e $x = (x_1, \ldots, x_n) \in k^n$. Então denotamos por $P(r)(x) = \{y = (y_1, \ldots, y_n) \in k^n, |x_i - y_i| \leq r_i, \forall\, i\}$ o polidisco de raio r centrado em x e por $P_0(r)(x) = \{y = (y_1, \ldots, y_n) \in k^n, |x_i - y_i| < r_i, \forall\, i\}$ o polidisco estrito de raio r centrado em x. Se $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ é um multi-índice e $s = (s_1, \ldots, s_n) \in \mathbb{R}^n$, denotamos o produto $s_1^{\alpha_1} \ldots s_n^{\alpha_n}$ por s^α e a soma $\alpha_1 + \cdots + \alpha_n$ por $|\alpha|$. Além disso, denotamos por X^α o produto formal $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$.

Uma série de potências $f = \sum c_\alpha X^\alpha$ é dita **convergente** em $P(r)(0)$ se a série $\sum |c_\alpha| r^\alpha$ converge em $\mathbb{R}$. A série f é dita convergente em $P_0(r)(0)$ se f converge em $P(r')(0)$ para todo $r' < r$. Se U é um aberto de k^n, uma função $\phi : U \to k$ é dita **analítica** se para todo $x \in U$, existem $f \in k[[X_1, \ldots, X_n]]$ e $r \in \mathbb{R}^n_{>0}$ tais que $P_0(r)(x) \subset U$, f converge em $P_0(r)(x)$ e para todo $h \in P_0(r)(0)$, tem-se $\phi(x+h) = f(h)$. Uma aplicação $\phi : U \to k^m$ de um aberto U de k^n é analítica se $\phi = (\phi_1, \ldots, \phi_m)$ com cada ϕ_j analítica. A composição de aplicações analíticas é analítica (vide [Ser00], segundo teorema de II.II).

Seja $f : U \to V$ uma função de um aberto de k^n para um aberto de k^m. f é dita **diferenciável** em $x \in U$ se existe uma transformação linear $Df(x) : k^n \to k^m$ tal que

$$\lim_{|h| \to 0} \frac{|f(x+h) - f(x) - Df(x)h|}{|h|} = 0.$$

Funções analíticas são diferenciáveis e, além disso, vale o teorema da função inversa: se $f : U \to k^n$, em que U é um aberto de k^n, é uma função analítica tal que $Df(x) : k^n \to k^m$ é um isomorfismo linear, então existe uma vizinhança aberta U_x de x em U tal que $f|_{U_x} : U_x \to f(U_x)$ é um isomorfismo analítico, isto é, $f|_{U_x}$ admite uma inversa analítica.

1.5 Álgebras de Lie

Seja R um anel comutativo com unidade. Uma ***R*-álgebra de Lie** é um R-módulo L munido de uma aplicação R-bilinear (colchete de Lie) $[\cdot, \cdot] : L \times L \to L$ satisfazendo

(i) $[x, x] = 0$, para qualquer $x \in L$;

(ii) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$, para quaisquer $x, y, z \in L$.

Por conveniência, chamamos uma $\mathbb{Z}_p$-álgebra de Lie que é um $\mathbb{Z}_p$-módulo livre de posto finito de **$\mathbb{Z}_p$-reticulado de Lie**.

É claro que todo R-módulo M possui uma estrutura de R-álgebra de Lie com colchete dado por $[x, x] = 0$ para todo $x \in M$. Tais R-álgebras de Lie são ditas **abelianas**. Construímos agora um exemplo mais interessante: se A é uma R-álgebra associativa, então tomando $[x, y] = xy - yx, x, y, \in L$, é fácil ver que $(A, [\cdot, \cdot])$ é uma R-álgebra de Lie. Se M é um R-módulo livre de posto n, denotamos por $\mathrm{End}(M)$ a R-álgebra associativa dos endomorfismos R-lineares de M. Induzimos uma estrutura de R-álgebra de Lie em $\mathrm{End}(M)$ pela construção mencionada, obtendo uma R-álgebra de Lie, denotada por $\mathfrak{gl}_n(R)$.

Até o final da seção, toda álgebra de Lie será sobre um anel fixado R. Um ideal de uma álgebra de Lie L é uma subálgebra de Lie I (isto é, um submódulo de L fechado para operação $[\cdot, \cdot]$) tal que para todo $x \in L, y \in I$, $[x, y] \in I$. Se I é um **ideal** de uma álgebra de Lie L, podemos construir uma

álgebra de Lie no R-módulo quociente L/I tomando $[x+I, y+I] = [x,y]+I$. Um **homomorfismo** de álgebras de Lie é uma aplicação linear $\varphi : L \to L'$ satisfazendo $\varphi([x,y]) = [\varphi(x), \varphi(y)]$ para quaisquer $x, y \in L$. Uma **derivação** de uma álgebra de Lie L é uma aplicação linear $D : L \to L$ satisfazendo $D([x,y]) = [D(x), y] + [x, D(y)]$. Se L é uma álgebra de Lie, o conjunto $\operatorname{Der} L$ de todas as derivações de L tem uma estrutura natural de R-módulo. Além disso, tomando $[D, D'] = DD' - D'D$, o R-módulo $\operatorname{Der} L$ se torna uma álgebra de Lie, chamada de **álgebra de Lie de derivações**. Basta verificar que $[D, D']$ é, de fato, uma derivação de L, o que se checa com uma simples computação.

Se $\mathfrak{g}$ é uma álgebra de Lie e $x \in \mathfrak{g}$, definimos $\operatorname{ad} x : \mathfrak{g} \to \mathfrak{g}, y \mapsto [x,y]$, de forma que para todo $x \in \mathfrak{g}$, $\operatorname{ad} x$ é uma derivação de $\mathfrak{g}$. Definimos um homomorfismo de álgebras de Lie $\operatorname{ad} : \mathfrak{g} \to \operatorname{Der} \mathfrak{g}, x \mapsto \operatorname{ad} x$. Derivações na imagem de ad são ditas derivações **internas**.

Se $\mathfrak{g}$ e $\mathfrak{h}$ são álgebras de Lie e $\varphi : \mathfrak{h} \to \operatorname{Der} \mathfrak{g}$ é um homomorfismo, podemos construir uma álgebra de Lie $\mathfrak{g} \rtimes_\varphi \mathfrak{h}$ no R-módulo $\mathfrak{g} \oplus \mathfrak{h}$ com colchete dado por

$$[(x,y),(z,w)] = ([x,z] + \varphi(y)z - \varphi(w)x, [y,w]).$$

Essa construção é chamada **produto semidireto** e induz uma sequência exata curta de álgebras de Lie

$$0 \to \mathfrak{g} \to \mathfrak{g} \rtimes_\varphi \mathfrak{h} \to \mathfrak{h} \to 0.$$

Note que $\mathfrak{g}$ é um ideal de $\mathfrak{g} \rtimes_\varphi \mathfrak{h}$ e que $(\mathfrak{g} \rtimes_\varphi \mathfrak{h})/\mathfrak{g} = \mathfrak{h}$.

Se $\mathfrak{g}$ é uma álgebra de Lie e I e J são ideais de $\mathfrak{g}$, denotamos por $[I,J]$ a menor subálgebra de $\mathfrak{g}$ contendo todos os elementos da forma $[x,y], x \in I, y \in J$. É claro que $[I,J]$ é um ideal de $\mathfrak{g}$ e que $\mathfrak{g}/[\mathfrak{g},\mathfrak{g}]$ é uma álgebra de Lie abeliana. A **série central inferior** de $\mathfrak{g}$ é uma sequência descendente de ideais de $\mathfrak{g}$ dada por $\gamma_1(\mathfrak{g}) := \mathfrak{g}$ e $\gamma_{i+1}(\mathfrak{g}) := [\mathfrak{g}, \gamma_i(\mathfrak{g})]$. Uma álgebra de Lie $\mathfrak{g}$ é dita **nilpotente** se existe $n \in \mathbb{N}$ tal que $\gamma_n(\mathfrak{g}) = 0$ e sua classe de nilpotência é o menor $j \in \mathbb{N}$ tal que $\gamma_{j+1}(\mathfrak{g}) = 0$. Note que as álgebras de Lie nilpotentes de classe 1 são justamente as abelianas.

Definimos também a série derivada, dada por $D_1(\mathfrak{g}) := \mathfrak{g}$ e $D_{j+1}(\mathfrak{g}) := [D_j(\mathfrak{g}), D_j(\mathfrak{g})]$. Dizemos que $\mathfrak{g}$ é **solúvel** se existe $n \in \mathbb{N}$ tal que $D_n(\mathfrak{g}) = 0$ e seu comprimento derivado é o menor $j \in \mathbb{N}$ tal que $D_{j+1}(\mathfrak{g}) = 0$. É claro que toda álgebra de Lie nilpotente é solúvel, mas, por outro lado, nem toda álgebra de Lie solúvel é nilpotente.

Uma extensão de uma álgebra de Lie $\mathfrak{h}$ por uma álgebra de Lie $\mathfrak{n}$ é uma álgebra de Lie $\mathfrak{g}$ tal que exista uma sequência exata curta

$$0 \to \mathfrak{n} \to \mathfrak{g} \to \mathfrak{h} \to 0.$$

Note que uma extensão de uma álgebra de Lie solúvel por outra álgebra de Lie solúvel é novamente solúvel. Em particular, se $\mathfrak{a}, \mathfrak{b}$ são ideais solúveis de uma álgebra de Lie $\mathfrak{g}$, a soma $\mathfrak{a} + \mathfrak{b}$ (o ideal consistindo de elementos da forma $a+b$, com $a \in \mathfrak{a}$ e $b \in \mathfrak{b}$) é solúvel, já que existe uma sequência exata curta

$$0 \to \mathfrak{a} \to \mathfrak{a} + \mathfrak{b} \to \mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b}) \to 0.$$

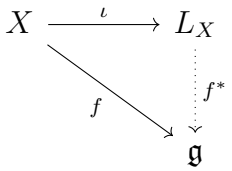
Segue-se que se $\mathfrak{g}$ tem dimensão finita, a soma de todos seus ideais solúveis é um ideal solúvel, dito radical solúvel de $\mathfrak{g}$. Uma álgebra de Lie é dita **semissimples** se seu radical solúvel é zero, isto é, se não possui ideais solúveis.

Seja $\mathfrak{g}$ uma k-álgebra de Lie de dimensão finita, em que k é um corpo de característica zero, e $\mathfrak{r}$ seu radical solúvel. Então pelo *Teorema da decomposição de Levi* (vide [Ser00], I.VI.4.1), a sequência exata curta

$$0 \to \mathfrak{r} \to \mathfrak{g} \to \mathfrak{g}/\mathfrak{r} \to 0$$

cinde, isto é, existe uma subálgebra $\mathfrak{h}$ de $\mathfrak{g}$ tal que $\mathfrak{g}$ é um produto semidireto de $\mathfrak{r}$ por $\mathfrak{h}$. Além disso, $\mathfrak{h}$ é semissimples.

Até o final da seção todas as álgebras de Lie são sobre uma $\mathbb{Q}$-álgebra fixada k. Uma **álgebra de Lie livre** sobre um conjunto X é uma álgebra de Lie L_X munida de uma função $\iota : X \to L_X$ possuindo a seguinte propriedade universal: para toda função $f : X \to \mathfrak{g}$, em que $\mathfrak{g}$ é uma álgebra de Lie, existe um único homomorfismo $f^* : L_X \to \mathfrak{g}$ tal que o diagrama



comuta. Demonstrações para as afirmações que faremos até o final da seção podem ser encontradas no Capítulo IV da Parte I de [Ser00]. Por um argumento padrão para propriedades universais, vê-se que se existir uma álgebra de Lie livre sobre um conjunto X, é unica a menos de isomorfismo. Ocorre que álgebras de Lie livres sempre existem e têm uma estrutura graduada no seguinte sentido: existem submódulos L_X^n de L_X tais que $L_X = \bigoplus_{n\in\mathbb{N}} L_X^n$ e $[L_X^n, L_X^m] \subseteq L_X^{n+m}$. Além disso, cada L_X^n (e, consequentemente, L_X) é um k-módulo livre. Definimos o completamento de L_X por $\widehat{L_X} := \prod_{n\in\mathbb{N}} L_X^n$.

Definimos também para um conjunto X a k-álgebra associativa livre sobre X, que é a k-álgebra associativa Ass_X com a propriedade universal análoga à possuída pela k-álgebra de Lie livre (ou pelo grupo livre). Sua descrição, porém, é mais simples. Ass_X é a álgebra tensorial sobre o k-módulo livre de base X, isto é:

$$\mathrm{Ass}_X := \bigoplus_{n\in\mathbb{N}} \bigotimes_{i=1}^{n} k^X,$$

em que a multiplicação é $\otimes$, definida estendendo a multiplicação natural $(v_1 \otimes \cdots \otimes v_k) \otimes (w_1 \otimes \cdots \otimes w_l) = v_1 \otimes \cdots \otimes v_k \otimes w_1 \otimes \cdots \otimes w_l$. Ass_X também possui uma estrutura de álgebra associativa graduada, isto é, $\mathrm{Ass}_X = \bigoplus_{n\in\mathbb{N}} T_X^n \left(T_X^n = \bigotimes_{i=1}^{n} k^X\right)$ tal que $T_X^i \otimes T_X^j \subseteq T_X^{i+j}$. Definimos o completamento de Ass_X por $\widehat{\mathrm{Ass}_X} := \prod_{n\in\mathbb{N}} T_X^n$. Desta forma, $\widehat{L}_X$ está canonicamente imerso em $\widehat{\mathrm{Ass}_X}$, de modo que a inclusão é um homomorfismo de Lie em relação à estrutura natural de álgebra de Lie da álgebra associativa $\widehat{\mathrm{Ass}_X}$.

Sendo $\hat{\mathfrak{m}}$ o ideal de $\widehat{\mathrm{Ass}_X}$ gerado por X (identificando X com suas imagens em $L_X, \widehat{L_X}, \mathrm{Ass}_X$ e $\widehat{\mathrm{Ass}_X}$), definimos as aplicações

$$\exp : \hat{\mathfrak{m}} \to 1 + \hat{\mathfrak{m}}, x \mapsto \sum_{n\in\mathbb{N}} \frac{x^n}{n!},$$

$$\log : 1 + \hat{\mathfrak{m}} \to \hat{\mathfrak{m}}, 1 + x \mapsto \sum_{n\geq 1} \frac{(-1)^{n+1} x^n}{n}.$$

Então $\exp \circ \log = \mathrm{id}$ e $\log \circ \exp = \mathrm{id}$. Note que $L_X \subset \hat{\mathfrak{m}}$.

Seja $X = \{x, y\}$ um conjunto com dois elementos. Então $\log(\exp(x)\exp(y)) \in \widehat{L_X}$ (vide [Ser00] I.IV.7.4). Além disso, temos uma expressão explícita para $z = \log(\exp(x)\exp(y))$. Escrevemos $z = \sum_{n=1}^{\infty} z_n$ com $z_n \in L_X^n$. Então:

$$z_n = \frac{1}{n} \sum_{p+q=n} (z'_{p,q} + z''_{p,q}),$$

em que

$$z'_{p,q} = \sum_{\substack{p_1+\cdots+p_m=p \\ q_1+\cdots+q_{m-1}=q-1 \\ p_i+q_i\geq 1 \\ p_m\geq 1}} \frac{(-1)^{m+1}}{m} \frac{\operatorname{ad}(x)^{p_1}\ \operatorname{ad}(y)^{q_1} \ldots \operatorname{ad}(x)^{p_m}(y)}{p_1!\, q_1! \ldots p_m!},$$

$$z''_{p,q} = \sum_{\substack{p_1+\cdots+p_{m-1}=p-1 \\ q_1+\cdots+q_{m-1}=q \\ p_i+q_i\geq 1}} \frac{(-1)^{m+1}}{m} \frac{\operatorname{ad}(x)^{p_1}\ \operatorname{ad}(y)^{q_1} \cdots \operatorname{ad}(y)^{q_{m-1}}(x)}{p_1!\, q_1! \cdots q_{m-1}!}.$$

Capítulo 2

Variedades Analíticas

O estudo das variedades diferenciais reais é central em áreas como Geometria, Análise e Topologia Algébrica. Uma variedade real é um espaço topológico que se comporta localmente como o espaço euclideano, conceito que generaliza as noções intuitivas de superfícies para dimensões maiores. Em geral, estamos acostumados com as variedades reais ou complexas — essas que parecem com o espaço euclideano.

Entretanto $\mathbb{R}$ e $\mathbb{C}$ não são os únicos corpos com rica estrutura topológica (completude). Assim, podemos pensar em variedades sobre outros corpos, cujas propriedades são substancialmente diferentes das variedades reais ou complexas.

O objetivo deste capítulo é tratar desses objetos que, embora compartilhem de definições iguais às variedades usuais amplamente estudadas sob o viés geométrico e topológico, possuem propriedades e estruturas diferentes. Com efeito, variedades p-ádicas têm estrutura muito simples: veremos no decorrer do capítulo que variedades paracompactas sobre um corpo localmente compacto e ultramétrico são uniões disjuntas de bolas. Neste trabalho, nosso interesse nas variedades analíticas é voltado para fundamentar o estudo, nos próximos capítulos, dos grupos analíticos p-ádicos, nosso objeto de principal interesse.

O capítulo está dividido em duas seções. A primeira trata de aspectos gerais de variedades analíticas (sobre um corpo qualquer), em que tratamos das definições iniciais, dos espaços e das aplicações tangentes, de imersões e submersões, de formas diferenciais e de integração. Já a segunda trata da mencionada classificação das variedades p-ádicas, com duas demonstrações de um Teorema de Jean-Pierre Serre (vide [Ser65] e [Ser00]) sobre variedades compactas. As principais referências deste capítulo são [Ser00] e [Igu00], além do artigo mencionado.

2.1 Noções básicas

Seja k um corpo completo em relação a um valor absoluto não trivial. Se X é um espaço topológico qualquer, uma **carta** c de X é uma tripla (U, ϕ, n), em que U é um aberto de X, n é um inteiro não negativo e $\phi : U \to k^n$ é um homeomorfismo sobre um aberto de k^n. Chamamos n de dimensão da carta c. É claro que se V é um aberto de U, então a tripla $c\,|_V = (V, \phi\,|_V, n)$ é também uma carta de X.

Duas cartas $c = (U, \phi, n)$ e $c' = (U', \phi', n')$ são ditas **compatíveis** se, tomando-se $V = U \cap U'$, as aplicações $\phi' \circ \phi^{-1} : \phi(V) \to \phi'(V)$ e $\phi \circ \phi'^{-1} : \phi'(V) \to \phi(V)$ são aplicações analíticas entre abertos de

k^n. Note que a compatibilidade de cartas é transitiva e que se V é não vazio, então $n = n'$. Para cada $x \in X$, denotamos por $\dim_x X$ a dimensão de uma — e, portanto, de qualquer — carta $c = (U, \phi, n)$ tal que $x \in U$.

Uma família de cartas é dita uma cobertura para X se a união de seus respectivos abertos é igual a X. Dizemos que uma cobertura A por cartas de X é um **atlas** se quaisquer duas cartas de A são compatíveis. Um atlas A é dito maximal se qualquer carta de X compatível com A pertence a A. Uma estrutura de **variedade analítica** em um espaço topológico X é uma escolha de um atlas maximal em X.

Os exemplos mais básicos de variedades analíticas são os subconjuntos abertos de k^n (e, mais geralmente, subconjuntos abertos de outras variedades), munidos de um atlas maximal contendo a inclusão. Por exemplo, $\mathbb{Z}_p^n$ tem estrutura de variedade analítica quando $k = \mathbb{Q}_p$. Exemplos clássicos de variedades sobre $\mathbb{R}$ são curvas e superfícies, contudo estamos interessados aqui no caso ultramétrico e, principalmente, no caso p-ádico. Veremos, nas seções seguintes, que no caso p-ádico, toda variedade analítica paracompacta é isomorfa, como variedade analítica, a uma união disjunta de cópias de $\mathbb{Z}_p^n$.

Podemos construir outras variedades a partir de variedades já conhecidas. Por exemplo, podemos tomar uniões disjuntas (coprodutos) de variedades, com a estrutura natural, bem como produtos cartesianos finitos (produto), também com a estrutura natural. Além disso, se um espaço topológico X admite uma cobertura aberta por variedades analíticas $\left(X = \bigcup_{i \in I} U_i\right)$, de forma que as estruturas analíticas em $U_i \cap U_j$ herdadas por U_i e U_j coincidam, para quaisquer $i, j \in I$, X possui uma única estrutura de variedade analítica induzida por meio da "colagem" das estruturas de cada U_i.

Se X e Y são duas variedades analíticas, uma aplicação contínua $f : X \to Y$ é um **morfismo** (ou simplesmnte uma aplicação analítica entre variedades) se, sendo A e B os atlas relativos a X e Y, respectivamente, para quaisquer cartas $c = (U, \phi, m) \in A$ e $d = (V, \psi, n) \in B$, então, tomando $W = U \cap f^{-1}V$, a composição

$$\phi W \xrightarrow{\phi^{-1}} U \xrightarrow{f} V \xrightarrow{\psi} \psi V$$

é analítica. Assim, um morfismo é uma aplicação contínua entre variedades que, em coordenadas locais, é dada por séries de potência (a aplicação $\psi \circ f \circ \phi^{-1}$ é uma n-upla de funções analíticas em m variáveis). Como consequência direta da regra da cadeia para aplicações analíticas, a composição de morfismos é um morfismo. Note que a aplicação identidade é um morfismo de variedades. Assim, estabelecemos a categoria das variedades analíticas sobre um corpo fixo k.

2.1.1 Espaço tangente

Seja X uma variedade analítica sobre k e x um ponto de X. Considere o conjunto $\mathcal{U}_x$ dos pares (U, f) em que U é um aberto de X contendo x e $f : U \to k$ é uma função analítica (um morfismo). Consideremos a relação de equivalência $\sim$ em $\mathcal{U}_x$ dada por $(U, f) \sim (V, g)$ se existe um aberto W contido em $U \cap V$, contendo x e de forma que $f|_W = g|_W$. Chamamos de **espiga** (ou anel local) de x o conjunto quociente $\mathcal{O}_{X,x} := \mathcal{U}_x / \sim$. A espiga de x tem estrutura natural de anel comutativo com unidade: a soma da classe de (U, f) pela classe de (V, g) é a classe de $(U \cap V, f + g)$; a multiplicação é análoga à soma; e a unidade é a classe de $(X, 1)$, em que $1(x) = 1$ para todo $x \in X$. A espiga de x é um anel local (justificando o nome alternativo), cujo ideal maximal, denotado por, $\mathfrak{m}_x$ é composto pelas classes de funções que se anulam em x. De fato, o conjunto das funções que não se anulam em x é precisamente o conjunto dos

elementos invertíveis da espiga: se uma função f não se anula em x, por sua continuidade, não se anula em uma vizinhança de x e, portanto, em uma vizinhança de x podemos definir a função $1/f$. Note que o corpo residual $\mathcal{O}_{X,x}/\mathfrak{m}_x$ é k (a imagem da classe de uma função f no corpo residual é $f(x)$). Além disso, cada elemento de k define um elemento na espiga (a função constante respectiva) e, portanto, a sequência exata curta $0 \to \mathfrak{m}_x \to \mathcal{O}_{X,x} \to k \to 0$ de $\mathcal{O}_{X,x}$-módulos cinde e podemos identificar $\mathcal{O}_{X,x}$ com a soma direta $k \oplus \mathfrak{m}_x$.

Lema (L.2.1). Seja (U, ϕ, n) uma carta em x tal que $\phi(x) = 0$. Então $\overline{\phi} : \mathcal{O}_{k^n,0} \to \mathcal{O}_{X,x}, f \mapsto f \circ \phi$ é um isomorfismo satisfazendo $\overline{\phi}(\mathfrak{m}_0) = \mathfrak{m}_x$. Além disso, $\mathcal{O}_{k^n,0}$ é isomorfo ao anel das séries de potências convergentes em n variáveis.

Definimos o **espaço tangente** de X no ponto x, denotado por T_xX, como o espaço das derivações $v : \mathcal{O}_{X,x} \to k$, isto é, dos funcionais lineares v de $\mathcal{O}_{X,x}$ satisfazendo $v(fg) = v(f)g(x) + v(g)f(x)$. O dual de T_xX, denotado por T_x^*X, é chamado **espaço cotangente** de X em x. O espaço tangente pode ser identificado com o espaço vetorial dual $(\mathfrak{m}_x/\mathfrak{m}_x^2)^*$. De fato, se $v \in (\mathfrak{m}_x/\mathfrak{m}_x^2)^*$, v se estende forma linear em $\mathfrak{m}_x$ que se anula em $\mathfrak{m}_x^2$. Estendendo novamente v a um funcional linear da espiga $\mathcal{O}_{X,x} = k \oplus \mathfrak{m}_x$, declarando $v = 0$ em k, obtemos que v é uma derivação em $\mathcal{O}_{X,x}$. De fato, é k-linear e resta-nos checar que para quaisquer $f, g \in \mathcal{O}_{X,x}$, vale que $v(fg) = v(f)g(x) + f(x)v(g)$. Sendo tal equação linear tanto em f quanto em g, é suficiente considerarmos três casos:

1. $f, g \in k$: ambos os lados da equação são zero;
2. $f, g \in \mathfrak{m}_x$: ambos os lados da equação são zero;
3. $f \in k, g \in \mathfrak{m}_x$: sendo $v = 0$ em k, pela linearidade, $v(fg) = f(x)v(g) = f(x)v(g) + v(f)g(x)$.

Por outro lado, dada uma derivação $v : \mathcal{O}_{X,x} \to k$, é imediato que v é zero em k e em $\mathfrak{m}_x^2$. Consequentemente, apenas um funcional linear $\mathfrak{m}_x/\mathfrak{m}_x^2$ pode definir v por meio da construção acima.

Outra caracterização do espaço tangente (mais vinculada à noção usual para variedades diferenciáveis) é como classes de tangência de curvas em x (vide [Ser00], 2.3.8).

Se $f \in \mathcal{O}_{X,x}$, a imagem de $f - f(x)$ em $\mathfrak{m}_x/\mathfrak{m}_x^2 = T_x^*X$ é dita diferencial de f em x e denotada por $(df)_x$. Se $\phi : X \to Y$ é um morfismo de variedades que leva x em y, definimos uma aplicação $T_x^*\phi : T_y^*Y \to T_x^*X$ por $T_x^*\phi(df_y) = d(f \circ \phi)_x$, para todo $f \in \mathcal{O}_{X,x}$. A aplicação transposta de $T_x^*\phi$, $T_x\phi : T_xX \to T_yY$ é dita **aplicação tangente** de ϕ em x. Notemos que se $f : X \to k$ é uma função analítica, então $T_xf = df_x$.

Sendo (U, ϕ, n) uma carta em X, com $\phi(x) = (x_1, \ldots, x_n)$, consideremos as aplicações $x_i : U \to k$, $x \mapsto x_i$. As respectivas aplicações tangentes, denotadas por dx_i, constituem uma base do espaço cotangente T_x^*X.

Assim, estabelecemos um funtor covariante entre a categoria das variedades analíticas com ponto distinguido e a categoria dos espaços k-vetoriais de dimensão finita: associamos para cada variedade (X, x) o espaço tangente T_xX e a cada morfismo $\phi : (X, x) \to (Y, y)$ (satisfazendo $\phi(x) = y$), associamos $T_x\phi : T_xX \to T_yY$. Aqui, a funtorialidade é consequência direta da regra da cadeia.

O Teorema abaixo é consequência imediata do Teorema da Função Inversa para funções analíticas em k^n.

Teorema (T.2.2) (da Função Inversa). *Seja $\phi : X \to Y$ um morfismo de variedades satisfazendo $\phi(x) = y$. Então ϕ é um isomorfismo local em x se, e somente se, $T_x\phi$ é um isomorfismo linear.*

2.1.2 Um pouco de topologia diferencial

Sejam $\phi_i : X_i \to Y_i$ $(i = 1, 2)$ morfismos tais que $\phi_i(x_i) = y_i$. Dizemos que $(X_1, Y_1, x_1, y_1, \phi)$ é localmente $(X_2, Y_2, x_2, y_2, \phi_2)$ se existem vizinhanças abertas U_i de x_i em X_i e V_i de y_i em Y_i e isomorfismos analíticos $g : U_1 \to U_2, h : V_1 \to V_2$ tais que $\phi_i(U_i) \subset V_i$, $\phi_i(x_i) = y_i$ e que o diagrama abaixo comuta.

$$\begin{array}{ccc} U_1 & \xrightarrow{\phi_1} & V_1 \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ U_2 & \xrightarrow{\phi_2} & V_2 \end{array}$$

Proposição (P.2.3). Se $\phi : X \to Y$ é um morfismo entre variedades tal que $\phi(x) = y$, $\dim_x X = m$ e $\dim_y Y = n$, são equivalentes:

(1) $T_x\phi$ é injetivo;

(2) Existem vizinhanças abertas U de x em X, V de y em Y e W de 0 em k^{n-m}, um isomorfismo de variedades $\psi : V \to U \times W$ tais que $\phi(U) \subset V$ e, sendo $\iota : U \to U \times W$ a inclusão da primeira coordenada, $\iota(z) = \psi \circ \phi(z)$, para todo $z \in U$;

(3) (X, Y, x, y, ϕ) é localmente uma aplicação linear injetora entre espaços vetoriais;

(4) Existem sistemas de coordenadas $\{f_i\}$ em x e $\{g_j\}$ em y tais que $f_i = g_i \circ \phi$ se $i \leq m$ e $0 = g_j \circ \phi$ se $m + 1 \leq j \leq n$;

(5) Existem vizinhanças abertas U de x em X e V de y em Y e um morfismo $\sigma : V \to U$ tal que $\phi(U) \subset V$ e $\sigma \circ \phi = \mathrm{id}_U$.

Nesse caso dizemos que ϕ é uma **imersão** em x.

Demonstração: (1) $\implies$ (2) Sendo a questão local, assumimos que Y é um aberto de k^n, $\phi(x) = 0$ e $\operatorname{Im} T_x\phi = k^m \times \{0\} \subset k^m \times k^{n-m} = k^n$. Seja $W = \{0\} \times k^{n-m}$ e defina $\phi' : X \times W \to Y$ por $\phi'(x, w) = \phi(x) + w$. Pelo teorema da função inversa, ϕ' é um isomorfismo local. Refinando os conjuntos X, Y, W, podemos assumir que ϕ' é um isomorfismo. Tomando $\psi = \phi'^{-1}$, o resultado segue.

(2) $\implies$ (3) Transportando o problema para as cartas, podemos assumir que U é um aberto de k^m, V é um aberto de k^m e que $x, y = 0$. Então ι é uma aplicação linear injetora e, sendo ψ um isomorfismo de variedades, segue-se que ϕ é localmente ι;

(3) $\implies$ (4) Se ϕ é localmente uma aplicação linear L, basta escolher bases de k^n e k^m de forma que $L : k^m \to k^m \times k^{n-m} = k^n$ é a inclusão na primeira coordenada;

(4) $\implies$ (5) Se (f, U, m) e (g, V, n) são cartas de X e Y em x e y, respectivamente, obtidas pelos sistemas de coordenadas $\{f_i\}$ e $\{g_j\}$, de forma que $\phi(U) \subset V$, defina $\sigma = f^{-1} \circ g$. Então $\sigma \circ \phi = f^{-1} \circ g \circ \phi = \mathrm{Id}_U$;

(5) $\implies$ (1) Como $\sigma \circ \phi = \mathrm{Id}_U$, pela regra da cadeia, $T_y\sigma \circ T_x\phi = \mathrm{Id}_{T_xX}$. Logo $T_x\phi$ é injetivo. ■

Proposição (P.2.4). Se $\phi : X \to Y$ é um morfismo entre variedades tal que $\phi(x) = y$, $\dim_x X = m$ e $\dim_y Y = n$, são equivalentes:

(1) $T_x\phi$ é sobrejetivo;

(2) Existem vizinhanças abertas U de x em X, V de y em Y e W de 0 em k^{m-n}, um isomorfismo de variedades $\psi : V \to U \times W$ tais que $\phi(U) = V$ e, sendo $\mathrm{pr} : V \times W \to V$ a projeção na primeira coordenada, $\mathrm{pr} \circ \psi(z) = \phi(z)$, para todo $z \in U$;

(3) (X, Y, x, y, ϕ) é localmente uma aplicação linear sobrejetora entre espaços vetoriais;

(4) Existem sistemas de coordenadas $\{f_i\}$ em x e $\{g_j\}$ em y tais que $f_i = g_i \circ \phi$ para todo i;

(5) Existem vizinhanças abertas U de x em X e V de y em Y e um morfismo $\sigma : V \to U$ tal que $\phi(U) \subset V$ e $\phi \circ \sigma = \mathrm{id}_V$.

Nesse caso dizemos que ϕ é uma **submersão** em x.

Demonstração: Análoga ao caso da imersão. ■

Uma aplicação $\phi : X \to Y$ é uma **subimersão** em x se ϕ é localmente uma composição $\iota \circ s$, em que s é uma submersão e ι é uma imersão. Equivalentemente, a aplicação ϕ é uma subimersão se ela é localmente uma aplicação linear entre espaços vetoriais.

Lema (L.2.5). Seja $f : U \times V \to k$ uma função tal que a derivada em relação à coordenada V é identicamente nula. Se a característica de k é zero, então f é localmente independente da coordenada V.

Demonstração: Localmente, f é dada por uma série de potências convergente $\sum_\alpha f_\alpha(y)x^\alpha$. Como f tem derivada em relação a V identicamente nula, a derivada de f_α é zero para todo α. O problema foi, assim, reduzido a mostrar que séries de potência de derivada identicamente nula são constantes. Se $f = \sum_\beta b_\beta y^\beta$, a derivada de f ser zero implica que $b_\beta \beta_i = 0$, em que $\beta = (\beta_1, \ldots, \beta_n)$. Como a característica de k é zero, $b_\beta = 0$ sempre que β é não nulo, e, portanto, $f = b_0$. ■

Teorema (T.2.6). *Se a característica de k é zero, então um morfismo $\phi : X \to Y$ é uma subimersão em x se, e somente se,* $\operatorname{rank} T_{x'}\phi$ *é constante para todo x' em uma vizinhança aberta de x em X.*

Demonstração: Se ϕ é uma subimersão em x, é claro que $\operatorname{rank} T_{x'}\phi$ é constante em uma vizinhança de x, afinal, ϕ é localmente uma aplicação linear L e, portanto, em uma vizinhança de x, $\operatorname{rank} T_{x'}\phi = \operatorname{rank} L$.

Por outro lado, sendo $p = \operatorname{rank} T_x\phi = \dim_k \operatorname{Im} T_x\phi$ o posto de $T_{x'}\phi$ em uma vizinhança de x, como queremos provar uma propriedade apenas local, podemos assumir que $Y = V_1 \times V_2$, em que V_1 é aberto em k^p e V_2 é aberto em k^{n-p} (de fato, qualquer vizinhança aberta de um ponto a em k^n contém uma subvizinhança aberta de a com a propriedade desejada). Podemos assumir também que $\phi(x) = 0$ e que $\operatorname{Im} T_x\phi = k^p \times \{0\}$.

Seja $\pi : k^p \times k^{n-p} \to k^p$ a projeção na primeira coordenada. Então $\pi \circ \phi$ é uma submersão, visto que $\operatorname{Im} T_x\phi = k^p \times \{0\}$. Podemos assumir, portanto, que $X = V_1 \times U_2$, em que U_2 é aberto em k^{m-p} e que $\pi \circ \phi : V_1 \times U_2 \to V_1$ é a projeção na primeira coordenada.

Assim, $\phi : V_1 \times U_2 \to V_1 \times V_2$ é tal que $\phi(x_1, x_2) = (x_1, \psi(x_1, x_2))$. Podemos, é claro, assumir que o posto de $T_{x'}\phi$ é constante igual a p em $V_1 \times U_2$. Note que o posto de ψ é zero, já que tanto o posto da aplicação identidade em V_1 quanto o de ϕ são p. Segue-se que ϕ tem a derivada nula em relação à variável x_2. Logo, pelo lema anterior, ψ não depende de x_2 em uma vizinhança de zero. Logo, localmente,

ϕ é escrita como $V_1 \times U_2 \xrightarrow{\mathrm{pr}_1} V_1 \xrightarrow{\mathrm{Id}\times\psi}$. Sendo pr_1 uma submersão e $\mathrm{Id}\times\psi$ uma imersão (visto que ψ tem posto zero), segue-se que ϕ é uma subimersão. ■

Se X e Y são variedades analíticas, denotamos por $\mathrm{Mor}(X, Y)$ o conjunto de todas as aplicações analíticas (morfismos) $\phi : X \to Y$.

Proposição (P.2.7). Se X é um espaço topológico e A e B são dois atlas maximais em X, sejam X_A e X_B as estruturas de variedade associadas a A e B, respectivamente. Então são equivalentes:

(1) $A = B$;

(2) Para toda variedade Y, $\mathrm{Mor}(X_A, Y) = \mathrm{Mor}(X_B, Y)$;

(3) Para toda variedade Y, $\mathrm{Mor}(Y, X_A) = \mathrm{Mor}(Y, X_B)$.

Demonstração: É óbvio que (1) implica (2) e (3). Se vale (2), tomando $Y = X_A$, então $\mathrm{Mor}(X_A, X_A) = \mathrm{Mor}(X_B, X_A)$ e, portanto, $\mathrm{id}_X : X_B \to X_A$ é um morfismo. Similarmente, a aplicação $\mathrm{id}_X : X_A \to X_B$ é um morfismo. Logo os atlas A e B são compatíveis e, pela maximalidade, são iguais. A demonstração de que (3) implica (2) é completamente análoga. ■

A proposição abaixo é consequência direta das proposições 2.3 e 2.4.

Proposição (P.2.8). Seja $f : X \to Y$ um morfismo entre variedades e Z uma variedade. Então:

(1) Se f é uma imersão, então uma aplicação contínua $g : Z \to X$ é analítica se, e somente se, $f \circ g : Z \to Y$ é analítica.

(2) Se f é uma submersão, então uma aplicação $g : Y \to Z$ é analítica se, e somente se, $g \circ f : X \to Z$ também o é. Além disso, f é uma aplicação aberta.

Proposição (P.2.9). Seja X um espaço topológico, Y uma variedade e $f : X \to Y$ uma aplicação contínua. Se existir uma estrutura de variedade em X de forma que f é imersão, então essa estrutura é única.

