Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Sobre Grupos Profinitos de Posto Finito

por

Christe Hélida Moreira Montijo

Brasília

2018

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Christe Hélida Moreira Montijo

Sobre Grupos Profinitos de Posto Finito

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora:
Profa. Dra. Aline Gomes da Silva Pinto

Brasília

2018

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

M C554s

Montijo, Christe Hélida Moreira
Sobre Grupos Profinitos de Posto Finito / Christe Hélida Moreira Montijo; orientador Aline Gomes da Silva Pinto. - Brasília, 2018.
113 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2018.

1. Grupos Profinitos. 2. Posto Finito. 3. Uniformly Powerful. 4. Finitamente Apresentado. I. Pinto, Aline Gomes da Silva , orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre Grupos Profinitos de Posto Finito

por

Christe Hélida Moreira Montijo*

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

MESTRE EM MATEMÁTICA

Brasília, 24 de agosto de 2018.

Comissão Examinadora:

Profa. Dra. Aline Gomes da Silva Pinto - MAT/UnB (Orientador)

Profa. Dra. Cristina Acciarri – MAT/UnB (Membro)

Prof. Dr. Slobodan Tanushevski – UFF (Membro)

* A autora foi bolsista do CNPq durante a elaboração desta dissertação.

Agradecimentos

Primeiramente gostaria de agradecer a Deus por essa conquista tão especial.

À Minha família que sempre me apoiou incondicionalmente e por proporcionar todo o suporte necessário para eu prosseguir nessa caminhada.

À minha orientadora Aline Pinto, pela orientação, por ter acreditado em mim e por ter compartilhado comigo um pouquinho do seu valioso conhecimento.

Aos professores Cristina Acciarri e Slobodan Tanushevski por terem aceitado participar da banca examinadora e pelas sugestões e correções.

Agradeço aos meus professores da UnB, em especial os professores: Aline, Cátia, Daniela, Luciana, Leandro, Martino, Noraí, Ricardo e Pedro Roitman.

Agradeço ao professor Leandro Cioletti não somente pelas aulas tão inspiradoras, mas também, por acreditar e me apoiar quando mais precisei.

À professora Liliane Maia por permitir que essa conquista fosse possível. Agradeço por me incentivar quando podia simplesmente deixar eu desistir e por lembrar que "somos mulheres fortes". A senhora é incrível, gratidão eterna.

Aos meus professores da UFT, em especial o professor Adriano Rodrigues.

Aos meus amigos queridos: Alancoc, Alex, Alisson, Bruno, Carolzinha, Elaine, Fabian, Fábio, Felipe, Filipe, Francisca, Geovane, Jamer, Jhon, Jonathan, Josimar, Leo, Lizeth, Lumena, Nathalia, Rafael, Regiane, Roney, Sabrina, Sara, Valter, Wallef e Welinton. Aos meus amigos da colina e meus amigos do Tocantins.

À Sara Raissa por ser essa amiga tão especial, que presenciou cada momento da minha vida durante todo esse período, e que sempre esteve ao meu lado me apoiando e cuidando. Sou muito grata por tudo amiga linda.

À Carolzinha por toda cumplicidade e por me ensinar a evoluir como pessoa.

Agradeço ao Valter pela amizade sempre acompanhada de muito conhecimento e por todos os excelentes conselhos e cuidados.

E não poderia deixar de agradecer Alancoc, Elaine, Fabian, Jonathan, Lumena e Valter pelas madrugadas inesquecíveis na UnB de muito estudo e boas risadas.

À CAPES pelo apoio financeiro.

Meus sinceros agradecimentos a todos.

Dedicatória

À minha Família.

"Feliz é quem descobre a sabedoria e adquire a inteligência!
Pois com ela ganha-se mais do que com a prata,
e seu lucro é maior do que o do ouro;
é mais preciosa que as pérolas,
e nada é mais desejável do que ela".

Provérbios 3, 13-15

Resumo

Esta dissertação está dividida em duas partes e é baseada no Capítulo 8 do livro *Profinite Groups* [22] de J. S. Wilson, e no artigo *Uncountably many non-commensurable finitely presented pro-p groups* [19] de I. Snopce. A parte I é um estudo de grupos profinitos de posto finito. Estudamos grupos solúveis profinitos de posto finito e fornecemos uma série de caracterizações dos mesmos. Então mostramos que um grupo profinito arbitrário de posto finito é construído a partir de um grupo pronilpotente de posto finito, um grupo solúvel de posto finito e um grupo finito. E a Parte II é uma descrição de grupos pro-p de posto finito. Provamos que existe uma quantidade não enumerável de grupos pro-p uniformes metabelianos não comensuráveis de dimensão m, onde $m \geq 3$ é um inteiro positivo, e consequentemente, existe uma quantidade não enumerável de grupos pro-p finitamente apresentados não comensuráveis com um número minimal de geradores igual a m e um número minimal de relações igual a $\begin{pmatrix} m \\ 2 \end{pmatrix}$.

Palavras-chave: grupos profinitos, posto finito, uniformly powerful, finitamente apresentado.

Abstract

This master's dissertation was divided into two parts, and it is based on the Chapter 8 of the book *Profinite Groups* [22] of J. S. Wilson, and on the article *Uncountably many non-commensurable finitely presented pro-p groups* [19] of I. Snopce. Part I is a study of profinite groups of finite rank. We study profinite soluble groups of finite rank and we give a number of characterizations of them. Then we show that an arbitrary profinite group of finite rank is built up from a pronilpotent group of finite rank, a soluble group of finite rank, and a finite group. Part II is an account of pro-p groups of finite rank. It is proved that there are uncountably many non-commensurable metabelian uniform pro-p groups of dimension m, where $m \geq 3$ is a positive integer. Consequently, there are uncountably many non-commensurable finitely presented pro-p groups with minimal number of generators m and minimal number of relations $\begin{pmatrix} m \\ 2 \end{pmatrix}$.

Keywords: profinite groups, finite rank, uniformly powerful, finitely presented.

Conteúdo

Introdução

Um grupo profinito é, por definição, um grupo dado pelo limite inverso de grupos finitos. Grupos profinitos podem também ser caracterizados como os grupos topológicos de Hausdorff, totalmente desconexos e compactos. Uma classe especial de grupos profinitos, é a classe dos grupos pro-p, que são por definição limite inverso de p-grupos finitos.

Neste trabalho apresentamos propriedades dos grupos profinitos G, para os quais existe um inteiro r tal que cada subgrupo de G pode ser gerado por r elementos, esses grupos são chamados de grupos profinitos de posto finito. É importante observar que o termo 'posto' na teoria dos grupos profinitos não deve ser confundido com o seu uso em expressões como 'grupo livre de posto finito'; um exemplo claro desse fato é que os grupos profinitos livres finitamente gerados não têm posto finito, uma vez que possuem subgrupos profinitos que não são finitamente gerados. Com a atenção sempre voltada para os grupos profinitos de posto finito, este trabalho está dividido em duas partes, a primeira parte apresentamos um estudos mais geral dos grupos profinitos de posto finito, baseado principalmente no Capítulo 8 do livro de J. S. Wilson [22], e a segunda parte está baseada no artigo de I. Snopce [19] "Uncountably many non-commensurable finitely presented pro-p groups".

No primeiro capítulo apresentamos um estudo preliminar sobre grupos profinitos, no qual construimos a definição de grupos profinitos a partir do limite inverso de um sistema inverso de grupos topológicos, em seguida mostramos que grupos profinitos podem ser caracterizados de outras maneiras, e mostramos também que exemplos importantes e naturais de grupos profinitos podem ser construídos a partir de grupos abstratos, como por exemplo o anel dos inteiros p-ádicos, que é o completamento pro-p

de $\mathbb{Z}$, denotado por $\mathbb{Z}_p$. E então direcionando para os grupos profinitos de posto finito estudamos grupos solúveis profinitos de posto finito e apresentamos uma série de caracterizações dos mesmos. E finalmente, estudamos os grupos profinitos arbitrários de posto finito, obtendo o seguinte teorema:

Teorema 1.5.23 *Seja G um grupo profinito de posto finito. Então G tem uma série*

$$1 \leq C \leq N \leq G$$

de subgrupos normais tal que C é pronilpotente, N/C é solúvel e G/N é finito.

Em outras palavras o Teorema 1.5.23 nos diz que um grupo profinito de posto finito possui uma série (pronilpotente-por-solúvel)-por-finito. Mas como os grupos pronilpotentes são os produtos cartesianos de seus subgrupos de Sylow, direcionamos a atenção para os grupos pro-p de posto finito. E assim, nos capítulos seguintes nos restringimos aos grupos pro-p.

No segundo capítulo, mostramos como dotar o conjunto subordinado de um grupo pro-p uniforme G com uma estrutura aditiva, tornando-o um $\mathbb{Z}_p$-módulo livre. E então com o objetivo de obter mais propriedades em relação a estrutura do grupo G, definimos uma segunda operação capaz de transformar o $\mathbb{Z}_p$-módulo livre em uma álgebra de Lie sobre $\mathbb{Z}_p$. Além disso, mostramos que vale o processo inverso, ou seja, dado uma álgebra de Lie powerful, ela pode se tornar um grupo pro-p uniforme. Por fim apresentamos o seguinte resultado, que garante que existe uma correspondência biunívoca entre os grupos pro-p uniformes e as álgebras de Lie powerful sobre $\mathbb{Z}_p$:

Teorema 2.3.27 *As aplicações*

$$G \longmapsto L_G, \quad L \longmapsto (L, *)$$

são isomorfismos mutuamente inversos entre a categoria de grupos pro-p uniformes e categoria de álgebras de Lie powerful sobre $\mathbb{Z}_p$.

Muitos dos resultados do Capítulo 2 estão contidos no longo e importante artigo de Lazard [6], "Groupes analytiques p-adiques", dedicado ao estudo dos grupos pro-p de posto finito, na perspectiva de grupos analíticos p-ádicos. Já no livro de J. D. Dixon; M. P. F. Du Sautoy; A. Mann; D. Segal [2], "Analytic pro-p Groups", podme ser encontrados alguns dos resultados deste artigo, de um ponto de vista teórico de

grupos, e de resultados de Lubotzky e Mann dos artigos [8] "Powerful p-Groups. I. Finite Groups", e [9] "Powerful p-Groups, II. p-Adic Analytic Groups" ligando diferentes caracterizações desses grupos. Em [9], Lubotzky e Mann provaram que se G é um grupo pro-p de posto finito, então G tem um subgrupo aberto característico powerful, e que também vale a recíproca. Garantindo assim que um grupo pro-p tem posto finito se, e somente se, tem um subgrupo característico aberto uniforme, esse resultado é usado para fornecer caracterizações alternativas para grupos pro-p de posto finito. Um resultado anterior de Lazard [6], afirma que um grupo pro-p tem estrutura de um grupo analítico p-ádico se, e somente se, tem um subgrupo normal aberto uniforme.

No terceiro capítulo, apresentamos a demonstração do seguinte teorema de I. Snopce do artigo [19]:

Teorema 3.2.3 *Seja $m \geq 3$ um inteiro positivo. Existe uma quantidade não enumerável de grupos pro-p uniformes, metabelianos, não comensuráveis de dimensão m. Consequentemente, existe uma quantidade não enumerável de grupos pro-p finitamente apresentados não comensuráveis com um número minimal de geradores igual a m (e o número minimal de relações igual a* $\binom{m}{2}$*).*

Para isso usamos o Teorema 2.3.27, que permite associar ao grupo pro-p uniforme uma $\mathbb{Z}_p$-álgebra de Lie e depois 'retornar' para o grupo pro-p uniforme sem perder propriedades. Além disso, usamos resultados contidos em J. D. Dixon; M. P. F. Du Sautoy; A. Mann; D. Segal [2], apresentados no Capítulo 3, que garantem que todo grupo pro-p de posto finito tem uma apresentação finita que pode ser dada explicitamente (confira teorema 3.1.1), assim como limitar o número mínimo de relações da apresentação de um grupo pro-p powerful finitamente gerado (confira teorema 3.1.4).

A questão da existência de uma quantidade não enumerável de grupos pro-p finitamente apresentados não-isomórficos foi levantada por A. Lubotzky na conferência "Geometric and Combinatorial Group Theory" em homenagem a E. Rips e por E. Zelmanov na conferência "XX Coloquio Latinoamericano de Álgebra". Entretanto Zelmanov atribuiu a questão a Lubotzky.

Capítulo 1

Grupos Profinitos

Neste capítulo faremos uma breve introdução da teoria de grupos topológicos, para então definir o limite inverso de um sistema inverso de grupos topológicos com o objetivo de definir os grupos profinitos, dando uma atenção especial aos grupos pro-p, que é um caso particular de grupos profinitos, uma vez que, nosso objetivo final ao estudar essa teoria é estudar os grupos pro-p de posto finito. Também daremos algumas caracterizações dos grupos profinitos, com o intuito de obter mais ferramentas de estudos e definiremos o completamento de grupos abstratos e, em particular, o completamento pro-p dos inteiros. E por fim daremos uma série de caracterizações para os grupos profinitos solúveis de posto finito e de maneira geral, forneceremos uma estrutura para grupos profinitos de posto finito. As principais referências utilizadas neste capítulo são J. S. Wilson [22], L. Ribes; P. Zalesskii [15] e J. R. Munkres [13].

1.1 Grupos Topológicos

Antes de definir os grupos topológicos é importante relembrar a definição de espaço topológico e comentar algumas propriedades que serão utilizadas posteriormente, para um estudo mais detalhado veja o livro de J. R. Munkres [13].

Definição 1.1.1 *Uma topologia em um conjunto X é uma coleção τ de subconjuntos de X satisfazendo as seguintes propriedades:*

(a) *O conjunto vazio $\emptyset$ e X pertencem a τ;*

(b) *A união de elementos de qualquer subcoleção de τ pertence a τ;*

(c) *A interseção de elementos de qualquer subcoleção finita de τ pertence a τ.*

Um conjunto X munido de uma topologia τ é chamado espaço topológico (X, τ).

Mas, em geral, omitiremos τ se não houver risco de ambiguidade, nos referindo assim "ao espaço topológico X".

Definição 1.1.2 *Seja (X, τ) um espaço topológico e Y um subconjunto de X.*

1. *Dizemos que $U \subseteq X$ é um conjunto aberto se $U \in \tau$. Por outro lado, um subconjunto de X é um conjunto fechado se o complementar é um conjunto aberto.*
2. *O fecho $\overline{Y}$ de Y é a interseção de todos os fechados contendo Y.*
3. *Dizemos que Y é denso em X se $\overline{Y} = X$.*
4. *Uma vizinhança aberta de um elemento $x \in X$ é um conjunto aberto que contém x.*
5. *Uma base para uma topologia em X é uma coleção $\{U_\lambda \mid \lambda \in \Lambda\}$ de conjuntos abertos tal que todo conjunto aberto é uma união de conjuntos U_λ.*
6. *O espaço topológico X com uma topologia no qual cada subconjunto de X é aberto é chamado espaço discreto e tal topologia é chamada topologia discreta.*
7. *A coleção de todos os subconjuntos da forma $Y \cap U$, com U aberto em X é uma topologia em Y. E com essa topologia, Y é chamado de subespaço topológico de X.*

Para a próxima definição usaremos a seguinte defnção auxiliar:

Definição 1.1.3 (Propriedade da interseção finita) *Uma coleção Γ de subconjuntos de X tem a propriedade da interseção finita se, para toda subcoleção $\{C_1, \ldots, C_n\}$, temos que*

$$\bigcap_{j=1}^{n} C_j \neq \emptyset.$$

Definição 1.1.4 *Um espaço topológico X é compacto se toda cobertura por abertos de X possui uma subcobertura finita. Equivalentemente, X é compacto se toda coleção Γ de subconjuntos fechados de X contendo a propriedade da interseção finita, satisfaz*

$$\bigcap_{C \in \Gamma} C \neq \emptyset.$$

Outras duas definições importantes para a teoria dos grupos profinitos são as definições dos espaços topológicos de Hausdorff e os espaços topológicos totalmente desconexos.

