Dimensão de Hausdorff em grupos pro-p com aplicações em grupos analíticos p-ádicos

Arbey Efren Lopez Garcia

Dissertação de Mestrado apresentada ao Programa de Pos-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários a obtenção do título de Mestre em Matemática.

Orientador: Ilir Snopche

Rio de Janeiro
Agosto de 2016

DIMENSÃO DE HAUSDORFF EM GRUPOS PRO-P COM APLICAÇÕES EM GRUPOS ANALÍTICOS P-ÁDICOS

Arbey Efren Lopez Garcia
Orientador: Ilir Snopche

Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários a obtenção do titulo de Mestre em Matemática.

Aprovada por:

____
Presidente, Prof. Ilir Snopche Ph.D.

____
Prof. Amílcar Pacheco Ph.D. -UFRJ.

____
Prof. Mikhail Belolipetsky Ph.D. -IMPA.

Rio de Janeiro
Agosto de 2016

Lopez, Arbey Efren Garcia.

Dimensão de Hausdorff em grupos pro-p com aplicações em grupos analíticos p-ádicos/ Arbey Efren Lopez Garcia. -Rio de Janeiro: UFRJ/PGIM, 2016.

vii, 40f.;30 cm.

Orientador: Ilir Snopche

Dissertação (mestrado) - UFRJ/PGIM Programa de Pós-graduação do Instituto de Matemática, 2016.

Referências Bibliográficas: f. 41.

1. Algebra 2. Grupos profinitos. 3. Grupos analíticos. I. Snopche, Ilir. II. Universidade Federal do Rio de Janeiro, Programa de Pós-graduação do Instituto de Matemática. III. Título.

RESUMO

DIMENSÃO DE HAUSDORFF EM GRUPOS PRO-P COM APLICAÇÕES EM GRUPOS ANALÍTICOS P-ÁDICOS

Arbey Efren Lopez Garcia
Orientador: Ilir Snopche

Resumo da Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários a obtenção do titulo de Mestre em Matemática.

O principal objetivo deste trabalho é o estudo da dimensão de Hausdorff para grupos pro-p, com um foco especial na classe de grupos analíticos p-ádicos. Este trabalho mostra que além de fractais, também grupos pro-p têm uma dimensão de Hausdorff interessante. Isto é possível uma vez que grupos pro-p podem ser tornados espaços métricos com respeito de alguma escolha de filtração no grupo. A dimensão de Hausdorff é uma ferramenta muito útil na avaliação da estrutura de subgrupos de grupos onde a estrutura é complicada e longe de ser transparente. Foi Abercrombie que iniciou o estudo da dimensão de Hausdorff para grupos profinitos. Os resultados mais interessantes foram obtidos no artigo seminal de Barnea e Shalev, no qual este trabalho é baseado.

No primeiro capítulo deste trabalho apresentamos a teoria básica de grupos profinitos e grupos pro-p. No capítulo 2, estudamos os principais resultados relativos às classes de grupos pro-p powerful e de grupos analíticos p-ádicos, respectivamente. Em seguida, no terceiro capítulo, cobrimos as propriedades básicas da dimensão de Hausdorff para grupos profinitos. O último capítulo aborda o estudo da dimensão de Hausdorff na classe de grupos pro-p analíticos p-ádicos e contém os principais resultados deste trabalho. Mostramos que a dimensão de Hausdorff de um subgrupo fechado de um grupo pro-p analítico p-ádico generaliza o conceito de dimensão em um grupo de Lie. Além disso, damos uma caracterização de grupos pro-p analíticos p-ádicos em termos de dimensão de Hausdorff.

Palavras-chave: Algebra, Grupos Profinitos, Grupos analíticos.

Rio de Janeiro
Agosto de 2016

ABSTRACT

HAUSDORFF DIMENSION OF PRO-P GROUPS WITH APPLICATIONS IN P-ADIC ANALYTIC PRO-P GROUPS

Arbey Efren Lopez Garcia
Orientador: Ilir Snopche

Abstract da Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários a obtenção do titulo de Mestre em Matemática.

The main purpose of this work is the study of Hausdorff dimension for pro-p groups, with a special focus on the class of p-adic analytic pro-p groups. This work illustrates that besides fractals, also pro-p groups have an interesting Hausdorff dimension. This is possible since pro-p groups can be made into metric spaces with respect to some choice of filtration on the group. It turns out that Hausdorff dimension is a very useful tool in assessing the subgroup structure of groups where the structure is complicated and far from transparent. It was Abercrombie who initiated the study of Hausdorff dimension for profinite groups. The most interesting results were obtained in the seminal paper of Barnea and Shalev, on which this work is based.

In the first chapter of this work we present the basic theory of profinite groups and pro-p groups. In chapter 2 we study the main results regarding the classes of powerful pro-p groups and p-adic analytic pro-p groups, respectively. Next, in the third chapter, we cover the basic properties of Hausdorff dimension for profinite groups. The last chapter covers the study of Hausdorff dimension in the class of p-adic analytic groups and contains the main results of this work. We show that the Hausdorff dimension of a closed subgroup of a p-adic analytic pro-p group generalises the concept of dimension in a Lie group. Moreover, we give a characterization of p-adic analytic pro-p groups in terms of Hausdorff dimension.

Key-words: Algebra, Profinite Groups, Analytic Groups, Hausdorff dimension.

Rio de Janeiro
Agosto de 2016

AGRADECIMENTOS

Agradeço á Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo suporte financeiro. Ao professor Ilir por suas orientações e correções. E a todos meus companheiros e amigos. Ao Programa de Pós-graduação do Instituto de Matemática.

Sumário

Introdução

Grupos profinitos são grupos topológicos compactos e totalmente desconexos, que aparecem naturalmente como grupos de Galois de extensões de corpos. Tais grupos podem também ser pensados como limites inversos de grupos finitos. Uma subclasse particularmente interessante e importante dos grupos profinitos é a classe de grupos pro-p. Um grupo pro-p é um grupo profinito em que todo subgrupo aberto normal tem índice igual a uma potência de um primo p. Em outras palavras, um grupo pro-p é o limite inverso de um sistema inverso de p-grupos finitos. Os grupos pro-p na classe de grupos profinitos têm um papel análogo ao dos p-grupos na classe dos grupos finitos.

Quando se lida com grupos profinitos ou grupos pro-p parece útil ter uma ferramenta que mede o tamanho dos subgrupos de um grupo dado. Claramente, no caso de grupos finitos, a cardinalidade é uma medida natural. Grupos pro-p, grupos profinitos e grupos compactos em geral, possuem uma medida de Haar invariante, que pode ser usado para medir o tamanho de subconjuntos. No entanto, a medida de Haar não é muito informativa e útil quando aplicada a subgrupos de um grupo compacto, pois todos os subgrupos fechados de índice infinito têm medida de Haar 0, e a medida de Haar (normalizada) de um subgrupo aberto é simplesmente o inverso do seu índice. De modo que ao estudar os subgrupos fechados de grupos profinitos e de grupos pro-p que não são abertos, pode ser usado a dimensão de Hausdorff.

O principal objetivo deste trabalho é o estudo da dimensão de Hausdorff para grupos pro-p. Este trabalho mostra que além de fractais, também grupos pro-p têm uma dimensão de Hausdorff interessante. Isto é possível uma vez que grupos pro-p podem ser tornados espaços métricos com respeito de alguma escolha de filtração no grupo. A dimensão de Hausdorff é uma ferramenta muito útil na avaliação da estrutura de subgrupos de grupos onde a estrutura é complicada e longe de ser transparente. Foi Abercrombie que iniciou o estudo da dimensão de Hausdorff para grupos profinitos (veja [1]). Os resultados mais interessantes foram obtidos no artigo seminal de Barnea e Shalev (veja [2]), no qual este trabalho é baseado. O nosso foco vai ser nas aplicações da dimensão de Hausdorff para o estudo de grupos analíticos p-ádicos. Um grupo analítico p-ádico é uma variedade analítica p-ádica que também é um grupo, onde as operações do grupo são dadas por funções analíticas.

No primeiro capítulo deste trabalho apresentamos a teoria básica de grupos profinitos e grupos pro-p, seguindo os livros [11] e [3]. Primeiramente, fazemos uma revisão de grupos topológicos e limites inversos. Em seguida, introduzimos os conceitos de grupos profinitos e pro-p através de limites inversos e estudamos as suas propriedades básicas. Também consideramos alguns exemplos, incluindo os inteiros p-ádicos. No capítulo 2, estudamos os principais resultados relativos às classes de grupos pro-p powerful e de grupos analíticos p-ádicos, respectivamente. Primeiramente, introduzimos o conceito de p-grupo finito powerful e construímos gradualmente a teoria da estrutura de p-grupos finitos powerful. Em seguida, introduzimos os grupos pro-p powerful e estudamos as suas propriedades, usando a teoria da estrutura de p-grupos finitos powerful. Finalmente, nesse capítulo, apresentamos e estudamos os grupos analíticos p-ádicos. Em particular, damos uma caracterização de grupos analíticos p-ádicos como grupos topológicos que contem um subgrupo aberto que é um grupo pro-p powerful. A principal referência nesse capítulo é o livro [3]. No capítulo 3 cobrimos as propriedades básicas da dimensão de Hausdorff para grupos profinitos. O último capítulo aborda o estudo da dimensão de Hausdorff na classe de grupos pro-p analíticos p-ádicos e contém os principais resultados deste trabalho. Mostramos que a dimensão de Hausdorff de um subgrupo fechado de um grupo pro-p analítico p-ádico generaliza o conceito de dimensão em um grupo de Lie. Além disso, damos uma caracterização de grupos pro-p analíticos p-ádicos em termos de dimensão de Hausdorff. A principal referência nos capítulos 3 e 4 é o artigo [2].

Capítulo 1

Grupos profinitos e pro-p

Um grupo profinito é o limite inverso de um sistema inverso de grupos finitos. Equivalentemente, um grupo profinito é um grupo topológico compacto, Hausdorff e totalmente desconexo. Um grupo pro-p é um grupo profinito em que todo subgrupo aberto normal tem índice igual a uma potência de um primo p. Os grupos pro-p na classe de grupos profinitos têm um papel análogo ao dos p-grupos na classe dos grupos finitos. Nesse capítulo apresentamos a teoria básica de grupos profinitos e grupos pro-p, seguindo os livros [11] e [3].

1.1 Preliminares topológicos

Um conjunto X e uma família de subconjuntos U de X é um **espaço topológico** (X, U) se e somente se U é fechado sobre uniões quaisquer, fechada sobre intersecções finitas e $\emptyset, X$ pertencem a U. Nesse caso U é chamado de topologia de X e um elemento de U é chamado conjunto **aberto**. Um conjunto é **fechado** se o seu complemento é aberto. Dado um subconjunto W de X, o **fecho** $\overline{W}$ de W é o menor conjunto fechado contendo W. Dizemos que $W \subseteq X$ é **denso** em X se $\overline{W} = X$.Uma **vizinhança** de x em X é um aberto contendo x. Uma **base** B de um espaço topológico (X, U) é uma subfamília de U, tal que para todo aberto V existe W em B tal que $W \subset V$. Uma **Base de vizinhanças ou sistema fundamental de vizinhanças** de U em $x \in X$ é uma subfamília de vizinhanças B_x de x tal que se V é um aberto contendo x, então existe W em B_x tal que $W \subset V$.

Qualquer conjunto X pode ser considerado como um espaço topológico, considerando a **topologia discreta** $U = \mathbb{P}(X)$.

Se Y é um subconjunto de um espaço topológico (X, U), então Y pode ser considerado como um subespaço topológico, com a **topologia induzida** (os abertos de Y são da forma $Y \cap W$, onde W é um aberto de X).

Um espaço topológico X é **compacto**, se para qualquer família de abertos $\{U_\alpha | \alpha \in \Lambda\}$

cuja união é X, existe uma subfamília finita $U_{\alpha_1}, ..., U_{\alpha_n}$ cuja união é X.

Um espaço topológico X é **Hausdorff** se para cada dois elementos $x, y \in X$ existem vizinhanças U, V de x, y, tais que $U \cap V = \emptyset$. Se X for Hausdorff, então cada $x \in X$ é fechado.

Um espaço topológico X é **conexo** se não se pode escrever como a união disjunta de dois abertos não vazios. Dizemos que X é **totalmente desconexo** se todo subespaço conexo de X tem no máximo um elemento.

Lema 1.1.1. *Seja X um espaço Hausdorff, compacto e totalmente desconexo. Então todo aberto de X é uma união de conjuntos que são simultaneamente abertos e fechados.*

Dados dois espaços topológicos X, Y, dizemos que uma função $f : X \to Y$ **é uma função contínua** se a preimagem de cada aberto em Y é um aberto em X. Dada uma família de espaços topológicos $\{X_\lambda | \lambda \in \Lambda\}$ o **produto cartesiano** se define como

$$\prod_{\lambda \in \Lambda} X_\lambda := \{(x_\lambda)_{\lambda \in \Lambda} | x_\lambda \in X_\lambda\}.$$

A função

$$\pi_\mu : \prod X_\lambda \to X_\mu$$

dada por

$$\pi_\mu((x_\lambda)_{\lambda \in \Lambda}) := x_\mu$$

é chamada de **função projeção**. O conjunto produto cartesiano $\prod_{\lambda \in \Lambda} X_\lambda$ junto com a menor topologia, tal que as aplicações projeções são contínuas, é chamado de **produto topológico**.

Proposição 1.1.2. *[11, Teorema 0.2.1] Seja $\{X_\lambda | \lambda \in \Lambda\}$ uma família de espaços topológicos.*

(i) Se cada X_λ é Hausdorff, então o produto topológico $\prod_{\lambda \in \Lambda} X_\lambda$ também é Hausdorff.