Demonstração: Pela proposição anterior, para todo Z, $\mathrm{Mor}(Z, X)$ é determinado pela topologia de X e pela estrutura analítica de Y e, assim, pela Proposição 2.7, a estrutura de variedade de X é única. ■

Sejam X um espaço topológico, Y uma variedade analítica, $f : X \to Y$ uma aplicação contínua e x um ponto de X. Dizemos que (X, f) satisfaz a **condição ($\star$)** em um ponto x se existem uma vizinhança aberta de U em X, uma carta $c = (V, \phi, n)$ de Y e um subespaço vetorial E de k^n tais que $f(U) \subset V$, f é um homeomorfismo entre U e sua imagem e $(\phi \circ f)(U) = E \cap \phi(V)$.

Teorema (T.2.10). *Para que exista uma estrutura analítica em X de forma que f seja uma imersão em x, é necessário e suficiente que (X, f) satisfaça a condição $(\star)$ em x.*

Demonstração: Se X é uma variedade e $f : X \to Y$ é uma imersão, f é localmente uma inclusão linear e, portanto, (X, f) satisfaz $(\star)$.

Reciprocamente, se o par (X, f) satisfaz $(\star)$, escolha uma cobertura aberta $\{U_i\}_{i\in I}$ de X de forma que para todo $i \in I$, existam uma carta $c_i = (V_i, \phi_i, n_i)$ e um subespaço vetorial E_i de k^{n_i} tais que $f(U_i) \subset V$, f é homeomorfismo de U_i sobre sua imagem, $(\phi_i \circ f)(U_i) = E_i \cap \phi_i(V_i)$. Então existe uma

estrutura de variedade em U_i de forma que $f|_{U_i}$ é uma imersão (induzida pelo homeomorfismo f, que é localmente uma inclusão linear). As estruturas de variedade em $U_i \cap U_j$ concordam pela proposição anterior. Portanto, existe uma única estrutura de variedade em X compatível com a estrutura de cada U_i. Como f é uma imersão todo ponto de X (afinal, $\{U_i\}$ cobre X), f é uma imersão. ■

Se X é um subespaço de uma variedade Y, dizemos que X é uma **subvariedade** de Y se, sendo $\iota : X \to Y$ a inclusão, para todo $x \in X$, (X, ι) satisfaz $(\star)$ em x.

Proposição (P.2.11). Sejam $f : X \to Y$ um morfismo entre variedades, $b \in Y$ e $X_b = f^{-1}(b) \subset X$. Se para todo $x \in X_b$, f é uma subimersão em x, então X_b é uma subvariedade de X.

Demonstração: Pela definição de subimersão, a composição $X_b \xrightarrow{\iota} X \xrightarrow{f} Y$ é localmente $\operatorname{Ker} L \xrightarrow{i} E \xrightarrow{L} F$, em que $L : E \to F$ é linear e $i : \operatorname{Ker} L \to E$ é a inclusão. Evidentemente o par $(\operatorname{Ker} L, i)$ satisfaz $(\star)$. ■

Usualmente aplicamos a proposição acima para quando b é um valor regular de f. Se $f : X \to Y$ é um morfismo entre variedades, $b \in Y$ é dito **valor regular** de f se para todo $x \in f^{-1}(b)$, $T_x f : T_x X \to T_b Y$ é sobrejetiva (em outras palavras, f é uma submersão em todo ponto de $f^{-1}(b)$).

Corolário (C.2.12) (Imagem inversa de valor regular). *Sejam $f : X \to Y$ um morfismo de variedades e b um valor regular de f, então $X_b = f^{-1}(b)$ é uma subvariedade de X.*

Será-nos útil também definir **variedades quocientes**. Se R é uma relação de equivalência em uma variedade X, podemos pensar R como subconjunto da variedade produto $X \times X$. Não necessariamente o espaço quociente X/R tem estrutura de variedade. Porém, enunciamos, sem demonstração, um critério necessário e suficiente para que X/R seja uma variedade. Deixamos como referência [Ser00] 2.3.12.

Teorema (T.2.13) (Godement). *Seja R uma relação de equivalência em uma variedade X. Então X/R tem no máximo uma estrutura de variedade de forma que a projeção $\pi : X \to X/R$ seja uma submersão em x para todo $x \in X$. Essa estrutura existe se, e somente se, R é uma subvariedade de $X \times X$ e a projeção $\mathrm{pr}_2 : R \subset X \times X \to X$ é uma submersão.*

Sejam Y_1 e Y_2 subvariedades de uma variedade analítica X e $x \in Y_1 \cap Y_2$. Então:

Teorema (T.2.14). *As condições abaixo são equivalentes:*

(1) $T_x X = T_x Y_1 + T_x Y_2$;

(2) Existe uma carta $c = (U, \phi, n)$ em x tal que $\phi(U) = V_1 \times V_2 \times W$, $\phi(U \cap Y_1) = V_1 \times \{0\} \times W$ e $\phi(U \cap Y_2) = \{0\} \times V_2 \times W$;

(3) Existe um sistema de coordenadas $x_1, \ldots, x_n$ em x e inteiros $p \geq 0$ e $q \geq 0$ com $p+q \leq n$ tais que Y_1 é definido pelas equações $x_1 = \cdots = x_p = 0$ em uma vizinhança de x e Y_2 por $x_{p+1} = \cdots = x_{p+q} = 0$ em uma vizinhança de x.

Demonstração: A equivalência entre (2) e (3) é clara. Além disso, é claro que, assumindo (2), $T_x X = T_x Y_1 + T_x Y_2$. Vamos provar que (1) implica (3). Como a questão é puramente local, podemos "diminuir" X de forma que Y_1 seja dado pela imagem inversa de 0 por uma função $f_1 : X \to k^p$

(consequência direta da condição ($\star$)). Similarmente, podemos assumir que Y_2 é a imagem inversa de 0 por uma função $f_2 : X \to k^q$.

Sejam $(x_1, \ldots, x_p)$ e $(x_{p+1}, \ldots, x_{p+q})$ as componentes de f_1 e f_2. Como $T_xX = T_xY_1 + T_xY_2$, segue-se que $(f_1, f_2) : X \to k^{p+q}$ é uma submersão. Pela Proposição 2.4, $(x_1, \ldots, x_{p+q})$ é parte de um sistema de coordenadas em x. ■

Quando as condições do Teorema 2.14 são satisfeitas, dizemos que Y_1 e Y_2 são **transversais** em x. O corolário abaixo decorre imediatamente do item (2) do Teorema 2.14.

Corolário (C.2.15). *(1) Y_1 e Y_2 são transversais em uma vizinhança de x;*

(2) $Y_1 \cap Y_2$ é uma subvariedade de X numa vizinhança de x;

(3) $T_x(Y_1 \cap Y_2) = T_xY_1 \cap T_xY_2$.

Consideremos dois morfismos entre variedades $f_1 : Y_1 \to X$ e $f_2 : Y_2 \to X$. O produto fibrado de Y_1 e Y_2 sobre X é o conjunto $\{(y_1, y_2) \in Y_1 \times Y_2 \mid f_1(y_1) = f_2(y_2)\}$, denotado por $Y_1 \times_X Y_2$. Denotando por pr_i a projeção de $Y_1 \times_X Y_2$ em Y_i, denotamos por f a composição $f_1 \circ \mathrm{pr}_1 = f_2 \circ \mathrm{pr}_2$.

Se $(y_1, y_2) \in Y_1 \times_X Y_2$ e $x = f(y_1, y_2)$, dizemos que f_1 e f_2 são **transversais** em $y = (y_1, y_2)$ se $T_xX = \operatorname{Im} T_{y_1} f_1 + \operatorname{Im} T_{y_2} f_2$. Observamos que se f_1 é uma submersão, então $\operatorname{Im} T_{y_1} = T_xX$ e, portanto, f_1 e f_2 são transversais em cada ponto. Finalizamos essa seção mencionando algumas propriedades de morfismos transversais.

Teorema (T.2.16) ([Ser65], II.3.11 E). *Se f_1 e f_2 são transversais em y, então:*

(1) f_1 e f_2 são transversais em uma vizinhança de y em $Y_1 \times_X Y_2$;

(2) $Y_1 \times_X Y_2$ é uma subvariedade de $Y_1 \times Y_2$ em uma vizinhança de y;

(3) $T_y(Y_1 \times_X Y_2) = T_{y_1}(Y_1) \times_{T_xX} T_{y_2}Y_2$.

2.1.3 Formas diferenciais e integração

Brevemente relembramos a álgebra exterior de um espaço vetorial. Seja E um espaço vetorial de dimensão finita sobre um corpo k e $T(E)$ sua álgebra tensorial. A álgebra exterior $\Lambda(E)$ é o quociente $T(E)/\langle v \otimes v, v \in E\rangle$. Denotamos a imagem de $v \otimes w$ em $\Lambda(E)$ por $v \wedge w$. Denotamos por $\Lambda^p(E)$ o subespaço vetorial de $\Lambda(E)$ gerado por elementos da forma $v_1 \wedge \cdots \wedge v_p$, em que $v_i \in E$ para todo i. Vale notar que, aqui, entendemos o produto vazio como o elemento 1 de k, ou seja, o subespaço $\Lambda^0(E)$ é identificado com k. $\Lambda(E)$ é, assim, a soma direta das componentes $\Lambda^p(E)$, para $0 \leq p \leq \dim E$ (se $p > \dim E$, $\Lambda^p(E) = 0$). Segue-se que a dimensão de $\Lambda(E)$ é $2^{\dim E}$.

Fixemos agora uma carta (U, ϕ, n) em uma variedade analítica X contendo um ponto x. Como visto na subseção anterior, associamos à essa carta uma base do espaço cotangente $\{dx_i\}_{i=1}^n$. Consequentemente, a álgebra exterior do espaço cotangente T_x^*X possui como base o conjunto $\{dx_{i_1} \wedge \cdots \wedge dx_{i_p} |\ i_1 < \cdots < i_p, 0 \leq p \leq n\}$.

Uma **forma diferencial** de grau p (ou, simplesmente, uma p-forma) é uma regra que, a cada ponto x de X, associa um elemento de $\Lambda^p(T_x^*X)$. Uma forma α, escreve-se, no aberto U, como $\alpha(x) = \sum_{i_1 < \cdots < i_p} f^U_{i_1,\ldots,i_p}(x) dx_{i_1} \wedge \cdots \wedge dx_{i_p}$, em que $f^U_{i_1,\ldots,i_p}$ são funções de U para k. Dizemos que uma

p-forma é **analítica** se para toda carta (U, ϕ, n), as funções $f^U_{i_1,\dots,i_p}$ são analíticas. Todas as formas diferenciais com as quais trabalharemos serão analíticas. Por isso, omitiremos o termo.

Qualquer função analítica $f : X \to k$ pode ser identificada com uma 0-forma (e vice-versa). De fato, para cada $x \in X$, associamos o elemento $f(x) \in \Lambda^0(E) = k$. É óbvio que a forma f é analítica. Podemos identificar a aplicação tangente de f, denotada por df, com uma 1-forma, já que $(df)_x$ é um elemento de $T^*_x X = \Lambda^1(T^*_x X)$ para todo x. Já uma p-forma ω associa a cada ponto de X uma forma multilinear alternada $\omega(x) : \prod_{i=1}^{p} T_x X \to k$.

Veremos, na próxima seção, que uma variedade p-ádica compacta é uma união disjunta de bolas. Assim, a integração de formas diferenciais sobre variedades p-ádicas compactas se resume à integração sobre k^n — mais ainda, resume-se a integrar funções sobre $\mathcal{O}^n_k$.

Seja μ a medida de Haar de k^n normalizada de forma que $\mu(\mathcal{O}^n_k) = 1$. Se α é uma n-forma diferencial em $\mathcal{O}^n_k$ escrita como $\alpha(x) = f(x)\, dx_1 \wedge \cdots \wedge dx_n$, sua integral é

$$\int_{\mathcal{O}^n_k} |\alpha| = \int_{\mathcal{O}^n_k} |f(x)|\, d\mu.$$

Notemos que $|f(x)|$ assume apenas um conjunto discreto de valores e, assim, podemos escrever a integral de ω como $\sum_{k\in\mathbb{Z}} q^{-k}\mu(A_k)$, em que q é a cardinalidade do corpo residual de k e $A_k = \{x \in \mathcal{O}^n_k : |f(x)| = q^{-k}\}$.

Para nossos propósitos, isso é tudo que precisamos sobre integração. Deixamos como referência o capítulo 7 de [Igu00], em que é discutida a integração de variedades analíticas de forma mais aprofundada.

2.2 Classificação das variedades p-ádicas

Nesta seção, k é um **corpo local**, isto é, localmente compacto e completo em relação a um valor absoluto ultramétrico não trivial — como uma extensão finita de $\mathbb{Q}_p$ ou $\mathbb{F}_q((T))$. Além disso, as variedades têm dimensão fixa. Como mencionado no início do capítulo, a estrutura de variedades sobre esses corpos é bastante simples, como enunciado no teorema a seguir. Se (X, d) é um espaço métrico, x um elemento de X e r um número real positivo, a bola de raio r centrada em x é o conjunto dos elementos y de X tais que $d(x, y) < r$.

Teorema (T.2.17). *Toda variedade paracompacta sobre um corpo local é isomorfa a uma união disjunta de bolas.*

Exemplificando, seja T um transversal de $\mathbb{Z}_p$ em $\mathbb{Q}_p$. Então $\mathbb{Q}_p$ é a união disjunta das bolas $t + \mathbb{Z}_p$, para t em T.

Para variedades compactas, essa união é finita. Mas uma decomposição de uma variedade em bolas não é única. De fato, $\mathbb{Z}_p$ é uma bola que se escreve como união de p bolas, classes laterais de $p\mathbb{Z}_p$. Esse exemplo, em certo sentido, esgota as possibilidades de decomposição de uma bola em outras:

Teorema (T.2.18). *Seja k um corpo local com corpo residual de q elementos. Se variedades compactas X e Y são uniões disjuntas de r e r' bolas, respectivamente, então X é isomorfa a Y se, e somente se, $r \equiv r' (\mod q - 1)$.*

Podemos assim, para uma variedade X, definir um invariante $i(X)$ (a quantidade de bolas numa decomposição de X módulo $q-1$) que determina X a menos de isomorfismo.

O resultado acima foi demonstrado inicialmente em [Ser65] utilizando integração de formas diferenciais. Uma demonstração alternativa foi esboçada em [Ser00]. O objetivo deste capítulo é apresentar ambas as demonstrações.

Até o final do capítulo, k é um corpo local com corpo residual finito de q elementos.

Lema (L.2.19). Uma variedade paracompacta admite cobertura localmente finita por bolas.

Demonstração: Seja $\{V_\mu\}_{\mu\in M}$ um refinamento aberto localmente finito de uma cobertura $\{T_\lambda\}_{\lambda\in L}$ de X por bolas. Seja $\{W_\nu\}_{\nu\in N}$ um refinamento fechado localmente finito de $\{V_\mu\}_{\mu\in M}$. Sejam $\phi : M \to L, \psi : N \to M$ tais que $V_\mu \subset T_{\phi(\mu)}$ e $W_\nu \subset V_{\psi(\nu)}$ (em particular, $W_\nu \subset V_{\psi(\nu)} \subset T_{\phi\psi(\nu)}$). Sendo W_ν compacto e $V_{\phi(\nu)}$ aberto, podemos cobrir W_ν por um número finito de bolas $B_{i,\nu}, i \in I_\nu$, tais que $B_{i,\nu} \subset V_{\phi(\nu)}$. Afirmamos que $\{B_{i,\nu}\}_{\nu\in N, i\in I_\nu}$ é uma cobertura localmente finita de X. Com efeito, cada $B_{i,\nu}$ intersecta apenas um número finito de elementos de $\{V_\mu\}_{\mu\in M}$ e, portanto, apenas uma quantidade finita de bolas $B_{i',\nu'}$. ∎

Demonstração do Teorema 2.7: Seja $\{U_i\}_{i\in I}$ uma cobertura localmente finita de X consistindo de bolas. Seja $F(I)$ a família dos subconjuntos finitos de I. Para cada $J \in F(I)$, seja

$$U_J = \bigcap_{j\in J} U_j \cap \left(X - \bigcup_{i\notin J} U_i\right).$$

Então $(X - \bigcup_{i\notin J} U_i)$ é aberto e compacto. Se J é não vazio, esse conjunto é $\bigcap_{j\in J, i\notin J} (U_j - U_i)$, que é uma interseção finita se restringirmos $i \notin J$ tais que $U_j \cap U_i$ é não-vazio para algum $j \in J$. Sendo U_J subconjunto compacto e aberto de uma bola, U_J é união disjunta finita de bolas. Sendo a família $\{U_J\}_{J\in F(I)}$ dois a dois disjunta, o resultado segue. ∎

No final da demonstração anterior, utilizamos o lema a seguir, que faremos uso novamente na demonstração do Teorema 2.18.

Lema (L.2.20). Seja U um subconjunto aberto e fechado de uma bola B em k^n. Existe um raio r menor que o raio de B tal que U é uma união disjunta finita de bolas de raio r. Além disso, para todo raio $s < r$, U é união disjunta finita de bolas de raio s.

Demonstração: Seja $V = B - U$, sendo $\{U, V\}$ uma cobertura aberta de B. Segue-se que existe um raio r menor do que o raio de B tal que para todo $x \in B$, a bola centrada em x de raio r é um subconjunto de U ou de V. Então, U é união das bolas de raio r centradas em cada um de seus elementos. Como k é ultramétrico, essa união é disjunta e, por compacidade, é finita. O resultado se estende naturalmente para todo $s < r$. ∎

Demonstração do Teorema 2.8: Relembramos que denotamos por $\mathcal{O}_k^n$ a bola de raio 1 centrada em 0 em k^n e, por simplicidade, denotaremos por $m\mathcal{O}_k^n$ a união disjunta de m cópias de $\mathcal{O}_k^n$. Denotamos por π um uniformizador de $\mathcal{O}_k$ (isto é, um elemento de valor absoluto 1). O valor absoluto em k é normalizado, isto é, se $a \in k$, $|a| = q^{-v(a)}$, em que $v : k \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ é a valoração de k.

Note que, se $r \equiv r' \mod (q-1)$, então, é evidente que $r\mathcal{O}_k^n$ é isomorfo a $r'\mathcal{O}_k^n$. Com efeito, é suficiente mostrarmos que $q\mathcal{O}_k^n$ é isomorfo a $\mathcal{O}_k^n$. Escrevendo $\mathcal{O}_k^n$ como a união das q classes laterais de

$\pi\mathcal{O}_k \times \mathcal{O}_k^{n-1}$, obtemos uma decomposição em q bolas. Nos resta mostrar que se $r\mathcal{O}_k^n$ é isomorfo a $r'\mathcal{O}_k^n$, então $r \equiv r' \mod (q-1)$.

Se ω é uma n-forma diferencial sobre uma variedade X, então $\omega = f\ dx_1 \wedge \cdots \wedge dx_n$.

Lema (L.2.21). Seja ω uma forma diferencial sobre $X = r\mathcal{O}_k^n$ que não se anula em nenhum ponto de X (isto é, f não tem raízes em X). Então $\int_X |\omega| = a/q^b$, com $a \equiv r \mod(q-1)$.

Demonstração: Pela aditividade da integral, precisamos checar apenas o caso em que $r = 1$, ou seja, assumimos $X = \mathcal{O}_k^n$. A forma ω se escreve como $f\ dx_1 \wedge \cdots \wedge dx_n$. Como f não se anula e a valoração v é discreta, $|f|$ é localmente constante. Como $(\pi^h\mathcal{O}_k^n)_{h\in\mathbb{N}}$ é base de vizinhanças de 0 em X, existe um inteiro h tal que $|f|$ é constante nas classes laterais B_α de $\pi^h\mathcal{O}_k^n$. Seja q^{c_α} a imagem de B_α por $|f|$ ($c_\alpha \in \mathbb{Z}$). O volume de cada B_α é igual a q^{-nh}. Podemos, portanto, escrever:

$$\int_X |\omega| = \sum_\alpha q^{c_\alpha - nh} = \frac{a}{q^b},$$

em que a é um inteiro coprimo a q e $b + c_\alpha - nh \geq 0$ para todo α. Obtemos que $a = \sum_\alpha q^{b+c_\alpha-nh}$ e, sendo todos os somandos nessa expressão são congruentes a 1 módulo $q-1$ e $\pi^h\mathcal{O}_k^n$ possuindo nh classes laterais em X. segue-se que:

$$a \equiv q^{nh} \equiv 1 \mod(q-1).$$

■

Voltando ao Teorema, tomemos $\omega = dx_1 \wedge \cdots \wedge dx_n$. Se uma variedade X admite decomposição como união disjunta de r bolas e outra decomposição como união disjunta de r' bolas, pelo Lema 2.21, $\int_X |\omega| = \frac{a}{q^r}$ e $r \equiv a \equiv r' \mod(q-1)$.

■

Seguiremos agora para a demonstração alternativa esboçada em [Ser00]. Realizaremos uma sequência de simplificações para demonstração do Teorema 2.18.

Demonstração do Teorema 2.8: Sejam X uma variedade compacta dada e $\{U_i\}_{i\in I}$ e $\{V_j\}_{j\in J}$ duas decomposições de X por bolas fechadas disjuntas, com I e J finitos.

Inicialmente, assumiremos que $\{U_i\}_{i\in I}$ é um refinamento de $\{V_j\}_{j\in J}$ (tome um refinamento comum a ambas coberturas). Podemos assumir também que X é uma bola, isto é, que $J = \{j\}$ (como J é finito, o caso geral segue imediatamente).

Nos reduzimos, portanto, ao caso em que X é uma bola em k^n, $\{U_i\}_{i\in I}$ é uma coleção de bolas duas a duas disjuntas e uma família de isomorfismos analíticos $\phi_i : U_i \to \phi_i U_i \subset X$ (inclusões) tais que $X = \coprod_{i\in I} \phi U_i$. Sendo cada ϕ_i analítica, para cada $x \in U_i$, existe um raio $r_{i,x}$ de forma que ϕ_i é uma série de potências convergente em uma bola de raio $r_{i,x}$ em torno de x. Dessa forma, pela compacidade de U_i, escrevemos U_i como união de uma quantidade finita de bolas de raios variados. Sendo $r_0 = \inf\{r_{i,x}\}$, subdivida cada U_i em q bolas de mesmo raio iteradas vezes até que o raio de cada bola seja menor ou igual a r_0. Note que a nova coleção de bolas tem mesma cardinalidade a I módulo $q-1$. Via esse processo, podemos, então, assumir que cada ϕ_i é dada por uma série de potências convergente.

Sendo cada ϕ_i um isomorfismo analítico, o determinante da aplicação tangente $T_x\phi_i$ é não nulo para cada $x \in U_i$. Assim, a aplicação $x \mapsto |\det(T_x\phi_i)|$ é localmente constante (já que k tem valoração discreta). Podemos assumir que tal aplicação é constante.

Assumimos agora, sem perda de generalidade, que $U_i = \mathcal{O}_k^n$ e identificaremos k^n com o espaço tangente de X em 0. Defina a aplicação $\Psi_1 = T_0\phi_i^{-1} \circ \phi_i$, cuja derivada tem determinante 1. Seja τ uma translação de forma que $\Psi_2 := \tau \circ \Psi_1$ satisfaz $\Psi_2(0) = 0$ e σ_ν a homotetia $x \mapsto \pi^\nu x$. Reescrevemos, então, ϕ_i como $T_0\phi_i \circ \tau^{-1} \circ \Psi^{\sigma_\nu^{-1}}$, em que $\Psi := \Psi_2^{\sigma_\nu}$.

Para prosseguirmos com a demonstração, precisamos introduzir uma definição e enunciar um resultado que omitiremos a demonstração.

Dizemos que uma série de potências $f(x) = \sum_\alpha c_\alpha x^\alpha \in \mathcal{O}_k[[x]]$ $(x = (x_1, \ldots, x_n))$ é **restrita especial** se $c_0 = 0$ e $c_\alpha \equiv 0(\mod \pi^{|\alpha|-1})$ para todo α multi-índice diferente de 0.

Lema (L.2.22) ([Igu00], 2.2.1). Seja $g = (g_1, \ldots, g_n)$ com cada $g_i(x) \in \mathcal{O}_k[[x]]$ restrita especial com $|T_0 g| \not\equiv 0 \mod \pi$. Então g é um automorfismo analítico de $\mathcal{O}_k^n$.

Observe, agora, que, para ν suficientemente grande, cada coordenada de Ψ está em $\mathcal{O}_k[[x]]$ e é restrita especial. Além disso, $|T_0\Psi| = 1$. Assim, pelo lema acima, Ψ é automorfismo de $\mathcal{O}_k^n$, de forma que $\tau^{-1} \circ \Psi^{\sigma_\nu^{-1}}$ é um isomorfismo analítico de bolas.

Podemos, pois, assumir que cada aplicação ϕ_i é linear. Para todo i, $\phi_i U_i$ é compacto e aberto. Portanto, pelo Lema 2.20, existe um raio r_i de forma que para todo $s \leq r_i$, $\phi_i U_i$ é uma união disjunta de bolas de raio s. Seja $s = \min\{r_i\}_{i \in I}$.

Se X é decomposto em q^m bolas de raio s e cada $\phi_i U_i$ em q^{m_i} bolas de raio s, então:

$$1 \equiv q^m = \sum_{i \in I} q^{m_i} \equiv \sum_{i \in I} 1 \mod (q-1).$$

Resta-nos mostrar que se $U = \mathcal{O}_k^n$ e $L : U \to LU \subset \mathcal{O}_k^n$ um isomorfismo linear, então para $s > 0$ suficientemente pequeno, LU é a união de q^m bolas de raio s.

Seja s tal que LU é união de bolas de raio s e h o número de bolas de raio s em LU. Seja h' o número de classes laterais de LU em $\mathcal{O}_k^n$, tendo, pois, $\mathcal{O}_k^n$ hh' bolas de raio s. Seja m o inteiro tal que $\pi^m\mathcal{O}_k$ é a bola de raio s em $\mathcal{O}_k$, de forma que $(\pi^m\mathcal{O}_k)^n$ é a bola de raio s em $\mathcal{O}_k^n$. Como $\mathcal{O}_k/\pi^m\mathcal{O}_k$ tem q^m elementos, existem q^{mn} bolas de raio s em $\mathcal{O}_k^n$.

Mas h' é, também, uma potência de q. Como $\mathcal{O}_k^n/LU$ é um $\mathcal{O}_k$-módulo finitamente gerado e de torção (sendo LU aberto, para algum inteiro $N > 0$ suficientemente grande, $\pi^N\mathcal{O}_k^n \in LU$) e $\mathcal{O}_k$ é um domínio de ideais principais, segue-se que:

$$\frac{\mathcal{O}_k^n}{LU} = \bigoplus_{i=1}^{l} \frac{\mathcal{O}_k}{\pi^{m_i}\mathcal{O}_k}.$$

E, portanto, $h' = |\mathcal{O}_k^n/LU|$ é uma potência de q. Segue-se que h é potência de q, como queríamos demonstrar.

■

Capítulo 3

Grupos analíticos

No Capítulo anterior discutimos e estudamos variedades analíticas p-ádicas e suas principais propriedades. Isso nos dá os fundamentos para apresentarmos, neste Capítulo, o principal objeto de estudo deste trabalho.

Grupos de Lie constituem um objeto de investigação fundamental na Matemática contemporânea. Inicialmente estudados no final do século XIX por Sophus Lie no contexto de equações diferenciais, os grupos de Lie reais possuem papel de destaque no estudo da Geometria Diferencial do século XX.

Buscamos estudar, neste Capítulo, propriedades fundamentais e caracterizações dos grupos analíticos p-ádicos, grupos de Lie modelados sobre o corpo dos números p-ádicos. O Capítulo está dividido em quatro seções. A primeira introduz conceitos e propriedades iniciais dos grupos analíticos p-ádicos, além de apresentar uma vasta gama de exemplos. Aqui, seguimos de perto [Ser00], com diversos exemplos adicionais. A segunda e terceira seções discutem os grupos p-saturáveis e culminam na caracterização dos grupos analíticos p-ádicos, obtida originalmente por Lazard na década de 1960. Embora o material original desta parte seja [Laz65], tomamos como referência principal [Sch11].

3.1 Grupos formais e grupos padrão

Seja k um corpo completo em relação a um valor absoluto não trivial. Um **grupo analítico** sobre k é um objeto-grupo na categoria das variedades k-analíticas — ou seja, é um grupo G munido de uma estrutura de variedade k-analítica de forma que as aplicações de inversão e produto sejam morfismos de variedades. Nos dedicaremos especialmente aos **grupos analíticos p-ádicos**, isto é, ao caso em que $k = \mathbb{Q}_p$. Por isso, subentende-se que os grupos analíticos são sobre $\mathbb{Q}_p$, caso contrário, deixaremos claro o corpo base.

Se n é a dimensão de uma carta na identidade de um grupo analítico G, como a multiplicação em G é analítica, para todo $g \in G$, a aplicação $\phi_g : G \to G, x \mapsto xg$ é um isomorfismo na categoria das variedades analíticas e, portanto, a dimensão de uma carta em $\phi_g(1) = g$ deve ser igual a n. Ou seja, G tem dimensão constante igual a n.

Note também que, se G é um grupo analítico e H é um subgrupo aberto de G (escrevemos $H \leq_o G$), H também é um grupo analítico. De fato, H herda a estrutura de variedade de G e a inversão e o produto em H são evidentemente analíticos. Por outro lado, se H é um subgrupo fechado de G

(escrevemos $H \leq_c G$), H pode ou não possuir estrutura de variedade, a depender do corpo k: de fato, se k' é uma extensão finita de $\mathbb{Q}_p$, então o grupo aditivo de $\mathbb{Q}_p$ é um subgrupo fechado do grupo aditivo de k', mas não tem estrutura de k'-variedade. Veremos posteriormente que se o corpo base k é $\mathbb{R}$ ou $\mathbb{Q}_p$, subgrupos fechados de grupos analíticos são analíticos.

Exemplo (E.3.1). O grupo aditivo $\mathbb{Q}_p^n$ é um grupo analítico, já que a soma e a multiplicação por -1 são aplicações analíticas. Pela observação acima, como $\mathbb{Z}_p^n$ é aberto em $\mathbb{Q}_p^n$, o grupo $\mathbb{Z}_p^n$ é analítico.

Exemplo (E.3.2). Seja R uma k-álgebra associativa com unidade de dimensão finita. O grupo $\mathbb{G}_m(R)$ dos elementos invertíveis em R é analítico. Mostraremos que $\mathbb{G}_m(R)$ é um subconjunto aberto de R encontrando uma vizinhança de elementos de 1 que está em $\mathbb{G}_m(R)$. Note que existe uma vizinhança U de 0 em que a série de potências $\sum_{n=0}^{\infty} x^n$ converge. Então, o conjunto $V = \{1 - x : x \in U\}$ está contido em $\mathbb{G}_m(R)$ (visto que $(1-x)\sum_{n=0}^{\infty} x^n = 1$) e é homeomorfo a U. Então existe uma vizinhança de 1 em $\mathbb{G}_m(R)$ isomorfa, como variedade analítica, a um subconjunto aberto de k^n e, portanto, $\mathbb{G}_m(R)$ tem uma estrutura de variedade analítica. Como a multiplicação em R é bilinear, é, portanto, analítica. Logo $\mathbb{G}_m(R)$ é grupo analítico.

Exemplo (E.3.3). Similarmente ao exemplo acima podemos considerar uma álgebra sobre o anel de inteiros $\mathcal{O}_k$ de uma extensão finita k de $\mathbb{Q}_p$. Seu grupo multiplicativo também é analítico. Tomando $R = \mathrm{End}(\mathcal{O}_k^n)$, concluímos que $\mathrm{GL}_n(\mathcal{O}_k)$ é um grupo analítico p-ádico. Note que este grupo é compacto e, sendo também totalmente desconexo, é profinito. Em contrapartida, $\mathrm{GL}_n(k) = \mathbb{G}_m(\mathrm{End}(k^n))$ não é compacto.

Seja R um anel comutativo com unidade. Considere o anel das séries de potência $R[[X]] = R[[X_1, \ldots, X_n]]$ em n indeterminadas sobre R. Uma **lei formal de grupo** é uma n-upla $F = (F_i)_{i=1}^n$ de séries de potências $F_i \in R[[X, Y]]$, com $Y = (Y_1, \ldots, Y_n)$ tais que $F(X, 0) = X$, $F(0, Y) = Y$, e $F(U, F(V, W)) = F(F(U, V), W)$, isto é, F é associativa. Imediatamente observamos que $F_i(X, Y) = X_i + Y_i + \sum_{|\alpha|,|\beta|\geq 1} c_{\alpha,\beta} X^\alpha Y^\beta$ para todo i.

Exemplo (E.3.4) (Algumas leis formais). Consideremos o caso em que $n = 1$ e que $F(X, Y) = X + Y$. É claro que F é uma lei formal de grupo. Para $n = 1$ e $F(X, Y) = X + Y + XY$, verificamos facilmente que F é outro exemplo de lei formal de grupo.

Um exemplo mais interessante é se k é um corpo de característica diferente de p, $n = 2$ e $F(X, Y) = \left(X_1 + Y_1, X_2 + Y_2 + \frac{1}{p}\left(X_1^p + Y_1^p - (X_1 + Y_1)^p\right)\right)$, em que $X = (X_1, X_2)$ e $Y = (Y_1, Y_2)$. Verificamos a seguir que F é associativa. Seja $Z = (Z_1, Z_2)$.

$$F(F(X,Y)) = \left(X_1 + Y_1 + Z_1, X_2 + Y_2 + Z_2 + \frac{1}{p}\left(X_1^p + Y_1^p + Z_1^p - (X_1 + Y_1 + Z_1)^p\right)\right) = F(X, F(Y, Z)).$$

Seja $F(X, Y)$ uma lei formal sobre $\mathbb{Z}_p$ em $2n$ indeterminadas e seja $G = \{(x_1, \ldots, x_n), x_i \in p\mathbb{Z}_p\} \subset \mathbb{Z}_p^n$. Defina a multiplicação em G por $xy = F(x, y)$. Dizemos, neste caso, que G é um **grupo padrão**. A proposição a seguir mostra que G é, de fato, um grupo.

Proposição (P.3.5). O conjunto G, como definido acima, é um grupo analítico p-ádico.

Demonstração: Este resultado é uma consequência imediata do corolário da Proposição 10 de [Bou81] IV.35. ■

Seja X uma variedade analítica p-ádica, $1 \in X$ e U uma vizinhança aberta de 1 em X. Sejam $\phi : U \times U \to X$, $\psi : U \to U$ aplicações analíticas tais que:

(1) Existe uma vizinhança V_1 de 1 contida em U tal que, para todo $x \in V_1$, $x = \phi(x, e) = \phi(e, x)$;

(2) Existe uma vizinhança V_2 de 1 contida em U tal que, para todo $x \in V_2$, $1 = \phi(x, \psi(x)) = \phi(\psi(x), x)$;

(3) Existe uma vizinhança V_3 de 1 contida em U tal que $\phi(V_3 \times V_3) \subset U$ e, para todos $x, y, z \in V_3$, $\phi(x, \phi(y, z)) = \phi(\phi(x, y), z)$.

Dizemos então que $(X, 1, U, \phi, \psi)$, ou simplesmente X, é uma **peça de grupo *p*-ádica**. É claro que todo grupo analítico é uma peça de grupo. Sejam X e Y peças de grupo p-ádicas. Em geral, escreveremos xy para $\phi(x, y)$ e x^{-1} para $\psi(x)$. Um **homomorfismo local** $f : X- \to Y$ é uma aplicação analítica $f_U : U \to Y$ tal que $f(1_X) = 1_Y$ e exista V vizinhança de 1_X contida em U tal que $f(xy) = f(x)f(y)$ para quaisquer $x, y \in V$. Homomorfismos locais $f_1, f_2 : X- \to Y$ são ditos equivalentes se existe uma vizinhança U_0 de 1 contida em U tal que $f_1|_{U_0} = f_2|_{U_0}$

Duas peças de grupos p-ádicas X e Y são ditas isomorfas se existem homomorfismos locais $f : X- \to Y$ e $g : Y- \to X$ tais que $f \circ g$ é equivalente a identidade em Y e $g \circ f$ é equivalente a identidade em X.

Exemplo (E.3.6). Se G é um grupo analítico p-ádico e H é um subgrupo aberto de G, então a aplicação identidade em H se estende a um homomorfismo local $f : G- \to H$. A inclusão $\iota : H \to G$ é um homomorfismo local e $f \circ \iota$ é a identidade em H e $\iota \circ f$ é equivalente a identidade em G. Portanto, G e H são peças de grupos isomorfas.

Proposição (P.3.7). Qualquer peça de grupo p-ádica contém um subgrupo aberto padrão.

Demonstração: Seja G uma peça de grupo p-ádica. Utilizando coordenadas locais, podemos assumir que G é uma vizinhança de 0 em $\mathbb{Q}_p^n$. Além disso, existe uma vizinhança aberta de 0 em que a multiplicação de G é dada por uma série de potências convergente em uma bola de raio ε centrada em 0. Escreva $xy = F(X, Y) = x + y + \sum_{|\alpha|,|\beta| \geq 1} c_{\alpha,\beta} x^\alpha y^\beta$, $c_{\alpha,\beta} \in k^n$. Realizaremos uma mudança de coordenadas. Se $x, y \in G$ tem produto definido e igual a z, tome $x' = \mu x$, $y' = \mu y$, $z' = \mu z$, em que $\mu \in \mathbb{Q}_p^*$. Então:

$$z = z + y + \sum_{|\alpha|,|\beta| \geq 1} c_{\alpha,\beta} x^\alpha y^\beta \text{ implica que } z' = x' + y' + \sum_{|\alpha|,|\beta| \geq 1} \frac{c_{\alpha,\beta}}{\mu^{|\alpha|+|\beta|-1}} x'^\alpha y'^\beta.$$

Obtemos, assim, uma nova lei de grupo F_μ, cujos coeficientes são $\frac{c_{\alpha,\beta}}{\mu^{|\alpha|+|\beta|-1}}$. Como F converge, $|c_{\alpha,\beta}|$ é limitado. Se escolhemos μ de forma que $|\mu| \geq \sup\{|c_{\alpha,\beta}|, 1, 1/\varepsilon\}$, então:

$$\frac{|c_{\alpha,\beta}|}{|\mu|^{|\alpha|+|\beta|-1}} \leq \frac{\sup\{|c_{\alpha,\beta}|\}}{|\mu|} \leq 1,$$

ou seja, os coeficientes de F_μ estão em $\mathbb{Z}_p$. Como $(x', y') = \mu(x, y)$ e F converge em uma bola de raio ε, F_μ converge em uma bola de raio $|\mu|\varepsilon \geq 1$. Sendo H a bola estrita de raio 1, H é um subgrupo padrão de G. ■

Argumentando como no Exemplo 3.6, obtemos:

Corolário (C.3.8). *Toda peça de grupo p-ádica é isomorfa, como peça de grupo, a um grupo analítico p-ádico.*

3.1.1 Fórmulas para leis formais

Como $F(X,Y) = X+Y+\sum_{|\alpha|,|\beta|\geq 1} c_{\alpha,\beta}X^{\alpha}Y^{\beta}$, a série de potências $\sum_{|\alpha|,|\beta|=1} c_{\alpha,\beta}X^{\alpha}Y^{\beta}$ é uma forma bilinear, que denotamos por $B(X,Y)$. Denotamos por $\phi(X)$ a série de potência formal que representa a inversão, isto é, $\phi(X)$ é a série de potências que satisfaz $F(X,\phi(X)) = F(\phi(X),X) = 0$. Utilizamos a notação $O(d^0 \geq j)$ para uma série de potência formal cujos monômios têm grau ao menos j.