Definição 1.1.5 *Seja X um espaço topológico.*

1. *Dizemos que X é um espaço de Hausdorff se dados dois elementos distintos x e y em X, existem vizinhanças abertas U e V de x e y, respectivamente, tais que $U \cap V = \emptyset$.*

2. *Dizemos que X é conexo se não pode ser escrito como a união disjunta de dois conjuntos abertos não vazios. E dizemos que X é totalmente desconexo se todo subespaço conexo tem no máximo um elemento.*

Lema 1.1.6 *Seja X um espaço de Hausdorff compacto.*

(a) *Se C e D são subconjuntos fechados de X tal que $C \cap D = \emptyset$, então existem subconjuntos abertos U e V tais que $C \subseteq U$, $D \subseteq V$ e $U \cap V = \emptyset$.*

(b) *Seja $x \in X$ e A a interseção de todos os subconjuntos de X contendo x que são simultaneamente abertos e fechados. Então A é conexo.*

(c) *Se X é também totalmente desconexo, então todo conjunto aberto é uma união de conjuntos que são simultaneamente abertos e fechados.*

A demonstração será omitida, mas pode ser encontrada em [22, Lemma 0.1.1].

Definição 1.1.7 *Sejam X e Y espaços topológicos.*

1. *Uma aplicação $f : X \longrightarrow Y$ é contínua se para cada aberto U de Y o conjunto $f^{-1}(U) = \{x \in X \mid f(x) \in U\}$ é aberto em X. Equivalentemente, a aplicação f é contínua se $f^{-1}(C)$ é fechado em X para todo subconjunto fechado C de Y.*

2. *Uma aplicação $f : X \longrightarrow Y$ é um homeomorfismo se f é uma bijeção e f e f^{-1} são contínuas.*

Lema 1.1.8 (a) *Todo subconjunto fechado de um espaço compacto é compacto.*

(b) *Todo subconjunto compacto de um espaço de Hausdorff é fechado.*

(c) *Se $f : X \longrightarrow Y$ é contínua e X é compacto, então $f(X)$ é compacto.*

(d) *Se $f : X \longrightarrow Y$ é contínua e bijetiva, X é compacto e Y é um espaço de Hausdorff, então f é um homeomorfismo.*

(e) *Se $f : X \longrightarrow Y$ e $g : X \longrightarrow Y$ são contínuas e Y é um espaço de Hausdorff, então $\{x \in X \mid f(x) = g(x)\}$ é fechado em X.*

A demonstração pode ser encontrada em [22, Lemma 0.1.2].

Lema 1.1.9 *Seja X um espaço totalmente desconexo. Então $\{x\}$ é fechado em X, para cada $x \in X$.*

A demonstração pode ser encontrada em [22, Lemma 0.1.3].

Definição 1.1.10 *Seja X um espaço topológico e ρ uma relação de equivalência em X. Defina X/ρ o conjunto quociente e $q : X \longrightarrow X/\rho$ a aplicação quociente que associa cada elemento de X a sua classe de equivalência. A topologia quociente em X/ρ é a topologia cujos conjuntos abertos são os subconjuntos V de X/ρ tais que $q^{-1}(V)$ é aberto em X.*

Assim, com a topologia quociente, X/ρ é um espaço topológico, e consequentemente, a aplicação q é contínua.

Outra definição importante para a teoria dos grupos profinitos é a definição de topologia produto. Relembrando que o produto cartesiano de uma família não vazia de conjuntos $\{X_\lambda \mid \lambda \in \Lambda\}$ é o conjunto

$$\prod_{\lambda\in\Lambda} X_\lambda = \{f : \Lambda \longrightarrow \bigcup_{\lambda\in\Lambda} X_\lambda \mid f(\lambda) \in X_\lambda\},$$

e $x \in \prod_{\lambda\in\Lambda} X_\lambda$ é denotado por $(x_\lambda)_{\lambda\in\Lambda}$.

E o produto cartesiano de uma família finita de conjuntos $X_1, \ldots, X_n$ é denotado por $X_1 \times \ldots \times X_n$.

Definição 1.1.11 *Seja X_λ um espaço topológico, para cada $\lambda \in \Lambda$. E considere a aplicação $\pi_\lambda : \prod_{\lambda\in\Lambda} X_\lambda \longrightarrow X_\lambda$ definida por $x = (x_\lambda)_{\lambda\in\Lambda} \longmapsto x_\lambda$, para cada $\lambda \in \Lambda$. A topologia produto em $\prod_{\lambda\in\Lambda} X_\lambda$ é a topologia que tem como abertos as uniões de conjuntos da forma*

$$\pi_{\lambda_1}^{-1}(U_1) \cap \ldots \cap \pi_{\lambda_n}^{-1}(U_n),$$

com n finito, para cada λ_i em Λ e U_i um aberto em X_{λ_i}.

Teorema 1.1.12 *Seja $(X_\lambda \mid \lambda \in \Lambda)$ uma família de espaços topológicos e denote $C = \prod_{\lambda\in\Lambda} X_\lambda$.*

(a) *Se cada X_λ é um espaço de Hausdorff, então C também é um espaço de Hausdorff;*

(b) *Se cada X_λ é totalmente desconexo, então C também é totalmente desconexo;*

(c) *Se cada X_λ é compacto, então C também é compacto.*

A demonstração pode ser encontrada em [22, Theorem 0.2.1].

O item (c) deste teorema é o famoso teorema de Tychonoff, e uma demonstração mais detalhada do mesmo pode ser encontrada em [13, Theorem 37.3].

Com tais definições e resultados, estamos prontos para definir os grupos topológicos e apresentar os resultados que auxiliarão na definição e caracterização dos grupos profinitos.

Definição 1.1.13 *Um grupo topológico é um conjunto G que é ao mesmo tempo um grupo e um espaço topológico tal que a aplicação*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & xy^{-1} \end{array}$$

é contínua. Estamos considerando $G \times G$ com a topologia produto.

No lema a seguir apresentaremos alguns resultados elementares, porém fundamentais, sobre grupos topológicos.

Lema 1.1.14 *Seja G um grupo topológico.*

(a) *A aplicação $(x, y) \longmapsto xy$ de $G \times G$ em G é contínua e a aplicação $x \longmapsto x^{-1}$ de G em G é um homeomorfismo. E para cada $g \in G$, as aplicações $x \longmapsto xg$ e $x \longmapsto gx$ de G em G são homeomorfismos.*

(b) *Se H é um subgrupo aberto (resp. fechado) de G, então toda classe lateral Hg ou gH de H em G é aberta (resp. fechada).*

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

(d) *Se H é um subgrupo contendo um subconjunto aberto não vazio U de G, então H é aberto em G.*

(e) *Se H é um subgrupo de G e K é um subgrupo normal de G, então H é um grupo topológico com respeito a topologia induzida e G/K é um grupo topológico com respeito a topologia quociente. Além disso, a aplicação quociente $q : G \longrightarrow G/K$ leva subconjunto aberto em subconjunto aberto.*

(f) *G é um espaço de Hausdorff se, e somente se, $\{1\}$ é um subconjunto fechado de G. E se K é um subgrupo normal de G, então G/K é Hausdorff se, e somente se, K é fechado em G. Se G é totalmente desconexo, então G é Hausdorff.*

(g) *Se G é compacto e Hausdorff e se C e D são subconjuntos fechados, então CD é fechado.*

(h) *Suponha que G é compacto e seja $\{X_\lambda \mid \lambda \in \Lambda\}$ uma família de subconjuntos fechados com a propriedade que para todo $\lambda_1, \lambda_2 \in \Lambda$ existe um elemento $\mu \in \Lambda$ tal que $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$. Se Y é um subconjunto fechado de G, então $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y = \bigcap_{\lambda\in\Lambda} X_\lambda Y$.*

A demonstração pode ser encontrada em [22, Lemma 0.3.1]

Lema 1.1.15 *Seja G um grupo topológico compacto. Se C é um subconjunto aberto e fechado e contém 1, então C contém um subgrupo normal aberto.*

A demonstração pode ser encontrada em [22, Lemma 0.3.2].

Proposição 1.1.16 *Seja G um grupo topológico, compacto e totalmente desconexo.*

(a) *Todo conjunto aberto em G é uma união de classes laterais de subgrupos normais abertos.*

(b) *Um subconjunto de G é ao mesmo tempo aberto e fechado se, e somente se, é uma união de uma quantidade finita de classes laterais de subgrupos normais abertos.*

(c) *Se X é um subconjunto de G, então o fecho $\overline{X}$ satisfaz $\overline{X} = \bigcap\{NX \mid N \trianglelefteq_\circ G\}$.*

Em particular, $C = \bigcap\{NC \mid N \trianglelefteq_\circ G\}$, para cada subconjunto fechado C, e a interseção dos subgrupos normais abertos de G é trivial.

A demonstração pode ser encontrada em [22, Proposition 0.3.3].

O próximo resultado garante que o produto cartesiano de uma família de grupos topológicos é um grupo topológico e a demonstração segue da definição de topologia produto.

Lema 1.1.17 *Sejam $\{G_\lambda \mid \lambda \in \Lambda\}$ uma família de grupos topológicos e $C = \prod_{\lambda\in\Lambda} G_\lambda$ o produto cartesiano dos G_λ. Defina em C a operação componente a componente, ou seja, $(x_\lambda)(y_\lambda) = (x_\lambda y_\lambda)$, para todos $(x_\lambda), (y_\lambda) \in C$. Então C é um grupo topológico com respeito a esta operação e a topologia produto.*

O próximo lema mostra como construir um grupo topológico a partir de um grupo abstrato qualquer o que o torna uma ferramenta muito útil, por exemplo no estudo da teoria do completamento de grupos.

Lema 1.1.18 *Sejam G um grupo abstrato e L uma família não vazia de subgrupos normais com a seguinte propriedade: se $K_1, K_2 \in L$ e K_3 é um subgrupo normal contido em $K_1 \cap K_2$, então $K_3 \in L$. E seja τ a família de todas as uniões de conjuntos de classes laterais Kg com $K \in L$ e $g \in G$. Então τ é uma topologia em G e G é um grupo topológico com respeito a essa topologia.*

Demonstração: Primeiramente veremos que τ é uma topologia para G. Considere a família das classes laterais Kg, onde $K \in L$ e $g \in G$. Temos que a interseção de quaisquer duas classes laterais distintas é vazia e a união de todas as classes laterais de K em G é igual a G, uma vez que o conjunto das classes laterais de K em G é uma partição de G, sendo assim os conjuntos $\emptyset$ e G pertencem a τ. Agora tome g_1, $g_2 \in G$ e K_1, $K_2 \in L$. Se $K_1g_1 \cap K_2g_2 \neq \emptyset$, então existe $x \in K_1g_1 \cap K_2g_2$, daí

$$K_1g_1 \cap K_2g_2 = K_1x \cap K_2x = (K_1 \cap K_2)x = \cup_{y \in k_1 \cap k_2} K_3y$$

onde $K_3 \subseteq K_1 \cap K_2$ e $K_3 \in L$. Então $K_1g_1 \cap K_2g_2$ pertence a τ. Logo, τ é uma topologia onde as classes laterais formam a base de τ.

Agora mostraremos que G é um grupo topológico. Considere $\varphi : G \times G \to G$, uma aplicação definida por, $(x, y) \mapsto xy^{-1}$. Mostraremos que φ é contínua. Tome g_1, $g_2 \in G$ tal que $g_1g_2^{-1} \in W$, para algum subconjunto W aberto em G, então $(g_1, g_2) \in \varphi^{-1}(W)$. Pela definição de τ, existe $N \in L$ tal que $Ng_1g_2^{-1} \subseteq W$. Defina $U = Ng_1$ e $V = Ng_2$. Então $\varphi(U \times V) = UV^{-1} = Ng_1g_2^{-1} \subseteq W$, logo, $(g_1, g_2) \in U \times V \subseteq \varphi^{-1}(W)$, onde $U \times V$ é aberto em $G \times G$. Portanto, φ é contínua e, consequentemente, G é um grupo topológico. ■

1.2 Limites Inversos

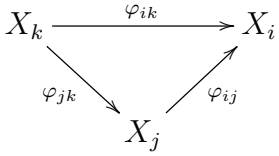
Nesta seção introduziremos a definição de limite inverso e algumas de suas principais propriedades com o objetivo de obter mais informações sobre os grupos profinitos, que por definição são limites inversos de grupos finitos. Começaremos então com a defi-

nição de sistema inverso, seguindo com alguns exemplos para tornar clara tal definição, e por fim definiremos o limite inverso.

Antes da definição de sistema inverso é importante saber a definição de conjunto dirigido, uma vez que de agora em diante, sempre tomaremos espaços topológicos indexados por um conjunto dirigido.

Definição 1.2.1 *Um conjunto dirigido é um conjunto parcialmente ordenado I com respeito a uma relação de ordem "$\leq$" tal que para todos $i_1, i_2 \in I$ existe um elemento $j \in I$ no qual $i_1 \leq j$ e $i_2 \leq j$.*

Definição 1.2.2 *Um sistema inverso (X_i, φ_{ij}) de espaços topológicos indexados por um conjunto dirigido I, consiste de uma família $\{X_i \mid i \in I\}$ de espaços topológicos e uma família $\{\varphi_{ij} : X_j \longrightarrow X_i \mid i, j \in I, i \leq j\}$ de aplicações contínuas tais que φ_{ii} é a aplicação identidade id_{X_i}, para cada i, e $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ sempre que $i \leq j \leq k$, ou seja, o diagrama abaixo comuta.*



Se cada X_i é um grupo topológico e cada φ_{ij} é um homomorfismo contínuo, então (X_i, φ_{ij}) é chamado um sistema inverso de grupos topológicos. E similarmente, podemos definir um sistema inverso de anéis topológicos.

Os conjuntos para os quais nenhuma topologia é especificada serão considerados como espaços topológicos com a topologia discreta.

O exemplo a seguir é de suma importância para o desenvolvimento da teoria do completamento dos inteiros, que será apresentada mais adiante.

Exemplo 1.2.3 *Sejam $I = \mathbb{N}$ um conjunto dirigido com a relação de ordem usual e p um primo. Para cada $j \geq i$, defina*

$$\begin{array}{rccc} \varphi_{ij}: & \mathbb{Z}/p^j\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^i\mathbb{Z} \\ & n + p^j\mathbb{Z} & \longmapsto & n + p^i\mathbb{Z}, \end{array}$$

para cada $n \in \mathbb{Z}$.

Veja que φ_{ij} está bem definida.

De fato, observe que φ_{ij} está bem definida se, e somente se, $p^j\mathbb{Z} \subseteq p^i\mathbb{Z}$.

Dado $p^j \in p^j\mathbb{Z}$, temos que, $p^j \in p^i\mathbb{Z}$ se, e somente se, $p^i \mid p^j$, mas $p^i \mid p^j$ se, e somente se, $j \geq i$. Logo, $p^j\mathbb{Z} \subseteq p^i\mathbb{Z}$, e portanto, φ_{ij} está bem definida.

Segue que, $\varphi_{ii} = id$, para todo $i \in I$ e se $i \leq k \leq j$, tem-se $\varphi_{ik}\varphi_{kj} = \varphi_{ij}$.

De fato, seja $n + p^j\mathbb{Z} \in \mathbb{Z}/p^j\mathbb{Z}$, então

$$(\varphi_{ik}\varphi_{kj})(n+p^j\mathbb{Z}) = \varphi_{ik}(\varphi_{kj}(n+p^j\mathbb{Z})) = \varphi_{ik}(n+p^k\mathbb{Z}) = n+p^i\mathbb{Z} = \varphi_{ij}(n+p^j\mathbb{Z}),$$

com $i \leq k \leq j$.

Logo, $(\mathbb{Z}/p^i\mathbb{Z}, \varphi_{ij})$ é um sistema inverso de anéis finitos.

Observe que, o exemplo acima é também um sistema inverso de grupos topológicos. E de modo mais geral, temos o seguinte exemplo.

Exemplo 1.2.4 *Sejam G um grupo e I uma família de subgrupos normais de G com a propriedade que para todo $U_1, U_2 \in I$ existe um subgrupo $V \in I$ tal que $V \leq U_1 \cap U_2$. Podemos considerar I um conjunto dirigido com respeito a ordem $\leq'$, definida por*

$$U \leq' V \text{ se, e somente se, } V \leq U.$$

Para $U \leq' V$, considere a aplicação definida por

$$\begin{array}{rccc} q_{UV}: & G/V & \longrightarrow & G/U \\ & Vg & \longmapsto & Ug. \end{array}$$

Então $(G/U, q_{UV})$ é um sistema inverso de grupos.