(ii) Se cada X_λ é totalmente desconexo, então o produto topológico $\prod_{\lambda \in \Lambda} X_\lambda$ também é totalmente desconexo.

(iii) Se cada X_λ é compacto, então o produto topológico $\prod_{\lambda \in \Lambda} X_\lambda$ também é compacto.

Um **grupo topológico** G é um espaço topológico que tem uma estrutura de grupo, tal que o mapa $G \times G \to G : (x, y) \mapsto xy^{-1}$ é contínuo.

Lema 1.1.3. *[11, Lema 0.3.1] Seja G um grupo topológico.*

(i) Todo subgrupo aberto de G é fechado e todo subgrupo fechado de índice finito é aberto. Se G é compacto, então todo subgrupo aberto tem índice finito.

(ii) Se H é um subgrupo de G contendo um conjunto aberto não vazio, então H é um subgrupo aberto.

(iii) Se H é um subgrupo de G e K é um subgrupo normal de G, então H é um subgrupo topológico com a topologia induzida, e G/K é um grupo topológico com a topologia quociente.

(iv) O grupo G é Hausdorff se e somente se $\{1\}$ é fechado. Em particular, G/K é Hausdorff se e somente se K é fechado em G.

(v) Se G é totalmente desconexo, então é Hausdorff.

Lema 1.1.4. *Seja G um grupo topológico. Se Y é um subconjunto aberto e fechado que contem a identidade 1, então Y contem um subgrupo aberto e normal.*

Proposição 1.1.5. *[11, Proposição 0.3.3] Seja G um grupo topológico compacto e totalmente desconexo.*

(i) Todo subconjunto aberto de G é uma união de classes laterais de subgrupos normais abertos.

(ii) Um subconjunto de G é aberto e fechado se e somente se é a união de um número finito de classes laterais de subgrupos normais abertos.

(iii) Se X é um subconjunto de G, então o fecho topológico $\overline{X}$ satisfaz

$$\overline{X} = \bigcap (NX | N \textit{ é um subgrupo normal aberto de } G\ ).$$

1.2 Inteiros p-ádicos

Seja $\mathbb{Q}$ o corpo de números racionais e seja p um número primo fixo. Dado um número racional $x \neq 0$, podemos escrever x de maneira única como

$$x = p^n \frac{a}{b}$$

com $n, a, b \in \mathbb{Z}$, $b > 0$, $\text{mcd}(a, b) = 1$ e $p \nmid ab$. Nesse caso definimos a função

$$v_p : \mathbb{Q}^x \to \mathbb{Z}, \text{ tal que } v_p(p^n \frac{a}{b}) = n.$$

A função v_p é uma valorização discreta sobre $\mathbb{Q}$, i.e., satisfaz:

(i) $v_p(xy) = v_p(x) + v_p(y)$.

(ii) v_p é sobrejetiva.

(iii) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$ para todo $x, y \in \mathbb{Q}$, com $x + y \neq 0$.

Agora que temos uma valorização sobre $\mathbb{Q}$, podemos definir uma norma sobre $\mathbb{Q}$, dada por

$$|x|_p = \begin{cases} p^{-v_p(x)}, & x \neq 0 \\ 0, & x = 0. \end{cases}$$

Não é difícil de ver que $|.|_p$ satisfaz as propriedades de uma norma sobre $\mathbb{Q}$. Mais precisamente, $|.|_p$ é uma norma não arquimediana, i.e., $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ para todo $x, y \in \mathbb{Q}$. Consideramos seqüencias de Cauchy com respeito a esta norma. E definimos duas seqüencias de Cauchy $\{a_i\}$ e $\{b_i\}$ equivalentes se $|a_i - b_i| \to 0$ quando $i \to 0$. O completamento de $\mathbb{Q}$ é o conjunto de classes de equivalência de seqüencias de Cauchy.

Podemos ver facilmente que este completamento é um corpo, denotado por $\mathbb{Q}_p$ e chamado de números p-ádicos. O corpo $\mathbb{Q}_p$ é completo, i.e., todas as seqüencias de Cauchy de elementos de $\mathbb{Q}_p$ são convergentes. Os racionais podem ser identificados com um subcorpo de $\mathbb{Q}_p$ que consiste das seqüencias de Cauchy constantes.

Definimos uma norma sobre $\mathbb{Q}_p$, como uma extensão da norma $|.|_p$ em $\mathbb{Q}$, na forma seguinte: para $x \in \mathbb{Q}_p$

$$|x|_p := \lim_{i\to\infty} |x_i|_p, \text{ onde, } x_i \in \mathbb{Q}$$

e (x_i) é uma seqüencia de Cauchy tal que $\lim_{i\to\infty} x_i = x$. O subconjunto de $\mathbb{Q}_p$, denotado por $\mathbb{Z}_p$ e definido por

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\},$$

é chamado o anel de inteiros p-ádicos. Não é difícil mostrar [7, Teorema 2, pagina 11] que $x \in \mathbb{Z}_p$ se e somente se existe uma sequência de Cauchy da forma $x = \{a_i\}$ tal que:

(i) $0 \leq a_i \leq p-1$, para $i = 1, 2, \ldots$.

(ii) $a_i \equiv a_{i+1} \mod p^i$, para $i = 1, 2, \ldots$.

Portanto podemos identificar $\mathbb{Z}_p$ com o seguinte conjunto

$$\mathbb{Z}_p = \{\sum_{n=0}^{\infty} a_n p^n \mid 0 \leq a_n \leq p-1\}.$$

1.3 Limites inversos

Um conjunto dirigido é um conjunto parcialmente ordenado não vazio $(I, \leq)$ com a propriedade que para todo $i_1, i_2 \in I$ existe $i_3 \in I$ tal que $i_1 \leq i_3, i_2 \leq i_3$.

Definição 1.3.1. Um sistema inverso (X_i, φ_{ij}, I) de espaços topológicos (grupos, grupos topológicos, anéis, etc.) indexado por um conjunto dirigido $(I, \leq)$ é uma família $(X_i \mid i \in I)$ de espaços topológicos (grupos, grupos topológicos, anéis, etc.) e funções contínuas (homomorfismos de grupos, homomorfismos contínuos, homomorfismo de anéis, etc.) $\varphi_{ij} : X_j \to X_i$ para cada $i \leq j$ que satisfaz as seguintes propriedades:

(i) $\varphi_{ii} = \mathrm{Id}_{X_i}$ para cada $i \in I$;

(ii) $\varphi_{ik} = \varphi_{ij}\varphi_{jk}$ para cada $i \leq j \leq k$, i.e., o seguinte diagrama comuta.

$$\begin{tikzcd} X_k \arrow[rr, "\varphi_{jk}"] \arrow[dr, "\varphi_{ik}"'] & & X_j \arrow[dl, "\varphi_{ij}"] \\ & X_i & \end{tikzcd}$$

Definição 1.3.2. Dado um sistema inverso (X_i, φ_{ij}, I), uma família compatível (X, ψ_i) é um espaço topológico X e mapas contínuos $\psi_i : X \to X_i$, tais que $\psi_i = \varphi_{ij}\psi_j$.

Definição 1.3.3. O limite inverso de um sistema inverso (X_i, φ_{ij}, I) é uma família compatível (X, ψ_i) que satisfaz a seguinte propriedade universal: se (Y, ϕ_i) é uma outra família compatível de (X_i, φ_{ij}, I), então existe um único mapa continuo $\tau : X \to Y$ tal que $\psi_i = \phi_i \tau$ para todo $i \in I$, i.e., o seguinte diagrama é comutativo.

$$\begin{tikzcd} X \arrow[rr, "\tau"] \arrow[dr, "\psi_i"'] & & Y \arrow[dl, "\phi_i"] \\ & X_i & \end{tikzcd}$$

Proposição 1.3.4. *Seja (X_i, φ_{ij}, I) um sistema inverso.*

(i) Seja X o subconjunto do produto cartesiano (com a topologia induzida) $\prod_{i \in I} X_i$ dado por

$$X := \{(x_i) \in \prod_{i \in I} X_i | \varphi_{ji}(x_i) = x_j \text{ se } i \geq j\}$$

e considere os mapas

$$\pi_i|_X : X \to X_i,$$

onde $\pi_i : \prod_{j \in I} X_j \to X_j$ são as projeções. Então (X, π_i) é o limite inverso do sistema inverso (X_i, φ_{ij}, I).

(ii) O limite inverso é único no seguinte sentido: Se (X, ψ_i) e (Y, ϕ_i) são limites inversos do sistema inverso (X_i, φ_{ij}, I), então existe um único homeomorfismo $\tau : X \to Y$, tal que $\psi_i = \phi_i \tau$ para todo $i \in I$.

O limite inverso de um sistema inverso (X_i, φ_{ij}, I) vai ser denotado por:

$$X = \lim_{\leftarrow} X_i.$$

Proposição 1.3.5. *Seja (X_i, φ_{ij}, I) um sistema inverso e seja $X = \lim_{\leftarrow} X_i$ o seu limite inverso.*

(i) Se cada X_i é Hausdorff, então X também é Hausdorff.

(ii) Se cada X_i é totalmente desconexo, então X também é totalmente desconexo.

(iii) Se cada X_i é compacto, então X também é compacto.

Proposição 1.3.6. *[5] Seja (X_i, φ_{ij}, I) um sistema inverso de espaços compactos, Hausdorff e não vazios. Então o limite inverso*

$$X = \lim_{\leftarrow} X_i$$

também é não vazio.

Seja G um grupo e I uma familia de subgrupos normais de índice finito. Definimos $M \preceq N$ se $N \leq M$. Se $M, N \in I$ e $M \preceq N$, então seja

$$\varphi_{MN} : G/N \to G/M \text{ o epimorfismo natural.}$$

Então $\{G/N, \varphi_{MN}\}$ é um sistema inverso de grupos finitos. O limite inverso deste sistema inverso de grupos finitos é conhecido como completamento pro-I e é denotado por $\hat{G}_I$. Quando I consiste de todos os subgrupos normais de índice finito de G dizemos que $\hat{G}_I$ é o completamento profinito de G, e denotamos $\hat{G}_I$ por $\hat{G}$.

Exemplo 1.3.7. Consideremos o grupos dos números inteiros $\mathbb{Z}$. A familia I de todos os subgrupos normais de índice finito é dada por $\{n\mathbb{Z}\}_{n \in \mathbb{N}}$. Então $n\mathbb{Z} \leq m\mathbb{Z} \Leftrightarrow m|n \Leftrightarrow m\mathbb{Z} \preceq n\mathbb{Z}$. Se $m\mathbb{Z} \preceq n\mathbb{Z}$ definimos

$$\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

$$\varphi_{mn} : x \mod n \mapsto x \mod m.$$

Claramente $(\varphi_{mn}, \mathbb{Z}/n\mathbb{Z}, \preceq)$ é um sistema inverso, e o limite inverso $\hat{\mathbb{Z}} = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z}$ é o completamento profinito de $\mathbb{Z}$.

Exemplo 1.3.8 (Os inteiros p-ádicos como um limite inverso)**.** Seja p um primo fixo. Consideramos o conjunto $I = \mathbb{N}$ com a ordem usual. Os grupos finitos $\{\mathbb{Z}/p^i\mathbb{Z}\}_{i\in\mathbb{N}}$, junto com os epimorfismos naturais $\varphi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$, formam um sistema inverso. Pela Proposição 1.3.4, o limite inverso do sistema inverso $(\varphi_{ij}, \mathbb{Z}/p^i\mathbb{Z})$ é igual a

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid \varphi_{mn}(a_n) = a_m \text{ para todo } m \leq n \right\}. \tag{1.1}$$

Seja $x = (a_n)$ um elemento de $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Então os inteiros a_n satisfazem:

$$a_2 \equiv a_1 \mod p$$

$$a_3 \equiv a_2 \mod p^2$$

$$a_{n+1} \equiv a_n \mod p^n$$

Já que $a_1 \in \mathbb{Z}/p\mathbb{Z}$, temos que $0 \leq a_1 \leq p-1$. Pegamos $b_0 := a_1$. Como $a_2 \equiv a_1 \mod p$, segue que existe um inteiro b_1, tal que $0 \leq b_1 \leq p-1$ e $a_1 = b_0 + b_1 p$. Por indução, existem inteiros $\{b_m\}$ entre 0 e $p-1$ satisfazendo $a_n = b_0 + b_1 p + \ldots + b_n p^n$. Assim, cada elemento do limite inverso (1.1) pode ser identificado com uma expressão da forma $\sum_{i=1}^{\infty} b_i p^i$. Portanto

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

Podemos definir operações de soma e multiplicação em $\mathbb{Z}_p$, que o tornam um anel. Por isso $\mathbb{Z}_p$ é chamado o anel de inteiros p-ádicos. O anel $\mathbb{Z}_p$ tem incontáveis elementos. O anel $\mathbb{Z}_p$ contem uma copia de $\mathbb{Z}$, e todos os seus ideais não nulos são da forma $p^n\mathbb{Z}_p$ para algum $n \in \mathbb{N}$. O ideal $p\mathbb{Z}_p$ é o único ideal maximal de $\mathbb{Z}_p$.

1.4 Grupos profinitos

Cada grupo finito munido com a topologia discreta pode ser considerado como um grupo topológico. Tomando o limite inverso de grupos finitos obtemos um grupo topológico profinito. O nosso objetivo é dar uma caracterização de grupos profinitos, e notar como é que eles herdam muitas das propriedades de grupos finitos, como por exemplo o Teorema de Lagrange e o Teorema de Sylow.

Definição 1.4.1. Um grupo profinito é o limite inverso de um sistema inverso de grupos finitos.

Uma caracterização de grupos profinitos é que são grupos topológicos compactos, Hausdorff, e totalmente desconexos. Por tanto suas propriedades são meramente topológicas.

Teorema 1.4.2. *As seguintes condições sao equivalentes.*

(i) G é um grupo profinito.