Proposição (P.3.9). Sejam F uma lei formal, B e ϕ definidos como acima e $[X,Y] = B(X,Y) - B(Y,X)$, então

(1) $\phi(X) = -X + B(X,X) + O(d^0 \geq 3)$;

(2) $XYX^{-1} = Y + [X,Y] + O(d^0 \geq 3)$ e $X^{-1}YX = Y - [X,Y] + O(d^0 \geq 3)$;

(3) $X^{-1}Y^{-1}XY = [X,Y] + O(d^0 \geq 3)$;

(4) $[X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0$ (Fórmula de Jacobi);

(5) sendo $f_0(X) = 0$ e $f_{m+1}(X) = F(X, f_m(X))$ para todo $m > 0$, então $f_m(X) = mX + O(d^0 \geq 2)$.

Demonstração:

(1) De fato, escrevendo $\phi(X) = \sum_{i\in\mathbb{N}} \phi_i(X)$, em que ϕ_i é um polinômio homogêneo de grau i, como $0 = F(X,\phi(X)) = X + \phi_1(X) + O(d^0 \geq 2)$, segue-se que $\phi_1(X) = -X$. Além disso, $0 = F(X,\phi(X)) = X + (-X + \phi_2(X) + \dots) + B(X, -X + \dots) + \cdots = \phi_2(X) - B(X,x) + O(d^0 \geq 3)$ e segue-se que $\phi_2(X) = B(X,X)$;

(2) $XYX^{-1} = F(F(X,Y),X^{-1}) = F(X + Y + B(X,Y) + \dots, -X + B(X,X) + \dots) = X + Y + B(X,Y) - X + B(X,X) - B(Y,X) - B(X,X) + \cdots = Y + [X,Y] + O(d^0 \geq 3)$. A outra igualdade é similar;

(3) $X^{-1}Y^{-1}XY = F(X^{-1}, Y^{-1}XY) = F(-X + B(X,X) + \dots, X + [X,Y] + \dots) = -X + B(X,X) + X + [X,Y] + B(X,-X) + \cdots = [X,Y] + O(d^0 \geq 3)$;

(4) denote por (X,Y) o comutador $X^{-1}Y^{-1}XY$. Por uma identidade de P. Hall para grupos, escrevendo X^Y para $Y^{-1}XY$, $(X^Y,(Y,Z))(Y^Z,(Z,X))(Z^X,(X,Y)) = 0$. Note que, pelo item (2), $X^Y = X + O(d^0 \geq 2)$ e que, pelo item (3), $(Y,Z) = [Y,Z] + O(d^0 \geq 3)$. Assim, $(X^Y,(Y,Z)) = (X + O(d^0 \geq 2), [Y,Z] + O(d^0 \geq 3)) = [X,[Y,Z]] + O(d^0 \geq 4)$. Observando os termos de grau 3 da identidade de P. Hall, obtemos a fórmula de Jacobi.

■

3.1.2 Quocientes

Sejam G um grupo analítico, H um **subgrupo de Lie** de G (isto é, um subgrupo que é uma subvariedade) e G/H o espaço das classes laterais.

Teorema (T.3.10). *A relação de equivalência $R = \{(x, y) \in G \times G \mid x^{-1}y \in H\}$ é regular. Logo G/H tem uma única estrutura de variedade analítica de forma que a projeção $\pi : G \to G/H$ seja uma submersão.*

Demonstração: Pelo Teorema 2.13, precisamos verificar que R é uma subvariedade de $G \times G$ e que $\mathrm{pr}_2 : R \to G$ é uma submersão.

Defina $p : G \times G \to G$ por $p(x, y) = x^{-1}y$, de forma que $R = p^{-1}(H)$. Note que R é o produto fibrado de $p : G \times G \to G$ pela inclusão $\iota : H \to G$, isto é, é o conjunto $\{(x, y, z) \in G \times G \times H \mid x^{-1}y = z\}$.

$$\begin{array}{ccc} R & \xrightarrow{\iota} & G \times G \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ H & \xrightarrow{\iota} & G \end{array}$$

Assim, pelo Teorema 2.16, se p for uma submersão, então R será uma subvariedade de $G \times G$. Seja $(x, y) \in G \times G$ e defina $\phi : G \to G \times G$ por $\phi(z) = (x, xz)$. Então $\phi(x^{-1}y) = (x, y)$ e $p \circ \phi$ é a identidade em G. Pela caracterização local das submersões, p é submersão em (x, y).

Considere agora a composição $G \times H \xrightarrow{\psi} R \xrightarrow{\mathrm{pr}_2} G$, em que $\psi(x, h) = (xh, x)$ para todo $(x, h) \in G \times H$. Então $\mathrm{pr}_2 \circ \psi$ é a projeção em G, que é uma submersão. Logo pr_2 é uma submersão em todo ponto na imagem de ψ. Como ψ é sobrejetiva, o resultado segue. ■

Note que a ação de G em G/H é analítica e que, se H é um subgrupo normal em G, então G/H é um grupo analítico.

Dizemos que um grupo analítico G **age** sobre uma variedade analítica X se é dado um morfismo de variedades $\phi : G \times X \to X$ possuindo as propriedades usuais de ação de grupos (em particular, fixado $g \in G$, a aplicação $\psi(x) = \phi(x, g)$ é um isomorfismo de variedades). Sejam, assim, G um grupo analítico agindo sobre variedade X e x_0 um ponto de X. Sejam também $\phi_0 : G \to X, g \mapsto x^g$ e H o estabilizador de x_0.

Teorema (T.3.11). *Se ϕ_0 é uma subimersão, então H é um subgrupo de Lie de G e a aplicação quociente $\overline{\phi_0} : G/H \to X$ é uma imersão.*

Demonstração: Pelo Teorema 2.11, H é subvariedade de G. Além disso, como $\mathrm{Ker}(T_g\phi_0) = T_g(gH)$, segue-se que $\mathrm{Ker}(T_{gH}\overline{\phi}_0) = 0$. ■

Corolário (C.3.12). *Se $\psi : G_1 \to G_2$ é um homomorfismo de grupos analíticos que é uma subimersão, então $\mathrm{Ker}\,\psi$ é um subgrupo de Lie normal de G_1 e a aplicação induzida $\psi : G/K \to G_2$ é uma imersão.*

Teorema (T.3.13). *Se k tem característica zero, então ϕ_0 é uma subimersão.*

Demonstração: Seja $g_0 \in G$ tal que o posto de $T_g\phi_0$ é maximal. Então, como $\mathrm{rank}(T_g\phi_0)$ é semicontínua inferiormente, em uma vizinhança de g_0, $\mathrm{rank}\, T_g\phi_0$ é constante. Como G é um grupo, segue-se que o posto de $T_g\phi_0$ é constante e, pelo 2.6, ϕ_0 é uma subimersão. ■

Com os resultados acima, podemos livremente tomar quocientes de grupos analíticos sobre corpos de característica zero, obtendo uma estrutura analítica canônica nos quocientes.

3.1.3 Outros exemplos de grupos

Nesta subseção colecionamos alguns exemplos interessantes de grupos analíticos p-ádicos.

Exemplo (E.3.14). Seja $\mathcal{K}$ uma álgebra de divisão sobre $\mathbb{Q}_p$ ou $\mathbb{Z}_p$. Então o grupo $\mathrm{GL}_n(\mathcal{K})$ dos elementos invertíveis em $\mathrm{End}(\mathcal{K}^n)$ é analítico pelo exemplo 3.2.

Estudemos um outro exemplo concreto: $\mathrm{SL}_1(\mathbb{D}_p)$. Seja p um primo ímpar e $\eta \in \{1, \dots, p-1\}$ um não quadrado módulo p. Seja $\mathbb{D}_p$ a álgebra sobre $\mathbb{Q}_p$ gerada por u e v sujeita às relações $u^2 = \eta$, $v^2 = p$ e $uv = -vu$. Então $\{1, u, v, uv\}$ é uma base para $\mathbb{D}_p$. Definimos Δ_p como $\mathbb{Z}_p + \mathbb{Z}_p u + \mathbb{Z}_p v + \mathbb{Z}_p uv$ (o único subanel compacto maximal dentro de $\mathbb{D}_p$). Note que todo elemento de $x \in \mathbb{D}_p$ é da forma $p^{-s}z$, com $z \in \Delta_p$ e $s \geq 0$.

Definimos a norma reduzida em $\mathbb{D}_p$ por $N(\alpha + \beta u + \gamma v + \delta uv) = \alpha^2 - \eta\beta^2 - p\gamma^2 + \eta p\delta^2 \in \mathbb{Q}_p$. Vamos mostrar que se $N(x) = 0$, então $x = 0$. Notemos que é suficiente mostrarmos isso para $x \in \Delta_p$. Seja $x = \alpha + \beta u + \gamma v + \delta uv \in \Delta_p$ tal que $N(x) = 0$. Aplicando a redução módulo p, obtemos que $\alpha^2 - \eta\beta^2 \equiv 0 \mod p$, o que implica α e β serem múltiplos de p. Escrevendo $\alpha = p\alpha'$ e $\beta = p\beta'$, obtemos que $p^2\alpha'^2 - \eta p^2\beta'^2 - p\gamma^2 + \eta p\delta^2 = 0$. Dividindo por p, $p\alpha'^2 - \eta p\beta'^2 - \gamma^2 + \eta\delta^2 = 0$ e, após reduzir a módulo p novamente, obtemos que $\eta\delta^2 - \gamma^2 \equiv 0 \mod p$, implicando γ e δ serem múltiplos de p. Ou seja, $x = pz$, com $z \in \Delta_p$. Como $N(x) = p^2 N(z)$, $N(z) = 0$ e, similarmente, z é múltiplo de p. Consequentemente, $x \in p^n\Delta_p$ para todo n. Logo $x = 0$.

Podemos, assim, definir o inverso de um elemento não nulo de $\mathbb{D}_p$. Definimos o conjugado de um elemento $z = \alpha + \beta u + \gamma v + \delta uv$ em $\mathbb{D}_p$ por $z^* = \alpha - \beta u - \gamma v - \delta uv$. É rotineiro verificarmos que $zz^* = N(z)$. Como se $N(z) = 0$ apenas quando $z = 0$, para $z \neq 0$ definimos $z^{-1} = z^*/N(z)$. Assim, concluímos que $\mathbb{D}_p$ é uma álgebra de divisão sobre $\mathbb{Q}_p$. Segue-se que $\mathrm{GL}_n(\mathbb{D}_p)$ é um grupo analítico de dimensão $4n$.

Observe que $N : \mathbb{D}_p \to \mathbb{Q}_p$ é uma aplicação analítica entre $\mathbb{Q}_p^4$ e $\mathbb{Q}_p$. Se $q = (a, b, c, d)$, a diferencial de N no ponto q é expressa pela matriz $\begin{pmatrix} 2a & -2\eta b & 2pc & 2\eta pd \end{pmatrix}$. Assim, fica claro que $dN_q : \mathbb{Q}_p^4 \to \mathbb{Q}_p$ é sobrejetiva para todo $q \neq 0$. Portanto, todo elemento não nulo da imagem de N é um valor regular. Em particular, $N^{-1}(1)$ tem estrutura de variedade. Note também que se x e y são elementos de norma 1, então xy também tem norma 1, bem como x^{-1} e y^{-1}. Portanto, $N^{-1}(1)$ tem estrutura de grupo. Denotamos esse grupo por $\mathrm{SL}_1(\mathbb{D}_p)$. É claro que a multiplicação no grupo é analítica, já que $\mathrm{GL}_1(\mathbb{D}_p)$ é grupo analítico.

Proposição (P.3.15). O grupo $\mathrm{SL}_1(\mathbb{D}_p)$ é compacto.

Demonstração: Seja $x \in \mathrm{SL}_1(\mathbb{D}_p)$. Escrevemos $x = \alpha + \beta u + \gamma v + \delta uv$. Então $\alpha^2 - \eta\beta^2 - p\gamma^2 + p\eta\delta^2 = 1$. Note que $v_p(\alpha^2 - \eta\beta^2)$ é par, enquanto $v_p(p\eta\delta^2 - p\gamma^2)$ é ímpar. Portanto $0 = v_p(\alpha^2 - \eta\beta^2 - p\gamma^2 + p\eta\delta^2) = \min\{v_p(\alpha^2 - \eta\beta^2), v_p(p\eta\delta^2 - p\gamma^2)\}$. Ou seja, tanto $\alpha^2 - \eta\beta^2$ quanto $p\eta\delta^2 - p\gamma^2$ estão em $\mathbb{Z}_p$. Como $v_p(p\eta\delta^2 - p\gamma^2)$ é ímpar e maior do que zero, concluímos que $\eta\delta^2 - \gamma^2$ também está em $\mathbb{Z}_p$.

Como $\alpha^2 - \eta\beta^2$ está em $\mathbb{Z}_p$. Escrevemos $\alpha = zp^n$, $\beta = z'p^m$ com z, z' invertíveis em $\mathbb{Z}_p$ e assumimos $m > n$. Então $\alpha^2 - \eta\beta^2 = p^{2n}(z^2 - \eta z'^2 p^{2(m-n)})$. Como $z^2 - \eta z'^2 p^{2(m-n)}$ é invertível, então $v_p(\alpha^2 - \eta\beta^2) = 2n$. Sabendo que $v_p(\alpha^2 - \eta\beta^2) > 0$, obtemos que $n > 0$. Como $m > n$, $\alpha, \beta \in \mathbb{Z}_p$. Similarmente, concluímos que $\delta, \gamma \in \mathbb{Z}_p$.

Ou seja, mostramos que $\mathrm{SL}_1(\mathbb{D}_p)$ está contido em Δ_p. Como N é contínua, $\mathrm{SL}_1(\mathbb{D}_p) = N^{-1}(1)$ é fechado em $\mathbb{D}_p$ e, portanto, em Δ_p. Como Δ_p é compacto, segue-se que $\mathrm{SL}_1(\mathbb{D}_p)$ é compacto. ■

Exemplo (E.3.16) (Um exemplo intruso). Aproveitamos o momento para definirmos a álgebra de Lie $\mathfrak{sl}_1(\mathbb{D}_p)$, uma álgebra de Lie simples associada a $\mathbb{D}_p$. O traço reduzido de um elemento $x = \alpha + \beta u + \gamma_v + \delta uv$ é $\mathrm{Tr}(x) = 2\alpha$. Os elementos de traço reduzido zero em $\mathbb{D}_p$ formam uma subágebra de Lie simples de $\mathbb{D}_p$, denotada por $\mathfrak{sl}_1(\mathbb{D}_p)$. Além disso, $\mathfrak{sl}_1(\mathbb{D}_p)$ não possui subálgebras de dimensão 2 e, portanto, é uma álgebra de Lie simples de dimensão 3 que não é isomorfa a $\mathfrak{sl}_2(\mathbb{Q}_p)$ (a álgebra de Lie das matrizes dois-por-dois de traço zero com entradas em $\mathbb{Q}_p$). Observamos que as duas álgebras de Lie simples mencionadas esgotam os exemplos de álgebras de Lie simples de dimensão 3 sobre $\mathbb{Q}_p$ (vide [KLGP97] XII.a).

Exemplo (E.3.17). Se k é uma extensão finita de $\mathbb{Q}_p$, os grupos $\mathrm{SL}_n(\mathcal{O}_k)$ e $\mathrm{SL}_n(k)$ são analíticos, sendo imagem inversa do valor regular 1 pelo determinante, que é uma aplicação analítica. É evidente que $\mathrm{SL}_n(\mathcal{O}_k)$ é compacto.

Exemplo (E.3.18). Se k é uma extensão finita de $\mathbb{Q}_p$, o grupo $\mathrm{PSL}_n(k) = \mathrm{SL}_n(k)/Z(\mathrm{SL}_n(k))$ é um exemplo de grupo analítico p-ádico simples (a estrutura de variedade desse quociente decorre do fato de que $Z(\mathrm{SL}_n(k))$, sendo finito, é trivialmente subvariedade de $\mathrm{SL}_n(k)$). O grupo $\mathrm{PSL}_n(k)$ tem como subgrupo aberto $\mathrm{PSL}_n(\mathcal{O}_k)$, que não é simples (pois é profinito).

Exemplo (E.3.19). Se H e K são grupos analíticos, um produto semidireto $K \rtimes H$ tem estrutura de grupo analítico se cada automorfismo induzido por um elemento de H é analítico, isto é, se a imagem do homomorfismo $\varphi : H \to \mathrm{Aut}\, K$ está contida no subgrupo $\mathrm{Aut}^*\, K$ dos automorfismos analíticos de K.

Desta forma podemos construir, por exemplo, o grupo afim $k^n \rtimes \mathrm{GL}_n(k)$ de dimensão $2n$. Similarmente, podemos construir grupos como $\mathcal{O}_k^n \rtimes \mathrm{GL}_n(k)$ e $\Delta_p \rtimes \mathrm{SL}_1(\mathbb{D}_p)$.

Exemplo (E.3.20). Seja G o produto semidireto de um grupo abeliano pro-p livre de base $(e_1, \ldots, e_{p-1})$ com o grupo pro-p $\overline{\langle g \rangle}$, com ação dada por $g \cdot e_{p-1} = -e_1 - \ldots - e_{p-2}$ e, para $1 \leq i < p-1$, $g \cdot e_i = e_{i+1}$. G é isomorfo a $\mathbb{Z}_p^{p-1} \rtimes_\varphi \overline{\langle g \rangle}$, em que $\varphi : \overline{\langle g \rangle} \to \mathrm{GL}_{p-1}(\mathbb{Z}_p) = \mathrm{Aut}(\mathbb{Z}_p^{p-1})$ é definida por

$$g \mapsto \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -1 & -1 & -1 & \ldots & -1 & 0 \end{pmatrix}$$

e estendida por continuidade. É claro que G é um grupo analítico, visto que todo automorfismo de $\mathbb{Z}_p^{p-1}$ é analítico.

Exemplo (E.3.21). O grupo de matrizes $\left(\begin{smallmatrix} 1 & \mathbb{Z}_p \\ 0 & 1+p^n\mathbb{Z}_p \end{smallmatrix}\right)$ é um grupo analítico de dimensão 2, isomorfo, como variedade, a $\mathbb{Z}_p \times (1 + p^n\mathbb{Z}_p)$.

Exemplo (E.3.22). O grupo $\mathrm{SL}_2(\mathbb{Z}_p)$ é profinito e, portanto, tem um subgrupo pro-p maximal G. Mostraremos que G é aberto em $\mathrm{SL}_2(\mathbb{Z}_p)$, concluindo que G é um grupo analítico pro-p. Consideremos a seguinte sequência exata de grupos:

$$1 \to L_2 \xrightarrow{\iota} \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}) \xrightarrow{\varphi_m} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1$$

Em que $L_2 = \{1+U : U \in M_2(p\mathbb{Z}/p^m\mathbb{Z})\}$ é um subgrupo de $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$ (de fato, se $g = \left(\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right) \in L_2$, então $\det g = (ad-bc)+a+d+1 \equiv 1(\mod p)$ é invertível em $\mathbb{Z}/p^m\mathbb{Z}$), ι é a inclusão e φ_m é a aplicação canônica de redução módulo p. Então $|\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})| = |L_2| \cdot |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = p^{4(m-1)}(p^2-1)(p^2-p) = p^{4m-3}(p^2-1)(p-1)$. Considere o homomorfismo sobrejetivo $\det : \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}) \to (\mathbb{Z}/p^m\mathbb{Z})^\times$. Seu núcleo é $\mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$ e, pelo teorema do isomorfismo, $|\mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})| = p^{3m-2}(p^2-1)$.

Notemos que $\varprojlim \mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}_p)$ possui ordem $\mathrm{mmc}\{p^{3m-2}(p^2-1)\} = p^\infty(p^2-1)$. Concluímos que um subgrupo pro-p maximal de $\mathrm{SL}_2(\mathbb{Z}/p^m\mathbb{Z})$ tem índice p^2-1 e o resultado segue.

O resultado é análogo para $\mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z})$ e $\mathrm{GL}_n(\mathbb{Z}/p^m\mathbb{Z})$, já que o índice de um subgrupo pro-p maximal desses grupos não depende de m.

3.2 Grupos p-saturáveis

Nesta seção, apresentamos a classe dos grupos p-valorados e p-saturados e expomos alguns resultados inicias sobre a estrutura deles. Esses grupos foram introduzidos em [Laz65], mas faremos uma síntese da exposição de [Sch11].

Seja G um grupo abstrato e $\omega : G \to \mathbb{R} \cup \{\infty\}$ uma função tal que para quaisquer $g, h \in G$:

(i) $\omega(g) = \infty$ se, e somente se $g = 1$;

(ii) $\omega(g) > \dfrac{1}{p-1}$;

(iii) $\omega(g^{-1}h) \geq \min\{\omega(g), \omega(h)\}$;

(iv) $\omega([g,h]) \geq \omega(g) + \omega(h)$;

(v) $\omega(g^p) = 1 + \omega(g)$.

Dizemos que ω é uma ***p*-valoração** sobre G e que o par (G, ω) é um **grupo *p*-valorado**. Definimos, para todo $\nu > 0$ os subgrupos normais de G

$$G_\nu := \{g \in G, \omega(g) \geq \nu\}, G_{\nu+} := \{g \in G, \omega(g) > \nu\},$$

de forma que $G_\nu/G_{\nu+}$ é um subgrupo central de $G/G_{\nu+}$, para todo $\nu > 0$. Tomando a família $\{G_\nu\}_{\nu>0}$ como sistema fundamental de vizinhanças abertas de 1 em G, o grupo G é um grupo topológico Hausdorff. Sempre pensaremos (G, ω) como grupo topológico com a topologia induzida por ω.

Para todo $\nu > 0$, o quociente $\mathrm{gr}_\nu G := G_\nu/G_{\nu+}$ é abeliano e será denotado aditivamente. Definimos o grupo abeliano graduado

$$\mathrm{gr}\, G = \bigoplus_{\nu>0} \mathrm{gr}_\nu G.$$

Observe que G é um $\mathbb{F}_p$-espaço vetorial, já que $p\xi = 0$ para todo $\xi \in \mathrm{gr}_\nu G$. O lema abaixo mostra que $\mathrm{gr}\, G$ tem uma estrutura canônica de $\mathbb{F}_p$-álgebra de Lie graduada.

Lema (L.3.23) ([Sch11], 23.4, 23.5). Para quaisquer $\nu, \nu' > 0$, a aplicação abaixo é bem-definida, $\mathbb{F}_p$-bilinear, antissimétrica e satisfaz a identidade de Jacobi.

$$[\cdot,\cdot]_\nu : \mathrm{gr}_\nu G \times \mathrm{gr}_{\nu'} G \to \mathrm{gr}_{\nu+\nu'} G,\ (\xi, \eta) \mapsto [\xi, \nu] := [g,h]G_{(\nu+\nu')+},$$

em que g, h são representantes de ξ e ν, respectivamente. Assim, podemos estender tais aplicações para um colchete de Lie $[\cdot,\cdot] : \operatorname{gr} G \times \operatorname{gr} G \to \operatorname{gr} G$.

Mais ainda, $\operatorname{gr} G$ tem uma estrutura de $\mathbb{F}_p[P]$-álgebra de Lie graduada, em que $\mathbb{F}_p[P]$ é o anel de polinômios em uma variável sobre $\mathbb{F}_p$. Esse é o conteúdo do lema abaixo:

Lema (L.3.24) ([Sch11], 25.1, 25.2, 25.3). Para qualquer $\nu > 0$, a aplicação abaixo é bem-definida e $\mathbb{F}_p$-linear.

$$\begin{aligned} P_\nu : \operatorname{gr}_\nu G &\to \operatorname{gr}_{\nu+1} G \\ gG_{\nu+} &\mapsto g^p G_{(\nu+1)+}. \end{aligned}$$

Estendemos por linearidade essas aplicações para uma aplicação $\mathbb{F}_p$-linear de grau um (isto é, leva elementos homogêneos de grau ν em elementos homogêneos de grau $\nu+1$) $P : \operatorname{gr} G \to \operatorname{gr} G$. Podemos, assim, enxergar $\operatorname{gr} G$ como $\mathbb{F}_p[P]$-módulo. Além disso, $\operatorname{gr} G$ é um $\mathbb{F}_p[P]$-módulo livre-de-torção e o colchete de Lie em $\operatorname{gr} G$ é $\mathbb{F}_p[P]$-bilinear, dando a $\operatorname{gr} G$ uma estrutura de $\mathbb{F}_p[P]$-álgebra de Lie.

Até o final da seção, (G, ω) é um grupo pro-p p-valorado cuja topologia induzida por ω coincide com a topologia de G (em particular, $G = \varprojlim G/G_\nu$). Dizemos que (G, ω) é de **posto finito** (como grupo p-valorado) se $\operatorname{gr} G$ é um $\mathbb{F}_p[P]$-módulo finitamente gerado. Como $\operatorname{gr} G$ é livre-de-torção e $\mathbb{F}_p[P]$ é um domínio de ideais principais, se (G, ω) tem posto finito, então $\operatorname{gr} G$ é livre e diremos que o posto de (G, ω) é o posto de $\operatorname{gr} G$ como $\mathbb{F}_p[P]$-módulo. **Atenção!** A princípio, esse posto não tem relação com o posto de G como grupo pro-p. Nesta seção, quando nos referirmos ao posto de um grupo p-valorado, sempre estaremos nos referindo ao posto de $\operatorname{gr} G$ como $\mathbb{F}_p[P]$-módulo.

Uma **base ordenada** de um grupo p-valorado (G, ω) é uma lista finita de elementos $(g_1, \dots, g_r)$ tais que a aplicação

$$\begin{aligned} \mathbb{Z}_p^r &\to G \\ (\lambda_i)_{i=1}^r &\mapsto g_1^{\lambda_1} \dots g_r^{\lambda_r} \end{aligned}$$

é um homeomorfismo e $\omega(g_1^{\lambda_1} \dots g_r^{\lambda_r}) = \min_i(\omega(g_i) + v_p(\lambda_i))$ para qualquer $(\lambda_i)_{i=1}^r \in \mathbb{Z}_p^r$. É claro que se $(g_1, \dots, g_r)$ é uma base ordenada de G, então $G = \langle g_1, \dots, g_r \rangle$.

Proposição (P.3.25) ([Sch11], 26.6, 26.7, 26.8). Todo grupo p-valorado (G, ω) de posto finito tem base ordenada de tamanho igual ao seu posto. Em particular, G é finitamente gerado como grupo pro-p. Além disso, elementos de uma base ordenada de (G, ω) não são potências de p.

Um grupo p-valorado (G, ω) de posto finito é ***p*-saturado** se todo $g \in G_{\frac{p}{p-1}+}$ é uma potência de p e se G é completo em relação à topologia definida pela filtração ω. Grupos p-saturados terão um papel fundamental até o final deste trabalho. Finalizamos esta seção coletando algumas propriedades que utilizaremos na próxima seção acerca de grupos p-valorados e p-saturados.

Proposição (P.3.26) ([Sch11], 26.10, 26.12, 26.15). Seja (G, ω) um grupo p-valorado de posto finito igual a $\operatorname{rank}(G, \omega)$. Valem:

(i) (G, ω) é p-saturado se, e somente se, $P(\operatorname{gr} G) = \bigoplus_{\nu > \frac{p}{p-1}} \operatorname{gr}_\nu G$;

(ii) Se (G,ω) é p-saturado, então $[G : G^{p^n}] = p^{n\,\mathrm{rank}(G,\omega)}$;

(iii) Qualquer outra valoração ω' sobre G define sua topologia e $\mathrm{rank}(G,\omega) = \mathrm{rank}(G,\omega')$;

(iv) G^{p^n} é um sistema fundamental de vizinhanças de 1 e $\mathrm{rank}(G,\omega) = \lim_{n\to\infty} \dfrac{v_p([G : G^{p^n}])}{n}$.

Dizemos que um grupo pro-p G é **p-valorável** se existe uma p-valoração ω que define a topologia de G e dizemos que G é **p-saturável** se existe uma p-valoração definindo a topologia de G de forma que (G,ω) é p-saturado.

3.3 Caracterização dos grupos analíticos

Nessa seção, caracterizaremos grupos analíticos p-ádicos como grupos topológicos com um subgrupo aberto p-saturável. Esta caracterização foi feita originalmente por Lazard em [Laz65]. A principal referência utilizada foi [Sch11].

Iniciamos esta seção demonstrando que grupos analíticos possuem um subgrupo aberto p-saturável. Antes, relembremos que se G é um grupo pro-p p-valorado de posto finito, pela Proposição 3.26, as topologias de G como grupo pro-p e grupo p-valorado coincidem. Usaremos esse fato extensivamente no decorrer do texto.

Teorema (T.3.27). *Seja G um grupo analítico p-ádico. Então existe um subgrupo aberto H de G compacto e uma p-valoração ω em H tomando valores inteiros e definindo a topologia em H de forma que (H,ω) é p-saturado e o posto de H como grupo p-valorado é igual à dimensão de G como variedade.*

Demonstração: Já que buscamos mostrar que G possui um subgrupo aberto p-saturável, pela Proposição 3.7, podemos supor, sem perda de generalidade, que G é um grupo padrão de dimensão r.

Definimos, para cada x em G, $\omega(x) = \min\{v_p(x_i)\}$ (em que $x = (x_1,\dots,x_n)$) e os subgrupos $G_n = \{x \in G, \omega(x) \geq n\}$ (segue-se da definição de lei formal de grupo que G_n é um subgrupo de G). Os subgrupos G_n para n inteiro constituem um sistema fundamental de vizinhanças da identidade em G. Seja $H = G_2$ e defina, para elementos de H, $\omega'(x) = \omega(x) - 1$ se $p > 2$ e $\omega'(x) = \omega(x)$ se $p = 2$. Então como consequência da Proposição 3.9, $\omega'(x) = \infty$ se, e somente se, $x = 0$, $\omega'(x^{-1}y) \geq \min\{\omega'(x), \omega'(y)\}$, $\omega'(x) > (p-1)^{-1}$ e $\omega'([x,y]) \geq \omega'(x) + \omega'(y)$. Note que, de fato, a mudança para o caso $p = 2$ é necessária, visto que se $p = 2$, em um elemento de H com $\omega(x) = 2$, $\omega(x) - 1 = (2-1)^{-1}$. Como $f_p(x) = px + Q(x)$, em que $Q(x)$ é uma série de potências cujos monômios têm grau pelo menos dois em x, se $x \in H$, $\omega'(f_p(x)) = \min\{\omega'(px), \omega'(Q(x))\} = \omega'(x) + 1$. Logo ω' é uma p-valoração em H.

Defina os subgrupos H_n, H_{n+} do grupo p-valorado H naturalmente. Note que como ω' toma valores inteiros, $H_{n+} = H_{n+1}$. H é pro-p e, portanto, $\mathrm{gr}_n(H)$ é um p-grupo abeliano finito para todo $n \in \mathbb{N}$ ($n \geq 2$ se $p = 2$). Como $\omega'(x^p) = \omega'(x) + 1$, se $x \in H_n - H_{n+1}$, $x^p \in H_{n+1} - H_{n+2}$. O que mostramos é que a aplicação $P : \mathrm{gr}_n(H) \to \mathrm{gr}_{n+1}(H)$ é injetiva e, como os grupos $\mathrm{gr}_m(H)$ são finitos, P é sobrejetiva. Isso mostra que $\mathrm{gr}(H)$ é gerado por $\mathrm{gr}_1(H)$ (no caso de $p > 2$, para $p = 2$ é gerado por $\mathrm{gr}_2(H)$) como $\mathbb{F}_p[P]$-módulo. Em particular, é finitamente gerado e, portanto H tem posto finito como grupo p-valorado. Note que em, $\mathrm{gr}(H) = \bigoplus_{n\geq\delta} \mathrm{gr}_n(H)$ a imagem de P é $\bigoplus_{n\geq\delta+1} \mathrm{gr}_n(H)$, em que $\delta = 1$ se $p > 2$ e $\delta = 2$ se $p = 2$. Como ω' toma apenas valores inteiros, $n \geq \delta + 1$ se, e somente se, $n > p(p-1)^{-1}$ e, portanto, $P(\mathrm{gr}(H)) = \bigoplus_{n>\frac{p}{p-1}} \mathrm{gr}_n(H)$ pela Proposição 3.26, H é p-saturado.

Resta-nos mostrar que $\text{rank}(H, \omega') = r$. Identificando o grupo G com $p\mathbb{Z}_p^r$, identificamos H com $p^2\mathbb{Z}_p^r$. Afirmamos que $f_p(H) = p^3\mathbb{Z}_p^r$. É claro que $f_p(H) \subseteq p^3\mathbb{Z}_p^r$. Agora, como H é p-saturado, qualquer elemento de $p^3\mathbb{Z}_p^r$ é uma potência de p. Seja μ a medida de Haar normalizada em $\mathbb{Z}_p^r$. Então o índice de H^p em H é igual a $\dfrac{\mu(p^2\mathbb{Z}_p^r)}{\mu(p^3\mathbb{Z}_p^r)} = p^r$. Pela Proposição 3.26, $\text{rank}(H, \omega') = \lim\limits_{n\to\infty} \dfrac{v([H : H^{p^n}])}{n}$ e $[H : H^{p^n}] = [H : H^p]^n = p^{rn}$. Assim, $\text{rank}(H, \omega') = \lim\limits_{n\to\infty} \dfrac{rn}{n} = r = \dim(G)$. ■

Podemos agora compreender melhor o significado do invariante i definido no Capítulo 2 (vide 2.18). Relembrando, se X é uma variedade p-ádica compacta, então X é uma união disjunta e finita de n bolas. Então $i(X)$ é a classe de n módulo $(p-1)$. Se G é um grupo analítico p-ádico compacto, então G é profinito. Pelo resultado acima, G é virtualmente pro-p (já que grupos p-valorados são pro-p) e, portanto, a ordem de G é $p^\infty N$, com n coprimo a p (se G é infinito). G tem um subgrupo aberto padrão H de índice igual a $p^m N$, para algum $m \geq 0$. Sabemos que grupos padrão são variedades isomorfas a $\mathbb{Z}_p^r$ e, portanto, bolas. G é a união disjunta das $p^m N$ classes laterais de H e, portanto, é a união disjunta de $p^m N$ bolas. Segue-se que $i(G) \equiv N \mod (p-1)$. Ou seja, $i(G)$ é o índice de um pro-p subgrupo de Sylow de G módulo $p-1$.

O lema abaixo é o coração da recíproca do Teorema acima. Omitiremos sua demonstração por ser extensa e técnica. Deixamos duas referências para o leitor interessado.

Lema (L.3.28) ([Laz65], 3.3.1.5; [Sch11], 29.2). Seja G um grupo p-valorado de posto finito r e $(x_i)_{i=1}^r$ uma base ordenada de G. Seja $(y_j)_{j=1}^s$ uma família finita qualquer de elementos de G. Para todo $\mu \in \mathbb{Z}_p^s$, associamos o elemento $\nu(\mu) = \prod\limits_{j=1}^{s} y_j^{\mu_j}$. Escrevendo $\nu(\mu)$ na base ordenada $(x_i)_{i=1}^r$, obtemos $\prod\limits_{j=1}^{s} y_j^{\mu_j} = \prod\limits_{i=1}^{r} x_i^{\lambda_i}$. A função $\lambda : \mathbb{Z}_p^s \to \mathbb{Z}_p^r, \mu \mapsto (\lambda_i)_{i=1}^r$ é analítica.

Imediatamente segue-se que:

Corolário (C.3.29) ([Laz65], 3.3.1.7). *Seja G é um grupo p-valorado de posto r e $x = (x_i)_{i=1}^r$ uma base ordenada de G. Defina uma estrutura analítica em G pelo homeomorfismo $f : \mathbb{Z}_p^r \to G$ induzido pela base ordenada x. Então a multiplicação e a inversão em G são aplicações analíticas, isto é, G é um grupo analítico.*

Mencionamos aqui um importante resultado de compatibilidade entre diferentes estruturas analíticas para um mesmo grupo p-valorável.

Lema (L.3.30) ([Laz65], 3.3.2.1). Se G é um grupo analítico e K é um subgrupo aberto de G p-valorável, a estrutura analítica em K como grupo p-valorável coincide com a estrutura herdada de G.

Tendo em vista os resultados enunciados nesta seção, concluímos:

Teorema (T.3.31). *Seja G um grupo topológico. Então G tem a estrutura de um grupo analítico p-ádico se, e somente se, G possui um subgrupo aberto H p-saturável.*

Demonstração: Se G é analítico, pelo Teorema 3.27, G possui um subgrupo aberto H p-saturável. Reciprocamente, se G possui um subgrupo aberto H p-saturável, H é um grupo analítico pelo Corolário

3.29. Daí G é a união disjunta das classes laterais de H, possuindo, portanto, estrutura de grupo analítico p-ádico. ■

Como dissemos, os resultados apresentados acima foram obtidos inicialmente em [Laz65]. Na década de 1980, nos artigos [LuMa87a] e [LuMa87b], os autores introduzem a classe dos p-grupos *powerful*, bem como os grupos pro-p uniformemente *powerful*, trazendo uma nova abordagem para caracterização dos grupos analíticos pro-p. Tal abordagem é feita do ponto de vista da teoria de grupos pro-p e, em certo sentido, é mais acessível e familiar. Finalizaremos essa seção relacionando as duas abordagens, culminando na caracterização obtida por Lubotzky e Mann.