De fato, como U é um subgrupo normal de G, então pelo Lema 1.1.14 item (e), G/U é um grupo topológico, para todo $U \in I$. E como $V \leq U$, então q_{UV} está bem definida.

Além disso, a aplicação $q_{UV} : G/V \longrightarrow G/U$ é um homomorfismo contínua, para todo $U \in I$ tais que $q_{UV} = q_{UW}q_{WV}$ sempre que, $U \leq' W \leq' V$ e, se $U = V$, $q_{UU} = id$. Com efeito, considere a aplicação $\psi_U : G \longrightarrow G/U$ com $U \in I$, temos que, $\psi_U = q_{UV}\psi_V$. E seja N um aberto em G/U, então $\psi_U^{-1}(N)$ é um aberto em G, mas pelo Lema 1.1.14 item (e), a aplicação quociente $\psi_V : G \longrightarrow G/V$ leva aberto em aberto, então $\psi_V(\psi_U^{-1}(N))$ é aberto em G/V. Mas note que,

$$q_{UV}(\psi_V(\psi_U^{-1}(N))) = q_{UV}(q_{UV}^{-1}(N)) = N.$$

Assim, dado N aberto em G/U, $q_{UV}^{-1}(N)$ é aberto em G/V, e portanto q_{UV} é contínua. E para mostrar que q_{UV} é um homomorfismo é imediato.

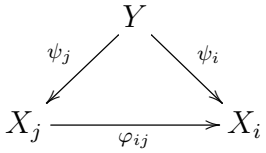
Agora observe que, dado $Vg \in G/V$ temos

$$(q_{UW}q_{WV})(Vg) = q_{UW}(q_{WV})(Vg) = q_{UW}(Wg) = Ug = q_{UV}(Vg).$$

Logo, $(G/U, q_{UV})$ é um sistema inverso de grupos.

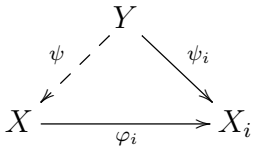
Para definir o limite inverso precisamos do seguinte conceito de família compatível de aplicações contínuas de um espaço topológico.

Definição 1.2.5 *Sejam (X_i, φ_{ij}) um sistema inverso de espaços topológicos sobre um conjunto dirigido I e Y um espaço topológico. Dizemos que uma família de aplicações contínuas $\{\psi_i : Y \longrightarrow X_i \mid i \in I\}$ é compatível se $\varphi_{ij}\psi_j = \psi_i$, sempre que $i \leq j$, ou seja, se para cada $i \in I$ e $i \leq j$, o diagrama abaixo é comutativo.*



Tendo em mãos tais conceitos, estamos aptos a definir o limite inverso.

Definição 1.2.6 *Um limite inverso (X, φ_i) de um sistema inverso (X_i, φ_{ij}) de espaços topológicos é um espaço topológico X juntamente com uma família compatível $\{\varphi_i : X \longrightarrow X_i\}$ de aplicações contínuas com a seguinte propriedade universal: sempre que $\{\psi_i : Y \longrightarrow X_i\}$ é uma família compatível de aplicações contínuas de um espaço topológico Y, existe uma única aplicação contínua $\psi : Y \longrightarrow X$ tal que $\varphi_i\psi = \psi_i$, para cada $i \in I$, ou seja, o seguinte diagrama é comutativo.*



De modo análogo, podemos definir o limite inverso de um sistema inverso de grupos topológicos e anéis topológicos.

Com essas informações estamos prontos para fazer a seguinte definição:

Definição 1.2.7 *Dizemos que G é um espaço, grupo ou anel profinito se é o limite inverso de espaços, grupos ou aneis finitos, respectivamente, dotados com a topologia discreta.*

No próximo resultado mostraremos que o limite inverso existe e é (em um sentido apropriado) único. Além disso, mostraremos como construir um limite inverso.

Proposição 1.2.8 *Seja (X_i, φ_{ij}) um sistema inverso de espaços topológicos (de grupos topológicos resp.), indexado por um conjunto dirigido I.*

(a) *Se $(X^{(1)}, \varphi_i^{(1)})$ e $(X^{(2)}, \varphi_i^{(2)})$ são limites inversos do sistema inverso (X_i, φ_{ij}), então existe homeomorfismo (isomorfismo topológico resp.) $\overline{\varphi} : X^{(1)} \longrightarrow X^{(2)}$ tal que $\varphi_i^{(2)}\overline{\varphi} = \varphi_i^{(1)}$, para cada $i \in I$.*

(b) *Sejam* $C = \prod_{i\in I} X_i$ *e para cada* $i \in I$ *considere* π_i *a aplicação projeção de* C *em* X_i. *Defina o seguinte conjunto*

$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c), \text{ para todo } i, j, \text{ com } j \geq i\}$$

e $\varphi_i = \pi_i \mid_X$, *para cada* i. *Então* (X, φ_i) *é um limite inverso de* (X_i, φ_{ij}).

(c) *Se* (X_i, φ_{ij}) *é um sistema inverso de grupos topológicos e homomorfismos contínuos, então* X *é um grupo topológico e as aplicações* φ_i *são homomorfismos contínuos.*

Demonstração:

(a) Primeiramente considere a família compatível $\{\varphi_i^{(1)} : X^{(1)} \longrightarrow X_i\}$ de aplicações contínuas (homomorfismos contínuos). A propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$ aplicada a família compatível $\{\varphi_i^{(2)} : X^{(2)} \longrightarrow X_i\}$ de aplicações contínuas (homomorfismos contínuos) nos dá que existe uma única aplicação contínua (homomorfismo contínuo) $\varphi^{(1)} : X^{(2)} \longrightarrow X^{(1)}$ tal que $\varphi_i^{(1)}\varphi^{(1)} = \varphi_i^{(2)}$, para cada i.

Agora considere a família compatível $\{\varphi_i^{(2)} : X^{(2)} \longrightarrow X_i\}$ de aplicações contínuas. A propriedade universal de $(X^{(2)}, \varphi_i^{(2)})$ aplicada a família compatível $\{\varphi_i^{(1)} : X^{(1)} \longrightarrow X_i\}$ de aplicações contínuas nos dá que existe uma única aplicação contínua $\varphi^{(2)} : X^{(1)} \longrightarrow X^{(2)}$ tal que $\varphi_i^{(2)}\varphi^{(2)} = \varphi_i^{(1)}$, para cada i.

Novamente, aplicando a propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$ a família $\{\varphi_i^{(1)} : X^{(1)} \longrightarrow X_i\}$ nos dá que existe uma única aplicação contínua $\psi : X^{(1)} \longrightarrow X^{(1)}$ tal que $\varphi_i^{(1)}\psi = \varphi_i^{(1)}$, para cada i. Entretanto, ambas as aplicações $\varphi^{(1)}\varphi^{(2)}$ e $id_{X^{(1)}}$, tem essa propriedade, uma vez que,

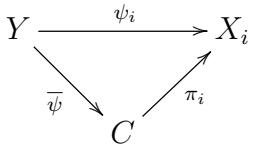
$$\varphi_i^{(1)} = \varphi_i^{(2)}\varphi^{(2)} \Rightarrow \varphi_i^{(1)} = (\varphi_i^{(1)}\varphi^{(1)})\varphi^{(2)} \Rightarrow \varphi_i^{(1)} = \varphi_i^{(1)}(\varphi^{(1)}\varphi^{(2)}).$$

Logo, pela unicidade de ψ, temos que, $\varphi^{(1)}\varphi^{(2)} = id_{X^{(1)}}$. E analogamente, $\varphi^{(2)}\varphi^{(1)} = id_{X^{(2)}}$. Portanto, $\varphi^{(2)} : X^{(1)} \longrightarrow X^{(2)}$ é um homeomorfismo (isomorfismo topológico resp.).

(b) Sejam Y um espaço topológico e $\{\psi_i : Y \longrightarrow X_i\}$ uma família compatível de aplicações contínuas. O objetivo é mostrar que existe uma única aplicação contínua $\psi : Y \longrightarrow X$ tal que $\varphi_i\psi = \psi_i$, para cada i.

Seja $\overline{\psi} : Y \longrightarrow C$ a aplicação que leva cada $y \in Y$ em $(\psi_i(y)) \in C$. Então, para todo $y \in Y$,

$$(\pi_i\overline{\psi})(y) = \pi_i(\overline{\psi}(y)) = \pi_i(\psi_i(y)) = \psi_i(y).$$



Logo, $\pi_i\overline{\psi} = \psi_i$. Além disso, $\overline{\psi}$ é contínua, pois sua composição com cada aplicação projeção é contínua.

Como $\{\psi_i : Y \longrightarrow X_i\}$ é uma família compatível de aplicações contínuas, então sempre que $j \geq i$, temos que $\psi_i = \varphi_{ij}\psi_j$. Assim, se $j \geq i$, então

$$\pi_i\overline{\psi} = \psi_i = \varphi_{ij}\psi_j = \varphi_{ij}\pi_j\overline{\psi}.$$

Logo, a imagem de $\overline{\psi}$ está contida em X. Agora defina $\psi : Y \longrightarrow X$ por $\psi(y) = \overline{\psi}(y)$, para cada y.

Temos que, ψ é contínua e $\varphi_i\psi = \psi_i$, para cada i.

Resta verificar a unicidade. Considere $\psi' : Y \longrightarrow X$ uma aplicação contínua satisfazendo $\varphi_i\psi' = \psi_i$, para cada $i \in I$. Então para cada $y \in Y$ e $i \in I$, $\psi'(y) = \psi(y)$ em X_i. Logo $\psi' = \psi$. Portanto, (X, φ_i) é um limite inverso de (X_i, φ_{ij}).

(c) Considere $C = \prod_{i\in I} X_i$ com a topologia produto e

$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c), \text{ para todo } i, j, \text{ com } j \geq i\}$$

com a topologia subespaço.

Por hipótese (X_i, φ_{ij}) é um sistema inverso de grupos toplógicos e homomorfismos contínuos. Então, pelo Lema 1.1.17, C é um grupo topológico com a topologia produto. Daí X é um grupo topológico com a topologia induzida. Segue que, a aplicação $\varphi_i = \pi_i \mid_X$ é contínua, pois a aplicação projeção é contínua, e a definição

de X garante que $\varphi_{ij}\varphi_j = \varphi_i$, sempre que $j \geq i$. E como φ_{ij} é um homomorfismo, por hipótese, então φ_i é um homomorfismo.

Portanto, X é um grupo topológico e a aplicação φ_i é um homomorfismo contínuo, para cada i.

■

Definição 1.2.9 *O limite inverso de um sistema inverso (X_i, φ_{ij}) é denotado por $\varprojlim(X_i, \varphi_{ij})$ ou simplesmente $\varprojlim X_i$. O limite inverso particular construído na Proposição 1.2.8 é denotado por $s\varprojlim X_i$.*

No exemplo a seguir, construiremos usando a proposição anterior, o limite inverso de $\mathbb{Z}/p^i\mathbb{Z}$. Esse exemplo será usado mais adiante, na Seção 1.4, na construção do completamento pro-p de $\mathbb{Z}$.

Exemplo 1.2.10 *O limite inverso de $\mathbb{Z}/p^i\mathbb{Z}$ é*

$$s\varprojlim \mathbb{Z}/p^j\mathbb{Z} = \{x \in C \mid x_j \equiv x_i \pmod{p^i},\ i \leq j,\ \text{onde } x_i,\ x_j \in \mathbb{Z}\},$$

onde C é o produto cartesiano de $\mathbb{Z}/p^i\mathbb{Z}$.

De fato, defina $C = \prod_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$ e a aplicação $\pi_i : C \longrightarrow \mathbb{Z}/p^i\mathbb{Z}$. Pela Proposição 1.2.8, temos que

$$s\varprojlim \mathbb{Z}/p^i\mathbb{Z} = \{x \in C \mid \varphi_{ij}\pi_j(x) = \pi_i(x),\ \text{para todo } i \leq j\}.$$

Considere $x \in s\varprojlim \mathbb{Z}/p^i\mathbb{Z}$, então $\varphi_{ij}\pi_j(x) = \pi_i(x)$, sempre que $i \leq j$. Segue que, $\varphi_{ij}\pi_j(x) = \varphi_{ij}(x_j + p^j\mathbb{Z}) = x_j + p^i\mathbb{Z}$ e $\pi_i(x) = x_i + p^i\mathbb{Z}$, assim $x_j + p^i\mathbb{Z} = x_i + p^i\mathbb{Z}$, o que implica que $x_j - x_i \in p^i\mathbb{Z}$, ou seja, $x_j \equiv x_i \pmod{p^i}$, sempre que $i \leq j$. Logo, $s\varprojlim \mathbb{Z}/p^j\mathbb{Z} = \{x \in C \mid x_j \equiv x_i \pmod{p^i},\ i \leq j\}$.

O próximo resultado nos diz que propriedades satisfeitas pelos espaços topológicos X_i de um sistema inverso podem ser estendidos para o limite inverso.

Proposição 1.2.11 *Seja (X_i, φ_{ij}) um sistema inverso indexado por um conjunto dirigido I, e escreva $X = \varprojlim X_i$.*

(a) *Se cada X_i é Hausdorff, então X é Hausdorff.*

(b) *Se cada X_i é totalmente desconexo, então X é totalmente desconexo.*

(c) *Se cada X_i é Hausdorff, então $s\varprojlim X_i$ é fechado no produto cartesiano $C = \prod_{i\in I} X_i$.*

(d) *Se cada X_i é compacto e Hausdorff, então X é compacto e Hausdorff.*

(e) *Se cada X_i é compacto, Hausdorff e não vazio, então X é não vazio.*

Demonstração: Observe que é suficiente mostrar que as afirmações são verdadeiras para $s\varprojlim X_i$, pois qualquer outro limite inverso é isomorfo a este. Como $s\varprojlim X_i$ é um subespaço topológico do produto cartesiano C, então as afirmações (a) e (b) seguem da Proposição 1.1.12. A afirmação (c) segue do Lema 1.1.8, item (e), uma vez que sendo as aplicações $\pi_i : X \longrightarrow X_i$ e $\varphi_{ij}\pi_j : X \longrightarrow X_i$ contínuas e X_i Hausdorff, então $\{x \in C \mid \varphi_{ij}\pi_j(x) = \pi_i(x),\ \text{para } i < j \ \text{ com } i, j \text{ fixos } \}$ é fechado em X, o que implica que

$$s\varprojlim X_i = \cap_{i<j}\{x \in C \mid \varphi_{ij}\pi_j(x) = \pi_i(x)\}$$

é fechado em C. Já a afirmação (d) segue das afirmações (a) e (c) juntamente com o Lema 1.1.8 e a Proposição 1.1.12. Resta mostrar a afirmação (e). Para $j > i$ considere o conjunto $D_{ij} = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\}$. Suponha por contradição que $s\varprojlim X_i = \emptyset$. Como cada D_{ij} é fechado e compacto então $\cap_{r=1}^{n} D_{i_r j_r} = \emptyset$, para algum inteiro n e $i_r, j_r \in I$. E como I é um conjunto dirigido, podemos encontrar $k \in I$ tal que $k \geq j_r$, para cada r. Escolha $x_k \in X_k$, defina $x_l = \varphi_{lk}(x_k)$, para $l \leq k$ e defina x_l arbitrariamente para todos os outros elementos de I. Desse modo, o elemento (x_i) do produto cartesiano está em $\cap_{r=1}^{n} D_{i_r j_r}$, o que é uma contradição. Portanto, $s\varprojlim X_i$ é não vazio.

■

Proposição 1.2.12 *Seja (X, φ_i) um limite inverso de um sistema inverso (X_i, φ_{ij}) de espaços de Hausdorff, compactos e não vazios, indexados por I. As seguintes afirmações são verdadeiras:*

(a) *$\varphi_i(X) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$, para cada $i \in I$.*

(b) *Os conjuntos $\varphi_i^{-1}(U)$ com $i \in I$ e U aberto em X_i, formam uma base para a topologia em X.*

(c) *Se Y é um subconjunto de X satisfazendo $\varphi_i(Y) = X_i$, para cada i, então Y é denso em X.*

(d) *Se θ é uma aplicação de um espaço Y em um espaço X, então θ é contínua se, e somente se, cada aplicação $\varphi_i\theta$ é contínua.*

(e) *Se $f : X \longrightarrow A$ é uma aplicação contínua para um espaço discreto, então para algum i, existe uma aplicação contínua $g : X_i \longrightarrow A$ satisfazendo $f = g\varphi_i$.*

Demonstração: Como foi dito anteriormente, é suficiente mostrar que os resultados são verdadeiros quando $X = s\varprojlim X_i$. Escreva $C = \prod_{i\in I} X_i$ e seja $\pi_i : C \longrightarrow X_i$ a aplicação projeção de modo que $\varphi_i = \pi_i \mid_X$.