(ii) G é um grupo topológico compacto, Hausdorff e a familia de subgrupos normais e abertos formam uma base de vizinhanças da identidade 1.

(iii) G é um grupo topológico compacto, Hausdorff, e totalmente desconexo.

Demonstração. ($1 \Rightarrow 2$) Seja G um grupo profinito. Então

$$G = \varprojlim_{i \in I} G_i$$

onde $\{G_i, \varphi_{ij}, I\}$ é um sistema inverso de grupos finitos G_i, com homomorfismos as projeções

$$\varphi_i : G \to G_i.$$

Considere os subgrupos $\{U_i \mid U_i = Ker(\varphi_i)\}$ de G. Os subgrupos U_i são abertos, pois G_i tem a topologia discreta, e os subgrupos U_i são normais, pois são núcleos de homomorfismos. Vamos mostrar que eles formam uma base de vizinhanças do 1 em G. De fato, qualquer aberto de $\prod_{i \in I} G_i$ contem uma vizinhança do $\{1\}$ do produto topológico, da forma

$$\left(\prod_{i \neq i_1, \ldots, i_t} G_i \right) \times \{1\}_{i_1} \times \ldots \times \{1\}_{i_t},$$

com $i_1, ..., i_t \in I$. Seja $i_0 \geq i_1, ..., i_t$. Então

$$G \cap \left[\left(\prod_{i \neq i_0} G_i \right) \times \{1\}_{i_0} \right] = Ker(\varphi_{i_0}) = U_{i_0}$$

são vizinhanças do $\{1\}$ em G.

($2 \Rightarrow 3$) Para ver que G é totalmente desconexo, basta mostrar que a componente conexa N da identidade em G é $\{1\}$. Seja $\{U_i\}$ uma base de vizinhanças do $\{1\}$. Tomamos $N_i = U_i \cap N$ para cada i. Os subgrupos N_i são abertos normais em N, e como N é conexo $N = N_i$ para todo i. Então

$$N = \bigcap_i N_i = \bigcap_i N \cap N_i = N \bigcap_i N_i = N \cap \{1\},$$

e por isso $N = \{1\}$.

(3 $\Rightarrow$ 1) Proposição 1.1.7 do Wilson [11]. $\square$

Seja G um grupo profinito. Então os seguintes fatos são facilmente demonstrados.

(i) Todo subgrupo aberto possui um subgrupo normal aberto.

(ii) A familia de todos os subgrupos abertos de G, tem intersecção $\{1\}$.

(iii) Um subconjunto é aberto se e somente se é união de classes laterais de subgrupos abertos e normais.

(iv) Seja H um subgrupo aberto de um grupo profinito G. Então H é fechado, de índice finito e contém um subgrupo aberto normal de G.

Seja G grupo topológico. Se X é um subgrupo aberto de G, subgrupo fechado de G, subgrupo normal aberto de G, subgrupo normal fechado de G, vamos escrever $X \leq_o G$, $X \leq_c G$,$X \lhd_o G$ e $X \lhd_c G$, respectivamente.

Uma das principais riquezas dos grupos profinitos é que herdam muitas das propriedades de grupos finitos. Facilmente podemos demonstrar análogos ao Teorema de Lagrange e ao Teorema de Sylow, entre outros.

Consideremos um grupo profinito

$$G = \varprojlim_{i \in I} G_i$$

onde cada G_i é um grupo finito. Se G for infinito então a cardinalidade de G nos da pouca ou nada de informação. Por isso existe uma noção de ordem em grupos profinito que reflete de maneira global as propriedades aritméticas dos grupos finitos G_i. Para introduzir este novo conceito precisamos da noção de números supernaturais. Um **número supernatural** é um produto da forma

$$n = \prod_p p^{n(p)}$$

onde p atravessa todos os números primos e $n(p)$ é um inteiro não negativo ou infinito.

Dado um outro número supernatural

$$m = \prod_p p^{n(p)},$$

diz-se que m divide n, notado por $m|n$, se $m(p) \leq n(p)$ para cada primo p.

Dada uma familia de números supernaturais

$$\{n_i = \prod_p p^{n(p,i)} \ \mid \ i \in I\}$$

definimos o produto, o mínimo múltiplo comum $m.m.c$ e o máximo comum divisor $m.c.d$, respectivamente, na forma seguinte:

$$\prod_{i\in I} n_i = \prod_p p^{s_p}, \text{ onde } s_p = \sum_{i\in I}\{n(p,i)\}$$

$$m.m.c(\{n_i\}_{i\in I}) = \prod_p p^{s_p}, \text{ onde } s_p = \max_i\{n(p,i)\}$$

$$m.c.d(\{n_i\}_{i\in I}) = \prod_p p^{s_p}, \text{ onde } s_p = \min_i\{n(p,i)\}$$

Definição 1.4.3. Seja G um grupo profinito e H um subgrupo fechado de G. O índice de H em G se define como

$$|G : H| = m.m.c\{|G : U| \ \mid \ H \subseteq U \lhd_o G\} = m.m.c\{|G/U : HU/U| \ \mid \ U \lhd_o G\}$$

A ordem de G é definido por

$$|G| = |G : 1| = m.m.c\{|G : U| \mid U \lhd_o G\}.$$

O seguinte teorema é o Teorema de Lagrange para grupos pro-finitos

Teorema 1.4.4. *Seja G um grupo pro-finito. Se $K \leq_c H \leq_c G$, então*

$$|G : K| = |G : H||H : K|.$$

Seja G um grupo profinito. Se diz que um subconjunto $X \subset G$ gera topologicamente G, se $G = \overline{\langle X\rangle}$ onde $\langle X\rangle$ é o subgrupo gerado por X como grupo. Se X é finto, então dizemos que G é finitamente gerado. Denotamos por $d(G)$ o tamanho do menor conjunto que gera G.

Proposição 1.4.5. *Seja G um grupo profinito finitamente gerado. Se H é um subgrupo aberto de G, então H é também finitamente gerado.*

Seja G um grupo profinito finitamente gerado. Pela proposição anterior todo subgrupo aberto H de G é finitamente gerado, porém não sempre o número mínimo de geradores $d(H)$ é limitado. No capítulo seguinte vamos estudar uma classe de grupos profinitos, grupos pro-p powerful, onde para cada subgrupo fechado H o número de geradores $d(H)$ é limitado.

O subgrupo de Frattini de um grupo profinito G, denotado por $\Phi(G)$, é definido por

$$\Phi(G) = \bigcap \{M \mid M \text{ é um subgrupo aberto maximal proprio de } G\}.$$

O subgrupo de Frattini coincide com o conjunto dos não geradores de G [5, Lema 2.8.1].

Proposição 1.4.6. *Seja G um grupo profinito.*

(i) $\Phi(G) \lhd_c G$;

(ii) Se $N \lhd_c G$ *e* $N \leq \Phi(G)$, *então* $\Phi(G/N) = \Phi(G)/N$;

(iii) Se $H \leq_c G$ *e* $H\Phi(G) = G$, *então* $H = G$;

(iv) Se G é finitamente gerado, então $d(G) = d(G/\Phi(G))$.

Demonstração. (i) O subgrupo de Frattini é um subgrupo característico, e por isso é um subgrupo normal. Como os subgrupos abertos de um grupo profinito são fechados, então $\Phi(G)$ como intersecção de subgrupos fechados é fechado.

(ii) Segue do seguinte fato: cada subgrupo maximal aberto de G/N é da forma $U = M/N$ com M um subgrupo aberto maximal de G contendo N.

(iii) Suponha que $H \neq G$. Como H é um subgrupo fechado, H é uma intersecção de subgrupos abertos que contem H. Assim existe um subgrupo maximal aberto $M \neq G$ contendo H. Logo $G = H\Phi(G) \leq M$, que é uma contradição, pois $M \neq G$.

(iv) Se X é um conjunto de geradores de G, então $X\Phi(G)$ é um conjunto de geradores de $G/\Phi(G)$. Assim, $d(G/\Phi(G)) \leq d(G)$. Para mostrar a outra desigualdade, consideramos a função canônica $\Psi : G \to G/\Phi(G)$, e tomamos $X \in G$ tal que $\Psi(X)$ é o menor conjunto gerador de $G/\Phi(G)$. Então $G = \overline{\langle X, \Phi(G) \rangle} = \overline{\langle X \rangle}\Phi(G)$, logo $\overline{\langle X \rangle} = G$, pelo item anterior. Logo $d(G) \leq d(G/\Phi(G))$.

□

1.5 Grupos pro-p

Como foi visto anteriormente, $\mathbb{Z}_p$ é o limite inverso de p-grupos finitos e tem propriedades muito valiosas que em geral grupos profinitos não tem. Por isso nos vamos focar nossa atenção aos grupos profinitos que são limites inversos de p-grupos finitos e vamos observar como eles refletem muitas das propriedades de p-grupos finitos.

Em qualquer grupo G o comutador $[x, y]$, de dois elementos $x, y \in G$, se define como

$$[x, y] = x^{-1}y^{-1}xy.$$

As seguintes propriedades podem ser verificadas facilmente.

(i) $[xy, z] = y^{-1}[x, z]y[y, z]$

(ii) $[x, yz] = [x, z]z^{-1}[x, y]z$

(iii) $[x^n, y] = \prod_{i=1}^{n} x^{-(n-i)}[x, y]x^{n-i}$

(iv) $[x, y^n] = \prod_{i=0}^{n-1} y^{-i}[x, y]y^i$

Claramente, $[x, y] = 1$ se e somente se x e y comutam. Dados dois subconjuntos H, K de G o comutador de H e K é dado por $[H, K] = \langle [h, k] \mid h \in H\ k \in k \rangle$. No caso de grupos topológicos $[H, K] = \overline{\langle [h, k] \mid h \in H,\ k \in k \rangle}$. O grupo $[G, G]$ se chama a subgrupo comutador de G. Note que G é abeliano se e somente se $[G, G] = 1$. Não é difícil ver que $[G, G]$ é um subgrupo normal de G.

Lema 1.5.1. *Seja G um grupo e $N \lhd G$. Então G/N é abeliano se e somente se $[G, G] \leq N$.*

Demonstração. Dados $a, b \in G$, note que $abN = baN$ se e somente se $(ab)^{-1}ba \in N$, se e somente se $b^{-1}a^{-1}ba \in N$, se e somente se $[a, b] \in N$. □

Proposição 1.5.2. *Seja $\Theta : G \to H$ um homomorfismo de grupos. Então $\Theta([x, y]) = [\Theta(x), \Theta(y)]$. Em particular, $\Theta([G, G]) \subset [H, H]$.*

Proposição 1.5.3. *Sejam x e y elementos de um grupo G. Então*

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2} \mod \gamma_3(G).$$

A **serie central descendente** é definido por $\gamma_1(G) = G$ e $\gamma_n(G) = [\gamma_{n-1}(G), G]$ para $n \geq 2$. Um grupo é nilpotente se existe uma constante $c \in \mathbb{N}$ tal que $\gamma_c(G) = 1$.

Seja G um grupo finito. Se $|G| = p^n$, para algum inteiro $n > 0$ nós dizemos que G é um p-grupo finito.

Teorema 1.5.4. *[4, Teorema 1, cap 6] Seja G um grupo finito.*

(i) G é nilpotente se e somente se $Z(G/N) > 1$ para tudo subgrupo normal $N \neq G$.

(ii) Se G é um p-grupo finito, então G é nilpotente

(iii) Se G é um p-grupo finito, então todo subgrupo maximal de G é normal e de índice p em G.

(iv) Se G é um grupo nilpotente e $1 < N \lhd G$, então $[N, G] < N$ e $N \cap Z(G) > 1$.

(v) Se G é um grupo nilpotente e $1 < N \lhd G$, então algum subgrupo maximal de N é normal em G.

(vi) Se G é nilpotente, então cada grupo quociente de G e cada subgrupo de G também é nilpotente.

(vii) Se G é nilpotente, então os elementos de ordem finito de G formam um subgrupo.

Definição 1.5.5. Um grupo pro-p é o limite inverso de um sistema inverso de p-grupos finitos.

Todo subgrupo fechado de um grupo pro-p é também um grupo pro-p.

Proposição 1.5.6. *Um grupo profinito G é pro-p se e somente se todo subgrupo normal aberto tem índice igual alguma potência de p.*

O subgrupo de Frattini joga um papel fundamental na teoria de grupos pro-p, como pode ser visto da seguinte proposição.

Proposição 1.5.7. *[5, Lema 2.8.7]*

(i) Todo subgrupo maximal fechado M de G tem índice p e é normal em G.

(ii) O Grupo quociente $G/\Phi(G)$ é um grupo abeliano elementar, e portanto um espaço vectorial sobre $\mathbb{F}_p$, onde $\mathbb{F}_p$ é o corpo com p elementos.

(iii) Se G é um grupo pro-p, então $\Phi(G) = \overline{G^p[G, G]}$, onde $G^p = \langle x^p \mid x \in G \rangle$.

Demonstração. (i) Seja $M_G = \bigcap_{g \in G} g^{-1} M g$ o núcleo de M em G (M_G é o maior subgrupo normal de G contido em M). Como M é maximal, então M/M_G é um subgrupo maximal do p-grupo G/M_G. Assim M/M_G é um subgrupo normal de índice p pelo Teorema 1.5.4. Por tanto M é normal de índice p em G.

(ii)

$$G/\Phi(G) = G/\bigcap M \hookrightarrow \prod G/M$$

onde M percorre os subgrupos maximais fechados de G. Pelo item anterior $G/M \cong \mathbb{Z}/p\mathbb{Z}$ para cada M, assim obtemos o resultado.