Um grupo pro-p G é ***powerful*** se $p > 2$ e G/G^p é abeliano ou se $p = 2$ e G/G^4 é abeliano.

Proposição (P.3.32). Sejam $p > 2$ e (G, ω) um grupo pro-p p-saturado. Se ω toma valores inteiros, então G/G^p é abeliano, isto é, G é *powerful*.

Demonstração: Como ω toma valores inteiros, $G_1 = G$ e $G_{1+} = G_2$. Como G é p-saturado, $G_2 = G^p$. Daí $G/G^p = G_1/G_2 = G_1/G_{1+}$ é abeliano. ■

Corolário (C.3.33). *Sejam $p > 2$ e (G, ω) um grupo pro-p p-saturado. Então G^p é powerful.*

Demonstração: Pela compacidade de G, existe $\mu > (p-1)^{-1}$ tal que $\omega(g) > \mu$ para todo $g \in G$. Assim, se $g \in G^p$, $\omega(g) > 1 + \mu$. Para $g \in G^p$, defina $\omega'(g) = \lfloor \omega(g) - \mu \rfloor$. Sejam $g, h \in G^p$. Então: (1) $\omega'(g^p) = \lfloor \omega(g^p) - \mu \rfloor = \lfloor \omega(g) + 1 - \mu \rfloor = 1 + \lfloor \omega(g) - \mu \rfloor = 1 + \omega'(g)$; (2) $\omega'(g^{-1}h) = \lfloor \omega(g^{-1}h) - \mu \rfloor \geq \lfloor \min\{\omega(g), \omega(h)\} - \mu \rfloor = \min\{\omega(g) - \mu, \omega(h) - \mu\} = \min\{\omega'(g), \omega'(h)\}$; (3) $\omega'([g,h]) = \lfloor \omega([g,h] - \mu \rfloor \geq \lfloor \omega(g) + \omega(h) - \mu \rfloor \geq \lfloor \omega(g) + \omega(h) - 2\mu \rfloor \geq \lfloor \omega(g) - \mu \rfloor + \lfloor \omega(h) - \mu \rfloor = \omega'(g) + \omega'(h)$; (4) $\omega'(g) \geq 1 > (p-1)^{-1}$. Assim, (G^p, ω') é um grupo p-valorado. Se $g \in G^p$ é tal que $\omega'(g) > p(p-1)^{-1} > 1$, como ω' toma valores inteiros, $\omega'(g) \geq 2$, ou seja $\omega(g) \geq 2 + \mu > 2 + (p-1)^{-1}$. Como (G, ω) é p-saturado, $g = h^{p^2}$, ou seja, existe $h^p \in G^p$ tal que $g = (h^p)^p$. Logo (G^p, ω') é p-saturado. Portanto, pela Proposição acima, G^p é *powerful*. ■

Apresentamos também as versões para o caso em que $p = 2$:

Proposição (P.3.34). Seja (G, ω) um grupo 2-saturado. Se ω toma valores inteiros, então G/G^4 é abeliano, isto é, G é *powerful*.

Demonstração: Como ω toma valores inteiros, $G_2 = G$. Como G é 2-saturado, $G^2 = G_3$ e $G^4 = G_4$. Se $g, h \in G_2$, $\omega([g,h]) \geq 4$, ou seja $[g,h] \in G_4$. Assim, $G_2/G_4 = G/G^4$ é abeliano. ■

Corolário (C.3.35). *Seja (G, ω) um grupo pro-2 2-saturado. Então G^4 é powerful.*

Demonstração: Pela compacidade de G, existe $\mu > 1$ tal que $\omega(g) > \mu$ para todo $g \in G$. Assim, se $g \in G^4$, $\omega(g) > 2 + \mu$. Para $g \in G^4$, defina $\omega'(g) = \lfloor \omega(g) - \mu \rfloor$. Sejam $g, h \in G^4$. Então: (1) $\omega'(g^2) = \lfloor \omega(g^2) - \mu \rfloor = \lfloor \omega(g) + 1 - \mu \rfloor = 1 + \lfloor \omega(g) - \mu \rfloor = 1 + \omega'(g)$; (2) $\omega'(g^{-1}h) = \lfloor \omega(g^{-1}h) - \mu \rfloor \geq \lfloor \min\{\omega(g), \omega(h)\} - \mu \rfloor = \min\{\omega(g) - \mu, \omega(h) - \mu\} = \min\{\omega'(g), \omega'(h)\}$; (3) $\omega'([g,h]) = \lfloor \omega([g,h]) - \mu \rfloor \geq \lfloor \omega(g) + \omega(h) - \mu \rfloor \geq \lfloor \omega(g) + \omega(h) - 2\mu \rfloor \geq \lfloor \omega(g) - \mu \rfloor + \lfloor \omega(h) - \mu \rfloor = \omega'(g) + \omega'(h)$; (4) $\omega'(g) \geq 2 > (2-1)^{-1}$. Assim, (G^4, ω') é um grupo 2-valorado. Se $g \in G^4$ é tal que $\omega'(g) > 2 = 2(2-1)^{-1}$, como ω' toma valores inteiros, $\omega'(g) \geq 3$, ou seja $\omega(g) \geq 3 + \mu > 3 + 1 = 4$. Como (G, ω) é 2-saturado e $\omega(g) > 3 + (2-1)^{-1}$, existe um h em G tal que $g = h^8$, isto é, $g = (h^4)^2$. Como $h^4 \in G^4$, (G^4, ω') é 2-saturado. Como ω' toma valores inteiros, G^4/G^{16} é abeliano, isto é, G^4 é *powerful*. ■

Corolário (C.3.36). *Um grupo pro-p p-saturável G é powerful se, e somente se, admite uma p-valoração ω de forma que (G,ω) é p-saturado e ω toma valores inteiros.*

Um grupo pro-p G é dito **uniformemente *powerful*** se é finitamente gerado, *powerful* e livre-de-torção. Enunciamos agora a caracterização de Lubotzky e Mann para os grupos analíticos p-ádicos.

Teorema (T.3.37). *Um grupo topológico possui a estrutura de grupo analítico p-ádico se, e somente se, possui um subgrupo aberto uniformemente powerful.*

Demonstração: Afirmamos que grupos uniformemente *powerful* são p-saturáveis. De fato, a família de subgrupos abertos G^{p^n} define a topologia de G (vide [DDMS99] 1.16, 3.6). Além disso, todo elemento de G^{p^n} é uma p^n-ésima potência (vide [DDMS99] 3.5). Assim, podemos definir uma p-valoração em G por $\omega(g) = \delta_p + \max_n\{g \in G^{p^n}\}$, em que $\delta_2 = 2$ e $\delta_p = 1$ se $p > 2$ (segue-se também de [DDMS99] 1.16 e 3.6 que $[G^{p_n}, G^{p^m}] \leq G^{p^{n+m}}$). Notemos que (G,ω) é p-saturado.

Por outro lado, pelos corolários 3.33 e 3.35, um grupo p-saturável possui um subgrupo aberto uniformemente *powerful*. Assim, o resultado segue do teorema 2.6. ■

Cuidado! Não mostramos que todo grupo p-saturado é *powerful*, mas sim que todo grupo p-saturado com sua p-valoração ω tomando valores inteiros é *powerful*. De fato, se G é um grupo p-saturado, G é analítico e possui um subgrupo aberto H que é p-saturado em relação a uma valoração tomando valores inteiros. H é uniformemente *powerful*. A questão de se todo grupo p-saturável é uniformemente *powerful* foi um problema em aberto por algumas décadas. Em [Klo05], o autor verifica que existem grupos p-saturáveis não uniformemente *powerful*. No Capítulo 5, verificaremos a existência de diversos grupos p-saturáveis não uniformemente *powerful*.

Finalizamos esta seção mostrando, por meio de um exemplo, que a classe dos grupos uniformemente *powerful* **não** é fechada para subgrupos abertos.

Exemplo (E.3.38). Se G é um grupo pro-p com apresentação

$$\langle x, y \mid [x,y] = x^{p^2} \rangle,$$

então G é uniformemente *powerful*. De fato, G é finitamente gerado, livre de torção e $G' = \langle x^{p^2} \rangle \leq G^p$. Considere o subgrupo $H = \langle x^p, y \rangle$. É claro que H é um subgrupo aberto de G. Observamos que

$$[x^p, y] = x^{-p}y^{-1}x^p y = x^{-p}(y^{-1}xy)^p = x^{-p}(x^{1+p^2})^p = x^{p^3},$$

que não pertence a H^p.

Capítulo 4

Teoria de Lie

Neste Capítulo apresentamos o principal método para investigação dos grupos analíticos p-ádicos: a Teoria de Lie. Nosso objetivo aqui é traduzir perguntas e problemas sobre grupos analíticos para perguntas e problemas sobre álgebras de Lie e, assim, buscar obter novas informações sobre nosso objeto original de estudo.

Para os grupos analíticos p-ádicos, podemos dizer que há duas "Teorias de Lie": aquela análoga à Teoria de Lie para grupos de Lie reais, em que basicamente traduzimos a maioria dos resultados clássicos para o caso p-ádico; e a elaborada por Lazard, a qual é particular aos grupos analíticos p-ádicos. Veremos no decorrer do Capítulo as vantagens e desvantagens de cada uma e a relação que se estabelece entre elas.

O Capítulo é dividido em cinco seções. As quatro primeiras exploram o último capítulo de [Ser00] e investigam a Teoria de Lie clássica, análoga ao caso real. Já a última seção é uma síntese de alguns dos principais resultados do capítulo IV de [Laz65] — aqui, novamente utilizamos como principal referência [Sch11].

4.1 A álgebra de Lie de um grupo de Lie

Seja $F(X,Y)$ uma lei formal sobre um corpo completo k. Vimos no Capítulo anterior que $F(X,Y) = X + Y + B(X,Y) + O(d^0 \geq 3)$, em que $B(X,Y)$ é uma forma bilinear em k^n. Vimos também que $[X,Y]_F = B(X,Y) - B(Y,X)$ satisfaz a identidade de Jacobi e, portanto, define uma estrutura de álgebra de Lie em k^n. Dizemos que $(k^n, [X,Y]_F)$ é a **álgebra de Lie do grupo formal F**.

Se G é uma peça de grupo sobre k, seja $L(G) = \mathfrak{g} = T_eG$. Para definirmos uma estrutura de álgebra de Lie em $\mathfrak{g}$, toma-se uma carta $c = (U, \phi, n)$ de G em e. A estrutura de grupo em G é induzida via $\phi : U \to k^n$ de uma lei formal de grupo F.

Seja $\overline{\phi} : \mathfrak{g} \to k^n$ a aplicação tangente de ϕ. Se $x, y \in \mathfrak{g}$, definimos $\overline{\phi}([x,y]_c) = [\overline{\phi}(x), \overline{\phi}(y)]_F$. Assim, definimos uma estrutura de álgebra de Lie em $\mathfrak{g}$, em que o colchete é dado por $[x,y]_c = \overline{\phi}^{-1}([\overline{\phi}(x), \overline{\phi}(y)]_F)$. Para que nossa definição seja satisfatória, é preciso que o colchete não dependa da escolha da carta em e.

Lema (L.4.1). Sejam $F(X,Y)$ e $F'(X',Y')$ duas leis formais de grupos e f um homorfismo formal de F para F'. Se f_1 é a componente linear de f (isto é, f_1 é linear e $f = f_1 + O(d^0 \geq 2)$), então $[f_1(X), f_1(Y)]_{F'} = f_1([X,Y]_F)$.

Demonstração: Pela Proposição 3.9, temos

$$f(X)^{-1}f(Y)^{-1}f(X)f(Y) = [f_1(X), f_1(Y)]_{F_1} + O(d^0 \geq 3)$$

$$f(X^{-1}Y^{-1}XY) = f_1([X,Y]_F) + O(d^0 \geq 3).$$

Basta compararmos os termos de grau 2. ■

Lema (L.4.2). Sejam G e G' peças de grupo, c e c' cartas em e e e' e $f : G- \to G'$ um homomorfismo local. Então $T_e f : \mathfrak{g} \to \mathfrak{g}'$ é um homomorfismo entre as álgebras de Lie dadas pelos colchetes $[\cdot,\cdot]_c$ e $[\cdot,\cdot]_{c'}$.

Demonstração: Podemos reduzir ao caso em que G e G' são dadas por leis formais de grupo. Assim, f pode ser vista como um homomorfismo formal entre as leis formais de grupo de G e G'. Sendo $T_e f$ a componente linear de f, pelo lema acima, é um homomorfismo entre álgebras de Lie. ■

Podemos aplicar o último lema ao caso em que c e c' são duas cartas em e. A mudança de coordenadas é um isomorfismo analítico e, portanto, a aplicação induzida entre as álgebras de Lie é um isomorfismo linear que, pelo último lema, é um homomorfismo de álgebras de Lie. Dizemos que $\mathfrak{g}$ com a estrutura de colchete herdada por uma carta qualquer em e é a **álgebra de Lie do grupo G** .

Exemplo (E.4.3). Seja R uma álgebra associativa com unidade de dimensão finita sobre k. Vimos que $\mathbb{G}_m(R)$ é um grupo analítico aberto em R. Daí, $T_1\mathbb{G}_m(R) = R$. A multiplicação em $\mathbb{G}_m(R)$ é da forma $(1+x)(1+y) = 1+x+y+xy$ e corresponde à lei formal de grupo $F(X,Y) = X+Y+XY$. Assim, o colchete de Lie em R é dado por $[x,y] = xy - yx$. Se $R = \mathrm{End}(k^n)$, obtemos $L(\mathrm{GL}_n(k)) \cong \mathfrak{gl}_n(k)$. Notemos que se $R = \mathrm{End}(\mathcal{O}_k^n)$ (visto como aberto em $\mathrm{End}(k^n)$), então $T_1(\mathrm{GL}_n(\mathcal{O}_k)) \cong \mathfrak{gl}_n(k) L(\mathrm{GL}_n(\mathcal{O}_k))$. Ou seja, grupos não isomorfos podem ter álgebras de Lie isomorfas.

4.2 Propriedades básicas e exemplos

Sejam G, H grupos analíticos e $f : H \to G$ um homomorfismo de grupos que é uma imersão, então f induz um homomorfismo injetivo $L(f) : L(H) \to L(G)$ entre as álgebras de Lie. Podemos, assim, identificar $L(H)$ com uma subálgebra de Lie de $L(G)$. Usaremos isso em particular no caso em que H é um subgrupo de Lie de G e f é a inclusão.

Teorema (T.4.4). *Se* $\mathrm{char}\, k = 0$ *e* H_1 *e* H_2 *são subgrupos de Lie de* G*, então* $H_1 \cap H_2$ *é um subgrupo de Lie de* G *e* $L(H_1 \cap H_2) = L(H_1) \cap L(H_2)$.

Demonstração: Pelo Teorema 3.10, G/H_1 é uma variedade. A ação natural de H_2 em G/H_1 tem como estabilizador da classe lateral H_1 o subgrupo $H_1 \cap H_2$ que, pelos Teoremas 3.11 e 3.13, é um subgrupo de Lie de G, já que $\mathrm{char}\, k = 0$. A imagem de $L(H_1 \cap H_2)$ em $L(G)$ é o núcleo da aplicação $\psi : T_e H_2 \to T_e G / T_e H_1$ induzida por $H_2 \to G/H_1, g \mapsto gH_1$. Mas $\mathrm{Ker}\, \psi = T_e H_2 \cap T_e H_1 = L(H_1) \cap L(H_2)$. ■

Corolário (C.4.5). *(1) Se* $L(H_1) \subset L(H_2)$*, então, em uma vizinhança de* e*,* $H_1 \subset H_2$*;*

(2) Se $L(H_1) = L(H_2)$*, então, em uma vizinhança de* e*,* $H_1 = H_2$*;*

(3) Sejam G_1, G_2 grupos analíticos e $\phi, \psi : G_1 \to G_2$ homomorfismos analíticos. Então ϕ e ψ concordam em uma vizinhança de e_1 se, e somente se, $L(\phi) = L(\psi)$.

Demonstração: Para demonstrarmos (1), basta observarmos que $L(H_1) \subset L(H_2)$, então $T_e(H_1 \cap H_2) = L(H_1) \cap L(H_2) = L(H_1) = T_e(H_1)$. Daí, em uma vizinhança de e, $H_1 \subset H_2$, já que os espaços tangentes de $H_1 \cap H_2$ e de H_1 coincidem. (2) é imediato a partir de (1).

Para demonstrarmos (3), consideremos os gráficos G_ϕ e G_ψ de ϕ e ψ:

$$G_\phi = \{(x, \phi(x)), x \in G_1\} \subset G_1 \times G_2,$$

$$G_\psi = \{(x, \psi(x)), x \in G_2\} \subset G_1 \times G_2.$$

Segue-se que

$$L(G_\phi) = \{(x, L(\phi)(x)), x \in L(G_1)\} \subset L(G_1) \times L(G_2),$$

$$L(G_\psi) = \{(x, L(\psi)(x)), x \in L(G_1)\} \subset L(G_1) \times L(G_2).$$

Obseve que $L(G_\phi) = L(G_\psi)$ se, e somente se, $L(\phi) = L(\psi)$. Por (2), $L(G_\phi) = L(G_\psi)$ se, e somente se, $G_\phi = G_\psi$ em um vizinhança de e. ■

Exemplo (E.4.6). Se $G = \mathrm{GL}_n(k)$, podemos considerar o determinante $\det : G \to \mathbb{G}_m(k) = k^*$. Para x em uma vizinhança de zero, $\det(1 + x) = 1 + \operatorname{tr} x + O(d^0 \geq 2)$. Assim, sendo tr a componente linear de det, obtemos $L(\det) = \operatorname{tr}$.

Proposição (P.4.7). Se $\phi : G \to H$ é um homomorfismo de grupos analíticos que é uma subimersão, se $K = \operatorname{Ker} \phi$, então $L(K) = \operatorname{Ker} T_e\phi$.

Exemplo (E.4.8). Consideremos novamente o determinante $\det : \mathrm{GL}_n(k) \to k^*$. Sabemos que $\operatorname{Ker}(\det) = \mathrm{SL}_n(k)$ e que $L(\det) = \operatorname{tr}$. Assim, obtemos que $L(\mathrm{SL}_n(k)) = \mathfrak{sl}_n(k) = \{x \in \operatorname{End}_n k \mid \operatorname{tr} x = 0\}$.

Se a caracterísica de k é zero, para qualquer ação de um grupo analítico G sobre uma variedade X, vimos que o estabilizador de um ponto $x \in X$, denotado por G_x é um subgrupo de Lie de G.

Uma **representação** de um grupo analítico G é um homomorfismo de grupos analíticos $\sigma : G \to \mathrm{GL}(V)$, em que V é um espaço vetorial sobre k. Obtemos dessa forma uma ação de G sobre V dada por $v^g = \sigma(g)(v)$, para todo $v \in V$. Obtemos, assim, uma representação de $L(G)$ pelo homomorfismo $L(\sigma) : L(G) \to \operatorname{End}(V)$.

Exemplo (E.4.9). Se $\sigma : G \to \mathrm{GL}(V)$ é uma representação de G e $v \in V$, então $L(G_v) = \{x \in L(G) \mid L(\sigma)(v) = 0\}$. De fato, se $\phi : \mathrm{GL}(V) \to V$ leva u em $u(v)$, então $T_e\phi : \operatorname{End}(V) \to V$ é a aplicação que leva y em $y(v)$. Como $G_v = \operatorname{Ker}(\phi \circ \sigma)$, então $T_eG_v = \operatorname{Ker}(T_e(\phi \circ \sigma)) = \operatorname{Ker}(T_e\phi \circ L(\sigma))$, que é o que havíamos afirmado.

Exemplo (E.4.10). Considere a aplicação $\star : \mathrm{GL}(V) \to \mathrm{GL}(V^*)$ (em que V^* é o espaço dual a V) dada por $\star(u) = {}^t u^{-1}$. É claro que $\star$ é um isomorfismo de grupos analíticos. Denotando por 1^* a identidade em $\mathrm{GL}(V^*)$, obtemos que, em uma vizinhança da identidade,

$$\star(1 + x) = (1^* + {}^t x)^{-1} = \sum_{n=0}^{\infty} (-1)^n (t^x)^n = 1^* - {}^t x + O(d^0 \geq 2),$$

e, portanto $L(\star)(x) = -{}^t x$.

Exemplo (E.4.11). Seja $\sigma : G \to \mathrm{GL}(V)$ uma representação de G e $f \in V^*$. Considere a representação $\star \circ \sigma : G \to \mathrm{GL}(V^*)$, em que $\star$ é a representação do exemplo acima. Seja G_f o estabilizador de f com respeito a essa representação. Afirmamos que $G_f = \{g \in G \mid f \circ \sigma(g) = f\}$ e que $L(G_f) = \{x \in L(G) \mid f \circ L(\sigma)(x) = 0\}$. Primeiro, como G_f é um grupo, é suficiente mostrarmos que $g^{-1} \in G_f$ se, e somente se $f \circ \sigma(g) = f$. Note que $\star \circ \sigma(g^{-1})(f) =^t \sigma(g^{-1})^{-1}(f) = f \circ \sigma(g)$. Se $g^{-1} \in G_f$, então $f \circ \sigma(g)(f) = \star \circ \sigma(g^{-1})(f) = f$ e, reciprocamente, se $f \circ \sigma(g) = f$, então $\star \circ (g^{-1})(f) = f$ e, portanto, $g^{-1} \in G_f$. Assim, de fato $G_f = \{g \in G : f \circ \sigma(g) = f\}$.

Agora para mostrarmos que $L(G_f) = \{x \in L(G) \mid f \circ L(\sigma)(x) = 0\}$, observamos que, pela caracterização de G_f, é suficiente mostrarmos que $L(\star \circ \sigma)(x)(f) = 0$ se, e somente se, $f \circ L(\sigma) = 0$. Mas, de fato, $L(\star \circ \sigma)(x)(f) = -{}^t L(\sigma)(x)(f) = -f \circ L(\sigma)(x)$ e o resultado segue.

Exemplo (E.4.12). Se $(V_i)_{i=1}^n$ é uma família de espaços vetoriais, denotemos por V o respectivo produto tensorial. Definimos uma representação $\theta : \mathrm{End}(V_1) \times \cdots \times \mathrm{End}(V_n) \to \mathrm{End}(V)$ por $\theta(u_1, \ldots, u_n) = u_1 \otimes \cdots \otimes u_n$ (lembramos que $u_1 \otimes u_2(v_1 \otimes v_2) = u_1(v_1) \otimes u_2(v_2)$). Notemos que a restrição de θ a $G = \prod_{i=1}^n \mathrm{GL}(V_i)$ é um homomorfismo analítico $\theta : G \to \mathrm{GL}(V)$ que, numa vizinhança da identidade, é dado por:

$$\theta(1 + x_1, \ldots, 1 + x_n) = 1 + \sum_{i=1}^n 1 \otimes \cdots \otimes x_i \otimes \cdots \otimes 1 + O(d^0 \geq 2)$$

e, portanto, $L(\theta)(x_1, \ldots, x_n) = \sum_{i=1}^n 1 \otimes \cdots \otimes x_i \otimes \cdots \otimes 1$.

Podemos agora caminhar para os exemplos mais relevantes dessa seção. Se $\sigma : G \to \mathrm{GL}(V)$ é uma representação de um grupo analítico G e $\beta \in (V \otimes V)^*$ (isto é, uma forma bilinear em V), então sejam $\theta : \mathrm{GL}(V)^2 \to \mathrm{GL}(V \otimes V)$ o homomorfismo definido no exemplo acima e $\tau = \theta \circ (\sigma \times \sigma) : G \to \mathrm{GL}(V \otimes V)$. Então pelos exemplos acima

$$G_\beta = \{g \in G \mid \beta(\sigma(g) \times \sigma(g)) = \beta\},$$

$$L(G_\beta) = \{x \in L(G) \mid \beta(L(\sigma)(x) \otimes 1 + 1 \otimes L(\sigma)(x)) = 0\}.$$

Além disso, perceba que $\beta(L(\sigma)(x) \otimes 1 + 1 \otimes L(\sigma)(x)) = 0$ é equivalente a $\beta(L(\sigma)(x)(u), v) + \beta(u, L(\sigma)(x)(v)) = 0$ para u, v elementos quaisquer de V e que $\beta(\sigma(g) \times \sigma(g)) = \beta$ é equivalente a $\beta(\sigma(g)(u), \sigma(g)(v)) = \beta(u, v)$ para quaisquer u, v em V.

Exemplo (E.4.13) (Grupo ortogonal). Na discussão acima, escolha $G = \mathrm{GL}_n(k)$, σ sendo a identidade e β a forma bilinear em k^n definida por $\beta(u, v) = \sum_{i=1}^n x_i y_i$, em que x_i e y_i são as coordenadas de x e y, respectivamente, na base canônica de k^n (ou seja, β é o produto interno usual). O grupo $G_\beta = \{g \in G \mid \beta(g(u), g(v)) = \beta(u, v)\}$ é dito grupo ortogonal de k^n. Note que, pela definição de β, para todo endomorfismo u de k^n, vale que $\beta(u(x), y) = \beta(x, u^t(y))$ para quaisquer vetores x e y (em que u^t é a aplicação transposta a u). Ou seja, a condição $\beta(x, y) = \beta(g(x), g(y))$ é equivalente a $\beta(x, y) = \beta(x, g^t g(y))$ para todo x, y. Pela não degenerabilidade de β, segue-se que $g \in G_\beta$ se, e somente se, $g^t g = 1$.

Similarmente, a condição $\beta(g(u),v)+\beta(u,g(v))=0$ é equivalente a $\beta(u,(g^t+g)(v))=0$ para quaisquer u e v. Como acima, obtemos que $L(G_\beta)=\{u\in\mathrm{End}(k^n)\mid u^t+u=0\}$.

Exemplo (E.4.14) (Grupo simplético). Seja $n=2m$ e β a forma bilinear em k^n definida por $\beta(x,y)=\sum_{i=1}^{m}x_iy_{m+i}-x_{m+i}y_i$ quando $x=(x_i)_{i=1}^n$ e $y=(y_i)_{i=1}^n$. O grupo G_β é dito grupo simplético de k^{2m}. Escreveremos endomorfismos de k^n como matrizes em blocos $\begin{pmatrix}A & B\\ C & D\end{pmatrix}$, em que $A,B,C,D\in\mathrm{End}(k^m)$. Pela definição de β, $\beta(ux,y)=\beta(x,u'y)$, em que se u é uma matriz em blocos como a escrita, $u'=\begin{pmatrix}{}^tD & -{}^tB\\ -{}^tC & {}^tA\end{pmatrix}$. Argumentando de maneira similar ao exemplo do grupo ortogonal, obtemos que:

$$G_\beta=\{g\in\mathrm{GL}_n(k)\mid g'g=1\}$$

$$L(G_\beta)=\{u\in\mathrm{End}(k^n)\mid u'+u=0\}.$$

Exemplo (E.4.15) (Grupo unitário). Seja σ uma involução de $\mathrm{Aut}(k)$ e β a forma bilininear em k^n definida por $\beta(x,y)=\sum_{i=1}^{n}x_iy_i^\sigma$ quando $x=(x_i)_{i=1}^n$ e $y=(y_i)_{i=1}^n$. O grupo $G_\beta=\{g\in\mathrm{GL}_n(k)\mid \beta(g(u),g(v))=\beta(u,v)\}$ é dito grupo unitário de k^n em relação à involução σ. Pela definição de β, para todo $u\in\mathrm{End}(k^n)$, $\beta(u(x),y)=\beta(x,u^\star(v))$, em que $u^\star=\sigma(u^t)$. Argumentando de maneira similar aos exemplos acima, obtemos que

$$G_\beta=\{g\in\mathrm{GL}_n(k)\mid g^\star g=1\}$$

$$L(G_\beta)=\{u\in\mathrm{End}(k^n)\mid u^\star+u=0\}$$

Ressaltamos que importantes exemplos de grupos (e álgebras de Lie) simples podem ser construidos a partir dos grupos ortogonais, simpléticos e unitários de maneira análoga ao grupo projetivo especial linear.

Exemplo (E.4.16) (Representação adjunta). Se G é um grupo analítico, para cada $g\in G$, consideramos o automorfismo interno respectivo $\phi_g:G\to G$, $x\mapsto x^g$. Se $\mathfrak{g}=L(G)$ e $\mathrm{Ad}:G\to\mathrm{GL}(\mathfrak{g})$ é a aplicação $g\mapsto T_e\phi_g$, então Ad é, evidentemente, um homomorfismo (pela regra da cadeia). Afirmamos que Ad é analítico. Como é um homomorfismo de grupos, é suficiente checar que é analítico em torno da identidade de G. Pela Proposição 3.9

$$\phi_g(x)=x-[g,x]+\sum d_{\alpha,\beta}g^\alpha x^\beta,$$

em que $|\alpha|,|\beta|\geq 1$ E $|\alpha|+|\beta|\geq 3$. Segue-se que $\mathrm{Ad}(g)(x)=x+[g,x]+\sum_{|\beta|=1}d_{\alpha,\beta}g^\alpha x^\beta$ e, portanto, é analítico em 1. Podemos, assim, considerar a aplicação induzida nas álgebras de Lie $L(\mathrm{Ad}):\mathfrak{g}\to\mathrm{End}(\mathfrak{g})$ que, pela fórmula acima, é dada por $L(\mathrm{Ad})(y)=[y,x]$.

4.3 Grupos e Álgebras de Lie

O objetivo dessa seção é apresentar a força da associação funtorial entre grupos analíticos e suas respectivas álgebras de Lie. Começamos enunciando o principal resultado:

Assumimos que $\mathrm{char}\,k=0$.

Teorema (T.4.17). *Seja L o funtor de Lie entre a categoria dos grupos formais sobre k e a categoria das álgebras de Lie de dimensão finita sore k. Então L é uma equivalência categórica, isto é, para quaisquer grupos formais F_1 e F_2, a aplicação $L_{F_1,F_2} : \mathrm{Hom}(F_1, F_2) \to \mathrm{Hom}(LF_1, LF_2)$ é uma bijeção e para toda k-álgebra de Lie de dimensão finita $\mathfrak{g}$, existe um grupo formal F sobre k tal que LF é isomorfo a $\mathfrak{g}$.*

O Teorema acima possui duas afirmações: L é completamente fiel e essencialmente sobrejetivo. Iremos nos restringir a demonstrar a última. A demonstração da primeira afirmação é mais técnica e pode ser consultada em [Ser00] (II.V.6.3) ou [Haz78] (14.2.3). Provaremos:

Teorema (T.4.18). *Se $\mathfrak{g}$ é uma álgebra de Lie de dimensão finita sobre k, então $\mathfrak{g}$ é a álgebra de Lie associada a alguma peça de grupo analítico.*

Demonstraremos o Teorema acima em etapas e utilizando alguns lemas. A ideia da demonstração é construir um grupo formal em n variáveis cuja álgebra de Lie seja $\mathfrak{g}$ e cuja lei formal de grupo seja uma série de potências convergente.

Fixemos uma base $x_1, \ldots, x_n$ de $\mathfrak{g}$ e escrevemos $[x_i, x_j] = \sum_{h=1}^{n} \gamma_{ij}^h x_h$. Note que as constantes de estrutura γ_{ij}^h dependem da base escolhida. Definimos $\gamma = \gamma(x_1, \ldots, x_n) = \max\{|\gamma_{ij}^h|\}$. Observe que multiplicando todos os elementos da base por um elemento $\lambda \in k \setminus \{0\}$, cada γ_{ij}^h é multiplicado por λ e γ por $|\lambda|$.

Sejam $R = k[[X, Y]] = k[[X_1, \ldots, X_n, Y_1, \ldots Y_n]]$ o anel das séries de potência em $2n$ variáveis (que devem ser interpretadas como funções em duas variáveis de k^n) e $E = R^n$. Definimos uma estrutura de Álgebra de Lie em E por

$$[(f_1, \ldots, f_n), (g_1, \ldots, g_n)] = \left(\sum_{i,j=1}^{n} \gamma_{ij}^1 f_i g_j, \ldots, \sum_{i,j=1}^{n} \gamma_{ij}^n f_i g_j \right).$$

Verifiquemos rapidamente que o colchete em E de fato satisfaz a identidade de Jacobi. Da identidade de Jacobi em $\mathfrak{g}$, obtemos a seguinte expressão:

$$\sum_{l=1}^{n} (\gamma_{ij}^l \gamma_{lk}^s + \gamma_{jk}^l \gamma_{li}^s + \gamma_{ki}^l \gamma_{lj}^s) = 0,$$

para quaisquer $i, j, k, s = 1, \ldots, n$. Defina $J_h(u, v, w)$ como a h-ésima componente de $[[u, v], w] + [[v, w], u] + [[w, u], v]$ para $u, v, w \in E$. Então uma simples computação nos mostra que

$$J_h(u, v, w) = \sum_{i,j,k=1}^{n} \left(\sum_{l=1}^{n} (\gamma_{ij}^l \gamma_{lk}^h + \gamma_{jk}^l \gamma_{li}^h + \gamma_{ki}^l \gamma_{lj}^h) \right) u_i v_j w_k = 0$$

Em que os elementos u, v, w de E são expressos como $(u_i), (v_i), (w_i), i = 1, \ldots, n$. Portanto $(E, [\cdot, \cdot])$ é, de fato, uma álgebra de Lie.

Se P é um polinômio homogêneo de grau r em E (isto é, uma n-upla de polinômios de grau r), denotamos por $||P||$ o máximo dos valores absolutos dos coeficientes de P.

Lema (L.4.19). Sejam $X = (X_1, \ldots, X_n)$ e $Y = (Y_1, \ldots, Y_n)$ e P um polinômio homogêneo de grau r. Então $\mathrm{ad}(X)(P), \mathrm{ad}(Y)(P)$ são polinômios homogêneos de grau $r + 1$ e $||\mathrm{ad}(X)(P)||, ||\mathrm{ad}(Y)(P)|| \leq n^2 \gamma ||P||$.

Demonstração: Sejam $\mathrm{ad}(X)(P) = (Q_1, \ldots, Q_n)$ e $P = (P_1, \ldots, P_n)$. Escrevemos também $P_j = \sum_{\alpha,\beta} a^j_{\alpha,\beta} X^\alpha Y^\beta$ e $Q_h = \sum_{\alpha,\beta} b^h_{\alpha,\beta} X^\alpha Y^\beta$. Pela definição do colchete em E, obtemos que $Q_h = \sum_{i,j} \gamma^h_{ij} X_i P_j$ e, portanto, Q é homogêneo de grau $r+1$.

Desenvolvendo a expressão de Q_h, obtemos que $Q_h = \sum_{i,j} \sum_{\alpha,\beta} \gamma^h_{ij} a^j_{\alpha,\beta} X^{\alpha+\delta_i} Y^\beta$ e, comparando com a outra expressão, obtemos que

$$b^h_{\alpha,\beta} = \sum_{i,j} \gamma^h_{ij} a^j_{\alpha-\delta_i,\beta}.$$

Segue diretamente que $|b^h_{\alpha,\beta}| \leq n^2 \gamma ||P||$, para quaisquer α, β. ■

Relembramos que R é um anel local com ideal maximal $\mathfrak{m}$ consistindo nas séries de potência de termo constante igual a zero.

Corolário (C.4.20). *Para todo $r \geq 0$, $\mathrm{ad}(X)(\mathfrak{m}^r E), \mathrm{ad}(Y)(\mathfrak{m}^r E) \subset \mathfrak{m}^{r+1} E$.*

Demonstração: Escrevendo um elemento F de $\mathfrak{m}^r E$ como soma de polinômios homogêneos de grau ao menos r, segue do lema anterior que $\mathrm{ad}(X)(F)$ é a soma de polinômios homogêneos de grau ao menos $r+1$. ■

Seja $S = \{\overline{x}, \overline{y}\}$ um conjunto de dois elementos e considere a álgebra de Lie livre L_S sobre S e seu completamento $\widehat{L}_S$ (que é produto de componentes homogêneas L^r_S). Seja $\theta : L_S \to E$ o único homomorfismo de álgebras de Lie estende a função $S \to \{X, Y\}, \overline{x} \mapsto X, \overline{y} \mapsto Y$.

Lema (L.4.21). Para todo $r > 0$, $\theta(L^r_S) \subset \mathfrak{m}^r E$.

Demonstração: Pela definição de θ, $\theta(L^1_S) \subset \mathfrak{m} E$. Pelo corolário acima, o resultado é obtido por indução em r. ■

Assim θ se estende a um homomorfismo de álgebras de Lie $\theta : \widehat{L}_S \to E$ (levando cada componente homogênea L^r_S em um elemento de $\mathfrak{m}^r E$ e somando). Sejam $\overline{z} \in \widehat{L}_S$ o único elemento de $\widehat{L}_S$ satisfazendo $e^{\overline{x}} e^{\overline{y}} = e^{\overline{z}}$ e $F = \theta(\overline{z})$.

Lema (L.4.22). Vale que F é uma lei formal de grupo em X e Y e $[X, Y]_F = [X, Y]$.

Demonstração: Seja $\Phi(X, Y)$ a fórmula de Hausdorff (isto é, $e^X e^Y = e^{\Phi(X,Y)}$). Então $\Phi(\Phi(X, Y), Z)$ é o único elemento T de $\widehat{L}_S$ tal que $e^T = e^{\Phi(X,Y)} e^Z = e^X e^Y e^Z = e^X e^{\Phi(Y,Z)}$. Portanto $\Phi(\Phi(X, Y), Z) = \Phi(X, \Phi(Y, Z))$.

Sabemos também que $\Phi(X, Y) = X + Y + \frac{1}{2}[X, Y] + O(d^0 \geq 3)$ e, portanto, a fórmula bilinear $B(X, Y)$ associada a F é $\frac{1}{2}[X, Y]$. Daí $[X, Y]_F = B(X, Y) - B(Y, X) = [X, Y]$ ■

Construímos, assim, uma lei formal de grupo cuja álgebra de Lie é $\mathfrak{g}$. Resta-nos mostrar sua convergência para finalizar a demonstração do Teorema 4.18. Precisaremos de dois lemas elementares:

Lema (L.4.23) ([Ser00] V.4, Lema 3). Para t suficientemente pequeno, a soma

$$\sum_{\substack{p_1,\ldots,p_m \\ q_1,\ldots,q_m \\ p_i+q_i \geq 1 \\ m \geq 1}} t^{\sum p_i + \sum q_i}$$

converge.