(a) Temos que $\{\varphi_i : X \longrightarrow X_i \mid i \in I\}$ é uma família compatível de aplicações contínuas, então $\varphi_i = \varphi_{ij}\varphi_j$, sempre que $i \leq j$. Assim, $\varphi_i(X) = \varphi_{ij}\varphi_j(X) \subseteq \varphi_{ij}(X_j)$, para todo $j \geq i$ e portanto, $\varphi_i(X) \subseteq \bigcap_{j\geq i} \varphi_{ij}(X_j)$.

Por outro lado, fixando $i \in I$, $a \in \bigcap_{j\geq i} \varphi_{ij}(X_j)$ e para $j \geq i$ o conjunto $Y_j = \{y \in X_j \mid \varphi_{ij}(y) = a\}$. Observe que, Y_j é a imagem inversa de um conjunto fechado por uma aplicação contínua, uma vez que sendo X_i Hausdorff, o conjunto unitário é fechado, então Y_j é fechado em X_j, logo é compacto, pois todo subespaço fechado de um conjunto compacto é compacto.

Se $i \leq j \leq k$ e $y_k \in Y_k$, ou seja, $\varphi_{ik}(y_k) = a$, então $\varphi_{ij}(\varphi_{jk}(y_k)) = \varphi_{ik}(y_k) = a$, pois (X_i, φ_{ij}) é um sistema inverso, logo, $\varphi_{jk}(y_k) \in Y_j$.

Assim, $\{Y_j \mid j \geq i\}$ é um sistema inverso de espaços de Hausdorff, não vazios e compactos, com respeito às restrições da aplicações φ_{ij}. E pelo item (e) da proposição anterior, $s\varprojlim_{j\geq i} Y_j$ é não vazio, então existe $(b_j) \in s\varprojlim_{j\geq i} Y_j$. Assim $\varphi_{jk}(b_k) = b_j$ se $i \leq j \leq k$ e $b_i = a$.

Se $l \in I$ e $i \not\leq l$, tome $j \in I$, com $j \geq i, l$ e defina $b_l = \varphi_{lj}(b_j)$. Observe que isso é independente de j, pois se tivermos também $j' \geq i, l$, podemos encontrar $k \geq j, j'$ e termos $\varphi_{lj}(b_j) = \varphi_{lj}(\varphi_{jk}(b_k)) = \varphi_{lj'}\varphi_{j'k}(b_k) = \varphi_{lj'}(b_{j'})$.

Assim, $\varphi_{jk}(b_k) = b_j$ para todo par de índices j, k com $j \leq k$ e consequentemente temos $b = (b_j)_{j\in I} \in s\varprojlim_{j\in I} Y_j \subseteq X$.

Além disso, $\varphi_i(b) = \pi_i(b) = a$, então $a \in \varphi_i(X)$. Logo, $\bigcap_{j\geq i} \varphi_{ij}(X_j) \subseteq \varphi_i(X)$.

Portanto, $\varphi_i(X) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$.

(b) Como X é um subespaço topológico do produto cartesiano C, então todo conjunto aberto em X é a união de conjuntos da forma

$$P = X \cap \pi_{i_1}^{-1}(U_1) \cap \ldots \cap \pi_{i_n}^{-1}(U_n)$$

com $n \in \mathbb{N}$, $i_1, \ldots, i_n \in I$ e U_r aberto em X_{i_r}, para cada r.

Observe que, basta mostrar que para todo $a \in P$, existe um conjunto $\varphi_k^{-1}(U)$ com U aberto em X_k e $a \in \varphi_k^{-1}(U) \subseteq P$.

Seja $a = (a_i) \in X$. Como I é um conjunto dirigido, podemos escolher $k \in I$ tal que $k \geq i_1, \ldots, i_n$. O conjunto $\varphi_{i_r k}^{-1}(U_r)$ é aberto em X_k, pois U_r é aberto em X_{i_r} e $\varphi_{i_r k}$ é contínua, e além disso, $\varphi_{i_r k}^{-1}(U_r)$ contém a_k, uma vez que $\varphi_{ik}(a_k) = a_i$, para $i \leq k$.

Agora escreva $U = \bigcap_{r=1}^{n} \varphi_{i_r k}^{-1}(U_r)$. Então U é uma vizinhança aberta de a_k em X_k e então $\varphi_k^{-1}(U)$ é uma vizinhança aberta de a em X. Entretanto, se $b = (b_i) \in \varphi_k^{-1}(U)$, então $b_k \in U$ de modo que $b_{i_r} = \varphi_{i_r k}(b_k) \in U_r$, para $r = 1, \ldots, n$. Logo, $\varphi_k^{-1}(U) \subseteq P$, como queríamos mostrar.

(c) Vamos mostrar que Y é denso em X. Por definição, Y é denso em X quando $\overline{Y} = X$, isso equivale a afirmar que todo aberto não vazio em X contém pontos de Y.

Para cada $i \in I$ e cada aberto não vazio U em X_i, temos que $\varphi_i(Y) \cap U \neq \emptyset$, pois $\varphi_i(Y) = X_i$, logo $Y \cap \varphi_i^{-1}(U) \neq \emptyset$. E como os conjuntos $\varphi_i^{-1}(U)$ com $i \in I$ e U aberto em X_i formam uma base para a topologia em X, então todo aberto não vazio em X contém pontos de Y. Portanto, Y é denso em X.

(d) Suponha que a aplicação $\theta : Y \longrightarrow X$ é contínua. Como $\varphi_i : X \longrightarrow X_i$ é contínua e a composta de funções contínuas é contínua então $\varphi_i\theta$ é contínua.

Por outro lado, suponha que $\varphi_i\theta$ é contínua, então por definição, para cada $i \in I$ e para cada aberto U em X_i, $(\varphi_i\theta)^{-1}(U)$ é aberto em Y. Pelo item (b), os conjuntos $\varphi_i^{-1}(U)$ com $i \in I$ e U aberto em X_i formam uma base para a topologia em X. Assim, $\varphi_i^{-1}(U)$ é aberto em X, para cada i e para cada U aberto em X_i. Logo,

$$\theta^{-1}(\varphi_i^{-1}(U)) = (\theta^{-1}\varphi_i^{-1})(U) = (\varphi_i\theta)^{-1}(U)$$

é aberto em Y. Assim, para todo aberto W em X, $\theta^{-1}(W)$ é aberto em Y. E portanto, θ é contínua.

(e) Como f é contínua em um espaço discreto e X é compacto, então a imagem A_0 de f é compacta e discreta, e consequentemente, finita. Para cada $a \in A_0$ o conjunto $Y_a = f^{-1}(a)$ é compacto e aberto, e então é uma união finita de abertos $\varphi_j^{-1}(U)$, com $j \in I$ e U aberto em X_j. Assim, existe uma quantidade finita de conjuntos $\varphi_{j_1}^{-1}(U_1), \ldots, \varphi_{j_n}^{-1}(U_n)$ tal que cada conjunto Y_a é uma união de alguns desses conjuntos. Escolha um índice k tal que $k \geq j_r$, para $r = 1, \ldots, n$. Temos que $\varphi_{j_r}^{-1}(U_r) = \varphi_k^{-1}(\varphi_{j_r k}^{-1}(U_r))$, para cada r, uma vez que, $\varphi_{j_r} = \varphi_{j_r k}\varphi_k$, e então para cada $a \in A_0$ podemos escrever $Y_a = \varphi_k^{-1}(V_a)$ onde V_a é um subconjunto aberto de X_k.

Escreva $D = X_k \setminus \bigcup_{a \in A_0} V_a$. E observe que, $D \cap \varphi_k(X) = \emptyset$, então por (a) temos que $D \bigcap (\bigcap_{l \geq k} \varphi_{kl}(X_l)) = \emptyset$. Logo, existe uma quantidade finita de índices $l_1, \ldots, l_s$ tal que $D \cap \varphi_{kl_1}(X_{l_1}) \cap \ldots \cap \varphi_{kl_s}(X_{l_s}) = \emptyset$, uma vez que, D e cada conjunto $\varphi_{kl}(X_l)$ são fechados e X_k é compacto.

Escolha $i \geq l_1, \ldots, l_s$. Para $k \leq l \leq i$ temos que

$$\varphi_{ki}(X_i) = \varphi_{kl}(\varphi_{li}(X_i)) \subseteq \varphi_{kl}(X_k)$$

e como $D \cap \varphi_k(X) = \emptyset$ e $\varphi_k = \varphi_{kl}(\varphi_l) \supseteq \varphi_{ki}$, então $D \cap \varphi_{ki}(X_i) = \emptyset$ e $\varphi_{ki}(X_i) \subseteq \bigcup_{a \in A_0} V_a$.

agora escreva $W_a = \varphi_{ki}^{-1}(V_a)$ para cada a. Assim cada W_a é aberto em X_i e $W_{a_1} \cap W_{a_2} = \emptyset$ para $a_1 \neq a_2$.

Seja $x \in X_i$. Então $\varphi_{ki}(x) \in U_a$ para algum a, e $x \in \varphi_{ki}^{-1}(V_a) = W_a$. Logo, $X_i = \bigcup_{a \in A_0} W_a$, e cada conjunto W_a também é fechado. Segue que a aplicação $g : X_i \longrightarrow A$ que leva W_a em a para cada $a \in A_0$ é contínua e satisfaz $f = g\varphi_i$, como queríamos.

■

1.3 Caracterização dos Grupos Profinitos

Mais importante que a definição dos grupos profinitos pelo limite inverso é a sua caracterização, uma vez que a partir dela, teremos as principais propriedades que permitem avançar na pesquisa dos grupos profinitos de posto finito e os grupos pro-p, como é nosso objetivo final com relação ao estudo dos grupos profinitos.

Seja G um grupo topológico. Escreveremos $H \leq G$ para dizer que H é um subgrupo fechado de G e $N \lhd_{\circ} G$ para dizer que N é um subgrupo normal aberto de G. E chamaremos a família I de subgrupos normais de um grupo arbitrário G de base filtrada se para todo $K_1, K_2 \in I$ existe um subgrupo $K_3 \in I$ tal que K_3 está contido em $K_1 \cap K_2$.

Proposição 1.3.1 *Sejam (G, φ_i) um limite inverso de um sistema inverso (G_i) de grupos topológicos Hausdorff, compactos e seja $L \lhd_{\circ} G$. Então $ker\varphi_i \leq L$, para algum i. Consequentemente, G/L é isomorfo, como grupo topológico, a um grupo quociente de um subgrupo de algum G_i, e se além disso, cada aplicação φ_i é sobrejetiva, então G/L é isomorfo a um grupo quociente de algum G_i.*

A ideia da demonstração segue da Proposição 1.2.12, item (b), para mostrar que $ker\varphi_i \leq L$, e o restante segue do teorema do isomorfismo, para mais detalhes veja [22, Proposition 1.2.1].

Proposição 1.3.2 *Sejam G um grupo topológico e I uma base filtrada de subgrupos normais fechados, e para $K, L \in I$ defina $K \leq' L$ se, e somente se, $L \leq K$. E escreva $(\widehat{G}, \varphi_K) = \varprojlim G/K$. Então as seguintes afirmações são verdadeiras.*

(a) *I é um conjunto dirigido com respeito a ordem $\leq'$.*

(b) *Os homomorfismos sobrejetivos $q_{KL} : G/L \longrightarrow G/K$, definidos para $K \leq' L$, tornam os grupos G/K um sistema inverso $(G/K, \varphi_{KL})$.*

(c) *Existe um homomorfismo contínuo $\theta : G \longrightarrow \widehat{G}$ tal que $Ker\theta = \bigcap_{K \in I} K$, a imagem $Im\theta$ é um subgrupo denso de $\widehat{G}$, e a aplicação $\varphi_K\theta$ é a aplicação quociente de G em G/K para cada $K \in I$.*

(d) *Se G é compacto então θ é sobrejetiva.*

(e) *Se G é compacto e $\bigcap_{K \in I} K = 1$, então θ é um isomorfismo de grupos topológicos, ou seja, θ é um isomorfismo de grupos e um homeomorfismo.*

Demonstração: Veja que, o item (a) segue da definição de conjunto dirigido. E o item (b) já foi mostrado no Exemplo 1.2.4.

(c) Podemos considerar $\widehat{G} = s\underleftarrow{lim}G/K$, e considere a aplicação $\overline{\theta} : g \longrightarrow (gK)_{K\in I}$ de G em $C = \prod_{K\in I} G/K$. Seja $y \in Im\overline{\theta}$, então $y = (gK)_{K\in I} \in C$, para algum $g \in G$. Segue que,

$$q_{KL}(\pi_L(y)) = q_{KL}(\pi_L((gK)_{K\in I})) = q_{KL}(gL) = gK = \pi_K((gK)_{K\in I}).$$

Assim, $y \in \widehat{G}$, e consequentemente, $Im\overline{\theta} \subseteq \widehat{G}$.

Agora considere a aplicação induzida $\theta : G \longrightarrow \widehat{G}$. Como o produto de $\overline{\theta}$ com as aplicações projeções são homomorfismos contínuos, então $\overline{\theta}$ é um homomorfismo contínuo, e consequentemente, θ é um homomorfismo contínuo. E além disso, a aplicação $\varphi_K\theta$ é a aplicação quociente de G em G/K para cada $K \in I$, onde $\varphi_K = \pi_K \mid_{\widehat{G}}$.

Agora, para verificar que $Ker\theta = \bigcap_{K\in I} K$, basta ver que, dado $g \in G$, temos que $g \in Ker\theta$ se, e somente se, $Kg = K$, para cada $K \in I$.

Resta verificar que $Im\theta$ é um subgrupo denso em $\widehat{G}$. Observe que, para cada $K \in I$, $\varphi(\theta(G)) = G/K$. Então pela Proposição 1.2.12 (c) $\theta(G) = Im\theta$ é denso em $\widehat{G}$.

(d) Como $K \in I$ é um subgrupo normal fechado de G, então pelo Lema 1.1.14 item (f) G/K é Hausdorff, para todo $K \in I$. E pelo Teorema 1.1.12 item (a) C é Hausdorff. Além disso, $Im\theta = \theta(G)$ é compacto, uma vez que, G é compacto e θ é contínua. Assim, temos $\theta(G)$ um subgrupo compacto de C, com C Hausdorff, então pelo Lema 1.1.8 item (b), $\theta(G)$ é fechado. Logo, $\theta(G) = \overline{\theta(G)}$. Mas pelo item anterior $\theta(G)$ é denso em $\widehat{G}$, então $\widehat{G} = \overline{\theta(G)}$. E portanto, θ é sobrejetiva.

(e) Temos que $Ker\theta = \bigcap_{K\in I} K = 1$, então θ é injetiva, e como θ também é sobrejetiva, então θ é bijetiva. Além disso, G é compacto, $\widehat{G}$ é Hausdorff e θ é contínua, então pelo Lema 1.1.8 item (d), θ é um homeomorfismo.

■

Considere agora uma classe $\mathcal{C}$ não vazia de grupos finitos, ou seja, $\mathcal{C}$ contém todas as imagens isomórficas de grupos de $\mathcal{C}$. Assim, se $\mathcal{C}$ é uma classe e se $F_1 \in \mathcal{C}$ e $F_2 \cong F_1$, então $F_2 \in \mathcal{C}$.

Dizemos que um grupo F é um $\mathcal{C}$-grupo se $F \in \mathcal{C}$, e que G é um grupo pro-$\mathcal{C}$ se G é um limite inverso de um sistema inverso com homomorfismos sobrejetivos de $\mathcal{C}$-grupos. Observe que um $\mathcal{C}$-grupo é um grupo pro-$\mathcal{C}$, correspondente a um sistema inverso com respeito a um conjunto dirigido contendo só um elemento. Além disso, dizemos que a classe $\mathcal{C}$ é fechada para subgrupos (respectivamente quocientes) se cada subgrupo (respectivamente grupos quocientes) de um $\mathcal{C}$-grupo é um $\mathcal{C}$-grupo. E dizemos que a classe $\mathcal{C}$ é fechada para produtos diretos se $F_1 \times F_2 \in \mathcal{C}$, sempre que, $F_1 \in \mathcal{C}$ e $F_2 \in \mathcal{C}$. Algumas classes importantes são:

(i) A classe de todos os grupos finitos;

(ii) A classe dos p-grupos finitos, onde p é um primo fixado;

(iii) E a classe de todos os grupos cíclicos finitos.