(iii) Peguemos $G_0 = \overline{G^p[G,G]}$. Já que $G/\Phi(G)$ é um grupo abeliano elemental temos que $G_0 \leq \Phi(G)$. Vamos ver que estes dois subgrupos são de fato iguais, consideremos $x \notin G_0$. Pela compacidade de G_0 existe un subgrupo normal aberto de G tal que $xU \cap G_0U = \emptyset$, então $(G/U)/(G_0U/U$ é um grupo abeliano finito com ordem p, e a imagem $\bar{x}$ de x em $(G/U)/(G_0U/U$ é não trivial. Já que $(G/U)/(G_0U/U$ é uma soma direta finita da forma $\mathbb{Z}/p\mathbb{Z}$, então existe um subgrupo maximal de $(G/U)/(G_0U/U$ que não contem $\bar{x}$. Por tanto existe um subgrupo maximal de G que não contem x, e assim $x \notin \Phi(G)$.

□

Proposição 1.5.8. *Um grupo pro-p G é finitamente gerado se e somente se $\Phi(G)$ é um subgrupo aberto de G.*

Demonstração. ($\Rightarrow$) Todo subgrupo maximal fechado de um grupo pro-p G tem índice p. Por tanto se G é finitamente gerado, então para cada $n \in \mathbb{N}$ existe um número finito de subgrupo abertos de G de índice n, em particular o número de subgrupos maximais fechados é finito, conseqüentemente sua intersecção tem índice finito e assim $\Phi(G)$ é aberto.

($\Leftarrow$)Se $\Phi(G)$ é aberto, então $G/\Phi(G)$ é finito. Assim existe um subconjunto finito X de G tal que $G = X\Phi(G)$, então X gera topologicamente G pela proposição 1.4.6. □

A **p-serie central descendente** de G é definida por:

$$P_1(G) = G \text{ e } P_{n+1}(G) = \overline{P_n(G)^p[P_n(G), G]} \text{ para } n = 1, 2, ...$$

Essa serie vai nos permitir a definir uma métrica num grupo pro-p.

Proposição 1.5.9. *Seja p um número primo e G um grupo pro-p.*

(i) *Se $K \lhd_c G$, então $P_n(G/K) = P_n(G)K/K$ para n=1,2,...*

(ii) *$P_n(G)/P_{n+1}(G)$ é um p-grupo abeliano elementar.*

(iii) *$[P_n(G), P_m(G)] \leq P_{n+m}(G)$, para todo $n, m \in \mathbb{N}$.*

(iv) *A serie*

$$G = P_1(G) \geq P_2(G) \geq \ldots \geq P_n(G) \geq \ldots$$

é uma serie central, i.e., $P_n(G)/P_{n+1}(G)$ é no centro de $G/P_{n+1}(G)$.

(v) *Se G é finitamente gerado, então os subgrupos de índice finito de G formam um sistema fundamental de vizinhanças de $\{1\}$ em G.*

O seguinte teorema nos diz que a estrutura topológica é completamente determinada pela estrutura algébrica. É mostrado para grupos pro-p finitamente gerados.

Teorema 1.5.10. *Se G é um grupo pro-p finitamente gerado, então todo subgrupo de índice finito de G é aberto em G.*

Para mostrar o anterior teorema precisamos dos próximos dois resultados.

Lema 1.5.11. *Seja G é um grupo pro-p. Se K é um subgrupo de índice finito em G, então $|G : K|$ é uma p-ésima potência de p.*

Proposição 1.5.12. *Se G é um grupo pro-p finitamente gerado, então o subgrupo comutador $[G, G]$ é fechado em G.*

Demonstração do Teorema 1.5.10. É suficiente mostrar que todo subgrupo normal de índice finito em um grupo pro-p finitamente gerado é aberto, pois todo subgrupo de índice finito contem um subgrupo aberto normal de índice finito.

Seja K um subgrupo normal de G de índice finito em G. Vamos mostrar por indução sobre o índice de K em G que K é aberto em G. Seja $M = G^p[G, G]$. Pelo Lema 1.5.11 G/K é um p-grupo, pois $K \leq M < G$.

Escrevemos $G^{\{p\}} = \{g^p \mid g \in G\}$. Este conjunto é compacto, e portanto é fechado em G. Já que $G/[G, G]$ é abeliano, temos que $G^p[G, G] = G^{\{p\}}[G, G]$, e pela Proposição 1.5.12 $G^p[G, G]$ é também fechado.Assim $G^p[G, G]$ é igual a $\Phi(G)$, e portanto é aberto em G pela Proposição 1.5.8. Portanto M é aberto em G. Como todo subgrupo aberto de um grupo pro-p é finitamente gerado, concluímos que M é finitamente gerado. Assim concluímos que M é um grupo pro-p finitamente gerado, e como o índice de K em M é menor que em G, pela hipóteses indutiva segue que K é aberto em M. Como já mostramos, M é aberto em G, e assim K aberto em G.

□

É conhecido que o Teorema 1.5.10 para grupos profinitos em geral não é valido (exemplo [5, 4.2.12]). A questão se o Teorema 1.5.10 vale para os grupos profinitos finitamente gerados foi um problema aberto por quase 50 anos. Esse problema finalmente foi resolvido por Nikolov e Segal em 2007 em seu artigo [9]. Mais precisamente eles provam que os subgrupos de índice finito de grupos profinitos finitamente gerados são subgrupos abertos. Os grupos que satisfazem esta propriedade são chamados fortemente completos.

Capítulo 2

Grupos powerful e analíticos p-ádicos

A teoria de p-grupos powerful foi criada por A. Lubotzky e A. Mann em 1987. Os grupos powerful tem extensas aplicações na teoria de p-grupos finito, automorfismos de p-grupos finitos, grupos de posto finito, etc. Nós vamos usar os grupos powerful para estudar a estrutura analítica de grupos pro-p analíticos p-ádicos. Se pode dizer que os grupos powerful refletem as propriedades lineares de grupos pro-p analíticos p-ádicos.

2.1 Grupos finitos powerful

Seja G um p-grupo finito e seja $G^p = \langle x^p \mid x \in G \rangle$ o subgrupo gerado pelas p-potências de G. Não é difícil de ver que o subgrupo de Frattini de um p-grupo finito é dado por $\Phi(G) = G^p[G,G]$.

Definição 2.1.1.

1. Um p-grupo finito é powerful se p é ímpar e o grupo G/G^p é abeliano, ou se $p = 2$ e G/G^4 é abeliano.
2. Um subgrupo N de um p-grupo finito é powerfully embedded em G (denotamos por N p.e. G), se p é ímpar e $[N,G] \leq N^p$, ou se $p = 2$ e $[N,G] \leq N^4$.

Observe que um p-grupo finito G é powerful se e somente se G é p.e. em G. De fato, se p é ímpar então G/G^p é abeliano se e somente se $[G,G] \leq G^p$ se e somente se G é p.e. em G. Analogamente podemos tratar o caso $p = 2$.

Note que, se N é p.e. em G, então N é normal e powerful. De fato, $[N,G] \leq N^p \leq N$ implica que N é normal em G. No outro lado, $[N,N] \leq [N,G] \leq N^p$ implica que N/N^p é abeliano, e conseqüentemente N é powerful.

Proposição 2.1.2. *Seja G um p-grupo finito e $N \leq G$. Se N p.e. G, então N^p p.e. G.*

Lembramos que a p-serie central descendente de um grupo pro-p (p-grupo finito) G é definido por:

$$P_1(G) = G \text{ e } P_{n+1}(G) = \overline{P_n(G)^p[P_n(G), G]} \text{ para } n = 1, 2, ...$$

Lema 2.1.3. *Seja G um p-grupo finito powerful e seja $G_i = P_i(G)$.*

(i) Para cada i, G_i p.e. G e $G_{i+1} = G_i^p = \Phi(G_i)$.

(ii) Para cada i, o mapa $x \mapsto x^p$ induz um homomorfismo de G_i/G_{i+1} para G_{i+1}/G_{i+2}.

Demonstração. Vamos provar (i) por indução sobre i. Se $i = 1$, então $G_1 = G$ é powerful, e pela observação anterior G p.e. G. Agora suponha que G_i p.e G. Vamos mostrar que G_{i+1} p.e G.

Note que $G_{i+1} = G_i^p[G_i, G]$ e pela hipóteses indutiva $[G_i, G] \leq G_i^p$. Logo $G_{i+1} = G_i^p$. Pela Proposição 2.1.2 temos que se G_i é p.e. em G então G_i^p é p.e. em G. Por isso G_{i+1} é p.e. em G.

Por outro lado $G_i^p \leq \Phi(G_i) = G_i^p[G_i, G_i] \leq G_i^p[G_i, G] = G_{i+1} = G_i^p$, portanto $G_{i+1} = G_i^p = \Phi(G_i)$.

Para provar (ii), suponhamos inicialmente que $i = 1$. Então precisamos mostrar que o mapa

$$\Psi : G/G_2 \to G_2/G_3 \text{ onde } xG_2 \mapsto x^pG_3$$

é um homomorfismo. Note que se $x \in G$, então $x^p \in G^p$, e por isso $x^p \in G^p[G, G] = G_2$.

Vamos ver que $\Psi(xyG_2) = (xy)^pG_3 = x^py^pG_3 = \Psi(xG_2)\Psi(yG_2)$.

Se p=2, então pela formula 1.5.3, temos que

$$(xy)^2 \equiv x^2y^2[y, x] \mod [[G, G], G]$$

$$(xy)^2 \equiv x^2y^2[y, x] \mod [G, G]$$

$$(xy)^2 \equiv x^2y^2 \mod [G, G].$$

Como G é powerful, G/G^4 é abeliano. Então pelo Lema 1.5.1, $[G, G] \leq G^4$, e por tanto

$$(xy)^2 \equiv x^2y^2 \mod G^4.$$

Como $G^4 = (G^2)^2 = (G_2)^2 = G_3$, então $(xy)^2 \equiv x^2y^2 \mod G_3$, i.e., $(xy)^pG_3 = x^py^pG_3$ quando $p = 2$.

Quando p é ímpar, pela formula 1.5.3, temos que

$$(xy)^p \equiv x^py^p[y, x]^{p(p-1)/2} \mod [[G, G], G].$$

Como $[G,G] \leq G_2$ e G_2 p.e. G, segue que $[G_2, G] \leq G_2^p = G_3$. Logo $[[G,G],G] \leq G_3$ e portanto

$$(xy)^p \equiv x^p y^p [y,x]^{p(p-1)/2} \mod G_3.$$

Agora come $[y,x]^{(p-1)/2} \in [G,G]$, temos que $[y,x]^{(p-1)/2} \in G^p[G,G] = G_2$, e portanto $[y,x]^{p(p-1)/2} \in G_2^p = G_3$. Assim

$$(xy)^p \equiv x^p y^p \mod G_3, \text{ i.e.,}$$

$$(xy)^p G_3 = x^p y^p G_3.$$

Assim, provamos que se G é powerful, então o mapa $x \mapsto x^p$ induz um homomorfismo

$$\Psi : P(G)/P_2(G) \to P_2(G)/P_3(G).$$

Agora lembramos que $P_i(G) = G_i$. Como G_i p.e. G, temos que G_i é powerful. Tomando $G = G_i$ e observando que $G_{i+1} = P_2(G_i)$ e $G_{i+2} = P_3(G_i)$, obtemos o resultado para $i > 1$.

□

Lema 2.1.4. *Se $G = \langle a_1, ..., a_d \rangle$ é um p-grupo finito powerful, então $G^p = \langle a_1^p, ..., a_d^p \rangle$.*

Demonstração. Da prova do lema anterior podemos concluir que a função $x \mapsto x^p$ é um homomorfismo modulo G_3. Logo, se $x \in \langle a_1, ..., a_d \rangle$, então $x^p \in \langle a_1^p, ..., a_d^p \rangle \mod G_3$. Assim $G^p = \langle a_1^p, ..., a_d^p \rangle G_3$. Pela parte (i) do lema anterior temos que $G_3 = \Phi(G^p)$. Portanto $G^p = \langle a_1^p, ..., a_d^p \rangle \Phi(G^p)$. Como o subgrupo de Frattini é formado pelos não geradores, concluímos que $G^p = \langle a_1^p, ..., a_d^p \rangle$. □

Proposição 2.1.5. *Se G é um p-grupo powerful, então todo elemento de G^p é uma p-potência de algum elemento de G, i.e., $G^p = \{x^p \mid x \in G\}$.*

Demonstração. Argumentamos por indução sobre $|G|$. Se $|G| = 1$, então $G^p = \{1\}$. Suponha que a afirmação seja valida para todo grupo de ordem menor que G. Seja $g \in G^p$. Como a função $\phi : G/G_2 \to G_2/G_3$ dada por $xG_2 \mapsto x^p G_3$ é sobrejetiva, existe $x \in G$ tal que $x^p G_3 = gG_3$. Logo existe $y \in G_3$ tal que $g = x^p y$. Tomando $H = \langle x, G^p \rangle$, temos que H é powerful. Como $y \in G_3 = G_2^p = (G^p)^p \leq H^p$ e $x^p \in H^p$, segue que $g \in H^p$. Se $H \neq G$, então pela hipótese indutiva g é uma p-potência de algum elemento de $H \leq G$. No outro lado, se $H = G$, então $G = \langle x, \Phi(G) \rangle$. Logo $G = \langle x \rangle$, e por isso todo elemento de G^p é uma p-potência de algum elemento em G. □

Teorema 2.1.6. *Seja $G = \langle a_1, ..., a_d \rangle$ um p-grupo finito powerful e seja $G_i = P_i(G)$ para cada i.*

(i) G_i *p.e.* G.

(ii) $G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ *para cada* $k \geq 0$.

(iii) $G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \left\langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}} \right\rangle$.

(iv) Para cada i *e* k *o mapa* $x \mapsto x^{p^k}$ *induz um homomorfismo de* G_i/G_{i+1} *para* G_{i+k}/G_{i+k+1}.