Lema (L.4.24) ([Ser00] V.4, Lema 4). Existe uma constante $a \in (0,1]$ tal que $|n!| \geq a^n$ e $|n| \geq a^n$ para todo $n > 0$.

Demonstração do Teorema 4.3: Inicialmente multipliquemos a base $\{x_1, \ldots, x_n\}$ de $\mathfrak{g}$ por $\lambda \in k$ de forma que $|\lambda|\gamma \leq \frac{1}{n^2}$. Assim, refinamos o Lema 4.19 para

Lema (L.4.25). Se P é um polinômio homogêneo de grau r em E, então $||\operatorname{ad}(X)(P)||, ||\operatorname{ad}(Y)(P)|| \leq ||P||$.

Utilizaremos agora a forma explícita da fórmula de Hausdorff para $F = \theta(\overline{z})$. Escrevemos $F(X,Y)$ como a soma $\sum_\nu f_\nu(X,Y)$ de suas componentes homogêneas $f_\nu(X,Y)$, em que cada $f_\nu(X,Y)$ tem expressão

$$f_\nu(X,Y) = \frac{1}{\nu} \sum_{p+q=\nu} \left(f'_{p,q}(X,Y) + f''_{p,q}(X,Y) \right),$$

em que

$$f'_{p,q} = \sum_{\substack{p_1+\cdots+p_m=p \\ q_1+\cdots+q_{m-1}=q-1 \\ p_i+q_i\geq 1 \\ p_m \geq 1}} \frac{(-1)^{m+1}}{m} \frac{\operatorname{ad}(X)^{p_1} \operatorname{ad}(Y)^{q_1} \ldots \operatorname{ad}(X)^{p_m}(Y)}{p_1!q_1! \ldots p_m!}$$

$$f''_{p,q} = \sum_{\substack{p_1+\cdots+p_{m-1}=p-1 \\ q_1+\cdots+q_{m-1}=q \\ p_i+q_i\geq 1}} \frac{(-1)^{m+1}}{m} \frac{\operatorname{ad}(X)^{p_1} \operatorname{ad}(Y)^{q_1} \ldots \operatorname{ad}(Y)^{q_{m-1}}(X)}{p_1!q_1! \ldots q_{m-1}!}$$

Pelo Lema 4.25, os numeradores nas expressões acima são polinômios homogêneos de grau ν com coeficientes de valor absoluto menor do que 1. Pela definição de $[\cdot,\cdot]$, cada vez que aplicamos $\operatorname{ad}(X)$ ou $\operatorname{ad}(Y)$ em um monômio, obtemos uma soma de no máximo n^2 monômios e, portanto, as expressões nos numeradores são somas de no máximo $n^{2\nu}$ monômios. Podemos, portanto, majorar os valores absolutos dos numeradores por um polinômio real em X e Y de grau ν que é a soma de $n^{2\nu}$ monômios com coeficiente 1. Em um cubo de aresta $2s$ centrado em 0 em $\mathbb{R}^{2n}$ (isto é, uma bola de raio s na norma do máximo), esse polinômio é sempre menor ou igual a $n^{2\nu}s^\nu = (n^2 s)^{p+q}$.

Pelo Lema 4.24, $|\nu| \geq a^\nu = a^{p+q}$, $|m| \geq a^m \geq a^{p+q}$ e $|p_1!q_1!\ldots p_m!|, |p_1!q_1!\ldots q_{m-1}!| \geq a^{\sum p_i + \sum q_i} = a^{p+q-1} \geq a^{p+q}$. Assim, tomando $t = \frac{n^2 s}{a^3}$, obtemos que as componentes homogêneas de f_ν são majoradas pelo dobro da soma do Lema 4.23, que converge para t suficientemente pequeno. Diminuindo s conforme necessário, obtemos que f_ν converge uniformemente e, portanto, F converge. ■

Corolário (C.4.26). *Toda álgebra de Lie de dimensão finita sobre $\mathbb{Q}_p$ é a álgebra de Lie de um grupo analítico p-ádico.*

Demonstração: Segue diretamente do Teorema acima e do Corolário 3.8. ■

Adicionamos uma observação: buscamos com o Teorema 4.17 criar uma ponte sólida entre grupos analíticos e álgebras de Lie e, para isso, gostaríamos que homomorfismos de grupos formais convergissem, isto é, correspondessem a homomorfismos entre grupos de analíticos. Sobre isso, mencionamos o resultado a seguir:

Teorema (T.4.27) ([Ser00] II.V.7.1). *Sejam G_1 e G_2 peças de grupos analíticos e F_1 e F_2 suas correspondentes leis formais de grupos, então todo homomorfismo formal $\tau : F_1 \to F_2$ induz um homomorfismo local $\hat{\tau} : G_1 - \to G_2$.*

A demonstração deste resultado é apresentada com detalhes em [Ser00] e recai fortemente em um resultado de existência e unicidadade de solução de uma equação diferencial formal.

O seguinte resultado é fundamental para nós:

Corolário (C.4.28). *Se G e H são grupos analíticos p-ádicos com álgebras de Lie isomorfas, então G e H possuem subgrupos abertos isomorfos.*

Demonstração: Pelo Teorema 4.17, G e H possuem leis formais de grupo isomorfas. Pelo Teorema acima, isso induz um isomorfismo de peças de grupos entre G e H. Pelo Corolário 3.8, G e H possuem subgrupos abertos padrão isomorfos. ■

O significado do resultado acima é que, a partir da álgebra de Lie de um grupo analítico p-ádico, podemos recapturar o grupo a menos de comensurabilidade.

4.4 Subgrupos de Lie

Já vimos que subgrupos abertos de grupos analíticos são novamente grupos analíticos. Mas a questão de se um subgrupo fechado de um grupo analítico é novamente um grupo analítico é mais sensível e depende do corpo base sobre o qual estamos trabalhando. A resposta é afirmativa se $k = \mathbb{R}$ ou $\mathbb{Q}_p$. Demonstraremos o caso p-ádico.

Teorema (T.4.29). *Um subgrupo fechado de um grupo analítico p-ádico é analítico p-ádico.*

Demonstração: Seja G um grupo analítico p-ádico com álgebra de Lie $\mathfrak{g}$. Substituindo G por um subgrupo aberto suficientemente pequeno, podemos assumir que G é um subgrupo aberto de $\mathfrak{g}$ visto como grupo via fórmula de Hausdorff e que H é um subgrupo fechado de G. Daí para todo $x \in H$, $n \in \mathbb{Z}$, $x^n = nx \in H$ (em que x^n é a n-ésima potência de x em G e nx é a soma iterada de x n vezes em $\mathfrak{g}$). Como H é fechado, por continuidade, para todo $\lambda \in \mathbb{Z}_p$, $x^\lambda = \lambda x$.

Sejam $x_1, \ldots, x_m$ elementos de H linearmente independentes em $\mathfrak{g}$ com m maximal e V o espaço vetorial gerado por $\{x_i\}$. Então, pela maximalidade de m, $H \subseteq V$.

Defina $f : \mathbb{Z}_p^m \to V, (\lambda_i)_{i=1}^m \mapsto (\lambda_1 x_1) \ldots (\lambda_m x_m)$, de forma que f é analítica e sua derivada é invertível em zero. Daí f é localmente um isomorfismo de variedades analíticas e, portanto, a imagem de f é uma vizinhança de 0 em V. Mas a $\mathrm{Im}(f) \subseteq H$ e, portanto H contém um aberto de V e, portanto, tem estrutura analítica. ■

Corolário (C.4.30). *Todo homomorfismo contínuo entre grupos analíticos p-ádicos é analítico. Além disso, todo homomorfismo de grupos abstratos entre grupos analíticos pro-p é analítico.*

Demonstração: Seja $\phi : G_1 \to G_2$ um homomorfismo contínuo entre dois grupos analíticos p-ádicos. Então o gráfico $\Gamma \leq G_1 \times G_2$ é um subgrupo fechado de $G_1 \times G_2$ e, portanto, é analítico. A projeção $\pi : \Gamma \to G_1$ é um homomorfismo analítico com núcleo trivial e, portanto $L(\pi)$ também tem núcleo trivial e π é uma imersão que é também um homeomorfismo. Pela Proposição 2.8, π é um isomorfismo analítico. Sendo $\pi' : \Gamma \to G_2$ a projeção na segunda coordenada, $\phi = \pi' \circ \pi^{-1}$ e, portanto, ϕ é analítica.

A segunda afirmação segue do fato de que todo homomorfismo de grupos abstratos entre grupos pro-p finitamente gerados é contínuo (isto é, todo subgrupo de índice finito em um grupo pro-p finitamente gerado é abertos). ■

Por fim, relembramos o Teorema 3.10, que nos mostra que a classe dos grupos analíticos p-ádicos é fechada para quocientes, e mencionamos o Teorema 9.7 de [DDMS99], que afirma que essa classe também é fechada para extensões.

4.5 A correspondência de Lazard

Como mencionamos na seção anterior, a construção das álgebras de Lie para grupos analíticos p-ádicos captura bem as informações dos grupos a menos de comensurabilidade. Podemos, porém, para grupos saturáveis, construir uma associação mais poderosa que nos será muito útil no próximo capítulo. Associaremos a cada grupo saturável uma $\mathbb{Z}_p$-álgebra de Lie saturável. Para isso construiremos um objeto maior do qual poderemos extrair essa associação.

Embora o material dessa seção tenha sido originalmente desenvolvido em [Laz65], seguiremos [Sch11] de perto.

4.5.1 A álgebra grupo de um grupo p-valorado

Começaremos nossa discussão com uma série de definições. Sejam (G, ω) um grupo p-valorado e $\Lambda(G)$ sua álgebra completa com respeito ao anel $\mathbb{Z}_p$. Fixando uma base ordenada $(g_1, \dots, g_r)$ de (G, ω), munimo-nos de um homeomorfismo

$$c : \mathbb{Z}_p^r \to G,$$

que induz um isomorfismo de $\mathbb{Z}_p$-módulos

$$c_* : \Lambda(\mathbb{Z}_p^r) \to \Lambda(G).$$

Note que c_* é apenas um isomorfismo de $\mathbb{Z}_p$-módulos! As álgebras grupo completas de $\mathbb{Z}_p^r$ e G não são isomorfas em geral! Sabe-se que o anel $\Lambda(\mathbb{Z}_p^r)$ é isomorfo ao anel de séries de potências formais em r indeterminadas (vide [Sch11] 20.1). Para cada elemento $g_i \in G$, definimos $C_i := g_i - 1$ e $C^\alpha = C_1^{\alpha_1} \dots C_r^{\alpha_r}$ se $\alpha = (\alpha_1, \dots, \alpha_r)$ é um multi-índice. Pelo resultado citado de [Sch11], obtemos que a aplicação

$$c_\star : \mathbb{Z}_p[[X_1, \dots X_r]] \to \Lambda(G), \sum_\alpha c_\alpha X^\alpha \mapsto \sum_\alpha c_\alpha C^\alpha$$

é um isomorfismo de $\mathbb{Z}_p$-módulos.

Definimos, assim, uma valoração em $\Lambda(G)$ dada por

$$\Omega\left(\sum_\alpha c_\alpha C^\alpha\right) = \inf_\alpha \left\{ v(c_\alpha) + \sum_{i=1}^r \alpha_i \omega(g_i) \right\},$$

de forma que $\Omega(x+y) \geq \min\{\Omega(x), \Omega(y)\}$.

O seguinte resultado nos será útil:

Lema (L.4.31) ([Sch11] 28.4, 28.5). (i) A função Ω é independente da escolha da base ordenada;

(ii) $\Omega(g-1) = \omega(g)$ para todo $g \in G$;

(iii) $\Omega(xy) = \Omega(x) + \Omega(y)$ para quaisquer $x, y \in \Lambda(G)$.

Estendemos naturalmente a valoração de $\Lambda(G)$ para $\Lambda'(G) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda(G)$ por $\Omega(a \otimes \lambda) = v(a) + \Omega(\lambda)$ quando $a \in \mathbb{Q}_p$ e $\lambda \in \Lambda(G)$ (em que v é a valoração p-ádica). Definindo a norma $||a \otimes \lambda||_\Omega = p^{-\Omega(a \otimes \lambda)}$, podemos construir o completamento $\Pi_\Omega(G)$ de $\Lambda'(G)$. Estendemos por continuidade a valoração Ω para $\Pi_\Omega(G)$.

Consideremos os homomorfismos $\Delta : G \to G \times G, g \mapsto (g, g)$, $\iota_i : G \to G \times G, g \mapsto (g, 1)$ e $\iota_2 : G \to G \times G, g \mapsto (1, g)$ e seus monomorfismos induzidos $\Delta_*, \iota_{1_*}, \iota_{2_*} : \Pi_\Omega(G) \to \Pi_{\Omega_2}(G \times G)$ entre as álgebras completas, em que a valoração em $G \times G$ é dada por $\Omega_2(g, h) = \min\{\Omega(g), \Omega(h)\}$.

Assim, definimos $\operatorname{Sat} G := \{g \in \Pi_\Omega(G), \Delta_*(g) = \iota_{1_*}(g)\iota_{2_*}(g)\}$. Embora misteriosa, tal definição se justifica pelo Teorema abaixo:

Teorema (T.4.32) ([Sch11], 30.7). *O grupo* $(\operatorname{Sat} G, \omega)$ *é p-saturado e contém* G *como subgrupo aberto, de forma que a inclusão é uma isometria. Além disso, se* (G, ω) *é p-saturado,* $\operatorname{Sat} G = G$.

4.5.2 exp e log

Apresentamos agora o $\mathbb{Z}_p$-reticulado de Lie associado a um grupo p-saturado (G, ω). Definimos $\operatorname{Lat}^* G := \{x \in \Pi_\Omega(G), \Delta_*(x) = \iota_{1_*}(x) + \iota_{2_*}(x)\}$. Lembremos que, sendo $\Pi_\Omega(G)$ uma $\mathbb{Q}_p$-álgebra, podemos introduzir uma estrutura de álgebra de Lie em $\Pi_\Omega(G)$ com colchete dado por $[\lambda, \mu] = \lambda\mu - \mu\lambda$. Note que $\Omega([\lambda, \mu]) \geq \Omega(\lambda) + \Omega(\mu)$ pra quaisquer $\lambda, \mu \in \Pi_\Omega(G)$.

Além disso, $\Delta_*([\lambda, \mu]) = \Delta_*(\lambda)\Delta_*(\mu) - \Delta_*(\mu)\Delta_*(\lambda) = (\iota_{1_*}(\lambda) + \iota_{2_*}(\lambda))(\iota_{1_*}(\mu) + \iota_{2_*}(\mu)) - (\iota_{1_*}(\mu) + \iota_{2_*}(\mu))(\iota_{1_*}(\lambda) + \iota_{2_*}(\lambda)) = \iota_{1_*}([\lambda, \mu]) + \iota_{2*}([\lambda, \mu]) + \iota_{2_*}(\lambda)\iota_{1_*}(\mu) + \iota_{1_*}(\lambda)\iota_{2_*}(\mu) - \iota_{2_*}(\mu)\iota_{1_*}(\lambda) - \iota_{1_*}(\mu)\iota_{2_*}(\lambda) = \iota_{1_*}([\lambda, \mu]) + \iota_{2*}([\lambda, \mu])$. Portanto $\operatorname{Lat}^*(G)$ é uma subálgebra de Lie de $\Pi_\Omega(G)$.

Definimos agora as seguintes séries formais em $\Pi_\Omega(G)$:

$$\exp(\lambda) := \sum_{n \geq 0} \frac{1}{n!}\lambda^n, \log(\lambda) := \sum_{n \geq 1} \frac{(-1)^{n+1}}{n}(\lambda - 1)^n$$

Se $\Omega(\lambda) > \dfrac{1}{p-1}$, então

$$\Omega\left(\frac{1}{n!}\lambda^n\right) = n\Omega(\lambda) - v(n!) \geq n\left(\Omega(\lambda) - \frac{1}{p-1}\right) \to +\infty$$

e, assim, $\exp(\lambda)$ converge. Por outro lado, se $\Omega(\lambda - 1) > 0$, então

$$\Omega\left(\frac{1}{n}(\lambda - 1)^n\right) = n\Omega(\lambda - 1) - v(n) > n\Omega(\lambda - 1) - \log_p(n) \to +\infty$$

e, similarmente, $\log(\lambda)$ converge. Retornando ao caso em que $\Omega(\lambda) > \dfrac{1}{p-1}$, obtemos que

$$\Omega\left(\frac{1}{n!}\lambda^n\right) = n\Omega(\lambda) - v(n!) \geq n\Omega(\lambda) - \frac{n-1}{p-1} = n\left(\Omega - \frac{1}{p-1}\right) + \frac{1}{p-1} > \Omega(\lambda), n \geq 2.$$

Segue-se que $\Omega(\exp(\lambda)-1)=\Omega(\lambda)$. Já se $\Omega(\lambda-1)>\dfrac{1}{p-1}$, então

$$\Omega\left(\frac{1}{n}(\lambda-1)^n\right)=n\Omega(\lambda-1)-v(n!)+v((n-1)!)\geq n\Omega(\lambda-1)-\frac{n-1}{p-1}=$$

$$=n\left(\Omega(\lambda-1)-\frac{1}{p-1}\right)+\frac{1}{p-1}>\Omega(\lambda-1), n\geq 2.$$

O que implica $\Omega(\log(\lambda))=\Omega(\lambda-1)$. A seguir apresentamos algumas propriedades conhecidas das séries formais log e exp. A sutileza está na convergência, que foi discutida acima.

Lema (L.4.33). Se $\lambda,\lambda',\mu,\mu'\in\Pi_\Omega(G)$ são tais que $\Omega(\lambda),\Omega(\lambda'),\Omega(\mu-1),\Omega(\mu'-1)>\dfrac{1}{p-1}$, então

(i) $\log(\exp(\lambda))=\lambda$ e $\exp(\log(\mu))=\mu$;

(ii) $\exp(\lambda+\lambda')=\exp(\lambda)\exp(\lambda')$ e $\log(\mu\mu')=\log(\mu)+\log(\mu')$ sempre que $\lambda\lambda'=\lambda'\lambda$ e $\mu\mu'=\mu'\mu$;

(iii) $\exp(m\lambda)=\exp(\lambda)^m$ e $\log(\mu^m)=m\,\log(\mu)$ para todo $m\in\mathbb{Z}$.

Assim, pelo lema acima, obtemos que log e exp definem homeomorfismos inversos entre os conjuntos $\{\lambda\in\Pi_\Omega(G),\Omega(\lambda)\geq\nu\}$ e $\{\lambda\in\Pi_\Omega(G),\Omega(\lambda-1)\geq\nu\}$ para todo $\nu>\dfrac{1}{p-1}$. Definimos agora o conjunto $\operatorname{Lat} G=\left\{x\in\operatorname{Lat}^*(G),\Omega(x)>\dfrac{1}{p-1}\right\}$, que será o **$\mathbb{Z}_p$-reticulado de Lie do grupo G** .

Proposição (P.4.34). As aplicações exp e log se restringem a homeomorfismos inversos entre $\operatorname{Lat} G$ e $\operatorname{Sat} G=G$ e, além disso, $\log(g^\lambda)=\lambda\log g$ para todo $g\in G$ e $\lambda\in\mathbb{Z}_p$.

Demonstração: A segunda afirmação segue-se por continuidade aplicando o lema anterior. Notemos que exp e log, sendo séries formais, comutam com os homomorfismos de álgebras Δ_*, ι_{1_*} e ι_{2_*}. Daí, se $\lambda\in\operatorname{Lat} G$ e $g\in G$, então:

$$\Delta_*(\exp(\lambda))=\exp(\Delta_*(\lambda))=\exp(\iota_{1_*}(\lambda)+\iota_{2_*}(\lambda))=\exp(\iota_{1_*}(\lambda))\exp(\iota_{2_*}(\lambda))=\iota_{1_*}(\exp(\lambda))\iota_{2_*}(\exp(\lambda)),$$

$$\Delta_*(\log(g))=\log(\Delta_*(g))=\log(\iota_{1_*}(g)\iota_{2_*}(g))=\log(\iota_{1_*}(g))+\log(\iota_{2_*}(g))=\iota_{1_*}(\log(g))+\iota_{2_*}(\log(g)).$$

Portanto $\log(g)\in\operatorname{Lat} G$ e $\exp(\lambda)\in G$. ■

Como consequência da proposição anterior, $\operatorname{Lat} G$ é uma $\mathbb{Z}_p$-álgebra de Lie. Tentemos agora compreender a funtorialidade de tal associação. Seja $\varphi:(G,\omega)\to(H,\omega')$ um homomorfismo de grupos p-saturados. Então φ induz um homomorfismo $\varphi_*:\Pi_\Omega(G)\to\Pi_{\Omega'}(H)$. Note que como φ_* é um homomorfismo de álgebras, induz, por restrição, um homomorfismo de Lie $\varphi_{\text{Lie}}:\operatorname{Lat} G\to\operatorname{Lat} H$. Assim, estabelecemos um funtor. Podemos ver o "contradomínio" desse funtor simplesmente como a categoria das $\mathbb{Z}_p$-álgebras de Lie de dimensão finita. Entretanto, o $\mathbb{Z}_p$-reticulado de Lie $\operatorname{Lat} G$ possui mais estrutura: é associado a uma valoração Ω. Como φ tem a propriedade de que $\omega'(\varphi(g))\geq\omega(g)$, a propriedade análoga vale para φ_{Lie}. Assim, devemos pensar tal associação como um funtor entre as categorias dos grupos p-saturados e dos $\mathbb{Z}_p$-reticulados de Lie p-valorados. Para avançarmos na discussão, precisamos dos resultados expressos no lema abaixo

Lema (L.4.35). Sejam $\lambda,\lambda'\in\operatorname{Lat} G$, então

(i) $\Omega(\log(\exp(\lambda)\exp(\lambda'))) = \Omega(\lambda + \lambda')$;

(ii) $\Omega(\log(\exp(\lambda)\exp(\lambda')\exp(-\lambda)\exp(\lambda))) = \Omega([\lambda, \lambda'])$;

(iii) se $\Omega(\lambda) > \dfrac{p}{p-1}$, então existe $\mu \in \operatorname{Lat} G$ tal que $p\mu = \lambda$;

(iv) $\Omega(p\lambda) = 1 + \Omega(\lambda)$.

Demonstração: A demonstração dos itens (i) e (ii) é feita por uma análise cautelosa da valoração p-ádica dos termos da fórmula de Hausdorff ([Sch11], proposições 32.3 e 32.5). Já para (iii), se $\Omega(\lambda) > \dfrac{p}{p-1}$, então $\Omega(\exp(\lambda) - 1) = \omega(\exp(\lambda)) > \dfrac{p}{p-1}$ e, portanto, existe h tal que $h^p = \exp(\lambda)$. Daí, $p\log(h) = \log\exp(\lambda) = \lambda$. Por fim, $\exp(p\lambda) = \Omega(\exp(p\lambda) - 1) = \omega(\exp(p\lambda)) = \omega(\exp(\lambda)^p) = 1 + \omega(\exp(\lambda)) = 1 + \Omega(\exp(\lambda) - 1) = 1 + \Omega(\lambda)$, o que demonstra (iv). ■

Assim, com as discussões anteriores e o lema acima, concluímos que $L(G) := \operatorname{Lat} G$ possui as seguintes propriedades:

(i) Para todo $x \in L(G)$, $\Omega(x) > (p-1)^{-1}$;

(ii) Se $x \in L(G)$ é tal que $\Omega(x) = \infty$, então $x = 0$;

(iii) Se $x \in L(G)$ é tal que $\Omega(x) > p(p-1)^{-1}$, então existe $y \in L(G)$ tal que $py = x$;

(iv) Se $x \in L(G)$, então $\Omega(px) = 1 + \Omega(x)$;

(v) Para quaisquer $x, y \in L(G)$, vale que $\Omega(x - y) \geq \min\{\Omega(x), \Omega(y)\}$;

(vi) Para quaisuqer $x, y \in L(G)$, vale que $\Omega([x, y]) \geq \Omega(x) + \Omega(y)$.

Chamaremos um $\mathbb{Z}_p$-reticulado de Lie munido de uma aplicação $\Omega : L \to \mathbb{R} \cup \{\infty\}$ possuindo as propriedades acima de um **$\mathbb{Z}_p$-reticulado de Lie p-saturado**. Apresentamos agora o principal resultado desta seção:

Teorema (T.4.36) ([Laz65] IV.3.2.6). *As categorias dos grupos p-saturados e dos $\mathbb{Z}_p$-reticulados de Lie p-saturados são isomorfas.*

A demonstração completa deste resultado exigiria uma exposição detalhada de resultados sobre álgebras envelopantes universais e sobre variadas propriedades de álgebras diagonais, o que foge bastante do escopo de nosso trabalho. Limitamo-nos aqui a enunciá-lo e apresentar os funtores envolvidos no isomorfismo. O leitor poderá consultar o capítulo IV de [Laz65] para detalhes.

Sejam $\mathcal{G}$ e $\mathcal{L}$ as categorias dos grupos saturáveis e dos $\mathbb{Z}_p$-reticulados de Lie saturáveis. Seja também $\mathcal{T}$ o funtor que associa a cada grupo G o $\mathbb{Z}_p$-reticulado $\mathcal{T}(G) = (\mathcal{T}(G), [\cdot, \cdot])$, em que $\mathcal{T}(G)$ tem o mesmo conjunto de elementos que G e $[g, h] = \exp([\log(g), \log(h)]_{L(G)})$. Homomorfismos de grupos $\varphi : G \to H$ são enviados para $\mathcal{T}(\varphi) := \exp_H \circ \varphi_{\text{Lie}} \circ \log_G : \mathcal{T}(G) \to \mathcal{T}(H)$.

Definiremos agora um funtor $\mathcal{H} : \mathcal{L} \to \mathcal{G}$. O natural seria a um $\mathbb{Z}_p$-reticulado de Lie L, associarmos o grupo $(\mathcal{H}(L), \star)$, em que $\mathcal{H}(L)$ tem o mesmo conjunto de elementos que $\mathcal{L}$ e $\lambda \star \mu := \log(\exp(\lambda)\exp(\mu))$. O problema é em que espaço as aplicações log e exp estariam definidas, já que não há, a priori, uma álgebra que contemple L como $\Pi_\Omega(G)$ contempla G. Para contornar isso, mergulhamos L em um

certo completamento $\widehat{UL}$ de sua álgebra envelopante universal UL, em que as aplicações exp e log são bem definidas e convergem nos domínios desejados. Além disso, $G(L) := \exp(L) \subset \widehat{UL}$ é um grupo homeomorfo a L. A álgebra $\widehat{UL}$ possui o mesmo papel de $\Pi_\Omega(G)$. Um homomorfismo $\varphi : L \to L'$, estende-se a um homomorfismo de álgebras associativas $\varphi_* : \widehat{UL} \to \widehat{UL'}$ que, por restrição, induz um homomorfismo de grupos $\varphi_{\mathrm{Gp}} : \exp(L) \to \exp(L')$. Assim, definimos $\mathcal{H}(\varphi) = \log_{L'} \circ \varphi_{\mathrm{Gp}} \circ \exp_L : \mathcal{H}(L) \to \mathcal{H}(L')$.

Notemos um fato fundamental: os funtores $\mathcal{T}$ e $\mathcal{H}$ preservam a estrutura de conjunto dos objetos em questão, isto é, se $\mathcal{F}$ é o funtor esquecimento ($\mathcal{F} : \mathcal{L}, \mathcal{G} \to \mathbf{Set}$), então $\mathcal{F} = \mathcal{F} \circ \mathcal{T}$ e $\mathcal{F} = \mathcal{F} \circ \mathcal{H}$. Dessa forma, obtemos que $\mathcal{H} \circ \mathcal{T}(G) = G$ e $\mathcal{T} \circ \mathcal{H}(L) = L$ para quaisquer $L \in \mathcal{L}$ e $G \in \mathcal{G}$ (ou seja, $\mathcal{H}$ e $\mathcal{T}$ estabelecem não só uma equivalência categórica, mas um isomorfismo). Além disso, os funtores $\mathcal{T}$ e $\mathcal{H}$ preservam a estrutura das funções! Isto é, as relações $\mathcal{F} = \mathcal{F} \circ \mathcal{T}$ e $\mathcal{F} = \mathcal{F} \circ \mathcal{H}$ valem também para homomorfismos de grupos e de $\mathbb{Z}_p$-reticulados de Lie. O leitor pode consultar o capítulo 9 de [DDMS99], em que a associação entre um grupo uniformemente *powerful* G e seu $\mathbb{Z}_p$-reticulado de Lie associado é dada por

$$[g, h]_{\mathrm{Lie}} = \lim_{n \to \infty} [g^{p^n}, h^{p^n}]^{p^{-2n}},$$

$$g +_{\mathrm{Lie}} h = \lim_{n \to \infty} (g^{p^n} h^{p^n})^{p^{-n}}.$$

Enquanto para os autores de [DDMS99] essas fórmulas são definições, para [Laz65], é um resultado (vide Proposição 3.2.3 do capítulo IV). De toda sorte, a fórmula mostra que associando um homomorfismo de grupos $f : G \to H$ para a mesma função $f : \mathcal{T}(G) \to \mathcal{T}(H)$, obtemos um homomorfismo de $\mathbb{Z}_p$-reticulados de Lie.

Finalizamos este capítulo com uma pergunta natural: qual a relação entre os $\mathbb{Z}_p$-reticulados de Lie construídos nesta seção e as álgebras de Lie construídas via grupos formais? Respondemos abaixo, sem demonstrar o resultado. O leitor pode consultar a discussão ao final do capítulo 32 de [Sch11].

Teorema (T.4.37). *Seja G um grupo p-saturável e $\mathfrak{g}$ sua álgebra de Lie associada. Então* $\mathfrak{g} = \mathrm{Lat}^*(G) \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{T}(G)$.

Capítulo 5

Grupos analíticos de dimensões pequenas

No capítulo anterior estabelecemos diversos resultados clássicos a respeito dos grupos analíticos p-ádicos. Estudamos a fundo a importante classe dos grupos saturáveis, que desempenham um papel crucial no decorrer do presente capítulo. O objetivo aqui é classificar, para primos $p > 3$, todos os grupos analíticos pro-p livres-de-torção de dimensão até 4.

O resultado fundamental, com o qual conseguimos tal classificação, é o de que todo grupo analítico pro-p livre-de-torção de dimensão menor do que p é p-saturável (vide [GoKl09], Teorema A). Esse fato está demonstrado na seção 2. A seção 1 apresenta uma caracterização alternativa dos grupos saturáveis, seguindo [GoSa07]. Posteriormente, construímos apresentações para todos os grupos analíticos pro-p livres-de-torção de dimensões 2 e 3, seguindo o citado artigo para o caso solúvel e [NoSn19] para o caso não-solúvel. Utilizando esses resultados, estabelecemos apresentações para todos os grupos analíticos pro-p livres-de-torção de dimensão 4, via um cálculo extenso das álgebras de derivações de todos os $\mathbb{Z}_p$-reticulados de Lie de dimensão 3.

5.1 De grupos saturáveis a filtrações potentes

Se G é um grupo pro-p e N é um subgrupo normal fechado de G, uma **filtração potente** de N em G é uma série de subgrupos normais fechados $(N_i)_{i\in\mathbb{N}}$ tal que $N_1 = N$, $\cap_{i\in\mathbb{N}} N_i = 1$, $[N_i, G] \leq N_{i+1}$ e $[N_i, {}_{p-1}\, G] \leq N_{i+1}^p$. Seguindo a terminologia utilizada em [GoSa07], se houver uma filtração potente de N em G, dizemos que N é PF-imerso em G. O grupo G é dito **grupo PF** se G é PF-imerso em G.

Veremos que grupos PF livres-de-torção finitamente gerados são saturáveis e vice-versa. Essa caracterização é poderosa, já que podemos tratar de problemas a cerca de grupos saturáveis do ponto de vista de teoria de grupos abstrata. Será fundamental para a classificação dos grupos de dimensões baixas. O material presente nessa seção foi originalmente desenvolvido em [GoSa07].

Apresentaremos, sem demonstrações, algumas propriedades importantes de PF-imersões. Demonstrações podem ser encontradas no já citado artigo e em [FGJ08].

Lema (L.5.1). Seja G um grupo pro-p, N, M subgrupos PF-imersos em G e $(N_i)_{i\in\mathbb{N}}, (M_i)_{i\in\mathbb{N}}$ filtrações potentes de N e M em G, respectivamente.

(1) N/K é PF-imerso em G/K para todo subgrupo normal fechado K de G;

(2) Sejam $g \in G$ e $x \in N_i$, então $(xg)^p \equiv x^p g^p \mod N_{i+1}^p$;

(3) $(N_i^p)_{i\in\mathbb{N}}$ e $([N_i, G])_{i\in\mathbb{N}}$ são filtrações potentes para os subgrupos N^p e $[N, G]$, respectivamente (consequentemente, N^{p^k} e $[N,_k G]$ são PF-imersos em G);

(4) $N^{p^k} = \{x^{p^k} : x \in N\}$;

(5) Para quaisquer $i, j \geq 0$, $[N^{p^i}, G^{p^j}] = [N, G]^{p^{i+j}}$;

(6) Se N é livre-de-torção e $x^{p^k} \in N^{p^k}$, então $x \in N$. Além disso, se $x^{p^k} = y^{p^k}$, então $x = y$;

(7) $(M_i N_i)_{i\in\mathbb{N}}$ é uma filtração potente para o subgrupo MN de G (consequentemente, MN é PF-imerso em G).

Lema (L.5.2). Seja G um grupo pro-p e N um subgrupo normal fechado de G com uma série descendente de subgrupos normais fechados $(N_i)_{i=1}^{t+1}$, em que $N_1 = N$, $N_{t+1} = [N, G]N^p$, $[N_i, G] \leq N_{i+1}$ e $[N_{i,p-1} G] \leq N_{i+1}^p$ se $i \leq t$. Então N é PF-imerso em G e

$$M_i = \begin{cases} [N_{s,j} G]N^p, & \text{se } i = jt + s \leq t(p-1) \text{ com } 1 \leq s \leq t, \\ M^p_{i-t(p-1)}, & \text{se } i > p(t-1). \end{cases}$$

é uma filtração potente de N em G.

Podemos agora enunciar e demonstrar a caracterização de grupos PF livres-de-torção como grupos p-saturáveis.

Teorema (T.5.3) ([GoSa07], Teorema A). *Seja G um grupo pro-p livre-de-torção finitamente gerado. Então G é p-saturável se, e somente se, G é um grupo PF.*

Demonstração: Suponha primeiro que G é um grupo PF. Considere uma família de subgrupos $G = N_1 \geq N_2 \geq \cdots \geq N_{t+1} = \Phi(G)$ tal que $[N_i, G] \leq N_{i+1}$ e $[N_{i,p-1} G] \leq N_{i+1}^p$ para todo $i \leq t$. Para cada inteiro positivo i, escreva $i = rt(p-1) + jt + s$ com $0 \leq j \leq p-2$ e $1 \leq s \leq t$, e defina $M_i = ([N_{s,j} G]G^p)^{p^r}$. Pelo Lema 5.2, $\{M_i\}$ é uma filtração potente em G.

Definimos agora uma valoração ω em G. Para cada $x \in M_i \setminus M_{i+1}$, seja

$$\omega(x) = \frac{1}{p-1}\left(\frac{2^{sp^{j+1}}}{2^{(t+1)p}} + j + 1\right) + r$$

e $\omega(1) = \infty$. É claro que $\omega(x) > (p-1)^{-1}$, para todo $x \in G$, que $\omega(x) = \infty$ se, e somente se, $x = 1$ e que $\omega(xy^{-1}) \geq \min\{\omega(x), \omega(y)\}$. Se $x^p \in ([N_{s,j}G]G^p)^{p^r}$, então, pelo item (6) do Lema 5.1, $x \in ([N_{s,j}G]G^p)^{p^{r-1}}$. Consequentemente $\omega(x^p) = \omega(x)+1$. Resta-nos verificar que $\omega([x_1, x_2]) \geq \omega(x_1)+\omega(x_2)$. Considere $x_1, x_2 \in G$ e suponha que $x_k \in M_{i_k} \setminus M_{i_k+1}$. Escreva $M_{i_k} = ([N_{s_k,j_k} G]G^p)^{p^{r_k}}$. Então, pelo Lema 5.1,

$$\begin{aligned}[x_1, x_2] &\in [([N_{s_1,j_1} G]G^p)^{p^{r_1}}, ([N_{s_2,j_2} G]G^p)^{p^{r_2}}] \\ &= [[N_{s_1,j_1} G]G^p, [N_{s_2,j_2} G]G^p]^{p^{r_1+r_2}} \leq ([N_{s_1,j_1+j_2+1} G]G^p)^{p^{r_1+r_2}}.\end{aligned}$$

Sem perda de generalidade, assumimos que $s_1 p + j_1 \geq s_2 p + j_2$. Se $j_1 + j_2 < p-2$, então

$$\omega([x_1, x_2]) \geq \frac{1}{p-1}\left(\frac{2^{s_1 p^{j_1+j_2+2}}}{2^{(t+1)p}} + j_1 + j_2 + 2\right) + r_1 + r_2.$$

Como

$$\omega(x_1)+\omega(x_2)=\frac{1}{p-1}\left(\frac{2^{s_1p^{j_1+1}}+2^{s_2p^{j_2+1}}}{2^{(t+1)p}}+j_1+j_2+2\right)+r_1+r_2$$

e

$$2^{s_1p^{j_1+j_2+2}}\geq 2^{s_1p^{j_1+2}}\geq 2^{s_1p^{j_1+1}}+2^{s_2p^{j_2+1}},$$

obtemos que $\omega([x_1,x_2])\geq\omega(x_1)+\omega(x_2)$. Por outro lado, se $j_1+j_2\geq p-2$, então

$$\begin{aligned}[x_1,x_2]&\in[[N_{s_1,j_1}\,G]G^p,[N_{s_2,j_2}\,G]G^p]^{p^{r_1+r_2}}\\&\leq([N_{s_1,j_1+j_2+1}\,G][N_{s_1,j_1+1}\,G]^p[N_{s_2,j_2+1}\,G]^{p^2}G^{p^3})^{p^{r_1+r_2}}\\&\leq([N_{s_1+1,j_1+j_2-p+2}\,G]^p[N_{s_1,j_1+1}\,G]^p[N_{s_2,j_2+1}\,G]^pG^{p^2})^{p^{r_1+r_2}}\\&\leq([N_{s_1+1,j_1+j_2-p+2}\,G]G^p)^{p^{r_1+r_2+1}},\end{aligned}$$

e o resultado é análogo.