E como já foi dito anteriormente, o limite inverso de grupos finitos é chamado *grupo profinito*. Já o limite inverso de p-grupos finitos é chamado *grupo pro-p*. E o limite inverso de grupos cíclicos finitos é chamado *grupo procíclico*.

O teorema a seguir fornece equivalências de algumas caracterizações de grupos pro-$\mathcal{C}$, garante por exemplo que se G é um grupo pro-$\mathcal{C}$, então G é profinito e G/N é um $\mathcal{C}$-grupo, para todo $N \lhd_\circ G$, onde $\mathcal{C}$ é uma classe de grupos finitos fechada para subgrupos, produtos diretos e quocientes.

Teorema 1.3.3 *Sejam $\mathcal{C}$ uma classe de grupos finitos que é fechada para subgrupos e produtos diretos e G um grupo topológico. As seguintes afirmações são equivalentes:*

(i) *G é grupo pro-$\mathcal{C}$;*

(ii) *G é isomorfo, como grupo topológico, a um subgrupo fechado de um produto cartesiano de $\mathcal{C}$-grupos;*

(iii) *G é compacto e $\bigcap(N \mid N \lhd_\circ G \, e \, G/N \in \mathcal{C}) = 1$;*

(iv) *G é compacto e totalmente desconexo, e para cada $L \lhd_\circ G$ existe um subgrupo $N \lhd_\circ G$ com $N \leq L$ e $G/N \in \mathcal{C}$.*

Além disso, $\mathcal{C}$ é fechado para quocientes, então (iv) pode ser substituído por

(iv)' *G é compacto e totalmente desconexo $G/L \in \mathcal{C}$ para cada $L \lhd_o G$.*

Demonstração:

(i) $\Rightarrow$ (ii) Seja G um grupo pro-$\mathcal{C}$, então por definição, G é um limite inverso de $\mathcal{C}$-grupos, onde $\mathcal{C}$ é uma classe de grupos finitos. Então podemos considerar a topologia discreta em $G_i \in \mathcal{C}$, para cada i, uma vez que, sendo G_i finito, consideraremos a topologia no qual os subconjuntos de G_i são abertos em G_i, para cada i. E sendo G_i um grupo topológico com a topologia discreta, para cada i, então G_i é Hausdorff, para cada i, e pela Proposição 1.2.11 item (c), $s\varprojlim G_i$ é fechado no produto cartesiano de $C = \prod_{i\in I} G_i$.

Por outro lado, o limite inverso de um sistema inverso é único a menos de isomorfismo, então $s\varprojlim G_i \cong G$. Portanto, G é isomorfo a um subgrupo fechado de um produto cartesiano de $\mathcal{C}$-grupos.

(ii) $\Rightarrow$ (iii) Note que, como $G_i \in \mathcal{C}$ é um grupo topológico com a topologia discreta, para cada i, então G_i é compacto, para cada i. E como o produto de compactos é compacto, então C é compacto. Por hipótese, G é isomorfo a um subgrupo fechado $\widehat{G}$ de C, então pelo Lema 1.1.8 item (a), $\widehat{G}$ é compacto, e consequentemente, G é compacto.

Agora, para cada i, defina K_i o núcleo da aplicação projeção de C em G_i e $N_i = K_i \cap \widehat{G}$. Como $K_i \lhd_o C$, então $N_i \lhd_o \widehat{G}$. Observe que, dado $x \in \bigcap_{i\in I} K_i$, então $\pi_i(x) = 1_i$, para todo $i \in I$, mas por outro lado, $\pi_i(x) = x_i$, para todo $i \in I$, então, $x_i = 1_i$, para todo $i \in I$, logo, $\bigcap_{i\in I} K_i = 1$ e consequentemente, $\bigcap_{i\in I} N_i = 1$. Além disso, pelo teorema do isomorfismo

$$\frac{\widehat{G}}{N_i} = \frac{\widehat{G}}{K_i \cap \widehat{G}} \cong \frac{\widehat{G}K_i}{K_i} \leq \frac{C}{K_i} \cong G_i,$$

e então, $\dfrac{\widehat{G}}{N_i} \in \mathcal{C}$, para cada i. Portanto, $\bigcap(N \mid N \lhd_o G \, e \, G/N \in \mathcal{C}) = 1$.

(iii) $\Rightarrow$ (i) Escreva $I = \{N \lhd_o G \mid G/N \in \mathcal{C}\}$. E considere $\psi : G \longrightarrow G/N_1 \times G/N_2$ uma aplicação definida por $\psi(g) = (N_1 g, N_2 g)$, onde $N_1, N_2 \in I$. Agora veja que ψ é contínua, pois as aplicações quocientes $G \longrightarrow G/N_1$ e $G \longrightarrow G/N_2$ são

contínuas. Além disso, ψ é um homomorfismo e $K = N_1 \cap N_2$ é o núcleo de ψ. De fato, dado $g_1, g_2 \in G$ temos que,

$$\begin{aligned}\psi(g_1g_2) &= (N_1(g_1g_2), N_2(g_1g_2)) = ((N_1g_1)(N_1g_2), (N_2g_1)(N_2g_2)) \\ &= (N_1g_1, N_2g_1)\,(N_1g_2, N_2g_2) = \psi(g_1)\,\psi(g_2),\end{aligned}$$

e

$$Ker\,\psi = \{g \in G \mid \psi(g) = (N_1, N_2)\} = \{g \in G \mid (N_1g, N_2g) = (N_1, N_2)\} = N_1 \cap N_2.$$

Assim, $N_1 \cap N_2 = Ker\,\psi \lhd_o G$. Pelo teorema do isomorfismo

$$\frac{G}{N_1 \cap N_2} \cong Im(\psi) \leq \frac{G}{N_1} \times \frac{G}{N_2}.$$

E como $G/N_1 \times G/N_2$ é um $\mathcal{C}$-grupo, então $\dfrac{G}{N_1 \cap N_2}$ é um $\mathcal{C}$-grupo. Dessa forma, temos que $N_1 \cap N_2 \lhd_o G$ e $\dfrac{G}{N_1 \cap N_2} \in \mathcal{C}$, então $N_1 \cap N_2 \in I$. Logo, pela Proposição 1.3.2 item (e), $G \cong \varprojlim G/N$, onde $N \in I$. E portanto, G é um grupo pro-$\mathcal{C}$.

(i) ⇒ (iv) Temos que $G_i \in \mathcal{C}$, para cada i, então G_i com a topologia discreta é compacto e totalmente desconexo, e pela Proposição 1.2.11, $G = \varprojlim G_i$ é compacto e totalmente desconexo. Além disso, G é Hausdorff, pela mesma proposição, então pela Proposição 1.3.1, dado $L \lhd_o G$, existe $N = Ker\,\varphi_i \lhd_o G$, com $N \leq L$, para algum i. E pelo teorema do isomorfismo $G/N \cong Im\varphi_i \leq G_i \in \mathcal{C}$, logo, $G/N \in \mathcal{C}$, como queríamos.

(iv) ⇒ (iii) É imediato da Proposição 1.1.16.

■

Assim, tomando $\mathcal{C}$ como a classe de todos os grupos finitos, obtemos uma importante caracterização de grupos profinitos:

Corolário 1.3.4 *Seja G um grupo topológico. São equivalentes.*

(i) *G é um grupo profinito;*

(ii) *G é isomorfo, como grupo topológico, a um subgrupo fechado de um produto cartesiano de grupos finitos;*

(iii) *G é compacto e $\bigcap\{N \mid N \lhd_o G\} = 1$;*

(iv) *G é compacto e totalmente desconexo.*

Para finalizar essa seção daremos um resultado que descreve como um grupo profinito e seus subgrupos e grupos quocientes podem ser representados explicitamente como limite inverso.

Teorema 1.3.5 **(a)** *Seja G um grupo profinito. Se I é uma base filtrada de subgrupos normais fechados de G tal que $\bigcap\{N \mid N \in I\} = 1$, então $G \cong \varprojlim G/N$, com $N \in I$.*

Além disso, $H \cong \varprojlim H/H\cap N$, para cada subgrupo fechado H e $G/K \cong \varprojlim G/KN$, com $K \in I$.

(b) *Se $\mathcal{C}$ é uma classe de grupos finitos que é fechado para subgrupos e produtos diretos, então subgrupos fechados, produtos cartesianos e limites inversos de grupos pro-$\mathcal{C}$ são grupos pro-$\mathcal{C}$. Se além disso, $\mathcal{C}$ é fechada para quocientes, então grupos quocientes de grupos pro-$\mathcal{C}$ por subgrupos normais fechados são grupos pro-$\mathcal{C}$.*

Demonstração:

(a) Primeiramente mostraremos que $G \cong \varprojlim_{N\in I} G/N$. Temos que, G é um grupo topológico, e por hipótese, I é uma base filtrada de subgrupos normais fechados de G, então aplicando a Proposição 1.3.2, existe um homomorfismo contínuo $\theta : G \longrightarrow \widehat{G}$, onde $\widehat{G} = \varprojlim_{N\in I} G/N$. Novamente pela hipótese, $\bigcap_{N\in I} N = 1$ e sabendo que G é compacto pelo Corolário 1.3.4, então pela Proposição 1.3.2, $G \cong \widehat{G} = \varprojlim_{N\in I} G/N$.

Agora mostraremos que $H \cong \varprojlim_{N\in I} H/(H \cap N)$, para H subgrupo fechado. Por G ser um grupo topológico, temos que H também é um grupo topológico. Assim, consideremos o conjunto $T = \{H \cap N \mid N \in I\}$. Note que T é uma base filtrada de subgrupos normais fechados de H, então aplicando a Proposição 1.3.2, obtemos que existe um homomorfismo contínuo $\theta : H \longrightarrow \widehat{H}$, onde $\widehat{H} = \varprojlim_{N\in I} H/(H\cap N)$. Por outro lado, como $\bigcap_{N\in I} N = 1$, obtemos $\bigcap_{N\in I}(H\cap N) = 1$ e sabendo que H é compacto pelo Corolário 1.3.4, segue pela Proposição 1.3.2, que $H \cong \widehat{H} = \varprojlim_{N\in I} H/(H \cap N)$.

Resta mostrar que, $G/K \cong \varprojlim_{N\in I} G/NK$. Considere a família $J = \{NK \mid N \in I\}$, temos que J é uma base filtrada de subgrupos normais fechados de G contendo K. Temos que

$$\cap\{M \mid M \in J\} = \cap\{NK \mid N \in I\} = (\cap\{N \mid N \in I\})\, K = K.$$

Agora considere φ o epimorfismo canônico de G em G/K. Daí, podemos trabalhar no quociente G/K e assumir que $K = 1$. Como G é um grupo topológico, então G/K é também um grupo topológico. Por outro lado, considere o conjunto $\varphi(J) = \{NK/K \mid N \in I\}$, temos que $\varphi(J)$ é uma base filtrada de subgrupos normais fechados de G/K. Assim, aplicando a Proposição 1.3.2 a G/K e o terceiro teorema do isomorfismo, temos que

$$\widehat{(G/K)} = \varprojlim_{N\in I} \frac{G/K}{NK/K} \cong \varprojlim_{N\in I} G/NK.$$

Assim, desde que $\bigcap_{N\in I} NK = K$, segue que $\bigcap_{N\in I} NK/K = 1$. Logo,

$$G/K \cong \widehat{(G/K)} = \varprojlim_{N\in I} \frac{G/K}{NK/K} \cong \varprojlim_{N\in I} G/NK.$$

e a afirmação segue.

(b) Observe que as afirmações sobre subgrupos e grupos quocientes seguem direto do item (a), ou seja, subgrupos fechados e grupos quocientes de grupos pro-$\mathcal{C}$ são grupos pro-$\mathcal{C}$.

Como subgrupos fechados de subgrupos fechados, são subgrupos fechados e produto cartesiano de produtos cartesiano são produtos cartesiano, então a afirmação segue da equivalência de (i) e (ii) do Teorema 1.3.3.

Agora, como grupos profinitos são Hausdorff, então pela Proposição 1.2.11 item (c), os limites inversos dos grupos pro-$\mathcal{C}$ são isomorfos a subgrupos fechados do produto cartesiano de grupos pro-$\mathcal{C}$, então são grupos pro-$\mathcal{C}$.

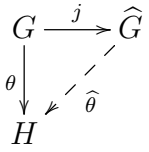
■

1.4 Completamento e Anel dos Inteiros p-Ádicos

Nesta seção mostraremos como um grupo profinito pode ser construído a partir de um grupo abstrato. Em particular, faremos tal construção para o anel $\mathbb{Z}_p$, o anel dos inteiros p-ádicos, que é o completamento pro-p de $\mathbb{Z}$ e apresentaremos algumas das suas principais propriedades. Construiremos também o completamento profinito de $\mathbb{Z}$.

Seja G um grupo abstrato e I uma base filtrada não vazia de subgrupos normais de índice finito. Lembrando que, se definirmos uma topologia onde um subconjunto de G é aberto se, e somente se, é uma união de classes laterais Kg, com K um subgrupo qualquer em I, o Lema 1.1.18 garante que G é um grupo topológico.

Definição 1.4.1 *O completamento de G com respeito a I consiste de um grupo profinito $\widehat{G}$ e um homomorfismo contínuo $j : G \longrightarrow \widehat{G}$ com a seguinte propriedade: sempre que $\theta : G \longrightarrow H$ é um homomorfismo contínuo, onde H é um grupo finito, existe um único homomorfismo contínuo $\widehat{\theta} : \widehat{G} \longrightarrow H$ tal que $\theta = \widehat{\theta} j$, ou seja, tal que o diagrama abaixo comuta.*



Proposição 1.4.2 *Sejam $\widehat{G} = s\varprojlim_I G/K$ e a aplicação $j : G \longrightarrow \widehat{G}$, definida por $g \longmapsto (Kg)$. Então, o par $(\widehat{G}, j)$ possui as propriedades do completamento de G com respeito a I.*

Demonstração: Pela Proposição 1.3.2 vemos que j é um homomorfismo contínuo. Seja $\theta : G \longrightarrow H$ um homomorfismo contínuo com H sendo um grupo finito. Então, $ker\theta$ é aberto. Assim, $ker\theta$ é uma união de classes laterais Lg para algum subgrupo L em I, logo $ker\theta$ contém algum L em I. Defina $\widehat{\theta} : \widehat{G} \longrightarrow H$ como a composição das aplicações ψ e γ, onde $\gamma : \widehat{G} \longrightarrow G/L$ é definida por $(Kg) \longmapsto Lg$ e $\psi : G/L \longrightarrow H$ é definida por $Lg \longmapsto \theta(g)$, ou seja, o homomorfismo induzido por θ no quociente G/L. Veja que, γ e ψ são homomorfismos contínuos, então $\widehat{\theta} = \psi\gamma$ é um homomorfismo contínuo.

Agora se $g \in G$, então $j(g) = (Kg) \in \widehat{G}$, logo $\widehat{\theta}(j(g)) = \widehat{\theta}(Kg) = \psi(\gamma(Kg)) = \psi(Lg) = \theta(g)$. Logo, $\widehat{\theta} j = \theta$.

Resta mostrar que $\widehat{\theta}$ é única. Seja $\varphi : \widehat{G} \longrightarrow H$ outro homomorfismo contínuo satisfazendo $\theta = \varphi j$, então temos que $\widehat{\theta}$ e φ coincidem em $j(G)$ e, pela Proposição

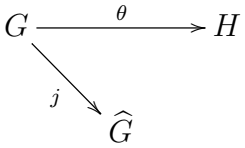
1.3.2, obtemos que $j(G)$ é denso em $\widehat{G}$, ou seja, $\overline{j(G)} = \widehat{G}$. Agora veja que, como as aplicações $\widehat{\theta}, \varphi : \widehat{G} \longrightarrow H$ são contínuas e H é Hausdorff, então pelo Lema 1.1.8 item (e), $\{x \in \widehat{G} \mid \widehat{\theta}(x) = \varphi(x)\}$ é fechado em $\widehat{G}$. Logo, $\widehat{\theta} = \varphi$ e o resultado segue. ■

O próximo passo é mostrar que o completamento de G com respeito a I é unicamente determinado, mas para isto precisamos reformular a definição de completamento em termos de uma propriedade universal.