Teorema 2.1.7. *Se* G *é um p-grupo finito powerful e* $H \leq G$*, então* $d(H) \leq d(G)$.

Demonstração. [6, Teorema 11.18] Seja $E_i = G^{p^i}/G^{p^{i+1}}$, E é um p-grupo abeliano elemental de posto $\leq d(G)$. Cada E_i pode ser visto como um espaço vectorial de dimensão $\leq d(G)$ sobre o corpo $\mathbb{F}_p$. Para um subgrupo arbitrário $H \leq G$, nos construímos um conjunto gerador de H por indução com elementos em $(H \cap G^{p^i})\ G^{p^{i+1}}$. Denotemos por V_i o grupo $(H \cap G^{p^i})G^{p^{i+1}}/G^{p^{i+1}}$ enxergado como um subespaço vetorial de E_i.

Escolhemos $h_1, \ldots, h_{n_1}$ em H tal que suas imagens em G/G^p formam uma base de $V_0 = HG^p/G^p$. Note que a $\dim(E_0/V_0) = d - n_1$.

Suponha que nós construímos elementos $h_1, h_2, \ldots, h_{n_1} \in H \cap G^{p^0}$, e elementos

$$h_{n_1+1}, \ldots, h_{n_2} \in H \cap G^{p^1}, \ldots, h_{n_{k-1}+1}, \ldots, h_{n_k} \in H \cap G^{p^{k-1}}$$

tal que as imagens de $h_1^{p^{k-1}}, \ldots, h_{n_1}^{p^k}, h_{n_1+1}^{p^{k-1}}, \ldots, h_{n_{k-1}+1}, \ldots h_{n_k}$ em E_{k-1} geram V_{k-1}, e $\dim(E_{k-1}/V_{k-1}) \leq d - n_k$.

Seja W os subespaço de E_k que gera as imagens dos $h_1^{p^k}, \ldots, h_{n_1}^{p^k}, h_{n_1+1}^{p^{k-1}}, \ldots, h_{n_k}^p$ em E_k. Então a $\dim(E_k/W) \leq d - n_k$, porque tomando p-ésima potências induzem um homomorfismo de E_{k-1}/V_{k-1} sobre E_k/W. Escolhemos elementos $h_{n_k+1}, \ldots, h_{n_{k+1}} \in H \cap G^{p^k}$ tal que suas imagens formam uma base de V_k/W. Então $\dim(E_k/V_k) = \dim(E_k/W) - (n_{k+1} - n_k) \leq d - n_{k+1}$. Completando a construção.

A anterior construção termina atingindo o subgrupo identidade $G^{p^\epsilon} = 1$ onde p^ϵ é a potência de G. A ultima desigualdade pra dimensão, $d - n_\epsilon \geq \dim(E_{\epsilon-1}/V_{\epsilon-1}) \geq 0$, implica que $n_\epsilon \leq d$, que é o número total de elementos h_j construídos e que a lo sumo são d. Provamos por indução sobre o expoente de G que os h_j geram H. Para $e = 1$ a afirmação é obvia. Para $e > 1$, nós temos $H \leq \langle h_1, \ldots, h_{n_\epsilon} \rangle\, G^{p^{\epsilon-1}}$ por hipóteses indutiva. Já que $\langle h_1, \ldots, h_{n_\epsilon} \rangle \leq H$.

□

O posto de um grupo finito é definido por

$$rk(G) = \sup\{d(H) \mid H \leq G\}.$$

Assim, podemos reescrever o teorema anterior na form seguinte: Se G é um p-grupo finito powerful, então $rk(G) = d(G)$.

Definição 2.1.8. Seja G um p-grupo finito. Dado um inteiro $r > 0$, denotamos por $V(G, r)$ a intersecção dos núcleos dos homomorfismos de G para $GL(r, p) = GL_r(\mathbb{F}_p)$.

Claramente, $V(G, r)$ é um subgrupo de G.

Lema 2.1.9. *[8, Lema 6.1.13] Seja G um p-grupo finito.*

(i) Se $N \lhd G$, então $V(G, r)N/N \leq V(G/N, r)$.

(ii) $V(G, r)$ é um subgrupo característico de G.

(iii) Se $N \lhd G$ e $d(N) \leq d$, então $[N, V(G, d)] \leq \Phi(N)$. Além disso, se $N \leq V(G, r)$, então $\Phi(N) = [N, V(G, d)]N^p$.

Teorema 2.1.10. *[8, Teorema 6.1.14] Seja G um p-grupo, r um inteiro positivo e $N \lhd G$ com $d(N) \leq r$.*

(i) Para p ímpar, se $N \leq V(G, r)$, então N p.e. $V(G, r)$.

(ii) Para $p = 2$, se $N \leq V(G, r)^2$, então N p.e. $V(G, 2)^2$.

Seja p um número primo fixo e G um p-grupo finito. A classe de $cla(G)$ é definida como o comprimento da serie central descendente, e a coclasse $cocla(G)$ é defina por $cocla(G) = n - cla(G)$, onde $|G| = p^n$. Leedham-Green e Newman introduziram o conceito de coclasse de um p-grupo finito em 1980 e formularam as conhecidas "conjeturas coclasse". Uma delas a "conjetura A"fala que: Todo p-grupo tem um subgrupo normal de coclasse 2 com índice dependendo só de p e sua coclasse. Shalev em 1994 demonstro esta conjetura como uma aplicação da teoria de grupos powerful. Esta e outras aplicações podem ser vistas no livro [8].

2.2 Grupos pro-p powerful

Neste seção desenvolvemos a teoria de grupos pro-p powerful, analogamente a como em p-grupos powerful. Muitos dos resultados se seguem direto do sues análogos para p-grupos powerful. O teorema mais importante é a caracterização de grupos pro-p de posto finito em termos de subgrupos powerful. A teoria de grupos pro-p powerful e grupos pro-p uniformes corresponde com os capítulos 3 e 4 do livro [3, Dixon].

Definição 2.2.1. Um grupo pro-p é dito powerful se

(i) p é um número ímpar e $G/\overline{G^p}$ é abeliano, ou

(ii) $p = 2$ e $G/\overline{G^4}$ é abeliano.

Um subgrupo aberto $N \leq_o G$ é powerfully embedded em G (denotado por N p.e. G), se p ímpar e $[N, G] \leq \overline{N^p}$ ou se $p = 2$ e $[N, G] \leq \overline{N^4}$.

Lema 2.2.2. *Seja G um grupo pro-p e $N \leq_o G$. Então N p.e G se e somente se NK/K p.e. G/K para todo subgrupo normal aberto K de G.*

Proposição 2.2.3. *Um grupo topológico G é um grupo pro-p powerful se e somente se é o limite inverso de um sistema inverso de p-grupos finitos powerful onde todos os mapas são sobrejetivos.*

Proposição 2.2.4. *Seja G um grupo pro-p, finitamente gerado e powerful. Então os elementos de G^p são p-potências de elementos de G, e $G^p = \Phi(G)$ é aberto em G. Se $p = 2$, então G^4 é aberto em G.*

Proposição 2.2.5. *Seja G um grupo pro-p, powerful e $G = \langle a_1, \ldots, a_d \rangle$. Então:*

(i) G_i p.e. G.

(ii) $G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$, para cada $k \geq 0$, e em particular $G_{i+1} = \Phi(G_i)$.

(iii) $G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \overline{\left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle}$.

(iv) O mapa $x \mapsto x^{p^k}$ induz um epimorfismo de $G_i/G_{i+1} \to G_{i+k}/G_{i+k+1}$.

Teorema 2.2.6. *Seja G um grupo pro-p, finitamente gerado e powerful, e seja $H \leq_c G$. Então $d(H) \leq d(G)$.*

Analogamente a definição 2.1.8 quando G é um grupo pro-p finitamente gerado denotamos por $V(G, r)$ a intersecção dos núcleos dos homomorfismos de G para o conjunto $GL(r, p)$ matrizes invertíveis de tamanho $r \times r$ com entradas em $\mathbb{F}_p$. E temos o resultado análogo que para p-grupos.

Proposição 2.2.7. *Sejam G um grupo pro-p finitamente gerado, r um inteiro positivo e $N \lhd G$ tal que $d(N) \leq r$.*

(i) Para p ímpar, se $N \leq V(G, r)$, então N p.e. $V(G, r)$.

(ii) Para $p = 2$, se $N \leq V(G, r)^2$, então N p.e. $V(G, r)^2$.

Teorema 2.2.8. *Seja G um grupo pro-p finitamente gerado e suponha que $r = \sup_{N \lhd_o G}\{d(N)\}$ seja finito. Então G contem um subgrupo aberto powerful característico de índice finito.*

Proposição 2.2.9. *Seja G um grupo profinito e sejam*

$r_1 = \sup\{d(H) \mid H \leq_c G\}$,

$r_2 = \sup\{d(H) \mid H \leq_c G \text{ e } d(H) < \infty\}$,

$r_3 = \sup\{d(H) \mid H \leq_o G\}$ *e*

$r_4 = \sup\{rk(G/H) \mid H \lhd_o G\}$

Então $r_1 = r_2 = r_3 = r_4$.

Definição 2.2.10. Seja G um grupo profinito. Definimos o posto $rk(G)$ de G , como o valor comum de r_1, r_2, r_3 e r_4.

Teorema 2.2.11. *Seja G é um grupo pro-p. Então G tem posto finito se e somente se G é finitamente gerado, e contem um subgrupo aberto powerful.*

Como vimos no anterior teorema grupos pro-p de posto finito possuem subgrupos abertos com propriedades especiais (subgrupos powerful), mas ainda podemos garantir a existência de subgrupos aberto com propriedades muito mais fortes, chamados grupos powerful uniformes. E as vantagens de grupos powerful uniformes é que suas operações de grupos podem ser suavizadas para dar uma nova estrutura análoga a grupos abelianos. Mas precisamente permite ver os grupos powerful uniformes finitamente gerados como $\mathbb{Z}_p$-módulos.

Definição 2.2.12. Um grupo pro-p G é dito powerful uniforme (ou uniforme) se G é finitamente gerado, powerful e $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$ para cada $i \geq 2$.

Como vimos no teorema 2.2.5 as condições de um grupos powerful uniforme implicam que o mapa $x \mapsto x^{p^k}$ induz isomorfismo de $G_i/G_{i+1} \to G_{i+k}/G_{i+k+1}$.

Teorema 2.2.13. *Seja G um grupo pro-p powerful finitamente gerado. Então $P_k(G)$ é uniforme para k suficientemente grande.*

O anterior teorema é fundamental para garantir a existência de subgrupos powerful uniformes.

Corolário 2.2.14. *Um grupo pro-p de posto finito contem um subgrupo aberto característico que é uniforme.*

Proposição 2.2.15. *Seja G um grupo pro-p powerful finitamente gerado. Então as seguintes afirmações são equivalentes.*

(i) G é uniforme.

(ii) $d(P_i(G)) = d(G)$ para todo $i \geq 1$.

(iii) $d(H) = d(G)$ para todo subgrupo aberto powerful H de G.

Lema 2.2.16. *Se H e K são subgrupos abertos uniformes de algum grupo pro-p G, então $d(H) = d(K)$.*

Definição 2.2.17. Seja G um grupo pro-p de posto finito. Então a dimensão de G é definida por

$$\dim(G) = d(H),$$

onde H é qualquer subgrupo aberto uniforme de G.

Pelo lema anterior a definição de dimensão é independente do subgrupo aberto uniforme de G .

Teorema 2.2.18. *Seja G um grupo pro-p de posto finito e $N \lhd_c G$. Então*

$$\dim(G) = \dim(N) + \dim(G/N).$$

Na seguinte seção vamos a definir o conceito de dimensão de uma variedade analítica p-ádica, a anterior definição coincidira com esta.

Seja G um grupo profinito. Dízimos que G tem quase uma propriedade **P** se G tem um subgrupo aberto normal H tal que H satisfaz a propriedade **P**.

Observação 2.2.19. Seja G um grupo pro-p. Então

(i) G é finitamente gerado e quase powerful.

(ii) G é finitamente gerado e quase uniforme.

e a $\dim(G)$ é igual:

(i) $d(H)$ onde H é qualquer subgrupo aberto uniforme de G.

(ii) $\dim(N) + \dim(G/N)$ onde N é qualquer subgrupo normal fechado de G.

E proximamente veremos que também é igual a:

(iii) $\displaystyle\lim_{k\to\infty} \frac{\log_p |G : G^{p^k}|}{k}$

(iv) A dimensão de um carta que da ha G estrutura de grupo analítico p-ádico.

Vejamos agora um exemplo de um grupo pro-p de posto finito que possui um subgrupo aberto uniforme.