Finalmente, precisamos provar que (G,ω) é p-saturado. Seja $x\in G$ tal que $\omega(x)>p(p-1)^{-1}$. Então existe i tal que $x\in M_i=([N_{s,j}G]G^p)^{p^r}$ com $r\geq 1$. Portanto, $x\in G^p$. Pelo Lema 5.1, existe $y\in G$ tal que $x=y^p$.

Reciprocamente, suponha que G possui uma p-valoração ω tal que G é um grupo p-saturável. Defina em $((p-1)^{-1},+\infty]$ a topologia cujos conjuntos abertos são aqueles da forma $(v,+\infty]$ com $v\geq(p-1)^{-1}$, juntamente com o conjunto vazio. Isso torna ω uma aplicação contínua, já que G_v é aberto em G. Agora, como G é compacto, $\omega(G)$ também é compacto. Assim, existe $\delta>0$ tal que $\omega(G)\subseteq[(p-1)^{-1}+\delta,+\infty]$. Vejamos que $N_i=\{x\in G\mid\omega(x)\geq(p-1)^{-1}+\delta i\}$ define uma filtração potente de G. É óbvio que $\{N_i\}_{i\in\mathbb{N}}$ forma uma série decrescente de subgrupos fechados com interseção trivial. Se $x\in N_i$ e $y\in G$, então

$$\omega([x,y])\geq\omega(x)+\omega(y)>(p-1)^{-1}+i\delta+(p-1)^{-1}+\delta>(p-1)^{-1}+(i+1)\delta.$$

Consequentemente $[N_1,G]\leq N_{i+1}$. Se $x\in N_i$ e $y_1,\ldots,y_{p-1}\in G$, então

$$\begin{aligned}\omega([x,y_1,\ldots,y_{p-1}])&\geq(p-1)^{-1}+i\delta+1+\delta(p-1)\\&>p(p-1)^{-1}+(i+1)\delta>p(p-1)^{-1}.\end{aligned}$$

Portanto, $[x,y_1,\ldots,y_{p-1}]=a^p$ com $\omega(a)=\omega([x,y_1,\ldots,y_{p-1}])-1\geq(p-1)^{-1}+(i+1)\delta$. Assim, $a\in N_{i+1}$ e $[N_i,{}_{p-1}G]\subseteq N_{i+1}^p$. ■

Corolário (C.5.4). *Se G é um grupo pro-p finitamente gerado e livre-de-torção satisfazendo $\gamma_p(G)\leq\Phi(G)^p$, então G é p-saturável.*

Demonstração: Pelo Teorema acima, basta construirmos uma filtração potente em G. Tomemos $G=G_1$ e $G_i:=[G_{i-1},G]G_{i-1}^p$ para $i\geq 2$. É óbvio que $\cap G_i=1$ e que $[G_i,G]\leq G_{i+1}$. Além disso. $[G_i,{}_{p-1}\,G]=\gamma_p(G)\leq\Phi(G)^p=G_2^p$. Por indução e utilizando o Lema 5.1, observamos que:

$$\begin{aligned}[G_i,{}_{p-1}\,G]&=[[G_{i-1},G]G_{i-1}^p,{}_{p-1}\,G]\leq[G_{i-1},{}_{p-1}\,G,G][G_{i-1}^p,{}_{p-1}\,G]\\&\leq[G_i^p,G][G_{i-1},{}_{p-1}\,G]^p\leq[G_i,G]^p(G_i^p)^p\leq G_{i+1}^p.\end{aligned}$$

■

5.2 Isoladores

Seja G um subgrupo fechado de um grupo p-saturável S. O **isolador** de G é o subgrupo

$$\mathrm{iso}_S(G) := \langle g \in S \mid \exists\, n \in \mathbb{N}, g^{p^n} \in G \rangle$$

de S. Pelo Teorema 5.3, S admite uma filtração potente $(S_i)_{i\in I}$. Utilizando o Lema 5.1, obtemos que $(\mathrm{iso}_S(G) \cap S_i)_{i\in I}$ é uma filtração potente de $\mathrm{iso}_S(G)$.

Definimos o análogo para $\mathbb{Z}_p$-reticulados de Lie. Se L é um subreticulado de Lie de um $\mathbb{Z}_p$-reticulado p-saturável S, então o **isolador** de L em S é o subreticulado

$$\mathrm{iso}_S(L) := \langle x \in S \mid \exists\, n \in \mathbb{N}, p^n x \in L \rangle.$$

Note que S e $\mathbb{Q}_p L$ são canônicamente imersos em $\mathbb{Q}_p \otimes S$ e que $S \cap (\mathbb{Q}_p \otimes L) = \mathrm{iso}_S(L)$. Tomando uma base $x_1, \ldots, x_k$ de L, vemos que $\mathrm{iso}_S(L)$ é gerado por $y_1, \ldots, y_k$, em que $y_i = p^{-a_i} x_i$ para certos inteiros a_i. Concluímos que o índice de L em $\mathrm{iso}_S(L)$ é finito e, em particular, L e $\mathrm{iso}_S(L)$ têm a mesma dimensão.

Podemos, via a correspondência de Lazard (que associa a exponenciação por p com a multiplicação por p), concluir que se G é um subgrupo de um grupo p-saturável S, então $[\mathrm{iso}_S(G) : G] < \infty$. De fato, G possui um subgrupo aberto p-saturável H e $[\mathrm{iso}_{L(S)} L(H) : L(H)] = [\mathrm{iso}_S H : H] = [\mathrm{iso}_S G : H] \geq [\mathrm{iso}_S G : G]$.

5.3 Grupos de dimensões pequenas

Demonstraremos agora o Teorema abaixo, o qual requere alguns resultados preliminares.

Teorema (T.5.5). *Todo grupo analítico p-ádico pro-p livre-de-torção de dimensão menor do que p é p-saturável.*

Um grupo pro-p infinito é dito de **coclasse finita** igual a r se $[G : \gamma_{c+1}(G)] = p^{c+r}$ para todo c suficientemente grande. Enunciamos dois resultados sobre grupos pro-p de coclasse finita:

Teorema (T.5.6) ([DDMS99], 10.1). *Um grupo pro-p de coclasse finita é um grupo virtualmente abeliano livre. Em particular, é analítico p-ádico.*

Proposição (P.5.7) ([DDMS99], 10.19). Se G é um grupo pro-p de coclasse finita, então G tem torção.

O seguinte lema nos será útil:

Lema (L.5.8) ([Klo05], A.3). Se G é um grupo pro-p p-saturável e S é um aberto de G, então $S^{\{p\}} := \{s^p, s \in S\}$ é aberto e $\mu(S) = p^{\dim G} \mu(S^{\{p\}})$, em que μ é a medida de Haar normalizada em G.

Demonstração do Teorema 5.2: Demonstraremos que $\gamma_p(G) \leq \Phi(G)^p$, o que é suficiente pelo Corolário 5.4. Se $p = 2$, então os únicos grupos analíticos pro-p livres-de-torção de dimensão menor do que 2 são $\mathbb{Z}_2$ e o grupo trivial, que trivialmente satisfazem a condição citada. Assumimos, assim, que $p \geq 3$. Seja G um grupo analítico pro-p livre-de-torção não trivial de dimensão menor que p. Seja

N um subgrupo normal aberto de G p-saturável. Pelo Teorema 5.3, N é um grupo PF. Por indução, podemos assumir que G/N tem ordem p.

Sendo N p-saturável, sabemos que $[N : N^p] = p^{\dim N} \leq p^{p-1}$. Portanto, $[G : N^p] \leq p^p$ e, assim, $\gamma_p(G/N^p) = \gamma_p(G)N^p/N^p = 1$. Segue-se que $\gamma_p(G) \leq N^p$.

Se $\gamma_{p-1}(G) \leq N^p$, então, pela fórmula de Hall, temos:

$$\gamma_p(G) \equiv [\gamma_{p-1}(G), G] \leqq [N^p, G] \leqq [G^p, G] \leqq \gamma_{p+1}(G) \mod [G, G]^p.$$

Como G é residualmente nilpotente, segue-se que $\gamma_p(G) \equiv 1 \mod [G, G]^p$, isto é, $\gamma_p(G) \leq [G, G]^p = \Phi(G)^p$.

Se $\gamma_{p-1}(G) \not\leq N^p$, então G/N^p é um p-grupo de ordem p^p e classe de nilpotência $p-1$ (um p-grupo de classe maximal). Definimos $N_1 := N$ e $N_i := \gamma_i(G)N^p$ para $i = 2, \ldots, p-1$. Então obtemos uma série central descendente

$$N^p < N_{p-1} < \cdots < N_2 < N_1 = N < G$$

de subgrupos normais fechados de G em que cada fator tem ordem p. Como G/N^p é um p-grupo de classe maximal, todo subgrupo normal de G contido estritamente em N está contido em N_2 (de fato, os subgrupos normais de G/N^p são apenas os maximais e os termos da série central inferior, vide [FeAl01] 3.5).

Se $\gamma_p(G) < N^p$, então, como $N/\gamma_p(G)$ é um p-grupo de classe de nilpotência menor que p, é regular. Assim, o conjunto dos elementos de ordem p em $N/\gamma_p(G)$ é um subgrupo. Portanto, $M = \{x \in N \mid x^p \in \gamma_p(G)\}$ é um subgrupo normal de G estritamente contido em N (já que $\gamma_p(G) \neq N^p$). Segue-se que $M \leq N_2$. Pelo Lema 5.1, $M^p = \gamma_p(G)$. Assim, $\gamma_p(G) = M^p \leq N_2^p = \Phi(G)^p$, como queríamos.

Já se $\gamma_p(G) = N^p$, encontraremos uma contradição. Definimos de maneira recursiva $N_i = N_{i-p+1}^p$ para $i \geq p$. Observamos que $N_i = \gamma_i(G)$ se $i \leq p$. Afirmamos que N_i está PF-imerso em N para todo i. Pelo Lema 5.1 (3), podemos assumir que $i \leq p-1$. Note que, pelo item 5 do mesmo lema, $[N^p,_{i-1} N] = \gamma_i(N)^p$. Obtemos, então:

$$[N_i,_{p-1} N] = [\gamma_i(G),_{p-1} N] \leq [\gamma_p(G),_{i-1} N] = [N^p,_{i-1} N] = \gamma_i(N)^p.$$

Mais uma vez retornando ao Lema 5.1, o item (3) nos garante que $\gamma_i(N)$ é PF-imerso em N. Assim, podemos definir uma filtração potente $N_{i,j}$ para N_i em N por $N_{i,1} = N_1$, $N_{i,2} = \gamma_i(N)$ e, para $j > 2$ $N_{i,j} = K_{j-1}$, em que $(K_j)_{j\in\mathbb{N}}$ é uma filtração potente para $\gamma_i(N)$ em N.

Notemos que se $i \leq p-1$, então $[N_i : N_{i+1}] = p$ (pois N/N_p tem ordem p^{p-1}). Pelo Lema 5.1 (4), $N_{j+p-1} = N_j^p = N_j^{\{p\}}$. Pelo Lema 5.8, $[N_j : N_{j+p-1}] = \dfrac{\mu(N_j)}{\mu(N_{j+p-1})} = p^{p-1}$. Portanto, por indução, $[N_i : N_{i+1}] = p$ para todo i.

Afirmamos, por fim, que $N_i = \gamma_i(G)$, para todo $i \geq 2$. Sabemos que isso ocorre se $i \leq p$. Seja $i > p$ e assuma que para todo $j < i$, $N_j = \gamma_j(G)$. Então $N_i = N_{i-p+1}^p = \gamma_{i-p+1}^p = [\gamma_{i-p}(G), G]^p = [N_{i-p}, G]^p$. Similarmente, $\gamma_i(G) = [\gamma_{i-1}(G), G] = [N_{i-1}, G] = [N_{i-p}^p, G]$. Pela fórmula de Hall-Petrescu, $[N_{i-p}^p, G] \equiv [N_{i-p}, G]^p \mod [G,_p N_{i-p}]$, ou seja:

$$N_i \equiv \gamma_i(G) \mod [G,_p N_{i-p}].$$

Ou seja, $N_i[G,_p N_{i-p}] = \gamma_i(G)[G,_p N_{i-p}] = \gamma_i(G)$. Note que $[G,_p N_{i-p}] = [G,_p \gamma_{i-p}(G)] \leq \gamma_i(G)$. Além disso, como N_{i-p+1} é PF-imerso em N, obtemos que

$$[G,_p N_{i-p}] = [G, \gamma_{i-p},_{p-1} N_{i-p}] \leq [\gamma_{i-p+1}(G),_{p-1} N] = [N_{i-p+1},_{p-1} N] \leq N^p_{i-p+2} = N_{i+1} \leq N_i.$$

Assim, segue-se que $N_i = N_i[G,_p N_{i-p}] = \gamma_i(G)$, como queríamos demonstrar. Então G é um grupo pro-p de coclasse 1. Logo G tem torção, mas isso é um absurdo. ■

Corolário (C.5.9). *Seja G um grupo pro-p p-saturável e N um subgrupo normal de G de dimensão menor do que p. Então N é PF-imerso em G.*

Demonstração: Pelos Teoremas 5.3 e 5.5, N e G são grupos PF. Seja $(G_i)_{i\in\mathbb{N}}$ uma filtração potente para G. Defina N_i por $N \cap G_i$. Como N é p-saturável de dimensão menor do que p, então $[N : N_p] \leq p^{p-1}$. Note que, $[N,_{p-1} G]$ tem índice ao menos p^{p-1} em G. Então $[N,_{p-1} G] \equiv 1 \mod N^p$, isto é, $[N,_{p-1} G] \leq N^p$. Portanto $[N_i,_{p-1} G] \leq N^p \cap G_{i+1}$. Pelos itens (4) e (6) do Lema 5.1, $N^p \cap G^p_{i+1} = (N \cap G_{i+1})^p = N^p_{i+1}$. Além disso, é claro que $[N_i, G] \leq N \cap G_{i+1} = N_{i+1}$. Portanto, $(N_i)_{i\in\mathbb{N}}$ é uma filtração potente para N em G. ■

Um $\mathbb{Z}_p$-reticulado de Lie é **residualmente nilpotente** se a interseção de sua série central inferior é 0. Enunciamos a versão análoga aos resultados anteriores para $\mathbb{Z}_p$-reticulados de Lie:

Teorema (T.5.10) ([GoKl09], 4.6). *Todo $\mathbb{Z}_p$-reticulado de Lie residualmente nilpotente de dimensão menor do que p é p-saturável. Além disso, se L é um $\mathbb{Z}_p$-reticulado de Lie p-saturável de dimensão qualquer e M é um ideal de L de dimensão menor do que p, então M é PF-imerso em L.*

Relembramos de seções anteriores que a Fórmula de Hausdorff e sua inversa induzem funtores entre as categorias de grupos analíticos saturáveis e $\mathbb{Z}_p$-reticulados de Lie saturáveis. Consequentemente:

Teorema (T.5.11) ([GoKl09], Teorema B). *Os funtores mencionados definem um isomorfismo entre a categoria dos grupos analíticos p-ádicos pro-p livres-de-torção de dimensão menor do que p e a categoria dos $\mathbb{Z}_p$-reticulados de Lie residualmente nilpotentes de dimensão menor do que p. Esses funtores associam subgrupos fechados e subreticulados, subgrupos normais e ideais e preservam classe de nilpotência e comprimento derivado.*

5.4 Dimensão 2

Nesta seção, utilizando os resultados obtidos nas seções anteriores, classificaremos os grupos analíticos p-ádicos pro-p livres-de-torção de dimensão 2. Para isso, nos restrigimos inicialmente ao caso $p > 2$. Por conveniência, adotamos a convenção $p^\infty = 0$ em $\mathbb{Z}_p$.

Proposição (P.5.12). Se $p \geq 3$, existe uma única família de grupos analíticos p-ádicos pro-p livres-de-torção de dimensão 2, parametrizada por $s \in \mathbb{N}^* \cup \{\infty\}$:

$$G(s) := \langle x, y \mid [x, y] = y^{p^s} \rangle.$$

Demonstração: Seja p um primo ímpar. Pelo Teorema 5.11, basta classificar os $\mathbb{Z}_p$-reticulados de Lie residualmente nilpotentes de dimensão 2. Seja L de tal forma. Assuma L não abeliano.

Seja u, v uma base de L com $[u, v] = au + bv$. Podemos assumir que a e b são potências de p, digamos p^n e p^m, respectivamente, e que $m > n$. Ou seja, $[u, v] = p^n(u + p^{m-n}v)$. Escrevendo $w = u + p^{m-n}v$, L é determinado por $[w, v] = [u, v] = p^n w$.

Concluímos que L existe uma base x, y de L tal que $[y, x] = p^s y$. Observe que se $s = 0$, L não é residualmente nilpotente. Além disso, s é um invariante na classe de isomorfismo de L. De fato, $[L, L]$ é o subreticulado gerado por $p^s y$ e seu centralizador é o subreticulado gerado por y. Daí, o índice do subreticulado derivado em seu centralizador é p^s. Como o derivado é um ideal característico de L, s é um invariante na classe de isomorfismo de L. Então, os $\mathbb{Z}_p$-reticulados de Lie residualmente nilpotentes de dimensão 2 têm apresentações:

$$L(s) := \langle x, y \mid [x, y] = p^s y \rangle.$$

E os grupos associados pela correspondência de Lazard são os grupos $G(s)$. ■

Se permitirmos que $s = 0$, o grupo $G(0)$ é o grupo abeliano pro-p livre de posto 1, tendo, portanto, dimensão 1. $G(\infty)$ é o grupo abeliano pro-p livre de posto 2.

Os grupos $G(s)$ são todos uniformemente *powerful*. De fato, sendo livres-de-torção e finitamente gerados, basta observar que $G(s)' = \overline{\langle y^{p^s} \rangle} \leq G(s)^p$.

Note que todos os grupos de dimensão 2 são extensões *split* de $\mathbb{Z}_p$ por $\mathbb{Z}_p$. A ação de x em y é dada por $y^x = y^{1+p^s}$. Para $s \neq \infty$, o grupo $G(s)$ não é nilpotente e tem comprimento derivado 2.

Note que $pL(s) = \langle px, py \mid [px, py] = p^{s+1} \cdot py \rangle \cong \langle x, y \mid [x, y] = p^{s+1} y \rangle = L(s + 1)$. Segue-se que $G(s)^p \cong G(s + 1)$. Em particular, quando $p > 2$, todo grupo analítico p-ádico pro-p livre-de-torção não abeliano de dimensão 2 é um subgrupo aberto de $G(1)$.

Exemplo (E.5.13). Consideremos o grupo afim $\mathrm{Aff}(\mathbb{Z}_p) = \mathbb{Z}_p \rtimes \mathbb{Z}_p^*$, o qual possui como subgrupos livres-de-torção maximais grupos do tipo $G := \mathbb{Z}_p \rtimes \overline{\langle x \rangle}$, em que x é um elemento de $\mathbb{Z}_p^*$ de ordem infinita. Tomando $x = p + 1$ e sendo y um gerador de $\mathbb{Z}_p$, obtemos que:

$$G = \langle x, y \mid x^y = (p + 1)y \rangle$$

Substituindo a relação $x^y = (p + 1)y$ por $[x, y] = py$ e utilizando notação multiplicativa, obtemos:

$$G = \langle x, y \mid [x, y] = y^p \rangle \cong G(1).$$

Se $p = 2$, $G(1)$ é o grupo $\langle x, y \mid [x, y] = y^2 \rangle$.

Para o caso $p = 2$, não podemos aplicar o Teorema 5.5 — tendo em vista que a dimensão dos grupos não é menor do que p, mas enunciamos uma classificação, cuja demonstração pode ser encontrada em [GoKl09].

Proposição (P.5.14). Existem duas famílias de grupos analíticos 2-ádicos pro-2 livres-de-torção de dimensão 2, parametrizados por $s \in \mathbb{N} \backslash \{0, 1\} \cup \{\infty\}$:

$$G_+(s) = \langle x, y \mid [x, y] = y^{2^s} \rangle \text{ e } G_-(s) = \langle x, y \mid [x, y] = y^{-2-2^s} \rangle.$$

5.5 Dimensão 3

Buscamos agora classificar os grupos analíticos p-ádicos pro-p livres-de-torção de dimensão 3. Para utilizar o Teorema 5.11, precisamos nos restringir ao caso em que $p > 3$. Dividiremos a classificação em duas: caso solúvel e caso não-solúvel. Inciamos pelo caso solúvel.

Seja L um $\mathbb{Z}_p$-reticulado de Lie solúvel de dimensão 3. Extendendo escalares a $\mathbb{Q}_p$ obtemos uma álgebra de Lie $\mathcal{L} := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L$ de dimensão 3. $\mathcal{L}$ possui um ideal abeliano $\mathcal{I}$ de dimensão 2 ([Jac79], Capítulo I, Seção 4) e, portanto, $I := \mathcal{I} \cap L$ é um ideal abeliano de dimensão 2 em L.

Sejam y_1, y_2 elementos de uma base em I e $x \notin I$. Seja K a subálgebra de Lie 1-dimensional de L gerada por x. L é um produto semidireto de I por K. O colchete de Lie em L é dado por:

$$[y_1, y_2] = 0,\ [y_1, x] = a_{11}y_1 + a_{12}y_2,\ [y_2, x] = a_{21}y_1 + a_{22}y_2,$$

para a_{ij} adequados. Defina a matriz $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathfrak{gl}_2(\mathbb{Z}_p)$, de forma que a ação de K em I é dada por $[uy_1 + vy_2, x] = (u, v) \cdot A$. É claro que L é abeliano se, e somente se, $A = 0$ e L é nilpotente se, e somente se, A é uma matriz nilpotente.

Destacamos que se L não é nilpotente, I é o centralizador do subreticulado derivado, sendo, portanto, característico. Lidaremos primeiro com esse caso.

A matriz A depende diretamente da base escolhida para I. Como I é unicamente determinado, A, a menos de mudança de base, determina L. Mudanças de base correspondem a multiplicação por elementos invertíveis e conjugações em $\mathfrak{gl}_2(\mathbb{Z}_p)$. Introduzimos a **classe de similaridade-multiplicativa** de uma matriz A em $\mathfrak{gl}_2(\mathbb{Z}_p)$: $\mathfrak{A} = \{uB^{-1}AB \mid u \in \mathbb{Z}_p^*, B \in \mathrm{GL}_2(\mathbb{Z}_p)\}$.

A classe $\mathfrak{A}$ determina completamente L. Assim, classificar os $\mathbb{Z}_p$-reticulados de Lie solúveis de dimensão 3 se resume a encontrar as classes de similaridade-multiplicativa de matrizes em $\mathfrak{gl}_2(\mathbb{Z}_p)$.

Proposição (P.5.15). Seja $p > 2$ e $\eta \in \mathbb{Z}_p^*$ um não quadrado módulo p. Toda matriz não nilpotente em $\mathfrak{gl}_2(\mathbb{Z}_p)$ tem a mesma classe de similaridade-multiplicativa de uma matriz da forma $p^s A_0$, em que $s \in \mathbb{N}$ e A_0 é uma das matrizes abaixo:

(1) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;

(2) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^r \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}$, em que $r \in \mathbb{N}^*$ e $d \in \mathbb{Z}_p$;

(3) $\begin{pmatrix} 0 & d \\ 1 & p^r \end{pmatrix}$, em que $r \in \mathbb{N}$ e $d \in \mathbb{Z}_p$;

(4) $\begin{pmatrix} 0 & p^r \\ 1 & 0 \end{pmatrix}$, em que $r \in \mathbb{N}$;

(5) $\begin{pmatrix} 0 & \eta p^r \\ 1 & 0 \end{pmatrix}$, em que $r \in \mathbb{N}$.

Demonstração: Para esta demonstração, recorremos a [ApOn83], observando que matrizes não escalares módulo p em $\mathfrak{gl}_2(\mathbb{Z}_p)$ são similares se possuem o mesmo polinômio característico, ou seja, mesmo traço

e determinante. Assuma que A é uma matriz não nula em $\mathfrak{gl}(\mathbb{Z}_p)$ de classe similar-multiplicativa $\mathfrak{A}$. Podemos escrever unicamente $A = p^s A_0$ de forma que $s \in \mathbb{Z}_{\geq 0}$ e $A_0 \not\equiv 0 \mod p$. Observemos que s é um invariante da classe $\mathfrak{A}$, bem como a classe similar-multiplicativa de A_0, $\mathfrak{A}_0$.

Caso 1. A_0 é escalar. Multiplicando por uma unidade $u \in \mathbb{Z}_p^*$ apropriada, evidencia-se que A_0 está na mesma classe da matriz identidade.

Caso 2. A_0 não é escalar, mas é escalar módulo p. Existe um único inteiro positivo r (invariante na classe de A_0), tal que A_0 é escalar módulo p^r, mas não é escalar módulo p^{r+1}. Então $A_0 = u\,\mathrm{Id} + p^r A_1$, em que A_1 não é escalar módulo p e u é uma unidade em $\mathbb{Z}_p$. É claro que podemos assumir $u = 1$. Então $A_0 = \begin{pmatrix} 1+p^r a & p^r b \\ p^r c & 1+p^r d \end{pmatrix}$. Multiplicando pelo elemento $1 + p^r l \in \mathbb{Z}_p^*$, em que $l = -\dfrac{a+d}{2+p^r(a+d)}$, obtemos a matriz $\begin{pmatrix} 1+p^r q & p^r b' \\ p^r c' & 1-p^r q \end{pmatrix} = \mathrm{Id} + p^r \begin{pmatrix} q & b' \\ c' & -q \end{pmatrix}$, em que $q = \dfrac{a-d}{2+p^r(a+d)}$, $b' = b(1+p^r l)$ e $c' = c(1+p^r l)$. Ou seja, podemos assumir que a matriz A_1 tem traço zero. Sendo $d = -\det(A_1) \in \mathbb{Z}_p$, já que as matrizes A_1 e $\begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}$ têm mesmo traço e determinante, são similares. Daí A_0 está na mesma classe de $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^r \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}$.

Caso 3. A_0 não é escalar módulo p e tem traço diferente de zero. Reescale A_0 por uma unidade u favorável (se $\mathrm{Tr}(A_0) = wp^r$, com w invertível, escolha $u = w^{-1}$), de forma que a matriz A_1 obtida tem traço p^r. r é um invariante da classe de A_0. Sendo $d = -\det(A_1)$, obtemos que a A_0 está na classe de $\begin{pmatrix} 0 & d \\ 1 & p^r \end{pmatrix}$.

Caso 4. A_0 não é escalar módulo p e tem traço zero. Seu determinante é zero ou da forma up^r, com u invertível. Se não é zero, a depender de se u é ou não resíduo quadrático módulo p, a matriz A_0 é múltipla escalar por uma unidade de uma matriz com determinante $-\eta p^r$ ou $-p^r$. Ou seja, A_0 é similar a $\begin{pmatrix} 0 & p^r \\ 1 & 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 & \eta p^r \\ 1 & 0 \end{pmatrix}$, em que $r \in \mathbb{N}$. Se $\det(A_0) = 0$, A_0 tem mesma classe de $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. ■

Durante a demonstração do resultado acima, mostramos também:

Proposição (P.5.16). Seja $p > 2$. Toda matriz nilpotente em $\mathfrak{gl}_2(\mathbb{Z}_p)$ tem a mesma classe similar-multiplicativa de uma das matrizes abaixo:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ ou } p^s \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, s \in \mathbb{N}.$$

Voltemos aos $\mathbb{Z}_p$-reticulados de Lie. Se L um $\mathbb{Z}_p$-reticulado nilpotente e não abeliano de dimensão 3, recorde que L é um produto semidireto $I \rtimes K$ com I abeliano de dimensão 3 e K de dimensão 1. A ação de K em I é dada por uma matriz da forma $p^s \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, em que $s = [\mathrm{iso}_L(L') : L]$. Assim, obtemos uma associação clara entre classes de isomorfismo de $\mathbb{Z}_p$-reticulados de Lie solúveis de dimensão 3 e as matrizes expressas nas proposições 5.15 e 5.16.

Para $p > 3$, podemos utilizar os Teoremas 5.5 e 5.11 para classificar os grupos analíticos pro-p solúveis livres-de-torção de dimensão 3. O reticulado L associado a uma classe $\mathfrak{A}$ é residualmente nilpotente se, e somente se, um representante A de $\mathfrak{A}$ são nilpotentes módulo p. O grupo associado ao reticulado L

é um produto semidireto $G := N \rtimes H$, em que N, H são grupos abelianos pro-p livres de posto 2 e 1, respectivamente. A ação de H em N é dada por $1 + A$ (note que como A é residualmente nilpotente, $\sum_{n\geq 0}(-1)^n A^n$ converge, sendo o inverso de A em $\mathrm{GL}_2(\mathbb{Z}_p)$). Para grupos nilpotentes, temos:

Proposição (P.5.17). Se $p > 3$, os grupos analíticos p-ádicos pro-p livres-de-torção nilpotentes de dimensão 3 são da forma:

$$G_0(s) = \langle x, y, z \mid [x, y] = z^{p^s}, [x, z] = [y, z] = 1\rangle,$$

em que $s \in \mathbb{N} \cup \{\infty\}$.

Seja $L_0(s)$ o $\mathbb{Z}_p$-reticulado associado ao grupo $G_0(s)$. $L_0(s)$ tem apresentação $\langle x, y, z \mid [x, y] = p^s z, [x, z] = [y, z] = 0\rangle$. Então $pL_0(s) = \langle px, py, pz \mid [px, py] = p^{s+1} \cdot pz, [px, pz] = [py, pz] = 0\rangle \cong L_0(s+1)$. Consequentemente, quando $p > 3$, todo grupo analítico p-ádico pro-p livre-de-torção nilpotente não abeliano é um subgrupo aberto do grupo $G_0(0)$.

Note que se A é uma das matrizes da Proposição 5.15, A é residualmente nilpotente se, e somente se $A^2 \equiv 0 \mod p$. De fato, se A é residualmente nilpotente, A é nilpotente $\mod p$ e, como $\mathbb{Z}/p\mathbb{Z}$ é um corpo e A é uma matriz 2 por 2, $A^2 \equiv 0 \mod p$. Se $A^2 \equiv 0 \mod p$, então para todo $n \geq 1$, existe $m \geq 1$ tal que $A^{2m} \equiv 0 \mod p^n$ e, portanto, A é residualmente nilpotente.

Verifiquemos quais classes de similaridade-multiplicativa em $\mathfrak{gl}_2(\mathbb{Z}_p)$ são residualmente nilpotentes:

(1) Se $A = p^s \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, então $A^2 = p^{2s} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é zero módulo p se, e somente se, $s > 0$.

(2) Se $A = p^s \begin{pmatrix} 1 & p^r d \\ p^r & 1 \end{pmatrix}$, então $A^2 = p^{2s} \begin{pmatrix} 1 + p^{2r} d & 2p^r d \\ 2p^r & 1 + p^{2r} d \end{pmatrix}$ é zero módulo p se, e somente se, $s > 0$.

(3) Se $A = p^s \begin{pmatrix} 0 & d \\ 1 & p^r \end{pmatrix}$, então $A^2 = p^{2s} \begin{pmatrix} d & dp^r \\ p^r & d + p^r \end{pmatrix}$ é zero módulo p se, e somente se, $s > 0$ ou $d \in p\mathbb{Z}_p$ e $r > 0$.

(4) Se $A = p^s \begin{pmatrix} 0 & p^r \\ 1 & 0 \end{pmatrix}$, então $A^2 = p^{2s+r} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é zero módulo p se, e somente se, $s > 0$ ou $r > 0$.

(5) Se $A = p^s \begin{pmatrix} 0 & \eta p^r \\ 1 & 0 \end{pmatrix}$, então $A^2 = p^{2s+r}\eta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é zero módulo p se, e somente se, $s > 0$ ou $r > 0$.

Tendo em vista o Teorema 5.11, obtemos:

Teorema (T.5.18). *Para $p > 3$, a seguir temos uma lista completa e não redundante de apresentações pro-p de grupos analíticos p-ádicos pro-p livres-de-torção solúveis de dimensão 3:*

(1) o grupo abeliano pro-p livre de posto 3,

$$G_0(\infty) = \langle x_1, x_2, x_3 \mid [x_1, x_2] = [x_1, x_3] = [x_2, x_3] = 1\rangle.$$

(2) os grupos de classe de nilpotência 2, subgrupos abertos do grupo $G_0(0)$, parametrizados por $s \in \mathbb{N}$,

$$G_0(s) = \langle x, y, z \mid [x, y] = z^{p^s}, [x, z] = [y, z] = 1 \rangle.$$

(3) a família abaixo de grupos parametrizados por $s \in \mathbb{N}^*$,

$$G_1(s) = \langle x, y_1, y_2 \mid [y_1, y_2] = 1, [y_1, x] = y_1^{p^s}, [y_2, x] = y_2^{p^s} \rangle.$$

(4) a família abaixo de grupos parametrizados por $s, r \in \mathbb{N}$ e $d \in \mathbb{Z}_p$, com $s \geq 1$,

$$G_2(s, r, d) = \langle x, y_1, y_2 \mid [y_1, y_2] = 1, [y_1, x] = y_1^{p^s} y_2^{p^{s+r}d}, [y_2, x] = y_1^{p^{s+r}} y_2^{p^s} \rangle.$$

(5) a família abaixo de grupos parametrizados por $s, r \in \mathbb{N}$ e $d \in \mathbb{Z}_p$ satisfazendo $s + r \geq 1$ e $d \in p\mathbb{Z}_p$,

$$G_3(s, r, d) = \langle x, y_1, y_2 \mid [y_1, y_2] = 1, [y_1, x] = y_2^{p^s d}, [y_2, x] = y_1^{p^s} y_2^{p^{s+r}} \rangle.$$

(6) a família abaixo de grupos parametrizados por $s, r \in \mathbb{N}$ satisfazendo $s \geq 1$ ou $r \geq 1$,

$$G_4(s, r) = \langle x, y_1, y_2 \mid [y_1, y_2] = 1, [y_1, x] = y_2^{p^{s+r}}, [y_2, x] = y_1^{p^s} \rangle.$$

(7) a família abaixo de grupos parametrizados por $s, r \in \mathbb{N}$ satisfazendo $s \geq 1$ ou $r \geq 1$,

$$G_5(s, r) = \langle x, y_1, y_2 \mid [y_1, y_2] = 1, [y_1, x] = y_2^{p^{s+r}\eta}, [y_2, x] = y_1^{p^s} \rangle,$$

em que $\eta \in \mathbb{Z}_p^*$ não é um quadrado módulo p.

Observe que nem todos os grupos acima são uniformemente *powerful*. De fato, basta verficar para um grupo da lista acima se $G' \leq G^p$, o que se mostra falso para $G_0(0), G_3(0, r, d), G_4(0, r)$ e $G_5(0, r)$ e verdadeiro para os outros grupos na lista.

Se $p = 2$ ou $p = 3$, a lista acima não satura todos os grupos analíticos p-ádicos pro-p livres-de-torção solúveis de dimensão 3, mas fornece uma grande quantidade de exemplos. Exibimos um grupo quando $p = 3$ que não está na lista acima:

Exemplo (E.5.19). Seja M um grupo abeliano pro-3 livre de posto 2 livremente gerado por x_1 e x_2 e $A = \langle \alpha \rangle \cong \mathbb{Z}_3$. Seja $G := M \rtimes A$ com ação dada por $x_1^\alpha = x_1 x_2$ e $x_2^\alpha = x_2 x_1^3$. G é um grupo analítico 3-ádico pro-3 livre-de-torção. Como $[x_1, \alpha] = x_2$ e $[x_2, \alpha] = x_1^3$, $[M, G, G] = M^3$. Afirmamos que G não é p-saturável (e, portanto, não aparece na lista expressa no Teorema 5.18). Assuma que G admite uma filtração potente $(G_i)_{i \in \mathbb{N}}$. Então $M^3 \leq \gamma_3(G) \leq G_2^3$, o que implica $M \leq G_2$. Indutivamente, $M \leq \bigcap G_i = 1$, absurdo. O grupo G possui a seguinte apresentação pro-3:

$$\langle x, y_1, y_2 \mid [y_1, y_2] = 1, [y_1, x] = y_2, [y_2, x] = y_1^3 \rangle.$$

Observe que os parâmetros s nas famílias de grupos exibidas no Teorema 5.18 não alteram a $\mathbb{Q}_p$-álgebra de Lie do grupo. Ilustramos com um exemplo:

Exemplo (E.5.20). As $\mathbb{Q}_p$-álgebras de Lie dos grupos $G_1(s)$ estão na mesma classe de isomorfismo. De fato, a $\mathbb{Q}_p$-álgebra de Lie do grupo $G_1(s)$ tem a seguinte apresentação:

$$\langle x, y_1, y_2 \mid [y_1, y_2] = 0, [y_1, x] = p^s y_1, [y_2, x] = p^s y_2 \rangle.$$

Tomando $z = p^{-s}x$, obtemos uma apresentação alternativa para $\mathcal{L}(G_1(s))$:

$$\langle z, y_1, y_2 \mid [y_1, y_2] = 0, [y_1, z] = y_1, [y_2, z] = y_2 \rangle,$$

que independe de s.