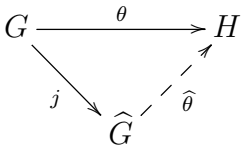
Proposição 1.4.3 *Sejam G e I como acima e suponha que $\widehat{G}$ é um grupo profinito e $j : G \longrightarrow \widehat{G}$ um homomorfismo contínuo. Então as seguintes afirmações são equivalentes:*

(i) *O par $(\widehat{G}, j)$ possui a propriedade que define um completamento de G com respeito a I.*

(ii) *Para cada diagrama*



onde H é um grupo profinito e θ é um homomorfismo contínuo, existe um único homomorfismo contínuo $\widehat{\theta} : \widehat{G} \longrightarrow H$ que torna o diagrama a seguir comutativo.



A demonstração desse resultado pode ser encontrada em [22, Proposition 1.4.2].

O próximo resultado nos garante que o completamento de G é único a menos de isomorfismo.

Proposição 1.4.4 *Se $(\widehat{G_1}, j_1)$ e $(\widehat{G_2}, j_2)$ são completamentos de G com respeito a I, então existe um isomorfismo $\alpha : \widehat{G_1} \longrightarrow \widehat{G_2}$ satisfazendo $\alpha j_1 = j_2$.*

Demonstração: Considerando o completamento $(\widehat{G_1}, j_1)$ e o homomorfismo contínuo $j_2 : G \longrightarrow \widehat{G_2}$, temos que existe um único homomorfismo contínuo $\alpha : \widehat{G_1} \longrightarrow \widehat{G_2}$ tal que $\alpha j_1 = j_2$. Analogamente, considerando $(\widehat{G_2}, j_2)$ como completamento de G e o homomorfismo contínuo $j_1 : G \longrightarrow \widehat{G_1}$, temos que existe um único homomorfismo contínuo $\beta : \widehat{G_2} \longrightarrow \widehat{G_1}$ tal que $\beta j_2 = j_1$. Assim, fazendo algumas substituições temos

que $j_1 = (Id_{\widehat{G_1}})j_1 = (\beta\alpha)j_1$. Agora considerando o completamento $(\widehat{G_1}, j_1)$ e o homomorfismo contínuo $j_1 : G \longrightarrow \widehat{G_1}$, temos que existe um único homomorfismo contínuo γ satisfazendo $\gamma j_1 = j_1$. Então, segue que $\beta\alpha = Id_{\widehat{G_1}}$. Agora, considerando o completamento $(\widehat{G_2}, j_2)$ obtemos $\alpha\beta = Id_{\widehat{G_2}}$, o que implica que α e β são inversas, Portanto, α é um isomorfismo.

■

Proposição 1.4.5 *Seja $(\widehat{G}, j)$ o completamento de G com respeito a I. Então as seguintes afirmações valem:*

(a) *A imagem $j(G)$ é densa em $\widehat{G}$;*

(b) *$kerj = \bigcap_{K\in I} K$.*

Demonstração: Observe que podemos considerar $\widehat{G} = s\varprojlim G/K$ e a aplicação $j : G \longrightarrow \widehat{G}$ tal que $g \longmapsto (Kg)$, pois nestas condições a Proposição 1.4.2 garante que $(\widehat{G}, j)$ tem a propriedade do completamento de G com respeito a I, e pela Proposição 1.4.4, se $(\widehat{G_1}, j_1)$ e $(\widehat{G_2}, j_2)$ são dois completamentos de G, então $\widehat{G_1}$ e $\widehat{G_2}$ são isomorfos. E como G é um grupo topológico e I é uma base filtrada, então pela Proposição 1.3.2, existe um homomorfismo contínuo $j : G \longrightarrow \widehat{G}$, $j(G)$ um subgrupo denso em $\widehat{G}$. E veja que, um elemento g pertencente ao $kerj$ se, e somente se, $j(g) = (K)$, para cada K em I, ou seja, se $Kg = K$. Segue que, $g \in K$ para todo $K \in I$, logo, $kerj = \bigcap_{K\in I} K$. E portanto, $j(G)$ um subgrupo denso em $\widehat{G}$ e $kerj = \bigcap_{K\in I} K$, o que prova (a) e (b).

■

Pensando nas ideias acima e de uma maneira geral nos grupos pro-$\mathcal{C}$, temos a seguinte definição:

Definição 1.4.6 *O* completamento pro-$\mathcal{C}$ *de G é o completamento de G com respeito à família de subgrupos normais K de G tais que $G/K \in \mathcal{C}$.*

Então, de acordo com essa definição, temos que:

(i) O *completamento profinito* de um grupo G é o completamento de G com respeito à família de todos subgrupos normais de índice finito.

(ii) Seja p um primo, o *completamento pro-p* de um grupo G é o completamento de G com respeito à família de todos subgrupos normais de índice igual a uma potência de p.

Observe que, se R é um anel, então será natural considerar seu completamento com respeito a família de ideais K de índice finito. A construção de $s\varprojlim R/K$ mostra que o completamento é um anel e que a aplicação de R em seu completamento é um homomorfismo de anéis. Isso se aplica ao completamento de $\mathbb{Z}$, uma vez que todos os subgrupos de $\mathbb{Z}$ são ideais.

Agora estamos prontos para construir o completamento pro-p de $\mathbb{Z}$.

Seja p um primo fixado. E considere o sistema inverso de anéis $(\mathbb{Z}/p^i\mathbb{Z})$, conforme vimos no Exemplo 1.2.3.

Seja $\mathbb{Z}_p = \{\sum_{j=0}^{\infty} a_j p^j \mid 0 \leq a_j < p, \text{ para cada } j\}$ o conjunto das somas formais infinitas. E defina para cada $i \geq 1$ as seguintes aplicações:

$$\begin{array}{rccc} \varphi_i & : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^i\mathbb{Z} \\ & & z = \sum_{j=0}^{\infty} a_j p^j & \longmapsto & \sum_{j=0}^{i-1} a_j p^j + p^i\mathbb{Z}. \end{array}$$

e

$$\begin{array}{rccc} \theta & : & \mathbb{Z}_p & \longrightarrow & s\varprojlim \mathbb{Z}/p^i\mathbb{Z} \\ & & z & \longmapsto & (\varphi_i(z) \mid i \geq 1). \end{array}$$

Nosso objetivo é mostrar que $\mathbb{Z}_p$ é o completamento pro-p de $\mathbb{Z}$. Para isso, precisamos mostrar que θ é uma bijeção. Lembrando que, pelo Exemplo 1.2.10, o limite inverso de $\mathbb{Z}/p^i\mathbb{Z}$ é

$$s\varprojlim \mathbb{Z}/p^j\mathbb{Z} = \{x \in C \mid x_j \equiv x_i \pmod{p^i},\ i \leq j, \text{ onde } x_i, x_j \in \mathbb{Z}\},$$

onde C é o produto cartesiano de $\mathbb{Z}/p^i\mathbb{Z}$.

Lema 1.4.7 *A aplicação θ é uma bijeção.*

Demonstração: Veja que, θ é injetiva, uma vez que $ker\theta = \bigcap_{i>1} p^i\mathbb{Z} = 1$.

Resta mostrar que θ é sobrejetiva.

Seja $x = (x_i + p^i\mathbb{Z} \mid i \geq 0) \in s\varprojlim \mathbb{Z}/p^j\mathbb{Z}$. Observe que podemos escolher $0 \leq x_i < p^i$. E defina $a_0 = x_1$. Como $x \in s\varprojlim \mathbb{Z}/p^j\mathbb{Z}$, então para $i \geq 1$, temos que

$$x_{i+1} \equiv x_i \pmod{p^i} \Rightarrow x_{i+1} - x_i = a_i p^i \Rightarrow x_{i+1} = x_i + a_i p^i.$$

Agora vamos abrir um parêntese e mostrar por indução sobre i que $0 \leq a_i < p$.

Se $i = 1$, então $x_2 \equiv x_1 \pmod{p}$, o que implica que, $x_2 = x_1 + a_1 p$. Mas $0 \leq x_1 < p$, e $0 \leq x_2 < p^2$, logo, $0 \leq x_1 + a_1 p < p^2$, assim $0 \leq a_1 < p$.

Suponha que a afirmação é verdadeira para todo a_j tal que $j < i$. E vamos mostrar que é verdade para i.

Temos que, $x_{i+1} = x_i + a_i p^i$ e $0 \leq x_{i+1} < p^{i+1}$, então $0 \leq x_i + a_i p^i < p^{i+1}$. Por outro lado, fazendo todas as substituições de x_k em x_i, com $k = \{1, 2, \ldots, i-1\}$, temos que

$$x_i = x_{i-1} + a_{i-1}p^{i-1} = x_{i-2} + a_{i-2}p^{i-2} + a_{i-1}p^{i-1} = \ldots = a_0 + a_1 p + \ldots + a_{i-1}p^{i-1}.$$

Assim, substituindo o valor de x_i em $0 \leq x_i + a_i p^i < p^{i+1}$, temos $0 \leq a_0 + a_1 p + \ldots + a_{i-1}p^{i-1} + a_i p^i < p^{i+1}$, onde $0 \leq a_j < p$, para todo $j \in \{0, 1, 2, \ldots, i-1\}$, por hipótese de indução, daí concluímos que $0 \leq a_i < p$. Portanto, $0 \leq a_i < p$, para todo $i \geq 1$.

Segue que, $x_{i+1} = x_i + a_i p^i = a_0 + a_1 p + \ldots + a_{i-1}p^{i-1} + a_i p^i = \sum_{j=0}^{i} a_j p^j$.

Agora observe que, tomando $z = \sum_{j=0}^{\infty} a_j p^j$, com $0 \leq a_j < p$, temos $\varphi_i(z) = \sum_{j=0}^{i-1} a_j p^j + p^i\mathbb{Z}$ e $\theta(z) = (\varphi_i(z) \mid i \geq 0) = (x_i + p^i\mathbb{Z} \mid i \geq 0) = x$. Assim, $x = \theta(\sum_{j=0}^{\infty} a_j p^j)$. Logo, θ é sobrejetiva. E portanto, é uma bijeção. ■

Lema 1.4.8 *$\mathbb{Z}_p$ é um completamento pro-p de $\mathbb{Z}$.*

Demonstração: Para mostrar que $\mathbb{Z}_p$ é o completamento pro-p de $\mathbb{Z}$ precisamos introduzir em $\mathbb{Z}_p$ uma estrutura de anel topológico, sendo assim, vamos definir as operações de soma e produto e quem são os conjuntos abertos.

Defina a seguinte topologia em $\mathbb{Z}_p$: Um subconjunto de $\mathbb{Z}_p$ é aberto se sua imagem com respeito a θ é um aberto. Agora sejam z_1 e z_2 elementos de $\mathbb{Z}_p$, a soma e o produto em $\mathbb{Z}_p$ são definidos por

$z_1 + z_2 =: \theta^{-1}(\theta(z_1) + \theta(z_2))$

$z_1 z_2 =: \theta^{-1}(\theta(z_1)\theta(z_2))$.

Assim, com essa operações $\mathbb{Z}_p$ é um anel topológico. Logo, θ é um homomorfismo bijetor, o que implica que, θ é um isomorfismo de anéis topológicos. E portanto

$$(\mathbb{Z}_p, \varphi_i) \cong \varprojlim \mathbb{Z}/p^i\mathbb{Z} \cong s\varprojlim \mathbb{Z}/p^i\mathbb{Z}.$$

E como $(\mathbb{Z}/p^i\mathbb{Z})$ é um sistema inverso de anéis finitos então, $\mathbb{Z}_p$ é um anel pro-p.

■

O anel $\mathbb{Z}_p$ é chamado o *anel dos inteiros p-ádicos*.

Observe que, podemos considerar $\mathbb{Z}$ como o subconjunto de $\mathbb{Z}_p$ formado pelas somas formais infinitas $\sum_{j=0}^{\infty} a_j p^j$ com $a_j = 0$ para todos exceto para uma quantidade finita de valores de j. Dessa forma, a aplicação θ coincide em $\mathbb{Z}$ com a aplicação natural j de $\mathbb{Z}$ em $s\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ (onde a aplicação natural é a aplicação inclusão), então pela Proposição 1.4.2, $(\mathbb{Z}_p, j)$ é o completamento pro-p de $\mathbb{Z}$, onde I é formado pelos subgrupos normais de $\mathbb{Z}$ da forma $p^i\mathbb{Z}$ cujo índice é uma potência de p.

Agora apresentaremos mais algumas propriedades relevantes de $\mathbb{Z}_p$:

(i) Os únicos subgrupos abertos de $\mathbb{Z}_p$ são os subgrupos da forma $p^i\mathbb{Z}_p$, com $i = 0, 1, 2, \ldots$.

De fato, seja H um subgrupo aberto de índice p^i, então $p^i(\mathbb{Z}_p/H) = 0_{\overline{H}}$, então $p^i\mathbb{Z}_p \leq H$. Além disso, $\mathbb{Z}_p/ker\varphi_i = \mathbb{Z}_p/p^i\mathbb{Z}_p \cong Im\varphi_i = \mathbb{Z}/p^i\mathbb{Z}$, e como $\mathbb{Z}/p^i\mathbb{Z}$ é cíclico de ordem p^i, então $\mathbb{Z}_p/p^i\mathbb{Z}_p$ é cíclico de ordem p^i, e consequentemente, $|\mathbb{Z}_p/p^i\mathbb{Z}_p| = p^i = |\mathbb{Z}_p/H|$, logo devemos ter que $H = p^i\mathbb{Z}_p$ com $i = 0, 1, 2, \ldots$.

(ii) Os subgrupos fechados de $\mathbb{Z}_p$ são os subgrupos abertos juntamente com o subgrupo $\{0\}$.

De fato, seja K um subgrupo fechado de $\mathbb{Z}_p$, então por definição, K é uma interseção de subgrupos abertos de $\mathbb{Z}_p$, mas os subgrupos abertos de $\mathbb{Z}_p$ são $p^i\mathbb{Z}_p$ com $i = 0, 1, 2, \ldots$, então $K = p^j\mathbb{Z}_p$ para algum $j \in \{0, 1, 2, \ldots\}$ ou $K = \{0\}$.

(iii) $\mathbb{Z}_p$ é um domínio de integridade.

De fato, seja $x \in \mathbb{Z}_p \setminus \{0\}$, então $x = \sum_{j=0}^{\infty} a_j p^j$, com $a_j \neq 0$ para algum j. Assim, o conjunto $\{u \in \mathbb{Z}_p \mid ux = 0\} = ker(u \longmapsto ux)$ é um subgrupo fechado. Veja que tal conjunto não contém $p^i\mathbb{Z}_p$, para nenhum i, então deve ser zero, uma vez que, os subgrupos fechados são interseções de subgrupos abertos juntamente com o subgrupo $\{0\}$. Logo, não existe $y \in \mathbb{Z}_p \setminus \{0\}$ tal que $xy = 0$. E portanto, $\mathbb{Z}_p$ é um domínio de integridade.

(iv) $ker\varphi_i = p^i\mathbb{Z}_p$.

De fato, basta observar que, $ker\varphi_i = \{\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p \mid \sum_{j=0}^{i-1} a_j p^j \text{ múltiplo de } p^i\}$.

(v) O ideal $p\mathbb{Z}_p$ é o único ideal maximal de $\mathbb{Z}_p$.

De fato, os ideais de $\mathbb{Z}_p$ são $p^i\mathbb{Z}_p$, então $p^i\mathbb{Z}_p \subseteq p\mathbb{Z}_p$, para todo $i \geq 1$. E como $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ é corpo, então $p\mathbb{Z}_p$ é ideal maximal de $\mathbb{Z}_p$ e, consequentemente, $p\mathbb{Z}_p$ é o único ideal maximal de $\mathbb{Z}_p$, como queríamos mostrar.

(vi) O grupo das unidades de $\mathbb{Z}_p$ é $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

De fato, se $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, então $x\mathbb{Z}_p \nsubseteq p\mathbb{Z}_p$. Mas $p\mathbb{Z}_p$ é o único maximal, logo $x\mathbb{Z}_p = \mathbb{Z}_p$, e portanto x é uma unidade de $\mathbb{Z}_p$.