Exemplo 2.2.20. Seja $\Gamma = GL_d(\mathbb{Z}_p)$ o grupo de matrizes invertíveis de tamanho $d \times d$ com entradas em $\mathbb{Z}_p$. Então $GL_d(\mathbb{Z}_p)$ é um grupo profinito. De fato,

$$GL_d(\mathbb{Z}_p) = \lim_{\leftarrow} GL_d(\mathbb{Z}/p^i\mathbb{Z}).$$

Uma base de vizinhanças da identidade é dada pelos subgrupos

$$\Gamma_i = \{\gamma \in \Gamma \mid \gamma \equiv 1_d \pmod{p^i}\},$$

para todo $i \geq 0$. Ademais, temos que

$$|\Gamma : \Gamma_1| = (p^d - 1)(p^d - p) \dots (p^d - p^{d-1}) \text{ e}$$

$$|\Gamma_1 : \Gamma_i| = p^{d^2(i-1)} \text{ para } i \geq 1.$$

Lema 2.2.21. *Se p é ímpar e $n \geq 2$, ou $p = 2$ e $n \geq 3$, então todo elemento de Γ_n é uma p-potência de um elemento de Γ_{n-1}.*

Demonstração. Afirmamos que para cada $a \in M_d(\mathbb{Z}_p)$ nos podemos resolver

$$1 + p^n a = (1 + p^{n-1}x)^p$$

com $x \in M_d(\mathbb{Z}_p)$. A solução é uma aproximação sucessiva. Note que $(1 + p^{n-1}a)^p \equiv 1 + p^n a \pmod{p^{n+1}}$. Pegamos $x_1 = a$, e suponhamos por indução que para $r \geq 1$ existe uma matrix x_r, comutando com a, tal que $(1 + p^{n-1}x_r)^p \equiv 1 + p^n a \pmod{p^{n+r}}$. Digamos

$$(1 + p^{n-1}x_r)^p = 1 + p^n a + p^{n+r}c.$$

Agora seja

$$z = (1 + p^{n-1}x_r)^{-(p-1)}c,$$

e seja $x_{r+1} = x_r - p^r z$. Note que x_r comuta com c, portanto com z, e x_{r+1} comuta com a. Um calculo direto mostra que

$$(1 + p^{n-1}x_{r+1})^p \equiv 1 + p^n a \pmod{p^{n+r+}}.$$

Assim nos obtemos um seqüencia (x_r) em $M_d(\mathbb{Z}_p)$, que tem limite x que satisfaz

$$1 + p^n a = (1 + p^{n-1}x)^p.$$

□

Proposição 2.2.22. *Para cada i, seja $\Gamma_i = \{\gamma \in GL_s(\mathbb{Z}_p) \mid \gamma \equiv 1_d(\mod p^i)\}$. Seja $G = \Gamma_1$ se p é ímpar e seja $G = \Gamma_2$ se p é par. Então G é um grupo pro-p uniforme e* $\dim(G) = rk(G) = d(G) = d^2$. *Além disso, $P_i(G) = \Gamma_{i+\epsilon}$, onde $\epsilon = 0$, se $p \neq 2$ e $\epsilon = 1$, se $p = 2$.*

Demonstração. Note que $P_1(G) = G = \Gamma_{1+\epsilon}$ por definição. Suponha que $r \geq 1$ e $P_r(G) = \Gamma_{r+\epsilon}$. Não é difícil ver que $P_r(G)^p[P_r(G), G] \leq \Gamma_{r+1+\epsilon}$. Pelo lema anterior temos que $\Gamma_{r+1+\epsilon} \leq \Gamma_{r+\epsilon}^p = P_r(G)^p$. Como $\Gamma_{r+1+\epsilon}$ é um subgrupo fechado de G, segue que $P_{r+1}(G) = \Gamma_{r+1+\epsilon}$.

Assim nos temos por indução que $P_i(G) = \Gamma_{i+\epsilon}$ para todo i. Além disso, $P_{i+1}(G) = P_i(G)^p$ para todo i. Pegando $i = 1$, nos vemos que G é powerful (quando $p = 2$, note que $[\Gamma_2, \Gamma_2] \leq \Gamma_4 \leq \Gamma_2^4$). Como $P_2(G) = \Gamma_{2+\epsilon}$ é aberto em G, Teorema 1.4.5 mostra que G é finitamente gerado. Como $|\Gamma_i : \Gamma_{i+1}| = p^{d^2}$ é constante para todo $i \geq 1$, segue que G é uniforme. Finalmente, já que $G/\Phi(G) = \Gamma_{1+\epsilon}/\Gamma_{2+\epsilon}$ é um grupo abeliano elementar de ordem p^{d^2}, temos que $d(G) = d(G/\Phi(G)) = d^2$. Logo, $\dim(G) = rk(G) = d(G) = d^2$. □

2.3 Grupos analíticos p-ádicos

Seja $\mathbb{Q}_p$ o corpo de números p-ádicos. Em outras palavras $\mathbb{Q}_p$ é o corpo de frações do anel de inteiros p-ádicos $\mathbb{Z}_p$.

Para falar sobre os grupos analíticos p-ádicos precisamos desenvolver a noção de função analítica e de variedade analítica sobre $\mathbb{Q}_p$.

Escrevemos $\mathbf{X} = (X_1, \ldots, X_r)$ para denotar a dependência das variáveis não comutativas $X_1, \ldots, X_r$. E $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, onde cada $\alpha_i \in \mathbb{N}$ para $1 \leq i \leq r$. Então escrevemos $\mathbf{X}^\alpha$ para denotar o produto

$$\mathbf{X}^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_r^{\alpha_r}.$$

Definição 2.3.1. O anel de series de potências nas variáveis $X_1, \ldots, X_r$ é o conjunto de series

$$F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^r} c_\alpha \mathbf{X}^\alpha$$

onde $c_\alpha \in \mathbb{Q}_p$ para cada $\alpha \in \mathbb{N}^r$. Denotado por $\mathbb{Q}_p[[\mathbf{X}]]$ ou $\mathbb{Q}_p[[X_1, \ldots, X_r]]$.

Iniciamos considerando funções sobre $\mathbb{Z}_p$. Um elemento $\mathbf{x} \in \mathbb{Q}_p^r$ é da forma $\mathbf{x} = (x_1, \ldots, x_r)$, onde $x_i \in \mathbb{Q}_p$, para $1 \leq i \leq r$. Analogamente $\mathbf{x} \in \mathbb{Z}_P^r$.

Para cada $\mathbf{y} \in \mathbb{Z}_p^r$ e $h \in \mathbb{N}$ pegamos

$$B(\mathbf{y}, p^{-h}) = \{\mathbf{z} \in \mathbb{Z}_p^r \mid |\mathbf{z}_i - \mathbf{y}_i|_p \leq p^{-h} \text{ para } i = 1, ...r\}$$

$$= \{\mathbf{y} + p^h\mathbf{x} \mid x \in \mathbb{Z}_p^r\}.$$

Definição 2.3.2. Seja V um subconjunto aberto não vazio de $\mathbb{Z}_p^r$ e

$$f = (f_1, \ldots, f_s)$$

uma função de $f : V \to \mathbb{Z}_p^s$.

(i) Se diz que f é analítica em $\mathbf{y} \in V$, se existe $h \in \mathbb{N}$ com $B(\mathbf{y}, p^{-h}) \subset V$ e series de potenciais $F_i(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]](i = 1, \ldots, s)$ tal que

$$f_i(\mathbf{y} + p^h\mathbf{x}) = F_i(\mathbf{x}) \text{ para todo } \mathbf{x} \in \mathbb{Z}_p^r.$$

(ii) Se diz f analítica em V se é analítica em todo ponto de V.

Composição de funções analíticas é analítica.

Definição 2.3.3. (i) Seja X um espaço topológico e U um aberto não vazio de X. Um triple (U, ϕ, n) é uma carta sobre X se ϕ é um homeomorfismo de U sobre um subconjunto aberto de $\mathbb{Z}_p^n$ para algum $n \in \mathbb{N}$. A dimensão da carta é n. A carta (U, ϕ, n) é global se $U = X$.

(ii) Duas cartas (U, ϕ, n) e (V, ψ, m) sobre X são compatíveis se os mapas $\psi\phi^{-1}|_{\phi(U\cap V)}$ e $\phi\psi^{-1}|_{\psi(U\cap V)}$ são funções analíticas.

(iii) Um atlas sobre um espaço topológico X é um conjunto de cartas compatíveis duas a duas, que formam uma cobertura de X.

Definição 2.3.4. Um espaço topológico X tem estrutura de variedade analítica p-ádica se existe um atlas compatível com X.

Exemplo 2.3.5. (i) Seja X um espaço topológico discreto. Então X é uma variedade analítica p-ádica com estrutura determinada pelo atlas $\{(\{x\}, \phi_x, 0) \mid x \in X\}$, onde $\phi_x : x \mapsto 0$.

(ii) Seja $\mathbb{Q}_p^n$. Consideremos os mapas $\phi_i : p^{-i}\mathbb{Z}_p^n \to \mathbb{Z}_p^n$ definidos por $\phi_i : x \mapsto p^i x$ para cada $i \in \mathbb{N}$. Então o conjunto $A = \{(p^{-i}\mathbb{Z}_p^n, \phi_i, n) \mid i \in \mathbb{N}\}$ é um atlas sobre X, já que $\{p^{-1}\mathbb{Z}_p^n \mid i \in \mathbb{N}\}$ são abertos que cobrem $\mathbb{Q}_p^n$. Este atlas da uma estrutura de variedade analítica p-ádica a X. Em particular este exemplo nós diz que na definição de atlas o subconjunto aberto de $\mathbb{Z}_p$ pode ser trocado por um aberto de $\mathbb{Q}_p$ e vamos obter as mesmas variedades analíticas p-ádicas.

(iii) Seja $X = GL_n(\mathbb{Q}_p)$ o conjunto de matrizes invertíveis com entradas em $\mathbb{Q}_p$. Consideremos X com a topologia induzida quando é visto como subespaço de $M_n(\mathbb{Q}_p) = Q_p^{n^2}$ (conjunto de matrizes com entradas em $\mathbb{Q}_p$), $Q_p^{n^2}$ é uma variedade analítica p-ádica com estrutura dada no item (ii) $A = \{(p^{-i}\mathbb{Z}_p^{n^2}, \phi_i, n^2) \mid i \in \mathbb{N}\}$. O atlas A induce um atlas sobre X dada por $B = \{X \cap (p^{-i}\mathbb{Z}_p^{n^2}, \phi_i, n^2) \mid i \in \mathbb{N}\}$. Portanto X é também uma variedade analítica p-ádica.

(iv) Seja G um grupo pro-p uniforme gerado topologicamente por o conjunto $\{a_1, \ldots, a_d\}$, então se pode mostrar que o mapa $\phi : G \to \mathbb{Z}_p^d$ dado por $\phi(x) = (\lambda_1, \ldots, \lambda_d)$, onde $x = a_1^{\lambda_1}, \ldots, a_d^{\lambda_d}$ é um homeomorfismo. Assim $A = \{(G, \phi, d)\}$ é um atlas global. Portanto todo grupo pro-p uniforme tem estrutura de variedade analítica p-ádica.

Definição 2.3.6. Um grupo topológico G é analítico p-ádico se G possui estrutura de uma variedade analítica p-ádica com as seguintes propriedades:

(i) a função $f : G \times G \to G$ dada por $(x, y) \mapsto xy$ é analítica;

(ii) a função $i : G \to G$ dada por $x \mapsto x^{-1}$ é analítica.

Teorema 2.3.7. *[3, Teorema 8.32] Seja G um grupo topológico. Então G é um grupo analítico p-ádico se e somente se G contém um subgrupo aberto que é um grupo pro-p uniforme.*

Corolário 2.3.8. *Um grupo topológico G é um grupo analítico p-ádico se e somente se G contém um subgrupo aberto que é um grupo pro-p de posto finito.*

Capítulo 3

Dimensão de Hausdorff

O conceito de dimensão de Hausdorff é fundamental para a geometria fractal, originalmente se define sobre os reais. Nós vamos extender este conceito a grupos topológicos com uma métrica. Logo vamos definir uma métrica sobre um grupo profinito, e dar um jeito de calcular a dimensão de Hausdorff com respeito dessa métrica.

Vamos supor que temos um grupo topológico métrico G, munido com uma métrica ρ.

Dado um conjunto não vazio $U \subseteq G$, definimos o **diâmetro** de U como $\operatorname{diam}(U) = \sup\{\rho(x,y) \ : \ x, y \in U\}$.

Seja $F \subseteq G$. Seja $\{U_i\}_{i=1}^{\infty}$ uma família enumerável de conjuntos que cubra F e com diâmetro menor ou igual do que δ, i.e. $F \subseteq \bigcup_{i=1}^{\infty} U_i$ com $0 \leq \operatorname{diam}(U_i) \leq \delta$ para cada i. Dizemos que tal $\{U_i\}_{i=1}^{\infty}$ é uma δ-cobertura de F.

Suponhamos que s é um número positivo fixo. Para cada $\delta > 0$, definimos

$$\mathcal{H}^s_\delta(F) = \inf \left\{ \sum_{i=1}^{\infty} \operatorname{diam}(U_i)^s \ : \ \{U_i\}_{i=1}^{\infty} \text{ é uma } \delta - \text{cobertura de } F \right\}. \tag{3.1}$$

Quando δ decresce o número de coberturas possíveis se reduce. Portanto, $\mathcal{H}^s_\delta(F) \leq \mathcal{H}^s_{\delta'}(F)$ para $\delta \leq \delta'$. Logo o seguinte limite existe:

$$\mathcal{H}^s(F) = \lim_{\delta \to 0} \mathcal{H}^s_\delta(F), \tag{3.2}$$

mas pode ser zero ou infinito. Note que $\mathcal{H}^s$ é uma medida externa, conhecida como medida de Hausdorff s-dimensional.

Como na equação (3.2) $\delta \to 0$, vamos supor que $\delta < 1$. Se $s < t$, então

$$0 \leq \operatorname{diam}(U_i) \leq \delta < 1 \Rightarrow \operatorname{diam}(U_i)^t < \operatorname{diam}(U_i)^s \text{ e } \operatorname{diam}(U_i)^{t-s} \leq \delta^{t-s}.$$

Logo temos que

$$\mathcal{H}^t_\delta(F) = \inf\left\{\sum_{i=1}^{\infty} \mathrm{diam}(U_i)^t \ : \ \{U_i\}_{i=1}^{\infty} \text{ é uma } \delta - \text{cobertura de } F\right\}$$

$$= \inf\left\{\sum_{i=1}^{\infty} \mathrm{diam}(U_i)^{t-s}\mathrm{diam}(U_i)^s \ : \ \{U_i\}_{i=1}^{\infty} \text{ é uma } \delta - \text{cobertura de } F\right\}$$

$$\leq \delta^{t-s} \inf\left\{\sum_{i=1}^{\infty} \mathrm{diam}(U_i)^s \ : \ \{U_i\}_{i=1}^{\infty} \text{ é uma } \delta - \text{cobertura de } F\right\} = \delta^{t-s}\mathcal{H}^s_\delta(F).$$

Portanto, $\mathcal{H}^t_\delta(F) \leq \delta^{t-s}\mathcal{H}^s_\delta(F)$. Fazendo $\delta \to 0$, obtemos que se $\mathcal{H}^s_\delta(F) < \infty$, então $\mathcal{H}^t_\delta(F) = 0$, provando o seguinte lema.