Exibimos agora uma classificação para as $\mathbb{Q}_p$-álgebras de Lie solúveis de dimensão 3 quando $p > 2$:

Teorema (T.5.21). *Seja $p > 2$, a seguir temos uma lista completa e não redundante de todas as $\mathbb{Q}_p$-álgebras de Lie solúveis de dimensão 3:*

(1) a álgebra de Lie abeliana,

$$\mathcal{L}_0(\infty) = \langle x_1, x_2, x_3 \mid [x_1, x_2] = [x_1, x_3] = [x_2, x_3] = 0 \rangle.$$

(2) a álgebra de Lie nilpotente de classe de nilpotência 2,

$$\mathcal{L}_0 = \langle x, y, z \mid [x, y] = z, [x, z] = [y, z] = 0 \rangle.$$

(3) a $\mathbb{Q}_p$-álgebra de Lie dos grupos G_1,

$$\mathcal{L}_1 = \langle x, y_1, y_2 \mid [y_1, y_2] = 0, [y_1, x] = y_1, [y_2, x] = y_2 \rangle.$$

(4) as $\mathbb{Q}_p$-álgebras de Lie dos grupos G_2, parametrizada por $r \in \mathbb{N}$ e $d \in \mathbb{Z}_p$,

$$\mathcal{L}_2(s, d) = \langle x, y_1, y_2 \mid [y_1, y_2] = 0, [y_1, x] = y_1 + p^r d y_2, [y_2, x] = p^r y_1 + y_2 \rangle.$$

(5) as $\mathbb{Q}_p$-álgebras de Lie dos grupos G_3, parametrizada por $r \in \mathbb{N}$ e $d \in \mathbb{Z}_p$,

$$\mathcal{L}_3(r, d) = \langle x, y_1, y_2 \mid [y_1, y_2] = 0, [y_1, x] = d y_2, [y_2, x] = y_1 + p^r y_2 \rangle.$$

(6) a $\mathbb{Q}_p$-álgebra de Lie dos grupos G_4 parametrizada por $r \in \mathbb{N}$,

$$\mathcal{L}_4(r) = \langle x, y_1, y_2 \mid [y_1, y_2] = 0, [y_1, x] = p^r y_2, [y_2, x] = y_1 \rangle.$$

(7) a $\mathbb{Q}_p$-álgebra de Lie dos grupos G_5 parametrizada por $r \in \mathbb{N}$,

$$\mathcal{L}_5(r) = \langle x, y_1, y_2 \mid [y_1, y_2] = 0, [y_1, x] = \eta p^r y_2, [y_2, x] = y_1 \rangle,$$

onde $\eta \in \mathbb{Z}_p^*$ não é um quadrado módulo p.

Podemos obter o resultado de duas formas: a partir do Teorema 5.18, calculando as $\mathbb{Q}_p$-álgebras de Lie de todos os grupos listados e observando que toda $\mathbb{Q}_p$-álgebra de Lie é realizada desta forma (aqui precisamos nos restringir ao caso em que $p \neq 3$) ou, com argumentos similares aos feitos para $\mathbb{Z}_p$-reticulados solúveis tridimensionais, calcular classes de similaridade multiplicativa em $\mathfrak{gl}_2(\mathbb{Q}_p)$, observando que neste caso p é invertível e que as matrizes associadas às álgebras não precisam ser residualmente nilpotentes. Pelo primeiro caminho, observamos quais $\mathbb{Q}_p$-álgebras de Lie são associadas a quais grupos e, pelo segundo, conseguimos entender o porquê da lista apresentada não ser redundante.

Demonstração: Seja $\mathcal{L}$ uma $\mathbb{Q}_p$-álgebra de Lie solúvel de dimensão 3. Então $\mathcal{L}$ se decompõe como produto semidireto de um ideal abeliano $\mathcal{I}$ de dimensão 2 por um complemento $\mathcal{K}$ de dimensão 1. Sejam y_1, y_2 elementos de uma base de $\mathcal{I}$ e x um elemento não nulo de $\mathcal{K}$. O colchete de Lie em $\mathcal{L}$ é dado por:

$$[y_1, y_2] = 0,\ [y_1, x] = a_{11}y_1 + a_{12}y_2,\ [y_2, x] = a_{21}y_1 + a_{22}y_2,$$

Obtemos, assim, uma matriz $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathfrak{gl}_2(\mathbb{Q}_p)$. A classe de similaridade-multiplicativa de A em $\mathfrak{gl}_2(\mathbb{Q}_p)$ determina $\mathcal{L}$. Note que podemos assumir que A tem coeficientes em $\mathbb{Z}_p$ (multiplicando por uma potência de p suficientemente grande). Em geral toda matriz em $\mathfrak{gl}_2(\mathbb{Q}_p)$ é uma potência inteira de p vezes uma matriz em $\mathfrak{gl}_2(\mathbb{Z}_p)$ e, assim, conjugar a matriz A por uma matriz de $\mathrm{GL}_2(\mathbb{Q}_p)$ é o mesmo que conjugá-la por uma matriz de $\mathrm{GL}_2(\mathbb{Z}_p)$. Consequentemente, classificar as classes de similaridade-multiplicativa de $\mathfrak{gl}_2(\mathbb{Q}_p)$ se reduz a observar as proposições 5.16 e 5.17 e ver quais classes em $\mathfrak{gl}_2(\mathbb{Z}_p)$ se diferem apenas por uma potência de p. Ou seja, são representantes das classes $\mathfrak{gl}_2(\mathbb{Q}_p)$ os representantes de $\mathfrak{gl}_2(\mathbb{Z}_p)$ de parâmetro s igual a zero. ■

Finalizado o caso solúvel, prosseguimos agora ao caso não-solúvel. Seja L um $\mathbb{Z}_p$-reticulado de Lie não-solúvel de dimensão 3. Então $\dim(L') = 3$ — se $\dim(L') \leq 2$, L' é solúvel e, portanto, L também. Seguindo [Jac79] (Capítulo I, Seção 4), seja (e_1, e_2, e_3) uma base de L e defina $f_1 = [e_2, e_3]$, $f_2 = [e_3, e_1]$, $f_3 = [e_1, e_2]$. Escreva $f_i = \sum_{j=1}^{3} \alpha_{ij} e_j$. Como $\dim(L') = 3$, (f_1, f_2, f_3) são linearmente independentes e a matriz $A = (\alpha_{ij})_{i,j=1}^{3}$ tem posto 3. A única desigualdade de Jacobi não trivial é

$$0 = [f_1, e_1] + [f_2, e_2] + [f_3, e_3] = (\alpha_{32} - \alpha_{23})f_1 + (\alpha_{13} - \alpha_{31})f_2 + (\alpha_{21} - \alpha_{12})f_2,$$

que implica $\alpha_{ij} = \alpha_{ji}$, *i.e.*, que a matriz A é simétrica. Realizando o mesmo processo com outra base acarreta em uma matriz B do tipo uP^TAP, onde $u \in \mathbb{Z}_p^*$ e $P \in \mathrm{GL}_3(\mathbb{Z}_p)$. É natural, assim, definir a **classe de congruência-multiplicativa** de uma matriz A: $\mathfrak{A} = \{uP^TAP | u \in \mathbb{Z}_p^*, P \in \mathrm{GL}_3(\mathbb{Z}_p)\}$. Dessa forma estabelecemos uma bijeção entre as classes de congruência-multiplicativa de matrizes simértricas de posto 3 em $\mathrm{GL}_3(\mathbb{Z}_p)$ e $\mathbb{Z}_p$-reticulados de Lie não solúveis de dimensão 3.

Gostaríamos, assim, de determinar representantes para tais classes. Tal problema é relacionado, naturalmente, à classificação de formas quadráticas não-degeneradas sobre $\mathbb{Z}_p$. Uma classificação nos é oferecida em [Cas78] (Capítulo 8, Teorema 3.1) e enunciamos sua simplificação para formas quadráticas em 3 variáveis:

Proposição (P.5.22). Seja $\eta \in \mathbb{Z}_p^*$ um não quadrado módulo p. Toda forma quadrática não-degenerada em três variáveis sobre $\mathbb{Z}_p$ é expressa, em alguma base, por exatamente uma das matrizes a seguir:

(1) $\text{diag}(\eta^{\varepsilon_0}p^{s_0}, \eta^{\varepsilon_1}p^{s_1}, \eta^{\varepsilon_2}p^{s_2})$, com $0 \leq s_0 < s_1 < s_2$ e $\varepsilon_i \in \{0,1\}$;

(2) $\text{diag}(p^{s_0}, \eta^{\varepsilon_0}p^{s_0}, \eta^{\varepsilon_1}p^{s_1})$, com $0 \leq s_0 < s_1$ e $\varepsilon_i \in \{0,1\}$;

(3) $\text{diag}(\eta^{\varepsilon_0}p^{s_0}, p^{s_1}, \eta^{\varepsilon_1}p^{s_1})$, com $0 \leq s_0 < s_1$ e $\varepsilon_i \in \{0,1\}$;

(4) $\text{diag}(p^{s_0}, p^{s_0}, \eta^{\varepsilon_0}p^{s_0})$, com $0 \leq s_0$ e $\varepsilon_0 \in \{0,1\}$.

Classes de equivalência de formas quadráticas não-degeneradas estão em correspondência a classes de congruência de matrizes simétricas de posto 3. Precisamos selecionar na lista acima representantes de classes de congruência-multiplicativa. Enunciamos antes um útil lema:

Lema (L.5.23) ([Cas78], 8.3.4, adaptado). Sejam $u_1, \ldots, u_n \in \mathbb{Z}_p^*$. As matrizes $\text{diag}(u_1p^{a_1}, \ldots, u_np^{a_n})$ e $\text{diag}(p^{a_1}, \ldots, p^{a_{n-1}}, up^{a_n})$ são congruentes, onde $u = \prod_{i=1}^{n} u_i$.

Proposição (P.5.24) ([NoSn19], 2.15). Seja $\eta \in \mathbb{Z}_p^*$ um não quadrado módulo p. A seguir temos uma lista completa e não redundante de representantes de classes de congruência-multiplicativa de matrizes simétricas de posto 3:

(1) $\text{diag}(p^{s_0}, \eta^{\varepsilon_1}p^{s_1}, \eta^{\varepsilon_2}p^{s_2})$, com $0 \leq s_0 < s_1 < s_2$ e $\varepsilon_i \in \{0,1\}$;

(2) $\text{diag}(p^{s_0}, \eta^{\varepsilon_0}p^{s_0}, p^{s_1})$, com $0 \leq s_0 < s_1$ e $\varepsilon_0 \in \{0,1\}$;

(3) $\text{diag}(p^{s_0}, p^{s_1}, \eta^{\varepsilon_1}p^{s_1})$, com $0 \leq s_0 < s_1$ e $\varepsilon_1 \in \{0,1\}$;

(4) $\text{diag}(p^{s_0}, p^{s_0}, p^{s_0})$, com $0 \leq s_0$.

Demonstração: Analisemos cada família de matrizes da Proposição 5.22. Seja A uma matriz simétrica de posto 3.

(1) $A \sim \text{diag}(\eta^{\varepsilon_0}p^{s_0}, \eta^{\varepsilon_1}p^{s_1}, \eta^{\varepsilon_2}p^{s_2})$. Multiplicando por η^{ε_0}, $A \sim \text{diag}(\eta^2p^{s_0}, \eta^{\varepsilon_1'}p^{s_1}, \eta^{\varepsilon_2'}p^{s_2})$, onde $\varepsilon_i' \in \{0,1\}$. Claramente, $A \sim \text{diag}(p^{s_0}, \eta^{\varepsilon_1'}p^{s_1}, \eta^{\varepsilon_2'}p^{s_2})$.

(2) $A \sim \text{diag}(p^{s_0}, \eta^{\varepsilon_0}p^{s_0}, \eta^{\varepsilon_1}p^{s_1})$. Se $\varepsilon_1 = 0$, $A \sim \text{diag}(p^{s_0}, \eta^{\varepsilon_0}p^{s_0}, p^{s_1})$. Se $\varepsilon_1 = 1$, multiplicando por η, obtemos $A \sim \text{diag}(\eta p^{s_0}, \eta^{1+\varepsilon_0}p^{s_0}, \eta^2p^{s_1})$. Pelo lema, $A \sim \text{diag}(p^{s_0}, \eta^{2+\varepsilon_0}p^{s_0}, \eta^2p^{s_1})$, que é claramente congruente a $\text{diag}(p^{s_0}, \eta^{\varepsilon_0}p^{s_0}, p^{s_1})$.

(3) $A \sim \text{diag}(\eta^{\varepsilon_0}p^{s_0}, p^{s_1}, \eta^{\varepsilon_1}p^{s_1})$. Se $\varepsilon_0 = 0$, $A \sim \text{diag}(p^{s_0}, p^{s_1}, \eta^{\varepsilon_1}p^{s_1})$. Se $\varepsilon_1 = 1$, multiplicando por η, obtemos $A \sim \text{diag}(\eta^2p^{s_0}, \eta p^{s_1}, \eta^{1+\varepsilon_1}p^{s_1})$ e, como feito no caso anterior, obtemos $A \sim \text{diag}(p^{s_0}, p^{s_1}, \eta^{\varepsilon_1}p^{s_1})$.

(4) $A \sim \text{diag}(p^{s_0}, p^{s_0}, \eta^{\varepsilon_0}p^{s_0})$. Se $\varepsilon_0 = 0$, $A \sim \text{diag}(p^{s_0}, p^{s_0}, p^{s_0})$. Se $\varepsilon_0 = 1$, multiplicando por η e utilizando o lema, obtemos que $A \sim \text{diag}(p^{s_0}, p^{s_0}, p^{s_0})$.

Ainda nos resta mostrar que duas matrizes na lista não tem mesma classe de congruência-multiplicativa. Sejam A, B duas matrizes distintas apresentadas na lista e assuma que $A \sim B$. Então A é congruente a uB, onde $u \in \mathbb{Z}_p^*$. Se u é um quadrado, A é congruente a B, então $A = B$. Se não, escrevendo $u = \eta v^2, v \in \mathbb{Z}_p^*$, segue-se que A é congruente a ηB. Analisaremos cada possibilidade para B e chegaremos a uma contradição em cada uma. Por conveniência, denotamos por Ω o conjunto das matrizes apresentadas no enunciado e por Ω^* o conjunto das matrizes apresentadas na Proposição 5.22. Mostremos que $A \in \Omega^* \backslash \Omega$, uma contradição.

(1) $B = \mathrm{diag}(p^{s_0}, \eta^{\varepsilon_1}p^{s_1}, \eta^{\varepsilon_2}p^{s_2})$. Então A é congruente a $\mathrm{diag}(\eta p^{s_0}, \eta^{1+\varepsilon_1}p^{s_1}, \eta^{1+\varepsilon_2}p^{s_2})$. Sendo ε_i' o elemento de $\{0,1\}$ congruente a $1+\varepsilon_i$ módulo 2, como $A \in \Omega \subset \Omega^*$, $A = \mathrm{diag}(\eta p^{s_0}, \eta^{\varepsilon_1'}p^{s_1}, \eta^{\varepsilon_2'}p^{s_2}) \notin \Omega$.

(2) $B = \mathrm{diag}(p^{s_0}, \eta^{\varepsilon_0}p^{s_0}, p^{s_1})$. Então A é congruente a $\mathrm{diag}(\eta p^{s_0}, \eta^{1+\varepsilon_0}p^{s_0}, \eta p^{s_1})$. Novamente pelo lema, A é congruente a $\mathrm{diag}(p^{s_0}, \eta^{\varepsilon_0}p^{s_0}, \eta p^{s_1}) \in \Omega\backslash\Omega^*$.

(3) $B = \mathrm{diag}(p^{s_0}, p^{s_1}, \eta^{\varepsilon_1}p^{s_1})$. Então A é congruente a $\mathrm{diag}(\eta p^{s_0}, \eta p^{s_1}, \eta^{1+\varepsilon_1}p^{s_1})$ que, por sua vez, é congruente a $\mathrm{diag}(\eta p^{s_0}, \eta p^{s_1}, \eta^{1+\varepsilon_1}p^{s_1})$. Pelo lema, $A = \mathrm{diag}(\eta p^{s_0}, p^{s_1}, \eta^{\varepsilon_1}p^{s_1}) \notin \Omega$.

(4) $B = \mathrm{diag}(p^{s_0}, p^{s_0}, p^{s_0})$. Então A é congruente a $\mathrm{diag}(\eta p^{s_0}, \eta p^{s_0}, \eta p^{s_0})$. Utilizando o lema mais uma vez, $A = \mathrm{diag}(p^{s_0}, p^{s_0}, \eta p^{s_0}) \notin \Omega$,

■

Podemos, agora, exibir apresentações para todas as classes de $\mathbb{Z}_p$-reticulados de Lie insolúveis de dimensão 3.

Proposição (P.5.25). Seja $p > 2$ e $\eta \in \mathbb{Z}_p^*$ um não quadrado módulo p. A seguir temos uma lista completa e não redundante de apresentações de todos os $\mathbb{Z}_p$-reticualdos de Lie insolúveis de dimensão 3.

(1) $L_1(s_0, s_1, s_2, \varepsilon_1, \varepsilon_2) = \langle x, y, z \mid [y,z] = p^{s_0}x, [z,x] = \eta^{\varepsilon_1}p^{s_1}y, [x,y] = \eta^{\varepsilon_2}p^{s_2}z\rangle$, onde $\varepsilon_1, \varepsilon_2 \in \{0,1\}$, $s_0, s_1, s_2 \in \mathbb{N}$ e $s_0 < s_1 < s_2$.

(2) $L_2(s_0, s_1, \varepsilon_0) = \langle x, y, z \mid [y,z] = p^{s_0}x, [z,x] = \eta^{\varepsilon_0}p^{s_0}y, [x,y] = p^{s_1}z\rangle$, onde $\varepsilon_0 \in \{0,1\}$, $s_0, s_1 \in \mathbb{N}$ e $s_0 < s_1$.

(3) $L_3(s_0, s_1, \varepsilon_1) = \langle x, y, z \mid [y,z] = p^{s_0}x, [z,x] = p^{s_1}y, [x,y] = \eta^{\varepsilon_1}p^{s_1}z\rangle$, onde $\varepsilon_1 \in \{0,1\}$, $s_0, s_1 \in \mathbb{N}$ e $s_0 < s_1$.

(4) $L_4(s_0) = \langle x, y, z \mid [y,z] = p^{s_0}x, [z,x] = p^{s_0}y, [x,y] = p^{s_0}z\rangle$, onde $s_0 \in \mathbb{N}$.

Precisamos verificar quais reticulados do resultado acima são residualmente nilpotentes. É claro que todos os reticulados em que s_0 é positivo são residualmente nilpotentes. Observemos que $L_4(0)$ não é residualmente nilpotente, já que é perfeito. $L_3 = L_3(0, s_1, \varepsilon_1)$ é residualmente nilpotente: $\gamma_3(L_3) \subset pL_3$ e indutivamente para todo n existe m tal que $\gamma_m(L_3) \subset p^nL_3$, ou seja $\bigcap_{m\in\mathbb{N}} \gamma_m(L_3) = 0$. $L_1 = L_1(0, s_1, s_2, \varepsilon_1, \varepsilon_2)$ também é residualmente nilpotente pela mesma razão de L_3. Já $L_2(0, s_1, \varepsilon_0)$ não é residualmente nilpotente: $x, y \in \gamma_2(L_2)$, assim $[y,z] = x, [\eta^{-\varepsilon_0}x, z] = y \in \gamma_3(L_2)$ e, indutivamente, $x, y \in \gamma_n(L_2)$ para todo n. Para a correspondência com grupos, precisamos de $p > 3$. Concluímos com o desejado:

Teorema (T.5.26). *Para $p > 3$, a seguir temos uma lista completa e não redundante de apresentações pro-p de grupos analíticos p-ádicos pro-p livres-de-torção insolúveis de dimensão 3:*

(1) $G_1(s_0, s_1, s_2, \varepsilon_1, \varepsilon_2) = \langle x, y, z \mid [y,z] = x^{p^{s_0}}, [z,x] = y^{\eta^{\varepsilon_1}p^{s_1}}, [x,y] = z^{\eta^{\varepsilon_2}p^{s_2}}\rangle$, *onde* $\varepsilon_1, \varepsilon_2 \in \{0,1\}$, $s_0, s_1, s_2 \in \mathbb{N}$ *e* $s_0 < s_1 < s_2$.

(2) $G_2(s_0, s_1, \varepsilon_0) = \langle x, y, z \mid [y,z] = x^{p^{s_0}}, [z,x] = y^{\eta^{\varepsilon_0}p^{s_0}}, [x,y] = z^{p^{s_1}}\rangle$, *onde* $\varepsilon_0 \in \{0,1\}$, $s_0, s_1 \in \mathbb{N}^*$ *e* $s_0 < s_1$.

(3) $G_3(s_0, s_1, \varepsilon_1) = \langle x, y, z \mid [y,z] = x^{p^{s_0}}, [z,x] = y^{p^{s_1}}, [x,y] = z^{\eta^{\varepsilon_1} p^{s_1}} \rangle$, *onde* $\varepsilon_1 \in \{0,1\}$, $s_0, s_1 \in \mathbb{N}$ *e* $s_0 < s_1$.

(4) $G_4(s_0) = \langle x, y, z \mid [y,z] = x^{p^{s_0}}, [z,x] = y^{p^{s_0}}, [x,y] = z^{p^{s_0}} \rangle$, *onde* $s_0 \in \mathbb{N}^*$.

Note que juntando os Teoremas 5.18 e 5.26, obtemos apresentações de todos os grupos analíticos p-ádicos pro-p livres-de-torção de dimensão 3 para $p > 3$.

Cabe aqui uma observação sobre o Teorema 5.26. Enunciamos na forma de proposição:

Proposição (P.5.27) ([GoKl09], Seção 7.3). Seja $p > 3$, todo grupo analítico pro-p livre-de-torção insolúvel de dimensão 3 é isomorfo a um subgrupo aberto de

$$\mathrm{SL}_2^{\Delta}(\mathbb{Z}_p) \cong \langle x, y, h \mid [x,y] = h, [x,h] = x^{-2p}, [y,h] = y^{2p} \rangle,$$

se sua álgebra de Lie for $\mathfrak{sl}_2(\mathbb{Q}_p)$ ou a um subgrupo aberto de

$$\mathrm{SL}_1^1(\Delta_p) \cong \langle x, y, z \mid [x,y] = z^p, [x,z] = y^{p\eta}, [y,z] = x^{-1} \rangle,$$

se sua álgebra de Lie é isomorfa a $\mathfrak{sl}_1(\mathbb{D}_p)$ (veja o Exemplo 3.16).

Observamos que determinar quais grupos listados no Teorema 5.26 possuem $\mathfrak{sl}_2(\mathbb{Q}_p)$ como sua álgebra de Lie e quais possuem $\mathfrak{sl}_1(\mathbb{D}_p)$ não é simples. Grupos de uma mesma família, mas com parâmetros distintos, podem ter álgebras de Lie distintas. Em [NoSn19] os autores realizam essa classificação (vide 2.27, 2.28 e 2.31 do artigo citado).

5.6 Dimensão 4

Agora buscaremos uma classificação dos grupos analíticos p-ádicos pro-p livres-de-torção de dimensão 4. Para que possamos utilizar as mesmas técnicas utilizadas em dimensão 3, nos restringimos ao caso em que $p > 3$. Assim, sabemos que um $\mathbb{Z}_p$-reticulado de Lie de dimensão 4 residualmente nilpotente L é p-saturável. Se L é solúvel, então $L/[L,L]$ tem dimensão no máximo 3 e, portanto, tem um ideal de codimensão 1. Tomando a imagem inversa pela abelianização, obtemos um ideal I de codimensão 1 em L. Logo I é um $\mathbb{Z}_p$-reticulado solúvel de dimensão 3 e L é um produto semidireto $I \rtimes \mathbb{Z}_p$.

Já se L não é solúvel, então $\dim[L,L] = 3$. De fato, se $\mathcal{L} = L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ é a $\mathbb{Q}_p$-álgebra de Lie associada a L, então $\mathcal{L}$ tem dimensão 4 e não é solúvel. É um fato conhecido que não existem álgebras de Lie simples de dimensão 4 sobre um corpo de característica zero (veja, por exemplo, a discussão após o Teorema 9 do capítulo IV de [Jac79]). Assim, pelo Teorema da Decomposição de Levi, $\mathcal{L}$ é um produto semidireto $\mathbb{Q}_p \rtimes \mathfrak{h}$, em que $\mathfrak{h}$ é simples de dimensão 3. Como $\mathfrak{h}$ é simples, esse produto é direto. Isto é, $\mathcal{L} \cong \mathbb{Q}_p \times \mathfrak{h}$ e, portanto, $[\mathcal{L}, \mathcal{L}]$ tem dimensão 3. Logo $[L,L]$ tem dimensão 3. Segue-se que L é um produto semidireto $I \rtimes \mathbb{Z}_p$, em que I é um ideal de dimensão 3.

Nossa estratégia consiste em encontrar todos os possíveis produtos semidiretos entre os $\mathbb{Z}_p$-reticulados de dimensão 3 (classificados na seção anterior) e $\mathbb{Z}_p$, isto é, entender todos os homomorfismos de Álgebras de Lie $\phi : \mathbb{Z}_p \to \mathrm{Der}\, I$. Como $\mathbb{Z}_p$ é 1-gerado, basta determinar $\mathrm{Der}\, I$ para todo $\mathbb{Z}_p$-reticulado de Lie de dimensão 3.

Começaremos pelo caso solúvel. Dividiremos nossa classificação em casos relativos às famílias $G_0(s), G_1(s), G_2(s,r,d), G_3(s,r,d), G_4(s,r), G_5(s,r)$ e ao grupo $G_0(\infty)$. Denotaremos os $\mathbb{Z}_p$-reticulados

associados a esses grupos com os mesmos índices e parâmetros, trocando G por L. É claro que qualquer elemento de $\mathfrak{gl}_3(\mathbb{Z}_p)$ define uma derivação em $\mathbb{Z}_p^3$ e, portanto, $\operatorname{Der} L_0(\infty) = \mathfrak{gl}_3(\mathbb{Z}_p)$.

Lema (L.5.28) (Caso $L_0(s)$). Uma aplicação linear $\varphi : L_0(s) \to L_0(s)$ é uma derivação se, e somente se, na base $\{x, y, z\}$, φ tem matriz do tipo $\begin{pmatrix} a_1^1 & a_1^2 & 0 \\ a_2^1 & a_2^2 & 0 \\ a_3^1 & a_3^2 & a_1^1 + a_2^2 \end{pmatrix}$, em que $a_i^j \in \mathbb{Z}_p$, $i, j = 1, 2$.

Demonstração: Seja $(a_j^i)_{i,j=1}^3$ a matriz de φ na base $\{x, y, z\}$. φ é uma derivação se, e somente se os elementos a_j^i de $\mathbb{Z}_p$ são soluções do seguinte sistema de equações lineares:

$$\begin{gathered} 0 = \varphi([x,z]) = [x, \varphi(z)] + [\varphi(x), z] = [x, a_2^3 y] = p^s a_2^3 z; \\ 0 = \varphi([y,z]) = [y, \varphi(z)] + [\varphi(y), z] = [y, a_1^3 x] = -p^s a_1^3 z; \\ p^s \varphi(z) = p^s(a_1^3 x + a_2^3 y + a_3^3 z) = \varphi([x,y]) = [x, \varphi(y)] + [\varphi(x), y] = [x, a_2^2 y] + [a_1^1 x, y] = p^s(a_1^1 + a_2^2) z, \end{gathered}$$

cuja solução é a descrita no enunciado. ■

Note que em todos os outros casos, o ideal $\langle y_1, y_2 \rangle$ é característico (igual ao isolador de $C_L([L,L])$). Portanto, se φ é uma derivação de L, $\varphi(y_1), \varphi(y_2) \in \langle y_1, y_2 \rangle$.

Lema (L.5.29) (Caso $L_1(s)$). Uma aplicação linear $\varphi : L_1(s) \to L_1(s)$ é uma derivação se, e somente se, na base $\{x, y_1, y_2\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & 0 & 0 \\ a_1^1 & a_1^2 & a_1^3 \\ a_2^1 & a_2^2 & a_2^3 \end{pmatrix}$, em que $a_i^j \in \mathbb{Z}_p$, $i = 1, 2$, $j = 1, 2, 3$.

Demonstração: Seja $(c_j^i)_{i,j=1}^3$ a matriz de φ na base $\{x, y_1, y_2\}$. Sabe-se que $c_1^j = 0, j = 1, 2, 3$. φ é uma derivação se, e somente se, os elementos $c_j^i \in \mathbb{Z}_p$ são soluções do seguinte sistema de equações lineares:

$$\begin{gathered} c_1^2 = c_1^3 = 0; \\ p^s \varphi(y_1) = p^s(c_2^2 y_1 + c_3^2 y_2) = \varphi([y_1, x]) = [\varphi(y_1), x] + [y_1, \varphi(x)] = p^s((c_1^1 + c_2^2) y_1 + c_3^2 y_2); \\ p^s \varphi(y_2) = p^s(c_2^3 y_1 + c_3^3 y_2) = \varphi([y_2, x]) = [\varphi(y_2), x] + [y_2, \varphi(x)] = p^s(c_3^2 y_1 + (c_1^1 + c_3^3) y_2). \end{gathered}$$

Verifica-se imediatamente que quaisquer $c_i^j \in \mathbb{Z}_p$ $(i \neq 1)$ satisfazem o sistema acima quando $c_1^j = 0, j = 1, 2, 3$. ■

Lema (L.5.30) (Caso $L_2(s, r, d)$). Uma aplicação linear $\varphi : L_2(s, r, d) \to L_2(s, r, d)$ é uma derivação se, e somente se, na base $\{x, y_1, y_2\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & 0 & 0 \\ a_1 & b_1 & b_2 \\ a_2 & db_2 & b_1 \end{pmatrix}$, em que $a_i, b_j \in \mathbb{Z}_p$, $i, j = 1, 2$.

Demonstração: Seja $(c_i^j)_{i,j=1}^3$ a matriz de φ na base $\{x, y_1, y_2\}$. Então φ é uma derivação se, e somente se, os elementos $c_i^j \in \mathbb{Z}_p$ são soluções do seguinte sistema de equações lineares:

$$\begin{gathered} c_1^2 = c_1^3 = 0; \\ (c_2^2 + p^r d c_2^3) y_1 + (c_3^2 + p^r d c_3^3) y_2 = (c_1^1 + c_2^2 + p^r c_3^2) y_1 + (p^r d c_1^1 + p^r d c_2^2 + c_3^2) y_2; \end{gathered}$$

$$(p^r c_2^2 + c_2^3)y_1 + (p^r c_3^2 + c_3^3)y_2 = (c_2^3 + p^r c_3^3 + p^r c_1^1)y_1 + (p^r d c_2^3 + c_3^3 + c_1^1)y_2.$$

Após manipulações simples, obtemos que o sistema acima é equivalente a:

$$\begin{gathered} c_1^1 = c_1^2 = c_1^3 = 0; \\ c_2^2 = c_3^3; \\ c_3^2 = d c_2^3. \end{gathered}$$

■

Lema (L.5.31) (Caso $L_3(s,r,d)$). Uma aplicação linear $\varphi : L_3(s,r,d) \to L_3(s,r,d)$ é uma derivação se, e somente se, na base $\{x, y_1, y_2\}$, φ tem matriz do tipo $\begin{pmatrix} -\alpha p^r & 0 & 0 \\ a_1 & \alpha & \alpha + \dfrac{p^{2r}\alpha}{d} \\ a_2 & d\alpha & \alpha + 2p^r\alpha + \dfrac{p^{3r}\alpha}{d} \end{pmatrix}$, em que $a_1, a_2 \in \mathbb{Z}_p$ e $\alpha \in p^u\mathbb{Z}_p$, sendo $u = \max\{0, v_p(d) - 2r\}$.

Demonstração: Seja $(c_i^j)_{i,j=1}^3$ a matriz de φ na base $\{x, y_1, y_2\}$. Então φ é uma derivação se, e somente se, os elementos $c_i^j \in \mathbb{Z}_p$ são soluções do seguinte sistema de equações lineares:

$$\begin{gathered} c_1^2 = c_1^3 = 0; \\ d c_2^2 y_1 + c_3^2 y_2 = c_3^2 y_1 + (d c_2^2 + p^r c_3^2 + d c_1^1)y_2; \\ (c_2^2 + p^r c_2^3)y_1 + (c_3^2 + p^r c_3^3)y_2 = (c_1^1 + c_3^3)y_1 + (d c_2^3 + p^r c_3^3 + p^r c_1^1)y_2. \end{gathered}$$

Após manipulações simples, obtemos que o sistema acima é equivalente a:

$$\begin{gathered} c_1^2 = c_1^3 = 0; \\ c_3^2 = d c_2^2; \\ p^r c_3^2 = -d c_1^1; \\ c_2^2 + p^r c_2^3 = c_1^1 + c_3^3; \\ c_3^2 = d c_2^3 + p^r c_1^1. \end{gathered}$$

Tomemos $c_2^2 = \alpha$. Então $c_3^2 = d\alpha$ e $c_1^1 = -\alpha p^r$. Daí $d c_2^3 = (d + p^{2r})\alpha$ e, portanto, d divide $(d + p^{2r})\alpha$ (e, portanto, divide $p^{2r}\alpha$) e $c_2^3 = \alpha + \dfrac{p^{2r}\alpha}{d}$. Por fim, $c_3^3 = \alpha + 2p^r\alpha + \dfrac{p^{3r}\alpha}{d}$.

Note que os termos c_2^1 e c_3^1 são livres e, por fim, perceba que d divide $p^{2r}\alpha$ se, e somente se, a valoração p-ádica de d é menor ou igual a $2r + v_p(\alpha)$. ■

Lema (L.5.32) (Caso $L_4(s,r)$). Uma aplicação linear $\varphi : L_4(s,r) \to L_4(s,r)$ é uma derivação se, e somente se, na base $\{x, y_1, y_2\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & 0 & 0 \\ a_1 & b_1 & b_2 \\ a_2 & p^r b_2 & b_1 \end{pmatrix}$, em que $a_i, b_j \in \mathbb{Z}_p$, $i, j = 1, 2$.

Demonstração: Poupemos algumas palavras. Precisamos resolver o seguinte sistema:

$$c_1^2 = c_1^3 = 0;$$

$$p^r c_2^3 y_1 + p^r c_3^3 y_2 = c_3^2 y_1 + p^r (c_1^1 + c_2^2) y_2;$$
$$c_2^2 y_1 + c_3^2 y_2 = (c_1^1 + c_3^3) y_1 + p^r c_2^3 y_2.$$

Parametrizamos as soluções por $c_2^2 = b_1, c_2^3 = b_2, c_2^1 = a_1, c_3^1 = a_2$. ■

Lema (L.5.33) (Caso $L_5(s,r)$). Uma aplicação linear $\varphi : L_5(s,r) \to L_5(s,r)$ é uma derivação se, e somente se, na base $\{x, y_1, y_2\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & 0 & 0 \\ a_1 & b_1 & b_2 \\ a_2 & p^r \eta b_2 & b_1 \end{pmatrix}$, em que $a_i, b_j \in \mathbb{Z}_p$, $i, j = 1, 2$.

Demonstração: O sistema da vez é:

$$c_1^2 = c_1^3 = 0;$$
$$p^r \eta c_2^3 y_1 + p^r \eta c_3^3 y_2 = c_3^2 y_1 + p^r \eta (c_1^1 + c_2^2) y_2;$$
$$c_2^2 y_1 + c_3^2 y_2 = (c_1^1 + c_3^3) y_1 + p^r \eta c_2^3 y_2.$$

Parametrizamos as soluções por $c_2^2 = b_1, c_2^3 = b_2, c_2^1 = a_1, c_3^1 = a_2$. ■

Assim, munidos dos resultados apresentados nos lemas acima, podemos construir apresentações para os $\mathbb{Z}_p$-reticulados de Lie solúveis residualmente nilpotentes de dimensão 4. Note que um produto semidreto $I \rtimes_\varphi \mathbb{Z}_p$ é residualmente nilpotente se, e somente se, a representação matricial de φ é residualmente nilpotente — o que ocorre exatamente quando $\varphi^3 \equiv 0 \pmod{p}$.

Proposição (P.5.34). A lista abaixo contém todos os $\mathbb{Z}_p$-reticulados solúveis de dimensão 4.

(1) A família $L_0(\infty, \varphi) = \langle x_1, x_2, x_3, z \mid [x_m, x_n] = 0, [x_k, z] = \varphi(x_k), m, n, k = 1, 2, 3 \rangle$, parametrizada por endomorfismos $\varphi \in \mathfrak{gl}_3(\mathbb{Z}_p)$;

(2) A família $L_0(s, a_i^j) = \langle x, y, z, w \mid [x, y] = p^s z, [x, z] = [y, z] = 0, [x, w] = a_1^1 x + a_2^1 y + a_3^1 z, [y, w] = a_1^2 x + a_2^2 y + a_3^2 z, [z, w] = (a_1^1 + a_2^2) z \rangle$, em que $a_i^j \in \mathbb{Z}_p$, $i = 1, 2, 3$, $j = 1, 2$, $s \in \mathbb{N}$;

(3) A família $L_1(s, a_i^j) = \langle x, y_1, y_2, w \mid [y_1, y_2] = 0, [y_1, x] = p^s y_1, [y_2, x] = p^s y_2, [x, w] = a_1^1 y_1 + a_2^1 y_2, [y_1, w] = a_1^2 y_1 + a_2^2 y_2, [y_2, w] = a_1^3 y_1 + a_2^3 y_2 \rangle$, em que $a_i^j \in \mathbb{Z}_p$, $i = 1, 2$, $j = 1, 2, 3$, $s \in \mathbb{N}$;

(4) A família $L_2(s, r, d, a_1, a_2, b_1, b_2) = \langle x, y_1, y_2, w \mid [y_1, y_2] = 0, [y_1, x] = p^s y_1 + p^{s+r} d y_2, [y_2, x] = p^{s+r} y_1 + p^s y_2, [x, w] = a_1 y_1 + a_2 y_2, [y_1, w] = b_1 y_1 + d b_2 y_2, [y_2, w] = b_2 y_1 + b_1 y_2 \rangle$, em que $a_1, a_2, b_1, b_2 \in \mathbb{Z}_p$, $s, r \in \mathbb{N}$, $d \in \mathbb{Z}_p$;

(5) A família $L_3(s, r, d, a_1, a_2, \alpha) = \langle x, y_1, y_2, w \mid [y_1, y_2] = 0, [y_1, x] = d p^s y_2, [y_2, x] = p^s y_1 + p^{s+r} y_2, [x, w] = -\alpha p^r x + a_1 y_1 + a_2 y_2, [y_1, w] = \alpha y_1 + d\alpha y_2, [y_2, w] = \left(\alpha + \frac{p^{2r}\alpha}{d}\right) y_1 + \left(\alpha(1 + p^r) + p^r \left(\alpha + \frac{p^{2r}\alpha}{d}\right)\right) y_2 \rangle$, em que $a_1, a_2 \in \mathbb{Z}_p$ e $\alpha \in p^u \mathbb{Z}_p$, sendo $u = \max\{0, v_p(d) - 2r\}$, $s, r \in \mathbb{N}$, $d \in \mathbb{Z}_p$;

(6) A família $L_4(s, r, a_1, a_2, b_1, b_2) = \langle x, y_1, y_2, w \mid [y_1, y_2] = 0, [y_1, x] = p^{s+r} y_2, [y_2, x] = p^s y_1, [x, w] = a_1 y_1 + a_2 y_2, [y_1, w] = b_1 y_1 + p^r b_2 y_2, [y_2, w] = b_2 y_1 + b_1 y_2 \rangle$, em que $a_1, a_2, b_1, b_2 \in \mathbb{Z}_p$, $s, r \in \mathbb{N}$;

(7) A família $L_5(s, r, a_1, a_2, b_1, b_2) = \langle x, y_1, y_2, w \mid [y_1, y_2] = 0, [y_1, x] = p^{s+r} \eta y_2, [y_2, x] = p^s y_1, [x, w] = a_1 y_1 + a_2 y_2, [y_1, w] = b_1 y_1 + p^r \eta b_2 y_2, [y_2, w] = b_2 y_1 + b_1 y_2 \rangle$, em que $a_1, a_2, b_1, b_2 \in \mathbb{Z}_p$, $s, r \in \mathbb{N}$.