O próximo resultado é fundamental na demonstração do teorema principal desse trabalho, tal resultado garante que as unidades de $\mathbb{Z}_p$ são não enumeráveis.

Lema 1.4.9 *O conjunto $\mathbb{Z}_p^*$ das unidades de $\mathbb{Z}_p$ é não enumeráveis.*

Demonstração: Tome $a = \sum_{j=0}^{\infty} a_j p^j \in \mathbb{Z}_p^*$ e veja que $a_0 \neq 0$. De fato, se $a_0 = 0$, então $a = a_1 p + a_2 p^2 + a_3 p^3 + \ldots = p(a_1 + a_2 p + a_3 p^2 + \ldots) \in p\mathbb{Z}_p$, o que não pode acontecer, uma vez que o grupo das unidades de $\mathbb{Z}_p$ é $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Assim, o conjunto das unidades de $\mathbb{Z}_p$ é formado pelos elementos da seguinte forma: $\mathbb{Z}_p^* = \{a_0 + a_1 p + \ldots + a_n p^n + \ldots \mid 0 \leq a_j < p, \text{ com } a_0 \neq 0\}$.

Dado um elemento $b = \sum_{j=0}^{\infty} b_j p^j \in \mathbb{Z}_p^*$ e tomando os coeficientes b_i de b, eles formam uma lista infinita e enumerável, digamos $X_1 = (b_0, b_1, \ldots, b_n, \ldots)$. Dessa forma, podemos identificar cada elemento de $\mathbb{Z}_p^*$ como uma lista infinita e enumerável, e então aplicando "método da diagonal de Cantor" obtemos que $\mathbb{Z}_p^*$ é não enumerável.

■

Mais informações sobre o "método da diagonal de Cantor", e algumas de suas propriedades podem ser encontradas em [7], Capítulo 2.

O próximo resultado nos diz que a operação de 'exponenciação p-ádica' é bem comportada. Lembrando que, a operação p-ádica é definida da seguinte maneira:

Definição 1.4.10 *Seja G um grupo pro-p, $g \in G$ e $\lambda \in \mathbb{Z}_p$. Então*

$$g^{\lambda} = \lim_{n \longrightarrow \infty} g^{a_n},$$

onde (a_n) é uma sequência de inteiros com $\lim_{n \longrightarrow \infty} a_n = \lambda$.

Essa definição faz sentido, uma vez que nas condições dadas, a seguência (g^{a_n}) converge em G, e os limites de quaisquer duas sequências (g^{a_n}) e (g^{b_n}) com $g \in G$ são iguais, a demonstração desse resultado pode ser encontrada em [2, Lemma 1.24].

Proposição 1.4.11 *Sejam G um grupo pro-p, $g, h \in G$ e $\lambda, \mu \in \mathbb{Z}_p$. As seguintes afirmações são verdadeiras:*

(i) $g^{\lambda+\mu} = g^{\lambda}g^{\mu}$ *e* $g^{\lambda\mu} = (g^{\lambda})^{\mu}$.

(ii) *Se* $gh = hg$ *então* $(gh)^{\lambda} = g^{\lambda}h^{\lambda}$.

(iii) *A aplicação* $\nu \longmapsto g^{\nu}$ *define um homomorfismo contínuo de* $\mathbb{Z}_p$ *em* G. *E sua imagem* $g^{\mathbb{Z}_p}$ *é o fecho em* G *de* $\langle g \rangle$.

A demonstração desse resultado pode ser encontrado em [2, Proposition 1.26].

Para finalizar a seção, vamos estudar o completamento profinito de $\mathbb{Z}$.

Lema 1.4.12 *Sejam* $D = \mathrm{Cr}(\mathbb{Z}_p \mid p \text{ primo})$, $\delta : \mathbb{Z} \longrightarrow D$ *a aplicação que leva cada* $x \in \mathbb{Z}$ *no vetor com todas as coordenadas igual a* x *e* $\mathbb{Z}'$ *a imagem de* δ. *Para cada inteiro* $n > 0$ *as seguintes afirmações são verdadeiras:*

(a) $nD + \mathbb{Z}' = D$.

(b) D/nD *é cíclico de ordem* n.

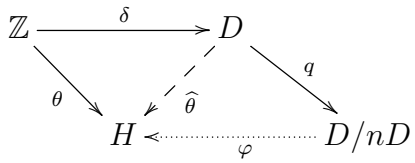
(c) $nD \cap \mathbb{Z}' = n\mathbb{Z}'$.

A demonstração desse resultado pode ser encontrada em [22, Lemma 1.5.1]. Usando esse lema, mostraremos que D juntamente com a aplicação δ é o completamento profinito de $\mathbb{Z}$.

Proposição 1.4.13 *O grupo* $D = \mathrm{Cr}(\mathbb{Z}_p \mid p \text{ primo})$ *juntamente com a aplicação* $\delta : \mathbb{Z} \longrightarrow D$, *como definida no lema anterior é o completamento profinito de* $\mathbb{Z}$.

Demonstração: Seja $\theta : \mathbb{Z} \longrightarrow H$ um homomorfismo contínuo, onde H é um grupo finito. Vamos mostrar que existe um único homomorfismo contínuo $\widehat{\theta} : D \longrightarrow H$ tal que $\theta = \widehat{\theta}\delta$. Suponhamos que H tenha ordem n. Seja q a aplicação quociente de D em D/nD, escreva $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. Note que aplicando o Lema 1.4.12, obtemos que a aplicação $q\delta : \mathbb{Z} \longrightarrow D/nD \cong \mathbb{Z}/n\mathbb{Z}$ é um homomorfismo sobrejetor, cujo núcleo $ker(q\delta) = n\mathbb{Z}$. Pelo Teorema de Lagrange tem-se $ker(q\delta) \subseteq ker\theta$. Então existe um

único homomorfismo $\varphi : D/nD \longrightarrow H$ tal que $\theta = \varphi(q\delta)$, isto é, φ torna o quadrilátero abaixo comutativo.



Note que φ é contínua. Agora, considerando $\widehat{\theta} = \varphi q$, segue que $\widehat{\theta}$ é um homomorfismo contínuo e com $\theta = \widehat{\theta}\delta$. Resta ver que $\widehat{\theta}$ é única. Veja que, se $\psi : D \longrightarrow H$ fosse outra aplicação com as mesmas propriedades que $\widehat{\theta}$, usando o Teorema de Lagrange obtemos que $ker(q) = nD \subseteq ker\psi$. Então, existe um único homomorfismo $\varphi_1 : D/nD \longrightarrow H$ tal que $\psi = \varphi_1 q$. Como o quadrilátero é comutativo, $\theta = \widehat{\theta}\delta = \psi\delta = \varphi(q\delta) = \varphi_1(q\delta)$, e resulta que $\varphi_1 = \varphi$. Portanto, $\widehat{\theta}$ é unicamente determinada e o resultado segue. ■

O próximo resultado é uma extensão da Proposição 1.4.11, dos grupos pro-p para os grupos profinitos.

Proposição 1.4.14 *Sejam G um grupo profinito, $\widehat{\mathbb{Z}}$ o completamento profinito de $\mathbb{Z}$ e considere $\mathbb{Z}$ contido em $\widehat{\mathbb{Z}}$. As seguintes afirmações são verdadeiras:*

(i) *Existe uma única aplicação contínua $\widehat{\mathbb{Z}} \times G \longrightarrow G$ tal que $(n, g) \longmapsto g^n$ para $n \in \mathbb{Z}$. Portanto, se $g \in G$ e $z \in \widehat{\mathbb{Z}}$, então a potência g^z está definida.*

(ii) *Se $g \in G$ e $z_1, z_2 \in \widehat{\mathbb{Z}}$, então*

(a) $g^{z_1+z_2} = g^{z_1}g^{z_2}$ *e*

(b) $(g^{z_1})^{z_2} = g^{z_1 z_2}$.

(iii) *Se $g_1, g_2 \in G$ e $z \in \widehat{\mathbb{Z}}$ e se g_1, g_2 comutam, então temos que $(g_1 g_2)^z = g_1^z g_2^z$.*

A demonstração pode ser encontrada em [22, Proposition 1.53].

1.5 Grupos Profinitos de Posto Finito

Nesta seção faremos um estudo detalhado dos grupos profinitos de posto finito, em especial, dos grupos profinitos solúveis de posto finito, em seguida apresentaremos uma série de caracterizações para os mesmos. Além disso, mostraremos que um grupo

profinito arbitrário de posto finito pode ser construído de forma simples a partir de um grupo pronilpotente de posto finito, um grupo solúvel também de posto finito e um grupo finito. Esta seção foi baseada no Capítulo 8 do livro de J. S. Wilson [22].

Começaremos exibindo propriedades gerais dos grupos profinitos, que serão úteis tanto no decorrer desta seção quanto no próximo capítulo.

Definição 1.5.1 *Seja G um grupo profinito. Dizemos que o subconjunto X de G gera G topologicamente se G é o fecho do subgrupo abstrato gerado por X, ou seja, $G = \overline{\langle X \rangle}$.*

Um grupo profinito G é dito um grupo *finitamente gerado* se pode ser gerado topologicamente por um conjunto finito. Neste caso, G é chamado de *d-gerado* (onde d é um inteiro positivo) se pode ser gerado topologicamente por um conjunto com no máximo d elementos.

O próximo resultado mostra que, X gera G topologicamente se, e somente se, a imagem de X em G/N gera G/N, para cada $N \lhd_\circ G$.

Proposição 1.5.2 *Seja G um grupo profinito e X um subconjunto de G.*

(i) *Se X gera G topologicamente, então a imagem de X em G/K gera G/K topologicamente, para cada $K \lhd_\circ G$.*

(ii) *Se a imagem de X em G/N gera G/N, para cada $N \lhd_\circ G$, então X gera G topologicamente.*

A demonstração pode ser encontrada em [22, Proposition 4.1.1].

Proposição 1.5.3 *Seja d um inteiro positivo e G um grupo profinito. Então G é um grupo d-gerado se, e somente se, G/N é um grupo d-gerado, para todo $N \lhd_\circ G$.*

O próximo resultado mostra que subgrupos abertos de grupos profinitos finitamente gerados são finitamente gerado.

Proposição 1.5.4 *Seja G um grupo profinito finitamente gerado e H um subgrupo aberto de G. Então H é finitamente gerado.*

A demonstração pode ser encontrada em [22, Proposition 4.3.1].

Seja H um grupo profinito finitamente gerado e escreva

$$d(H) = min\{|X| \mid X \subseteq H \text{ e } X \text{ gera } H\},$$

para denotar a cardinalidade mínima de um conjunto de geradores para H.

Definição 1.5.5 *Dizemos que um grupo profinito tem posto finito se existe um inteiro r tal que todo subgrupo de G pode ser gerado por r elementos.*

Assim, o posto de um grupo profinito G de posto finito é o menor inteiro r tal que todo subgrupo de G pode ser gerado por r elementos, que denotaremos por $rk(G)$. Dessa forma,

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

Um exemplo de grupo profinito de posto finito é $\mathbb{Z}_p$, tem posto finito igual a 1.

A próxima proposição, esclarece as várias definições possíveis de posto.

Proposição 1.5.6 *Seja G um grupo profinito e defina*
$r_1 = sup\{d(H) \mid H \leq_c G\}$,
$r_2 = sup\{d(H) \mid H \leq_c G \, e \, d(H) < \infty\}$,
$r_3 = sup\{d(H) \mid H \leq_\circ G\}$ *e*
$r_4 = sup\{rk(G/N) \mid N \lhd_\circ G\}$.
Então $r_1 = r_2 = r_3 = r_4$.

A demonstração deste resultado pode ser encontrada em [2, Proposition 3.11].

Por essa proposição, podemos concluir que o posto de um grupo profinito é o valor comum de r_1, r_2, r_3 e r_4. Essa informação é muito útil, uma vez que expande os meios para calcular o posto de um grupo profinito.

Proposição 1.5.7 *Seja G um grupo profinito.*

(a) Se G tem posto r, subgrupos e grupos quocientes de G tem posto no máximo r.

(b) Se $K \lhd G$ e se K e G/K têm posto finito, então G tem posto finito. Além disso,

$$rk(G) \leq rk(K) + rk(G/K).$$

(c) Se G é finitamente gerado, então

$$d(G) = sup\{d(G/M) \mid M \lhd_\circ G\}.$$

(d) Se G é um grupo pro-p finitamente gerado, então $G/\Phi(G)$ é um grupo abeliano elementar de ordem $p^{d(G)}$, e $\Phi(G/K) = K\Phi(G)/K$ para cada subgrupo normal K de G.

A demonstração pode ser encontrada em [22, Proposition 8.1.1].

Note que grupos profinitos livres finitamente gerados não têm posto finito, uma vez que possuem subgrupos profinitos que não são finitamente gerados.

Agora direcionaremos o estudo para os grupos profinitos solúveis de posto finito. Lembrando que um grupo abstrato G é dito *solúvel* se existe uma série finita, chamada *série solúvel*,

$$1 = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

de subgrupos tais que $G_{i-1} \lhd G_i$ e G_i/G_{i-1} é abeliano, para todo $i \leq n$. O menor inteiro n para o qual tal série existe é chamado *comprimento derivado*. Os grupos solúveis com comprimento derivados 1 são os grupos abelianos, já os grupos solúveis com comprimento derivado 2, são chamados grupos *metabelianos*.

Dizemos que G é um grupo profinito solúvel quando G é um grupo profinito e existe uma série finita com as propriedades acima tal que cada G_i é um subgrupo fechado de G. Se considerarmos uma série para um grupo profinito solúvel G como a que foi definida acima e, $H \leq G$ e $K \lhd G$ são subgrupos profinitos, então

$$1 = H \cap G_0 \leq H \cap G_1 \leq H \cap G_2 \leq \ldots \leq H \cap G_n = H$$

e

$$K/K = KG_0/K \leq KG_1/K \leq KG_n/K = G/K$$

são séries solúveis para H e G/K, respectivamente. E se além disso, $G \lhd L$, com L profinito, e

$$G/G = L_0/G \leq L_1/G \leq \ldots L_m/G = L/G$$

é uma série de subgrupos fechados para L/G com fatores abelianos, então

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n \leq L_1 \leq \ldots \leq L_m = L$$

é uma série para L com fatores abelianos. Portanto, a classe de grupos profinitos solúveis é fechada para subgrupos, grupos quocientes e extensões.

Proposição 1.5.8 *Seja A um grupo profinito abeliano aditivo. São equivalentes:*

(i) *A é finitamente gerado;*

(ii) *A tem posto finito;*

(iii) *A é uma soma direta de uma quantidade finita de grupos procíclicos;*

(iv) *Existe um inteiro r tal que cada subgrupo de Sylow de A pode ser gerado por r elementos.*

Demonstração:

(ii) ⇒ (i) Segue da definição de posto finito.

(i) ⇒ (iv) Pela Proposição 1.5.7, $d(A) = sup\{d(A/M) \mid M \lhd_\circ A\}$. Como cada subgrupo de Sylow de A é isomorfo a um grupo quociente de A, existe então um inteiro r tal que cada subgrupo de Sylow de A pode ser gerado por r elementos.

(iii) ⇒ (ii) Suponha que A é a soma direta de r subgrupos procíclicos, gerados por $a_1, a_2, \ldots, a_r$, e seja A_i o subgrupo gerado por $a_1, a_2, \ldots, a_i$, para $1 \leq i \leq r$. Então a série $1 \leq A_1 \leq \ldots \leq A_r = A$ tem fatores procíclicos.

Vamos mostrar por indução sobre r que $rk(A) \leq r$.

Se $r = 1$, então $1 = A_0 \leq A_1 = A$, o que implica que A é procíclico e consequentemente, tem posto finito. Seja $r > 1$ e considere a série

$$A_0 \leq A_1 \leq \ldots \leq A_{r-1} \leq A_r = A.$$

Por hipótese de indução A_{r-1} tem posto finito, e como A_r/A_{r-1} é procíclico, então $rk(A) \leq rk(A_{r-1}) + rk(A/A_{r-1}) \leq r$.