Lema 3.0.1. *Se $\mathcal{H}^s(F) < \infty$ e $s < t$, então $\mathcal{H}^t(F) = 0$.*

Definimos a **dimensão de Hausdorff** de um subconjunto $F \subseteq G$ como

$$\dim_H(F) = \sup\{s \mid \mathcal{H}^s(F) = \infty\} = \inf\{s \mid \mathcal{H}^s(F) = 0\}.$$

A dimensão de Hausdorff satisfaze o seguinte:

(**Monotonia**) Se $E \subseteq F$, então $\dim_H(E) \leq \dim_H(F)$, pois $\mathcal{H}^s(E) \leq \mathcal{H}^s(F)$.

(**Estabilidade contável**) Se $\{F_i\}_{i=1}^{\infty}$ é uma familia enumerável de subconjuntos de G, então

$$\dim_H(\bigcup_{i=1}^{\infty} F_i) = \sup_{1\leq i\leq\infty}\{\dim_H(F_i)\}.$$

De fato, pela monotonia $\dim_H(F_i) \leq \dim_H(\bigcup_{i=1}^{\infty} F_i)$ para todo i. Logo $\sup_{1\leq i\leq\infty}\{\dim_H(F_i)\} \leq \dim_H(\bigcup_{i=1}^{\infty} F_i)$. Para provar a outra desigualdade basta mostrar que se $\sup_{1\leq i\leq\infty}\{\dim_H(F_i)\} < s$, então $\dim_H(\bigcup_{i=1}^{\infty} F_i) \leq s$. Suponha que $\dim_H(F_i) < s$ para cada i. Então $\mathcal{H}^s(F_i) = 0$ e logo $\mathcal{H}^s(\bigcup_{i=0}^{\infty} F_i) \leq \sum_{i=0}^{\infty} \mathcal{H}^s(F_i) = 0$. Portanto, $\dim_H(\bigcup_{i=0}^{\infty} F_i) \leq s$.

Existem duas outras definições de dimensão chamadas **dimensões de caixas**. Seja F um subconjunto não vazio e limitado de um espaço métrico X. Seja $N_\delta(F)$ o menor número de conjuntos com diâmetro no máximo δ que cobrem F. Definimos

$$\underline{\dim}_B(F) = \liminf_{\delta\to 0} \frac{\log(N_\delta(F))}{-\log(\delta)},$$

$$\overline{\dim}_B(F) = \limsup_{\delta\to 0} \frac{\log(N_\delta(F))}{-\log(\delta)}.$$

A dimensão de Hausdorff é em geral diferente que as dimensões de caixas. Mas sempre temos uma desigualdade:

$$\dim_H(F) \leq \underline{\dim}_B(F).$$

De fato,

$$\mathcal{H}^s_\delta \leq N_\delta(F)\delta^s.$$

Se $1 < \mathcal{H}^s(F) = \lim_{\delta \to 0} \mathcal{H}^s_\delta(F)$, então $\mathcal{H}^s_\delta(F) > 1$ e $\log(N_\delta(F)) + s\log(\delta) > 0$ para todo δ. Se δ é suficientemente pequeno, então

$$s \leq \liminf_{\delta \to 0} \frac{\log(N_\delta(F))}{-\log(\delta)}.$$

Assim

$$\dim_H(F) \leq \underline{\dim}_B(F) \leq \overline{\dim}_B(F).$$

Vejamos que no caso de grupos profinitos podemos recuperar a igualdade. Vamos então definir uma métrica sobre um grupo profinito e posteriormente a dimensão de Hausdorff sobre estes.

Chamamos uma **filtração** $\{G_n\}_{n=0}^{\infty}$ a uma cadeia descendente de subgrupos normais abertos que formam uma base de vizinhanças da identidade.

Seja G um grupo profinito junto com uma filtração $\{G_n\}_{n=0}^{\infty}$:

$$G_0 \geq G_1 \geq G_2 \geq \dots$$

Definimos uma métrica sobre G por

$$\rho(x, y) = \inf\{|G : G_n|^{-1} \mid xy^{-1} \in G_n\}.$$

Afirmamos que ρ satisfaz as propriedades de uma métrica:

1. $\rho(x, y) = 0 \Leftrightarrow xy^{-1} \in G_n$ para todo $n \Leftrightarrow xy^{-1} \in \{1\} \Leftrightarrow x = y$.

2. $\rho(x, y) = \inf\{|G : G_n|^{-1} \mid xy^{-1} \in G_n\} = \inf\{|G : G_n|^{-1} \mid yx^{-1} \in G_n\} = \rho(y, x)$.

3. Sejam $x, y, z \in G$. Para cada $\epsilon > 0$, existem $n, m \in \mathbb{N}$ tal que $xz^{-1} \in G_n$, $zy^{-1} \in G_m$, e

   $$\frac{1}{|G : G_n|} \leq \rho(x, z) + \frac{\epsilon}{2} \quad \text{e} \quad \frac{1}{|G : G_m|} \leq \rho(z, y) + \frac{\epsilon}{2}.$$

   Suponha que $n \geq m$. Então $G_n \leq G_m$; logo $xy^{-1} \in G_m$ e

   $$\frac{1}{|G : G_m|} \leq \frac{1}{|G : G_m|} + \frac{1}{|G : G_n|} \leq \rho(x, z) + \rho(z, y) + \epsilon.$$

   Portanto, $\rho(x, y) \leq \rho(x, z) + \rho(z, y)$.

Pode se mostrar facilmente que os abertos gerados por esta métrica coincidem com os abertos da topologia de G. Logo todo grupo profinito que admite uma filtração é metrisavel.

Note que $0 \leq \rho(x,y) \leq 1$ para todos $x, y \in G$, e qualquer bola de raio ϵ com centro x é uma classe lateral à esquerda,

$$B_\epsilon(x) = \{y \in G \mid \rho(x,y) \leq \epsilon\} = G_n x \text{ com } n \text{ o menor número tal que } \frac{1}{|G : G_n|} \leq \epsilon.$$

Logo tem sentido só considerar raios da forma $\rho = |G : G_n|^{-1}$. Agora estamos prontos para definir dimensão de Hausdorff por caixas sobre grupos profinitos.

Seja $H \leq_c G$. Então $H = \bigcup_{x \in H} G_n x$. Logo $N_\rho(H) = |HG_n : G_n|$, onde $\rho = |G : G_n|^{-1}$. Portanto,

$$\underline{\dim}_B(H) = \liminf_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|},$$

$$\overline{\dim}_B(H) = \limsup_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|}.$$

Notemos que se um grupo profinito é metrisavel então podemos definir a dimensão de Hausdorff da maneira convencional e como foi visto sempre vamos obter a desigualdade.

$$\dim_H(F) \leq \underline{\dim}_B(F) \leq \overline{\dim}_B(F).$$

Foi Abercrombie em seu artigo [1] que prova que já que grupos profinitos são compactos possuem uma única medida invariante (medida de Haar), e fazendo uso desta e a métrica para grupos profinitos exposta anteriormente, a dimensão de Hausdorff é análoga a dimensão sobre R. Além ele prova na [1, Proposicão 2.6] que a desigualdade $\underline{\dim}_B(H) \leq \dim_H(H)$, é valida em grupos profinitos, logo temos o seguinte teorema.

Teorema 3.0.2. *Seja G um grupo profinito com uma filtração $\{G_n\}_{n=0}^{\infty}$, e seja $H \leq_c G$. Então*

$$\dim_H(H) = \underline{\dim}_B(H) = \liminf_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|} = \liminf_{n\to\infty} \frac{\log |H : H \cap G_n|}{\log |G : G_n|}$$

Observação 3.0.3. Notamos que se G é infinito, então todo subgrupo aberto H tem dimensão de Hausdorff 1. Para ver isso, primeiro note que

$$\log |G : G_n| = \log(|G : HG_n||HG_n : G_n|) = \log |G : HG_n| + \log |HG_n : G_n|.$$

Como H é aberto, $|G : H| < \infty$ e $HG_n = H$ para todo n suficientemente grande. Logo $\log |G : G_n| = \log |G : H| + \log |HG_n : G_n|$ para todo n suficientemente grande. Agora segue facilmente que

$$\dim_H(H) = \lim_{n\to\infty} \frac{\log |H : H \cap G_n|}{\log |G : H| + \log |H : H \cap G_n|} = 1.$$

Notamos também que se H é finito, então dimensão de Hausdorff de H é 0.

Contudo, a dimensão de Hausdorff depende da filtração que tomamos para definir a métrica. De fato, se tomamos filtrações diferentes, obtemos valores diferentes da dimensão.

Exemplo 3.0.4. Seja $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$ e $H = \{0\} \oplus \mathbb{Z}_p \;\leq \mathbb{Z}_p \oplus \mathbb{Z}_p$. Então calculando a dimensão de Hausdorff com respeito a filtração $G_n = p^n\mathbb{Z}_p \oplus p^n\mathbb{Z}_p, n \geq 0$, obtemos $H \cap G_n = \{0\} \oplus p^n\mathbb{Z}_p$,

$$|H : H \cap G_n| = |\{0\} \oplus \mathbb{Z}_p : \{0\} \oplus p^n\mathbb{Z}_p| = p^n,$$

$$|G : G_n| = |\mathbb{Z}_p \oplus \mathbb{Z}_p : p^n\mathbb{Z}_p \oplus p^n\mathbb{Z}_p| = p^{2n}.$$

Portanto,

$$\dim_H(H) = \liminf_{n\to\infty} \frac{\log_p |H : H \cap G_n|}{\log_p |G : G_n|} = \liminf_{n\to\infty} \frac{\log_p p^n}{\log_p p^{2n}} = \frac{1}{2}.$$

Por outro lado, se calculamos a dimensão de Hausdorff com respeito a filtração $G_n = p^{2n}\mathbb{Z}_p \oplus p^n\mathbb{Z}_p, n \geq 0$, então obtemos

$$|H : H \cap G_n| = |\{0\} \oplus \mathbb{Z}_p : \{0\} \oplus p^n\mathbb{Z}_p| = p^n,$$

$$|G : G_n| = \left|\mathbb{Z}_p \oplus \mathbb{Z}_p : p^{2n}\mathbb{Z}_p \oplus p^n\mathbb{Z}_p\right| = p^{3n},$$

e

$$\dim_H(H) = \liminf_{n\to\infty} \frac{\log_p |H : H \cap G_n|}{\log_p |G : G_n|} = \liminf_{n\to\infty} \frac{\log_p p^n}{\log_p p^{3n}} = \frac{1}{3}.$$

Capítulo 4

Dimensão de Hausdorff para grupos pro-p

Como observamos anteriormente, podemos definir a dimensão de Hausdorff para grupos profinitos. Porém, a dimensão de Hausdorff é dependente da filtração que escolhêssemos para definir a métrica. No caso de grupos pro-p finitamente gerados a filtração $\{P_n(G)\}_{n=0}^{\infty}$ (pelo Teorema 1.5.9 forma uma vizinhança da identidade) é uma filtração natural. Vimos que se o grupo pro-p G é powerful, temos que $P_{n+1}(G) = G^{p^n}$. Neste capítulo sempre vamos supor que o grupo G é um grupo pro-p finitamente gerado e restringiremos à filtração $\{G_n = G^{p^n}\}_{n=0}^{\infty}$.

Dados um grupo G e um número inteiro positivo n, definimos $G^{\{n\}} = \{g^n \mid g \in G\}$. Logo $G^{p^n} = \langle G^{\{p^n\}} \rangle$.

Consideremos um grupo profinito G munido da métrica proveniente da filtração $\{G_n = G^{p^n}\}_{n=0}^{\infty}$. Definimos o espectro de G como

$$Spec(G) = \{\dim_H(H) \mid H \text{ um subgrupo fechado de } G\}.$$

Como vimos no anterior capitulo a dimensão de Hausdorff de qualquer subgrupo aberto de G é 1 e subgrupo finitos de G tem dimensão Hausdorff zero. Assim

$$Spec(G) \subseteq [0, 1].$$

A seguir nos vamos focar em grupos pro-p que também sao grupos analíticos p-ádicos, e mostrar que neste caso o espectro é um conjunto de números racionais. Primeiramente precisamos mostrar alguns lemas.

Lema 4.0.1. *Seja G um grupo pro-p finitamente gerado powerful e seja H um subgrupo fechado de G. Então* *(i) Existe uma constante $c > 0$ tal que $H \cap G_n = (H \cap G_c)^{\{p^{n-c}\}}$ para todo $n \geq c$.*

(ii) Existe uma constante $c > 0$ tal que $H \cap G_n \leq H_{n-c}$ para todo $n \geq c$.

Demonstração. Já que G é powerful, temos que $U_n = G_n/G_{n+1}$ são grupos abelianos elementares, que podemos considerar como espaços vetoriais sobre o corpo $\mathbb{F}_p$. O mapa $x \mapsto x^p$ induz um epimorfismo $\phi_n : U_n \to U_{n+1}$. Como $\dim(U_n)$ é limitada por $d(G)$, para n suficientemente grande, ϕ_n é um isomorfismo.