A lista apresentada acima contém redundâncias. Por exemplo, sejam $s \in \mathbb{N}$ e $L_0(\infty, \varphi)$ um $\mathbb{Z}_p$-reticulado tal que $\varphi(x_3) = 0$, $\varphi(x_2) = 0$ e $\varphi(x_1) = p^s x_2$. Então é fácil verificar, comparando as apresentações, que $L_0(\infty, \varphi)$ é isomorfo a $L_0(s, a_i^j)$, em que $a_i^j = 0$ para todo i e todo j. Eliminar as redundâncias na família (1), por exemplo, exigiria classificar as classes de conjugação em $\mathfrak{gl}_3(\mathbb{Z}_p)$. Até o momento da confecção deste trabalho, não encontramos resultados conclusivos nesse sentido. Observamos também que ocorrem redundâncias entre as famílias. De fato, qualquer $\mathbb{Z}_p$-reticulado de Lie de dimensão 3 que seja da forma $L \oplus \mathbb{Z}_p$ ocorre na família (1) e em ao menos uma das outras famílias (a que contém os produtos semidiretos de L por $\mathbb{Z}_p$).

Seguimos agora para o caso não-solúvel.

Lema (L.5.35) (Caso $L_1(s_0, s_1, s_2, \varepsilon_1, \varepsilon_2)$). Uma aplicação linear $\varphi : L := L_1(s_0, s_1, s_2, \varepsilon_1, \varepsilon_2) \to L$ é uma derivação se, e somente se, na base $\{x, y, z\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & \alpha & \beta \\ -\eta_1^{\varepsilon_1} p^{s_1 - s_0}\alpha & 0 & \gamma \\ -\eta^{\varepsilon_2} p^{s_2 - s_0}\beta & -\eta^{\varepsilon_2 - \varepsilon_1} p^{s_2 - s_1}\gamma & 0 \end{pmatrix}$, em que $\alpha, \beta, \gamma \in \mathbb{Z}_p$.

Demonstração: Seja $(a_i^j)_{i,j=1}^3$ a matriz de φ na base $\{x, y, z\}$. Então φ é uma derivação se, e somente se, os coeficientes a_i^j são solução do sistema linear abaixo:

$$\begin{aligned}
a_1^1 x + a_2^1 y + a_3^1 z &= (a_2^2 + a_3^3)x - \eta^{\varepsilon_1} p^{s_1 - s_0} a_1^2 y - \eta^{\varepsilon_2} p^{s_2 - s_0} a_1^3 z; \\
\eta^{\varepsilon_1} p^{s_1 - s_0} a_1^2 x + \eta^{\varepsilon_1} p^{s_1 - s_0} a_2^2 y + \eta^{\varepsilon_1} p^{s_1 - s_0} a_3^2 z &= -a_2^1 x + \eta^{\varepsilon_1} p^{s_1 - s_0}(a_1^1 + a_3^3) y - \eta^{\varepsilon_2} p^{s_2 - s_0} a_2^3 z; \\
\eta^{\varepsilon_2} p^{s_2 - s_0} a_1^3 x + \eta^{\varepsilon_2} p^{s_2 - s_0} a_2^3 y + \eta^{\varepsilon_2} p^{s_2 - s_0} a_3^3 z &= -a_3^1 x - \eta^{\varepsilon_1} p^{s_1 - s_0} a_3^2 y + \eta^{\varepsilon_2} p^{s_2 - s_0}(a_1^1 + a_2^2) z.
\end{aligned}$$

Parametrizando as soluções por $a_1^2 = \alpha, a_1^3 = \beta$ e $a_2^3 = \gamma$, obtemos o resultado desejado. Note que $a_i^i = 0$, $i = 1, 2, 3$. ■

Lema (L.5.36) (Caso $L_2(s_0, s_1, \varepsilon_0)$). Uma aplicação linear $\varphi : L := L_2(s_0, s_1, \varepsilon_0) \to L$ é uma derivação se, e somente se, na base $\{x, y, z\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & \alpha & \beta \\ -\eta^{\varepsilon_0}\alpha & 0 & \gamma \\ -p^{s_1 - s_0}\beta & -\eta^{-\varepsilon_0} p^{s_1 - s_0}\gamma & 0 \end{pmatrix}$, em que $\alpha, \beta, \gamma \in \mathbb{Z}_p$.

Demonstração: Fazendo a construção análoga ao caso anterior, precisamos resolver o seguinte sistema:

$$\begin{aligned}
a_1^1 x + a_2^1 y + a_3^1 z &= (a_2^2 + a_3^3)x - \eta^{\varepsilon_0} a_1^2 y - p^{s_1 - s_0} a_1^3 z; \\
a_1^2 x + a_2^2 y + a_3^2 z &= -\eta^{-\varepsilon_0} a_2^1 x + (a_1^1 + a_3^3) y - \eta^{-\varepsilon_0} p^{s_1 - s_0} a_2^3 z; \\
p^{s_1 - s_0} a_1^3 x + p^{s_1 - s_0} a_2^3 y + p^{s_1 - s_0} a_3^3 z &= -a_3^1 x - \eta^{\varepsilon_0} a_3^2 y + p^{s_1 - s_0}(a_1^1 + a_2^2) z.
\end{aligned}$$

Parametrizando as soluções por $a_1^2 = \alpha, a_1^3 = \beta$ e $a_2^3 = \gamma$, obtemos o resultado desejado. Note que $a_i^i = 0$, $i = 1, 2, 3$.x ■

Lema (L.5.37) (Caso $L_3(s_0, s_1, \varepsilon_1)$). Uma aplicação linear $\varphi : L := L_3(s_0, s_1, \varepsilon_1) \to L$ é uma derivação se, e somente se, na base $\{x, y, z\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & \alpha & \beta \\ -p^{s_1 - s_0}\alpha & 0 & \gamma \\ -\eta^{\varepsilon_1} p^{s_1 - s_0}\beta & -\eta^{-\varepsilon_1}\gamma & 0 \end{pmatrix}$, em que $\alpha, \beta, \gamma \in \mathbb{Z}_p$.

Demonstração: Fazendo a construção análoga ao caso anterior, precisamos resolver o seguinte sistema:

$$a_1^1x + a_2^1y + a_3^1z = (a_2^2 + a_3^3)x - p^{s_1-s_0}a_1^2y - \eta^{\varepsilon_1}p^{s_1-s_0}a_1^3z;$$
$$p^{s_1}a_1^2x + p^{s_1}a_2^2y + p^{s_1}a_3^2z = -p^{s_0}a_2^1x + p^{s_1}(a_1^1 + a_3^3)y - \eta^{\varepsilon_1}p^{s_1}a_2^3z;$$
$$\eta^{\varepsilon_1}p^{s_1}a_1^3x + \eta^{\varepsilon_1}p^{s_1}a_2^3y + \eta^{\varepsilon_1}p^{s_1}a_3^3z = -p^{s_0}a_3^1x - p^{s_1}a_3^2y + \eta^{\varepsilon_1}p^{s_1}(a_1^1 + a_2^2)z.$$

Parametrizando as soluções por $a_1^2 = \alpha, a_1^3 = \beta$ e $a_2^3 = \gamma$, obtemos o resultado desejado. Note que $a_i^i = 0$, $i = 1, 2, 3$.x ■

Lema (L.5.38) (Caso $L_4(s_0)$). Uma aplicação linear $\varphi : L := L_4(s_0) \to L$ é uma derivação se, e somente se, na base $\{x, y, z\}$, φ tem matriz do tipo $\begin{pmatrix} 0 & \alpha & \beta \\ -\alpha & 0 & \gamma \\ -\beta & -\gamma & 0 \end{pmatrix}$, em que $\alpha, \beta, \gamma \in \mathbb{Z}_p$.

Demonstração: Fazendo a construção análoga ao caso anterior, precisamos resolver o seguinte sistema:

$$a_1^1x + a_2^1y + a_3^1z = (a_2^2 + a_3^3)x - a_1^2y - a_1^3z;$$
$$a_1^2x + a_2^2y + a_3^2z = -a_2^1x + (a_1^1 + a_3^3)y - a_2^3z;$$
$$a_1^3x + a_2^3y + a_3^3z = -a_3^1x - a_3^2y + (a_1^1 + a_2^2)z.$$

Parametrizando as soluções por $a_1^2 = \alpha, a_1^3 = \beta$ e $a_2^3 = \gamma$, obtemos o resultado desejado. Note que $a_i^i = 0$, $i = 1, 2, 3$.x ■

Como feito em dimensão 3, para associarmos grupos aos reticulados da proposição acima, precisamos exigir que sejam residualmente nilpotentes. Defina, para cada família nas listas obtidas acima, $\varphi : \langle x, y_1, y_2\rangle \to \langle x, y_1, y_2\rangle$ por $\varphi(v) = [v, w]$ (para os reticulados do tipo L_0, trocamos $\{x, y_1, y_2\}$ por $\{x, y, z\}$ ou $\{x_1, x_2, x_3\}$). Então o $\mathbb{Z}_p$-reticulado de Lie é residualmente nilpotente se, e somente se, $\varphi^3 \equiv 0 \mod p$.

Teorema (T.5.39). *Seja $p > 3$. Os grupos dados pelas apresentações abaixo constituem uma lista completa dos grupos analíticos p-ádicos pro-p livres-de-torção de dimensão 4.*

(1) A família de grupos parametrizados por $a_i^j \in \mathbb{Z}_p, i, j = 1, 2, 3$, gerados por x, y, z, w sujeitos às relações:

$$[x, y] = 1, [y, z] = 1, [z, x] = 1,$$
$$[x, w] = x^{a_1^1}y^{a_2^1}z^{a_3^1}, [y, w] = x^{a_1^2}y^{a_2^2}z^{a_3^2}, [z, w] = x^{a_1^3}y^{a_2^3}z^{a_3^3}.$$

(2) A família de grupos parametrizados por $s \in \mathbb{N}$, $a_i^j \in \mathbb{Z}_p, i = 1, 2, 3, j = 1, 2$, gerados por x, y, z, w sujeitos às relações:

$$[x, y] = z^{p^s}, [x, z] = 1, [y, z] = 1,$$
$$[x, w] = x^{a_1^1}y^{a_2^1}z^{a_3^1}, [y, w] = x^{a_1^2}y^{a_2^2}z^{a_3^2}, [z, w] = z^{a_1^1+a_2^2}.$$

(3) A família de grupos parametrizados por $0 < s \in \mathbb{N}$, $a_i^j \in \mathbb{Z}_p$, $i = 1, 2, j = 1, 2, 3$, gerados por x, y, z, w sujeitos às relações:

$$[x, y] = 1, [x, z] = x^{p^s}, [y, z] = y^{p^s},$$

$$[z,w]=x^{a_1^1}y^{a_2^1},[x,w]=x^{a_1^2}y^{a_2^2},[y,w]=x^{a_1^3}y^{a_2^3}.$$

(4) A família de grupos parametrizados por $s,r\in\mathbb{N},s>0$, $d\in\mathbb{Z}_p$, $a_1,a_2,b_1,b_2\in\mathbb{Z}_p$, *gerados por* x,y,z,w *sujeitos às relações:*

$$[x,y]=1,[x,z]=x^{p^s}y^{p^{s+r}d},[y,z]=x^{p^{s+r}}y^{p^s},$$

$$[z,w]=x^{a_1}y^{a_2},[x,w]=x^{b_1}y^{db_2},[y,w]=x^{b_2}y^{b_1}.$$

(5) A família de grupos parametrizados por $s,r\in\mathbb{N},s+r\geq 1,d\in p\mathbb{Z}_p,a_1,a_2\in\mathbb{Z}_p$, $\alpha\in p^u\mathbb{Z}_p$ *(*$u=\max\{0,v_p(d)-2r\}$*), gerados por* x,y,z,w *sujeitos às relações:*

$$[x,y]=1,[x,z]=y^{dp^s},[y,z]=x^{p^s}y^{p^{s+r}},$$

$$[z,w]=z^{-\alpha p^r}x^{a_1}y^{a_2},[x,w]=x^{\alpha}y^{d\alpha},[y,w]=x^{\alpha+\frac{p^{2r}\alpha}{d}}y^{\frac{p^{3r}\alpha}{d}+2p^r\alpha+\alpha}.$$

(6) A família de grupos parametrizados por $s,r\in\mathbb{N},s+r\geq 1,a_1,a_2,b_1,b_2\in\mathbb{Z}_p$, *gerados por* x,y,z,w *sujeitos às relações:*

$$[x,y]=1,[x,z]=y^{p^{s+r}},[y,z]=x^{p^s},$$

$$[z,w]=x^{a_1}y^{a_2},[x,w]=x^{b_1}y^{p^rb_2},[y,w]=x^{b_2}y^{b_1}.$$

(7) A família de grupos parametrizados por $s,r\in\mathbb{N},s+r\geq 1,a_1,a_2,b_1,b_2\in\mathbb{Z}_p$, *gerados por* x,y,z,w *sujeitos às relações:*

$$[x,y]=1,[x,z]=y^{p^{s+r}\eta},[y,z]=x^{p^s},$$

$$[z,w]=x^{a_1}y^{a_2},[x,w]=x^{b_1}y^{p^r\eta b_2},[y,w]=x^{b_2}y^{b_1}.$$

(8) A família de grupos parametrizados por $s_0<s_1<s_2\in\mathbb{N}$, $\varepsilon_1,\varepsilon_2\in\{0,1\}$, $\alpha,\beta,\gamma\in\mathbb{Z}_p$, *gerados por* x,y,z,w *sujeitos às relações:*

$$[y,z]=x^{p^{s_0}},[z,x]=y^{\eta^{\varepsilon_1}p^{s_1}},[x,y]=z^{\eta^{\varepsilon_2}p^{s_2}},$$

$$[x,w]=y^{-\eta^{\varepsilon_1}p^{s_1-s_0}\alpha}z^{-\eta^{\varepsilon_2}p^{s_2-s_0}\beta},[y,w]=x^{\alpha}z^{-\eta^{\varepsilon_2-\varepsilon_1}p^{s_2-s_1}\gamma},[z,w]=x^{\beta}y^{\gamma}.$$

(9) A família de grupos parametrizados por $0<s_0<s_2\in\mathbb{N}$, $\varepsilon_0\in\{0,1\}$, $\alpha,\beta,\gamma\in\mathbb{Z}_p$, *gerados por* x,y,z,w *sujeitos às relações:*

$$[y,z]=x^{p^{s_0}},[z,x]=y^{-\eta^{\varepsilon_0}p^{s_0}},[x,y]=z^{p^{s_2}},$$

$$[x,w]=y^{\eta_1^{\varepsilon}\alpha}z^{-p^{s_2-s_0}\beta},[y,w]=x^{\alpha}z^{\eta^{-\varepsilon_1}p^{s_2-s_0}\gamma},[z,w]=x^{\beta}y^{\gamma}.$$

(10) A família de grupos parametrizados por $s_0<s_1\in\mathbb{N}$, $\varepsilon_1\in\{0,1\}$, $\alpha,\beta,\gamma\in\mathbb{Z}_p$, *gerados por* x,y,z,w *sujeitos às relações:*

$$[y,z]=x^{p^{s_0}},[z,x]=y^{p^{s_1}},[x,y]=z^{-\eta^{\varepsilon_2}p^{s_1}},$$

$$[x,w]=y^{-p^{s_1-s_0}\alpha}z^{\eta^{\varepsilon_2}p^{s_1-s_0}\beta},[y,w]=x^{\alpha}z^{\eta^{\varepsilon_2}\gamma},[z,w]=x^{\beta}y^{\gamma}.$$

(11) A família de grupos parametrizados por $0 < s_0 \in \mathbb{N}$, $\alpha, \beta, \gamma \in \mathbb{Z}_p$, gerados por x, y, z, w sujeitos às relações:

$$[y,z] = x^{p^{s_0}}, [z,x] = y^{p^{s_0}}, [x,y] = z^{p^{s_0}},$$

$$[xw] = y^{-\alpha}z^{-\beta}, [y,w] = x^{\alpha}z^{-\gamma}, [z,w] = x^{\beta}y^{\gamma}.$$

Em que, utilizando a notação descrita acima, em todo caso, $\varphi^3 \equiv 0 \mod p$.

5.7 Propriedade CA

Dizemos que um grupo G possui a **propriedade CA** se o centralizador de cada elemento não trivial é abeliano. Essa propriedade é equivalente à comutatividade ser uma relação transitiva em $G - \{1\}$ e, por isso, é às vezes referida como propriedade CT. Para uma contextualização, veja [MWZ].

Grupos finitos com a propriedade CA foram classificados no século XX. De fato:

Teorema (T.5.40) ([Suz86], Exemplos da seção 6.2.1). *Um grupo finito G possui a propriedade CA se, e somente se,*

(i) é abeliano ou;

(ii) é de Frobrenius com núcleo abeliano e complemento cíclico ou;

(iii) é um grupo do tipo $\mathrm{PSL}(2, 2^m)$.

Uma pergunta natural no contexto de grupos profinitos (pro-p) é a de quais grupos profinitos (pro-p) possuem a propriedade CA. O primeiro trabalho nesse sentido é [SZZ19].

Exemplo (E.5.41). Seja π um conjunto de primos e considere o grupo diedral $D_\pi := \mathbb{Z}_\pi \rtimes C_2$, em que $\mathbb{Z}_\pi = \prod_{p \in \pi} \mathbb{Z}_p$. Então é claro que D_π possui a propriedade CA. Note que D_π é virtualmente abeliano e que quando $2 \notin \pi$, D_π é um grupo profinito de Frobenius (vide [RiZa10] 4.6).

Exemplo (E.5.42). Se G é um grupo profinito de Frobenius com núcleo abeliano e complemento cíclico, então G tem a propriedade CA. De fato, escrevendo $G = K \rtimes \langle h \rangle$, se $k \in K - \{1\}$, como $\langle h \rangle \cap \langle h^k \rangle = 1$, k e h não comutam e, portanto, $C_G(k) = C_K(k) = K$ e $C_G(h) = \langle h \rangle$. Reciprocamente, se G é um grupo profinito de Frobenius com a propriedade CA, K deve ser abeliano (já que é nilpotente — vide [RiZa10] 4.6.10 — e, portanto, possui centro). Além disso, H deve ser cíclico. De fato, para todo subgrupo normal aberto U de K, $K/U \rtimes H$ é um grupo de Frobenius com a propriedade CA (vide [RiZa10] 4.6.7) e, portanto, pelo Teorema 5.40, H é cíclico. Em particular, um grupo de Frobenius profinito com a propriedade CA tem torção.

O principal resultado de [SZZ19] mostra que os grupos pro-p livres-de-torção têm grande relevância no estudo da propriedade CA em grupos profinitos:

Teorema (T.5.43) ([SZZ19] Teoremas A e 3.1). *Seja G um grupo profinito com a propriedade CA. Então G é virtualmente abeliano ou virtualmente pro-p, para algum primo p. Além disso, se G é livre-de-torção, então é abeliano ou pro-p.*

Estamos interessados em estudar a propriedade CA em grupos analíticos p-ádicos. O seguinte lema será bastante útil para construção de exemplos:

Lema (L.5.44) ([FGRS16], 3.9). Se k é um corpo de característica zero, $\mathrm{PSL}_2(k)$ possui a propriedade CA se, e somente se, -1 não é a soma de dois quadrados.

E agora:

Lema (L.5.45) ([SZZ19], 5.3). Em $\mathbb{Q}_p$, para que -1 seja a soma de dois quadrados, é necessário e suficiente que $p > 2$.

Exemplo (E.5.46). Seja k uma extensão finita de $\mathbb{Q}_2$ em que -1 não é a soma de 2 quadrados. Então, pelo Lema 5.44, $\mathrm{PSL}_2(k)$ é um grupo analítico 2-ádico com a propriedade CA. Se $\mathcal{O}_k$ é o anel de valoração de k, $\mathrm{PSL}_2(\mathcal{O}_k)$ é um grupo analítico 2-ádico compacto (profinito) com a propriedade CA. Seu subgrupo analítico pro-2 maximal é um exemplo de grupo pro-p com a propriedade CA.

O **centralizador** de um elemento x de uma álgebra de Lie L é o conjunto dos elementos y de L tais que $[x, y] = 0$. Dizemos então que uma álgebra de Lie tem a **propriedade CA** se os centralizadores dos elementos não nulos são abelianos.

Proposição (P.5.47). Seja G um grupo p-saturável. Então G possui a propriedade CA se, e somente se, o $\mathbb{Z}_p$-reticulado de Lie associado a G também possui.

Demonstração: Retornemos brevemente à Seção 4.4. Se G é um grupo p-saturável, o colchete de Lie definido em seu $\mathbb{Z}_p$-reticulado de Lie associado tem a expressão:

$$[g, h]_{\mathrm{Lie}} = \lim_{n\to\infty} [g^{p^n}, h^{p^n}]^{p^{-2n}},$$

enquanto o comutador no grupo G é dado, em termos de sua estrutura como $\mathbb{Z}_p$-reticulado de Lie, pela fórmula de Hausdorff (vide Seção 1.5):

$$[g, h] = g + h + \frac{1}{2}[g, h]_{\mathrm{Lie}} + \frac{1}{12}\left([g, [g, h]]_{\mathrm{Lie}} + [h, [h, g]]_{\mathrm{Lie}}\right) + \dots$$

Consequentemente, elementos que comutam em G (com a estrutura de grupo), comutam em G com a estrutura de $\mathbb{Z}_p$-reticulado de Lie. Segue-se que se x é um elemento de G, os centralizadores de x em G como grupo e como $\mathbb{Z}_p$-reticulado de Lie coincidem. A expressão acima implica também que um é abeliano se, e somente se, o outro também o é. ■

Determinamos agora quais grupos analíticos pro-p livres-de-torção de dimensão 2 possuem a propriedade CA. Começamos por:

Proposição (P.5.48). Todo grupo analítico pro-p livre-de-torção de dimensão 2 possui a propriedade CA.

Demonstração: Pela Proposição anterior, é suficiente observar que os $\mathbb{Z}_p$-reticulados de Lie associados aos grupos não abelianos das Proposições 5.12 e 5.14 têm centralizadores de elementos não triviais de dimensão um. Considere, por exemplo, o $\mathbb{Z}_p$-reticulado de Lie

$$L(s) := \langle x, y \mid [x, y] = p^s y\rangle = L(G(s)), s \in \mathbb{N}.$$

Sejam $u = ax + by$ e $v = cx + dy$ elementos quaisquer de $L(s)$ tais que $[u, v] = 0$. Então

$$[u, v] = ad[x, y] + bc[y, x] = p^s(ad - bc)y = 0.$$

Ou seja, $ad - bc = 0$ e, portanto, u e v são linearmente dependentes, isto é, $u = \lambda v$ para algum $\lambda \in \mathbb{Z}_p$. ■

Seguimos agora para dimensão 3:

Proposição (P.5.49). Se p é um primo maior do que 3 e G é um grupo analítico pro-p não-solúvel livre-de-torção de dimensão 3, então G possui a propriedade CA.

Demonstração: Pela Proposição 5.27, basta mostrar que os grupos $\mathrm{SL}_2^{\Delta}(\mathbb{Z}_p)$ e $\mathrm{SL}_1^1(\Delta_p)$ possuem a propriedade CA. Como $\mathfrak{sl}_1(\mathbb{D}_p)$ não possui subálgebras de dimensão 2 (Exemplo 3.16), os desejados centralizadores de $\mathrm{SL}_1^1(\Delta_p)$ são todos unidimensionais e, portanto, abelianos. Para o caso de $\mathfrak{sl}_2(\mathbb{Z}_p)$, é conveniente observar o $\mathbb{Z}_p$-reticulado de Lie associado

$$\mathfrak{sl}_2^{\Delta}(\mathbb{Z}_p) := \langle x, y, h \mid [x, y] = h, [x, h] = -2px, [y, h] = 2py \rangle,$$

que está canonicamente incluído em $\mathfrak{sl}_2(\mathbb{Q}_p) = \langle x, y, h \mid [x, y] = h, [x, h] = -2x, [y, h] = 2y \rangle$. Uma computação simples mostra que os desejados centralizadores de $\mathfrak{sl}_2(\mathbb{Q}_p)$ são unidimensionais. ■

Proposição (P.5.50). Seja p um primo maior do que 3 e G é um grupo analítico pro-p livre-de-torção de dimensão 3, então G possui a propriedade CA se, e somente se, ele não é isomorfo a um dos seguintes grupos do Teorema 5.18:

$$G_0(s), \text{ para algum } s \geq 0, \text{ ou a}$$

$$G_3(s, r, 0), \text{ para } s \text{ e } r \geq 0 \text{ com } s + r \geq 1.$$

Demonstração: Resta-nos mostrar que os grupos citados acima são os únicos solúveis que não possuem a propriedade CA. Isso pode ser feito diretamente, computando os centralizadores de elementos em cada $\mathbb{Z}_p$-reticulado de Lie associado a um grupo da lista presente no Teorema 5.18. Podemos também observar que todos os grupos da lista são produtos semidiretos do tipo $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$ e que, portanto, possuem a propriedade CA se, e somente se, a ação é livre de pontos fixos, restando-nos determinar quais grupos do tipo $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$ têm ação livre de pontos fixos. Ocorre que os grupos $G_0(s)$ e $G_3(s, r, 0)$ são os únicos cuja ação têm pontos fixos. ■

Um produto semidireto de álgebras de Lie $\mathfrak{g} \rtimes \mathfrak{h}$ tem **ação livre de pontos fixos** se para quaisquer x em $\mathfrak{g}$ e $y \in \mathfrak{h}$, $[x, y] = 0$ implica $x = 0$ ou $y = 0$. Note que se $G_1 \rtimes G_2$ é um produto semidireto p-saturável de grupos p-saturáveis com ação livre de pontos fixos, então o produto semidireto $L(G_1) \rtimes L(G_2)$ dos $\mathbb{Z}_p$-reticulados de Lie associados a G_1 e G_2 tem ação livre de pontos fixos, o que justifica a nomenclatura. Ocorre que:

Teorema (T.5.51) ([MWZ], 1.2). *Uma álgebra de Lie solúvel sobre $\mathbb{Q}_p$ tem a propriedade CA se, e somente se, é um produto semidireto $\mathfrak{g} \rtimes \mathfrak{h}$ entre álgebras de Lie abelianas com ação livre de pontos fixos e $\dim \mathfrak{h} \leq \dim \mathfrak{g}$.*

Proposição (P.5.52). Um $\mathbb{Z}_p$-reticulado de Lie L tem a propriedade CA se, e somente se, $\mathbb{Q}_p \otimes L$ também a tem.

Demonstração: De fato, se L tem a propriedade CA e x é um elemento não nulo de $\mathbb{Q}_p \otimes L$, então sendo y e z elementos de $C_{\mathbb{Q}_p \otimes L}(x)$, podemos escrever $x = p^t x'$, $y = p^s y'$ e $z = p^r z'$, com y' e z' em L, para inteiros apropriados t, s e r. Notamos que y' e z' centralizam x' e, tendo L a propriedade CA, $[y', z'] = 0$. Segue-se que $[y, z] = p^{s+r}[y', z'] = 0$. Logo $C_{\mathbb{Q}_p \otimes L}(x)$ é abeliano.

Por outro lado, se todo elemento não nulo de $\mathbb{Q}_p \otimes L$ possui centralizador abeliano, considerando a inclusão canônica de L em $\mathbb{Q}_p \otimes L$, vemos que, para todo x em L, vale que $C_L(x) \subseteq C_{\mathbb{Q}_p \otimes L}(x)$. Concluímos, assim, que L possui a propriedade CA. ■

Consequentemente, obtemos a seguinte tradução do Teorema acima para o contexto de grupos, utilizando o Teorema 5.11:

Teorema (T.5.53). *Seja p um primo e G um grupo analítico pro-p livre-de-torção solúvel de dimensão menor do que p. Então G tem a propriedade CA se, e somente se, ele é isomorfo a um grupo do tipo $\mathbb{Z}_p^m \rtimes \mathbb{Z}_p^n$ com ação livre de pontos fixos.*

Finalizamos observando o que ocorre em dimensão quatro:

Proposição (P.5.54). Seja $p > 3$ e G um grupo analítico pro-p livre-de-torção de dimensão quatro. Se G tem a propriedade CA, então G é solúvel e, portanto, isomorfo a $\mathbb{Z}_p^3 \rtimes \mathbb{Z}_p$ ou $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p^2$ com ação livre de pontos fixos.

Demonstração. Como G possui a propriedade CA, seu $\mathbb{Z}_p$-reticulado de Lie associado $L(G)$ e, portanto, sua álgebra de Lie $\mathbb{Q}_p \otimes L(G)$ também a possuem. Se G não fosse solúvel, $\mathbb{Q}_p \otimes L(G)$ seria isomorfo, pelo Teorema da decomposição de Levi a $\mathbb{Q}_p \oplus \mathfrak{sl}_2(\mathbb{Q}_p)$ ou a $\mathbb{Q}_p \oplus \mathfrak{sl}_1(\mathbb{D}_p)$, que não possuem a propriedade CA. Logo G é solúvel e o resultado segue do Teorema acima. ■

Bibliografia

[ApOn83] **Appelgate, Harry e Onishi, Hironori**. *Similarity problem over* $\mathrm{SL}(n, \mathbb{Z}_p)$. Proceedings of the American Mathematical Society **87, No. 2** (1983), 233-238.

[Bou63] **Bourbaki, Nicolas**. *Intégration, Chapitres 7 et 8*. Éléments de Mathématique (1963), Springer.

[Bou71a] **Bourbaki, Nicolas**. *Topologie générale, Chapitres 1 à 4*. Éléments de Mathématique (1971), Springer.

[Bou71b] **Bourbaki, Nicolas**. *Variétés Différentielles et Analytiques, Fascicule de résultats*. Éléments de Mathématique (1971), Springer.

[Bou72a] **Bourbaki, Nicolas**. *Groupes et algèbres de Lie, Chapitre 1*. Éléments de Mathématique (1972), Springer.

[Bou72b] **Bourbaki, Nicolas**. *Groupes et algèbres de Lie, Chapitres 2 et 3*. Éléments de Mathématique (1972), Springer.

[Bou81] **Bourbaki, Nicolas**. *Algèbre, Chapitres 4 à 7*. Éléments de Mathématique (1981), Springer.

[Cas78] **Cassels, John**. *Rational Quadratic Forms*. London Mathematical Society Monographs **13** (1978), Academic Press.

[DDMS99] **Dixon, John; du Sautoy, Marcus; Mann, Avinoam e Segal, Dan**. *Analytic pro-p Groups*. Cambridge studies in advanced mathematics **61** 2nd edition (1999), Cambridge University Press.

[FeAl01] **Fernández-Alcober, Gustavo**. *An introduction to finite p-groups: regular p-groups and groups of maximal class*. Matemática Contemporânea **20** (2001), 155-226.

[FGJ08] **Fernández-Alcober, Gustavo; González-Sánchez, Jon e Jaikin-Zapirain, Andrei**. *Omega subgroups of pro-p groups*. Israel Journal of Mathematics **166** (2008), 393-412.

[FGRS16] **Fine, Benjamin; Gaglione, Anthony; Rosenberger, Gerhard; Spellman, Dennis**. *On CT and CSA Groups and Related Ideas*. Journal of Group Theory **19** (2016), 923-940.

[GoSa07] **González-Sánchez, Jon**. *On p-saturable groups*. Journal of Algebra **315** (2007), 809-823.

[GoKl09] **González-Sánchez, Jon e Klopsch, Benjamin**. *Analytic pro-p groups of small dimensions*. Journal of Group Theory **12** (2009), 711-734.

[Hall59] **Hall Jr., Marshall**. *The Theory of Groups*. The Macmillan Company, New York (1959).

[Haz78] **Hazewinkel, Michiel**. *Formal groups and applications*. Pure and Applied Mathematics **78** (1978). Academic Press, Inc.

[Hoo42] **Hooke, Robert**. *Linear p-Adic Groups and Their Lie Algebras*. Annals of Mathematics, Second Series **43, No. 4** (1942), 641-655.

[Igu00] **Igusa, Jun-ichi**. *An Introduction to the Theory of Local Zeta Functions*. Studies in Advanced Mathematics **14** (2000), American Mathematical Society.

[Jac79] **Jacobson, Nathan**. *Lie Algebras*. Dover Books on Mathematics (1979), Dover Publications.

[KLGP97] **Klaas, Gundel; Leedham-Green, Charles e Plesken, Wilhelm**. *Linear pro-p-groups of finite width*. Lectures Notes in Mathematics **1674** (1997), Springer.

[KNV11] **Klopsch, Benjamin; Nikolov, Nikolay e Voll, Christopher**. *Lectures on Profinite Topics in Group Theory*. London Mathematical Society Student Texts **77** (2011), Cambridge University Press.

[Klo05] **Klopsch, Benjamin**. *On the Lie theory of p-adic analytic groups*. Mathematische Zeitschrift **249** (2005), 713-730.

[Laz65] **Lazard, Michel**. *Groupes analytiques p-adiques*. Publications mathématiques de l'I.H.É.S. **26** (1965), 5-219.

[LuMa87a] **Lubotzky, Alexander e Mann, Avinoam**. *Powerful p-Groups I. Finite groups*. Journal of Algebra **105** (1987), 484-505.

[LuMa87b] **Lubotzky, Alexander e Mann, Avinoam**. *Powerful p-Groups II. p-Adic Analytic Groups*. Journal of Algebra **105** (1987), 506-515.

[MWZ] **Mendonça, Luis; Weigel, Thomas e Zapata, Theo**. *Compact p-adic analytic groups in which centralizers are abelian. Preprint* disponível em arxiv.org/abs/2411.03880 (2024).

[NoSn19] **Noseda, Francesco e Snopce, Ilir**. *On self-similarity of p-adic analytic pro-p groups of small dimension*. Journal of Algebra **540** (2019), 317-345.

[RiZa10] **Ribes, Luis and Zalesskii, Pavel**. *Profinite Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge **40** 2nd edition (2010), Springer.

[Sch11] **Schneider, Peter**. *p-adic Lie Groups*. Grundlehren der mathematischen Wissenschaften **344** (2011), Springer.

[Ser65] **Serre, Jean-Pierre**. *Classification des variétés analytiques p-adiques compactes*. Topology **3** (1965), 409-412.

[Ser00] **Serre, Jean-Pierre**. *Lie Algebras and Lie groups*. Lecture Notes in Mathematics **1500** 2nd edition (2000), Springer.

[SZZ19] **Shumyatsky, Pavel; Zalesskii, Pavel e Zapata, Theo**. *Profinite groups in which centralizers are abelian*. Israel Journal of Mathematics **230** (2019), 831-854.

[Suz86] **Suzuki, Michio**. *Group Theory II*. Grundlehren der mathematischen Wissenschaften **248** (1986), Springer-Verlag.

Índice Remissivo

$\mathbb{Z}_p$-reticulado de Lie, 16
  p-saturado, 57
  de um grupo p-saturado, 56
  residualmente nilpotente, 64
p-valoração, 39

aplicação
  analítica, 16
    entre variedades (morfismo), 21
  diferenciável, 16
  tangente, 22
apresentação de um grupo pro-p, 14
atlas, 21
ação
  de um grupo analítico, 36
  livre de pontos fixos (para álgebras de Lie), 83

base ordenada, 40

carta, 20
  compatível, 20
centralizador em álgebras de Lie, 82
classe de
  congruência-multiplicativa, 71
  similaridade-multiplicativa, 66
corpo local, 28

derivação, 17
  interna, 17

espaço
  cotangente, 22
  tangente, 22
espiga (anel local), 21

filtração potente, 59
forma diferencial, 27
  analítica, 28

grupo
  p-saturado, 40
  p-saturável, 41
  p-valorado, 39
    de posto finito, 40
  p-valorável, 41
  analítico, 32
    p-ádico, 32
  padrão, 33
  pro-p, 14
    powerful, 43
    de coclasse finita, 62
    finitamente gerado, 14
    PF, 59
    uniformemente *powerful*, 44
  profinito, 13
  topológico, 13

homomorfismo
  de álgebras de Lie, 17
  local, 34

ideal de uma álgebra de Lie, 16
imersão, 23
integração de formas diferenciais, 28
inteiros p-ádicos, 15
isolador
  de um $\mathbb{Z}_p$-subreticulado de Lie, 62
  de um subgrupo, 62

lei formal de grupo, 33
limite projetivo, limite inverso, 12

números p-ádicos, 15

ordem de um grupo profinito, 14

peça de grupo, 34
produto semidireto de álgebras de Lie, 17
propriedade CA, 81
    para álgebras de Lie, 82

representação de um grupo analítico, 47

subgrupo
    de Frattini, 14
    de Lie, 36
    verbal, 14
subimersão, 24
submersão, 24
subvariedade, 26
série central inferior
    de um grupo pro-p, 14
    de uma álgebra de Lie, 17
série de potências
    convergente, 16
    restrita especial, 31

transversalidade
    de morfismos, 27
    de subvariedades, 27

valor absoluto, 15
    ultramétrico, 15
valor regular, 26
variedade analítica, 21
    quociente, 26

álgebra de Lie, 16
    de derivações, 17
    abeliana, 16
    de um grupo analítico, 46
    de um grupo formal, 45
    livre, 18
    nilpotente, 17
    semissimples, 17
    solúvel, 17