Definimos $V_n = (H \cap G_n)G_{n+1}/G_{n+1}$. Então $V_n \leq U_n$ e $\phi_n(V_n) \leq V_{n+1}$. Como ϕ_n é injetiva para n suficientemente grande, a serie $\{\dim(V_n)\}$ é não decrescente para n grande. Porém, $\dim(V_n) \leq d(G)$ para todo n. Portanto, a serie $\{\dim(V_n)\}$ se estabiliza. Segue que existe uma constante $c > 0$ tal que se $n \geq c$, então ϕ_n induz um isomorfismo de V_n para V_{n+1}. Em particular, $\phi_n(V_n) = V_{n+1}$ para $n \geq c$.

Vamos provar que se $n \geq c$, então o mapa $x \mapsto x^p$ de $H \cap G_n$ para $H \cap G_{n+1}$ é sobrejetivo. Seja $h \in H \cap G_{n+1}$. Mostraremos por indução que para $k \geq 0$

$$h = (h_n h_{n+1} \dots h_{n+k})^p g_{n+k+2}, \tag{4.1}$$

onde $h_{n+m} \in H \cap G_{n+m}$ $(0 \leq m \leq k)$, e $g_{n+k+2} \in H \cap G_{n+k+2}$.

Se $k = 0$, então como $n \geq c$, $\phi_n(V_n) = V_{n+1}$. Portanto existe $h_n \in H \cap G_n$ e $g_{n+2} \in G_{n+2}$ tal que $h = h_n^p g_{n+2}$. Suponhamos agora que a afirmação seja valida para k e vamos prová-la para $k+1$. Visto que $n+k+2 \geq c$, existem elementos $h_{n+k+1} \in H \cap G_{n+k+1}$ e $\tilde{g} \in H \cap G_{n+k+3}$ tal que $g_{n+k+2} = h_{n+k+1}^p \tilde{g}$. Portanto, $h = (h_n h_{n+1} ... h_{n+k})^p h_{n+k+1}^p \tilde{g}$.

Já que G é um grupo powerful, nós temos que

$$\tilde{h} = [h_{n+k+1}, h_n h_{n+1} ... h_{n+k}] \in [G_{n+k+1}, G] \leq G_{n+k+2}$$

Além disso, se $p = 2$, nós temos que $\tilde{h} \in G_{n+k+3}$. Segue que, em G/G_{n+k+3}, a imagem de $\tilde{h}$ comuta com a imagem de h_{n+k+1} e de $h_n h_{n+1} ... h_{n+k}$.

Aplicando a Formula 1.5.3, temos que

$$h = (h_n h_{n+1} ... h_{n+k} h_{n+k+1})^p \tilde{h}^{p(p-1)/2} g' \tilde{g},$$

onde $g' \in H \cap G_{n+k+3}$. Note que $\tilde{h} \in G_{n+k+2}$ e se $p = 2$, $\tilde{h} \in G_{n+k+3}$. Portanto

$$h = (h_n h_{n+1} ... h_{n+k} h_{n+k+1})^p g_{n+k+3},$$

onde $h_{n+m} \in H \cap G_{n+m}$ para $0 \leq m \leq k+1$ e $g_{n+k+3} \in H \cap G_{n+k+3}$.

A sequência $\{h_n h_{n+1} ... h_{n+k}\}_{k=0}^{\infty}$ é uma sequência de Cauchy, assim converge para algum $h' \in H \cap G_n$. Por outro lado, segue de (4.1) que

$$h = \lim_{k\to\infty} (h_n h_{n+1} ... h_{n+k})^p,$$

e como $x \mapsto x^p$ é um mapa continuo, nós temos que $h = (h')^p$. O que prova que o mapa $x \mapsto x^p$ de $H \cap G_n$ para $H \cap G_{n+1}$ é sobrejetivo. Portanto, $H \cap G_{n+1} = (H \cap G_n)^{\{p\}}$. Usando repetidamente esta igualdade, obtemos que $H \cap G_n = (H \cap G_c)^{\{p^{n-c}\}}$ para $n \geq c$, provando (i).

A parte (ii) segue do (i). Em efeito,

$$H \cap G_n = (H \cap G_c)^{\{p^{n-c}\}} \leq H^{p^{n-c}} = H_{n-c}.$$

□

Lema 4.0.2. *Se G é um grupo pro-p p-ádico analítico, então existe um inteiro $a > 0$ tal que G_a é subgrupo powerful de G.*

Demonstração. Note que G_n é um subgrupo característico de G. Portanto $G_n \lhd G$. Como G é p-ádico analítico, $d(G_n) \leq d(G) = r$. Consideramos $V = V(G, r)$ (aberto em G). Como G_n é uma filtração, existe a tal que $G_a \leq V$. Então pela Proposição 3.9 do Dixon, G_a p.e. V. Logo G_a é powerful. □

Corolário 4.0.3. *Seja G um grupo pro-p analítico p-ádico e $H \leq_c G$. Então existe uma constante c tal que $H \cap G_n \leq H_{n-c}$, para todo $n \geq c$.*

Demonstração. Já que G é um grupo p-ádico analítico, pelo lema anterior existe uma constante $a > 0$ tal que G_a é powerful. Aplicando Lema 4.0.1 para o subgrupo $H \cap G_a$ de G_a, obtemos que existe uma constante b tal que para todo $n \geq b$,

$$H \cap G_{a+n} = H \cap G_a^{p^n} = (H \cap G_{a+b})^{\{p^{n-b}\}} \leq H_{n-b} = H_{a+n-(a+b)}.$$

Seja $c = a + b$. Então $H \cap G_n \leq H_{n-c}$ para todo $n \geq c$. □

o seguinte lema nos da outro jeito de calcular a dimensão de um grupo pro-p de postos finito.

Lema 4.0.4. *Seja G um grupo pro-p de posto finito. Então*

$$\dim(G) = \lim_{k\to\infty} \frac{\log_p |G : G^{p^k}|}{k}$$

Demonstração. Se G for um grupo pro-p de posto finito, então existe $n \in \mathbb{N}$ tal que G^{p^k} é uniforme para todo $k \geq n$. Note também que como G^{p^k} é aberto, $|G : G^{p^k}|$ é finito para todo k. Assim

$$\lim_{k\to\infty}\frac{\log_p|G:G^{p^k}|}{k}=\lim_{k\to\infty}\frac{\log_p|G:G^{p^n}||G^{p^n}:G^{p^k}|}{k}$$

$$=\lim_{k\to\infty}\frac{\log_p|G:G^{p^n}|}{k}+\lim_{k\to\infty}\frac{\log_p|G^{p^n}:G^{p^k}|}{k}=0+\lim_{k\to\infty}\frac{\log_p|G^{p^n}:(G^{p^n})^{p^{k-n}}|}{k}.$$

Seja $\Gamma=G^{p^n}$. Fazendo mudança de variáveis, $t=k-n$, temos

$$\lim_{k\to\infty}\frac{\log_p|G:G^{p^k}|}{k}=\lim_{t\to\infty}\frac{\log_p|\Gamma:\Gamma^{p^t}|}{t+n}.$$

Notemos que Γ é uniforme e aberto. Portanto,

$$|\Gamma:\Gamma^{p^t}|=|\Gamma:\Gamma^p||\Gamma^p:\Gamma^{p^2}|\dots|\Gamma^{p^{t-1}}:\Gamma^{p^t}|=|\Gamma:\Phi(\Gamma)|^t.$$

Logo

$$\lim_{t\to\infty}\frac{\log_p|\Gamma:\Gamma^{p^t}|}{t+n}=\lim_{t\to\infty}\frac{\log_p|\Gamma:\Phi(\Gamma)|^t}{t+n}=\log_p|\Gamma:\Phi(\Gamma)|\lim_{t\to\infty}\frac{t}{t+n}=\log_p|\Gamma:\Phi(\Gamma)|.$$

Como Γ é um subgrupo aberto uniforme de G, temos que $\dim(G)=d(\Gamma)=\log_p|\Gamma:\Phi(\Gamma)|$, provando a igualdade. □

O seguinte resultado indica que o conceito de dimensão de Hausdorff generaliza o conceito de dimensão para grupos de Lie.

Teorema 4.0.5. *Seja G um grupo pro-p p-ádico analítico e $H\leq_c G$. Então*

$$\dim_H(H)=\frac{\dim(H)}{\dim(G)}.$$

Demonstração. Vejamos que $\dim_H H\leq\dim(H)/\dim(G)$. Pelo lema anterior, temos que

$$\dim(G)=\lim_{k\to\infty}\frac{\log_p|G:G^{p^k}|}{k},$$

e

$$\dim(H)=\lim_{k\to\infty}\frac{\log_p|H:H^{p^k}|}{k}.$$

Note que $H^{p^k}\leq H\cap G^{p^k}=H\cap G_k$. Portanto,

$$\frac{\log_p|H:H\cap G_k|}{\log_p|G:G_k|}\leq\frac{\log_p|H:H^{p^k}|/k}{\log_p|G:G_k|/k}.$$

Como
$$\lim_{k\to\infty} \frac{\log_p |H : H^{p^k}|/k}{\log_p |G : G_k|/k} = \frac{\dim(H)}{\dim(G)},$$
segue de Teorema 3.0.2 que
$$\dim_H(H) = \liminf_{k\to\infty} \frac{\log_p |H : H \cap G_k|}{\log_p |G : G_k|} \leq \frac{\dim(H)}{\dim(G)}.$$

Agora vamos ver que $\dim(H)/\dim(G) \leq \dim_H(H)$. Pelo Corolário 4.0.3, existe c tal que $H \cap G_{k+c} \leq H_k$ para todo k. Portanto,

$$\dim_H(H) = \liminf_{k\to\infty} \frac{\log_p |H : H \cap G_{k+c}|}{\log_p |G : G_{k+c}|} \geq \lim_{k\to\infty} \frac{\log_p |H : H^{p^k}|/k}{\log_p |G : G_k|/k} = \frac{\dim(H)}{\dim(G)}.$$

□

Corolário 4.0.6. *Seja G um grupo pro-p analítico p-ádico. Então*
$$Spec(G) \subseteq \{0, 1/d, 2/d, \ldots, 1\}, \text{ onde } d = \dim(G).$$

Agora estamos prontos para provar o resultado mais importante desta dissertação que é uma caracterização de grupos analíticos p-ádicos em termos de dimensão de Hausdorff. Fazemos uso do teorema de Zelmanov [12, Teorema 1], que prova a conjetura de Burnside para grupos compactos.

Teorema 4.0.7 (Teorema de Zelmanov)**.** *Todo grupo pro-p periódico é localmente finito.*

Teorema 4.0.8. *Seja G um grupo pro-p finitamente gerado. As seguintes afirmações são equivalentes:*

(i) A dimensão de Hausdorff de um subgrupo fechado H de G é zero se e somente se H é finito.

(ii) G é p-ádico analítico.

Demonstração. Claro, podemos supor que G é infinito.

$((ii) \Rightarrow (i))$ Se H é um subgrupo finito de G, então $\dim_H(H) = 0$ pela Observação 3.0.3. Suponhamos que H é um subgrupo fechado de G tal que $\dim_H(H) = 0$. Então pelo Teorema 4.0.5, $\dim(H) = 0$, o que implica que H é finito.

$((i) \Rightarrow (ii))$ Suponhamos que G não seja p-ádico analítico. Então como G é um grupo infinito pro-p finitamente gerado, pelo Teorema de Zelmanov [12], não pode ser periódico, i.e., existe um elemento $h \in G$ de ordem infinito. Definimos $H = \overline{\langle h \rangle} \cong \mathbb{Z}_p$. Para obter uma contradição vamos mostrar que $\dim_H(H) = 0$. Suponhamos por contradição que $\dim_H(H) > 0$. Então, pelo Teorema 3.0.2, existe $\epsilon > 0$ tal que

$$\liminf_{n\to\infty} \frac{\log |H : H \cap G_n|}{\log |G : G_n|} > \epsilon$$

Como $H_n = H^{p^n} \leq H \cap G_n$, obtemos

$$\liminf_{n\to\infty} \frac{\log |H : H_n|}{\log |G : G_n|} > \epsilon.$$

Notamos que $|H : H_n| = p^n$. Portanto, para n suficientemente grande,

$$\frac{n}{\log_p |G : G_n|} > \epsilon.$$

Logo $|G : G_n| \leq p^{cn}$, onde $c = 1/\epsilon$. Finalmente, segue de [10, Teorema B] que G é um grupo analítico p-ádico. $\square$

Referências Bibliográficas

[1] A. G. Abercrombie, *Subgroups and subrings of profinite rings*, Mathematical Proceedings of the Cambridge Philosophical Society **116** (1994), 209–222.

[2] Yiftach Barnea and Aner Shalev, *Hausdorff dimension, pro-p groups, and kac-moody algebras*, Transactions of the American Mathematical Society **349** (1997), no. 12, 5073–5091.

[3] J.D. Dixon, *Analytic prop groups*, Springer-Verlag, New York, 1973.

[4] D.S. Dummit and R.M. Foote, *Abstract algebra*, Wiley, 2004.

[5] Luis Ribes e Pavel Zalesskii, *Profinite groups*, Springer-Verlag, New York, 1991.

[6] Evgenii I. Khukhro, *p-automorphisms of finite p-groups (london mathematical society lecture note series)*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1998.

[7] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, vol. 58, Springer Science & Business Media, 2012.

[8] Charles Richard Leedham-Green and Susan McKay, *The structure of groups of prime power order*, no. 27, Clarendon Press, 2002.

[9] Nikolay Nikolov, Dan Segal, and Nikolay Nikolav, *On finitely generated profinite groups, i: strong completeness and uniform bounds*, Annals of mathematics (2007), 171–238.

[10] Aner Shalev, *Growth functions, p-adic analytic groups, and groups of finite coclass*, Journal of the London Mathematical Society **2** (1992), no. 1, 111–122.

[11] John S. Wilson, *Profinite groups*, Oxford, eu, 1978.

[12] E. I. Zelmanov, *On periodic compact groups*, Israel Journal of Mathematics **77** (1992), no. 1, 83–95.