(iv) ⇒ (iii) Suponha que existe um inteiro r tal que todo subgrupo de Sylow de A pode ser gerado por r elementos. Pela Proposição 1.4.14, o p-subgrupo de Sylow A_p de A, para cada p primo, pode ser considerado como um $\mathbb{Z}_p$-módulo profinito e é gerado tanto como um $\mathbb{Z}_p$-módulo abstrato, como um $\mathbb{Z}_p$-módulo profinito, por um conjunto de r elementos. E como $\mathbb{Z}_p$ é um domínio de ideias principais, todo $\mathbb{Z}_p$-módulo gerado por r elementos é uma soma direta de r submódulos cíclicos (alguns deles possivelmente zero), e os $\mathbb{Z}_p$-módulos cíclicos são simplesmente grupos pro-p procíclicos. Portanto, podemos escrever cada p-subgrupo de Sylow A_p como uma soma direta de subgrupos procíclicos $A_{p,1}, \ldots, A_{p,r}$, onde r depende de p. Assim,

$$A \cong Cr(A_p \mid p\,primo) \cong Cr(A_{p,i} \mid p\,primo,\ 1 \leq i \leq r) \cong \oplus_{i=1}^{r} Cr(A_{p,i} \mid p\,primo)$$

onde cada grupo $Cr(A_{p,i} \mid p\,primo)$ é procíclico, e portanto o resultado segue.

■

Proposição 1.5.9 *Seja G um grupo profinito. Então G é um grupo solúvel de posto finito se, e somente se, G tem uma série*

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

tal que $G_{i-1} \lhd G_i$ e G_i/G_{i-1} é procíclico, para $1 \leq i \leq n$.

Demonstração: Primeiro suponha que G possui uma série

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

tal que $G_{i-1} \lhd G_i$ e G_i/G_{i-1} é procíclico, para $1 \leq i \leq n$. Então G é solúvel. Resta mostrar que G tem posto finito. Vamos mostrar por indução sobre o tamanho da série.

Se $n = 1$, então $1 = G_0 \leq G_1 = G$. Assim, $G/G_0 = G$ é procíclico e, consequentemente, G tem posto finito. Agora suponha que todo grupo profinito G que tem uma série $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ satisfazendo as hipóteses tem posto finito. E vamos mostrar que a afirmação é verdadeira para $n+1$, ou seja, suponha que G tem uma série $1 = G_0 \leq G_1 \leq \ldots \leq G_n \leq G_{n+1} = G$ tal que $G_{i-1} \lhd G_i$ e G_i/G_{i-1} é procíclico, para $1 \leq i \leq n+1$. Assim, $G_{n+1}/G_n = G/G_n$ é procíclico, logo tem posto finito, e por hipótese de indução G_n tem posto finito. E pela Proposição 1.5.7, item (b), $rk(G) \leq rk(G_n) + rk(G/G_n)$. Portanto, G tem posto finito.

Reciprocamente, suponha que G é um grupo profinito solúvel de posto finito. Então G tem uma série

$$1 = G_0 \leq G_1 \leq \ldots \leq G_s = G$$

com $G_{i-1} \lhd G_i$ e G_i/G_{i-1} abeliano, para $1 \leq i \leq s$. Mostraremos por indução sobre o comprimento s, que G possui uma série com fatores procíclicos.

Se $s = 1$, então G é grupo profinito abeliano de posto finito. Então, pela Proposição 1.5.8, G é a soma direta de uma quantidade finita de grupos procíclicos, ou seja, $G \cong C_1 \oplus \ldots \oplus C_r$, onde cada C_i é procíclico, e a série com o j-ésimo termo $C_1 \oplus \ldots \oplus C_j$, para $1 \leq j \leq r$, tem fatores procíclicos.

Agora suponha que a afirmação é verdadeira para todo G_j, com $1 \leq j \leq s-1$. Assim, G_{s-1} possui uma série

$$1 = H_0 \leq H_1 \leq \ldots \leq H_k = G_{s-1}$$

com $H_{i-1} \lhd H_i$ e H_i/H_{i-1} procíclico para cada $1 \leq i \leq k$.

Como G tem posto finito, então G/G_{s-1} tem posto finito. E sendo G/G_{s-1} abeliano, pela proposição anterior, G/G_{s-1} é a soma direta de uma quantidade finita de grupos procíclicos, gerados por $\overline{a_1}, \ldots, \overline{a_m}$. Suponha que L_i/G_{s-1} é um subgrupo gerado por $\overline{a_1}, \ldots, \overline{a_i}$, para $1 \leq i \leq m$. Logo, a série

$$1 = G_{s-1}/G_{s-1} = L_0/G_{s-1} \leq L_1/G_{s-1} \leq \ldots \leq L_m/G_{s-1}$$

tem fatores procíclicos, e como $\frac{L_i}{L_{i-1}} \cong \frac{L_i/G_{s-1}}{L_{i-1}/G_{s-1}}$, para todo $1 \leq i \leq m$, então a série

$$1 = H_0 \leq H_1 \leq \ldots \leq H_k = G_{s-1} = L_0 \leq L_1 \leq \ldots \leq L_m = G$$

tem fatores procíclicos, como queríamos mostrar.

■

O próximo resultado garante que, se G é um grupo profinito solúvel, o número de fatores que têm p-subgrupos de Sylow isomórficos a $\mathbb{Z}_p$ é independente da escolha da série.

Proposição 1.5.10 *Seja G um grupo profinito solúvel de posto finito e seja p um primo. Suponha que*

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

e

$$1 = H_0 \leq H_1 \leq \ldots \leq H_m = G$$

são duas séries para G com fatores procíclicos. (Assim os p-subgrupos de Sylow dos fatores G_i/G_{i-1}, H_i/H_{i-1} das duas séries são isomórficos a $\mathbb{Z}_p$ ou finitos.) Então as duas séries tem um número igual de fatores cujos p-subgrupos de Sylow são isomórficos a $\mathbb{Z}_p$.

Demonstração: Para simplificar chamaremos um grupo procíclico de *p-large* se seu p-subgrupo de Sylow é isomorfo a $\mathbb{Z}_p$. Sabemos que todo subgrupo não trivial de $\mathbb{Z}_p$

é aberto. A chave dessa demonstração segue da seguinte observação: se X é procíclico e $Y \leq X$, então no máximo, um deles Y ou X/Y pode ser p-large, e portanto, X é p-large se, e somente se, um desses grupos é p-large.

Argumentaremos por indução sobre $n+m$. O resultado é claro se $n \leq 1$ ou $m \leq 1$. Suponha que $n \geq 2$, e escreva $L = G_{n-1}$. Seja h o número de fatores p-large na primeira série e seja $\varepsilon = 1$ se G/L é p-large e $\varepsilon = 0$, caso contrário. Aplicando indução para as séries $(G_i)_{i=0}^{n-1}$ e $(L \cap H_j)_{j=0}^{m}$ para o grupo L e, para as séries $L/L \leq G/L$ e $(LH_j \cap L)_{j=0}^{m}$ para o grupo G/L, obtemos que $h - \varepsilon$ dos grupos $L \cap H_j / L \cap H_{j-1}$ e, ε dos grupos LH_j/LH_{j-1} são p-large. Entretanto,

$$L \cap H_j / L \cap H_{j-1} \cong (L \cap H_j)H_{j-1}/H_{j-1}$$

e

$$LH_j/LH_{j-1} \cong H_j/(LH_{j-1} \cap H_j) = H_j/(L \cap H_j)H_{j-1}.$$

Mas para cada j, no máximo, um dos grupos $(L \cap H_j)H_{j-1}/H_{j-1}$, $H_j/(L \cap H_j)H_{j-1}$ pode ser p-large e, H_j/H_{j-1} é p-large, precisamente quando um desses grupos é p-large. Então, segue que o número de H_j/H_{j-1} que são p-large é $(h-\varepsilon)+\varepsilon = h$, como queríamos mostrar.

■

Para cada grupo solúvel G de posto finito e cada primo p, definimos o $\mathbb{Z}_p$-*length* de G, denotado por $h_p(G)$, como sendo o número de fatores que têm p-subgrupos de Sylow isomórficos a $\mathbb{Z}_p$ em uma série com fatores procíclicos. Assim, como já foi dito, $h_p(G)$ independe da escolha da série, e é um invariante muito útil para provas de indução. Veja que o invariante $h_p(G)$ para um grupo solúvel de posto finito é um análogo do comprimento de Hirsch de um grupo policíclico. Para mais detalhes veja [16, 5.4.13].

Proposição 1.5.11 *Seja G um grupo profinito solúvel. Então G tem posto finito se, e somente se, existe um inteiro r tal que todo subgrupo de Sylow de G tem posto no máximo r.*

Demonstração: Suponha que G tem posto finito, digamos $rk(G) \leq r$, então por definição, cada subgrupo de G tem posto no máximo r.

Reciprocamente, suponha que cada subgrupo de Sylow de G tem posto no máximo

r. Como G é solúvel, então possui uma série

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G.$$

Mostraremos por indução sobre o comprimento n de tal série que G tem posto finito. Se $n = 1$, então G é abeliano e cada subgrupo de Sylow pode ser gerado por no máximo r elementos, e então pela Proposição 1.5.8, G tem posto finito.

Agora suponha que $n \geq 1$. Como cada subgrupo de Sylow de G_{n-1} está contido em um subgrupo de Sylow de G, então tem posto no máximo r, logo por hipótese de indução G_{n-1} tem posto finito. E como cada subgrupo de Sylow de G/G_{n-1} é uma imagem sobre a aplicação quociente de um subgrupo de Sylow de G, então cada subgrupo de Sylow de G/G_{n-1} tem posto no máximo r. E com G/G_{n-1} é abeliano, então o comprimento derivado é igual a 1, logo por hipótese de indução G/G_{n-1} tem posto finito. E portanto, pela Proposição 1.5.7 G tem posto finito. ■

Usando técnicas mais poderosas A. Lucchini [10] provou em 1989, que "se G é um grupo finito e cada subgrupo de Sylow de G pode ser gerado por d elementos, então G pode ser gerado por $d + 1$ elementos", e nesse mesmo ano R. M. Guralnick [4], provou que "$d(G) \leq r(G) + 1$, para todo grupo finito G, onde $r(G) = max\{r_p(G)\}$ e $r_p(G) = d(P)$ para todo p-subgrupo de Sylow P de G". Aplicando tais resultados para todos os subgrupos de um grupo finito G, deduzimos que, se cada subgrupo de Sylow tem posto no máximo r, então $rk(G) \leq r + 1$, e juntando esse fato à Proposição 1.5.7, concluímos que, se G é um grupo profinito cujos subgrupos de Sylow tem posto no máximo r, então $rk(G) \leq r + 1$.

Agora daremos uma caracterização de grupos profinitos solúveis de posto finito, através dos subgrupos abelianos. Para isso, precisamos de um resultado sobre subgrupos pronilpotentes em grupos prosolúveis e um limite para o número de geradores de certos grupos que agem em grupos pro-p abelianos de posto finito.

Definição 1.5.12 *Seja G um grupo profinito. Os subgrupos de Carter de G são subgrupos pronilpotentes maximais de G, com a propriedade de que suas imagens em grupos quocientes G/K também são pronilpotentes maximais de G/K.*

Grupos prosolúveis possuem subgrupos de Carter. Para ver essa e mais propriedades dos subgrupos de Carter, veja em [22, Exercise 2.7.7]

Lema 1.5.13 *Seja G um grupo prosolúvel e K um subgrupo normal tal que G/K é abeliano. Então existe um subgrupo pronilpotente H tal que $G = HK$.*

Demonstração: Como G é um grupo prosolúvel, então existe H um subgrupo de Carter de G. Daí, HK/K é um subgrupo pronilpotente maximal de G/K. E como $HK \leq G$, e H é maximal, então $HK = G$, como queríamos demonstrar. ■

Agora abordaremos um resultado de Philip Hall que estabelece um limite para o número de geradores de p-grupos finitos que agem em p-grupos abelianos de posto finito, para então generalizar o resultado para grupos pro-p. Esse resultado também pode ser encontrado em [22].

Lema 1.5.14 *Seja A um p-grupo abeliano finito de posto r, onde p é um primo. Suponha que A também é um G-módulo, onde G é um p-grupo finito, e que cada elemento não trivial de G age não trivialmente em A.*

(a) *Se cada elemento de G age trivialmente no módulo quociente A/p^2A, então $d(G) \leq r^2$.*

(b) *Em geral, $d(G) \leq \frac{1}{2}(5r^2 - r)$.*

Demonstração:

(a) Vamos mostrar que $d(G) \leq r^2$. Observe que r^2 é a dimensão do espaço vetorial das matrizes $r \times r$ sobre $\mathbb{F}_p$.

Para cada $g \in G \setminus \{1\}$, considere o maior inteiro m tal que g age trivialmente no módulo A/p^mA, ou seja, para cada $g \in G \setminus \{1\}$ e para todo $a \in A$, $(a + p^mA)g = a + p^mA$. Note que

$$\begin{aligned} ag + p^mA = a + p^mA &\Leftrightarrow \quad ag - a \in p^mA \\ &\Leftrightarrow \quad ag - a = p^ma', \text{ onde } a' \in A \\ &\Leftrightarrow \quad ag = a + p^ma', \text{ onde } a' \in A. \end{aligned} \tag{1.1}$$

Como G é finito, podemos escolher $\{g_1, g_2, \ldots, g_d\}$ um conjunto de geradores para G, com $d(G) = d$ e $\sum_{k=1}^{d} m(g_k)$ o maior possível (note que o valor do somatório pode mudar dependendo do conjunto de geradores escolhido, pois o valor de m varia dependendo de g_k). Escreva $m_k = m(g_k)$ para cada k. Podemos assumir

que $m_1 \leq m_2 \leq \ldots \leq m_d$ com $m_1 \geq 2$, pois por hipótese, cada elemento de G age trivialmente no módulo quociente A/p^2A.

Agora, como A é um grupo finito abeliano, podemos escrever $A = \langle a_1\rangle \oplus \cdots \oplus \langle a_r\rangle$. Então, por (1.1), temos que, para cada $k \leq d$

$$a_i g_k \;=\; a_i + p^{m_k} \sum_{j=1}^{r} u_{ij}^{(k)} a_j, \quad \text{para } i \leq r. \tag{1.2}$$

Com isso, podemos considerar as matrizes inteiras $r \times r$

$$u^{(k)} = \begin{pmatrix} u_{11}^{(k)} & \cdots & u_{1r}^{(k)} \\ \vdots & \ddots & \vdots \\ u_{r1}^{(k)} & \cdots & u_{rr}^{(k)} \end{pmatrix}$$

fornecidas pelos coeficientes inteiros da expressão (1.2).

Para mostrar que $d(G) \leq r^2$, vamos mostrar que as imagens de $u^{(1)}, \ldots, u^{(d)}$ no espaço vetorial das matrizes $r \times r$ sobre $\mathbb{F}_p$ são linearmente independentes, com isso $d(G) = d \leq r^2$.

Suponha que $u^{(1)}, \ldots, u^{(d)}$ são linearmente dependentes, e seja t o menor inteiro tal que

$$u^{(t)} \equiv \sum_{j=1}^{t-1} \lambda_j u^{(j)} \bmod p,$$

para inteiros λ_j adequados. Note que, estamos considerando módulo p, pois estamos tomando as matrizes com entradas em $\mathbb{F}_p$.

Escreva $g' = \prod_{j=1}^{t-1} g_j^{\mu_j}$, onde $\mu_j = \lambda_j p^{m_t - m_j}$. Temos de (1.2) que

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} g_j = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} + p^{m_j} u^{(j)} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} (1 + p^{m_j} u^{(j)}).$$

Daí, g_j age nos $a_{i's}$ como $(1 + p^{m_j} u^{(j)})$.

Pelo binômio de Newton,

$$\begin{aligned}(1+p^{m_j}u^{(j)})^{\mu_j} &= \sum_{l=0}^{\mu_j}\begin{pmatrix}\mu_j\\ l\end{pmatrix}(p^{m_j}u^{(j)})^l = \sum_{l=0}^{\mu_j}\begin{pmatrix}\lambda_j p^{m_t-m_j}\\ l\end{pmatrix}p^{lm_j}(u^{(j)})^l\\ &= 1+\lambda_j p^{(m_t-m_j)}p^{m_j}u^{(j)} + \sum_{l=2}^{\mu_j}\begin{pmatrix}\lambda_j p^{m_t-m_j}\\ l\end{pmatrix}p^{lm_j}(u^{(j)})^l\\ &\equiv 1+\lambda_j p^{m_t}u^{(j)} \mod p^{m_t+1}\end{aligned}$$

pois, $m_t+(l-1)m_j \geq m_t+1$ para todo $l\geq 2$, já que $m_j\geq 2$ para todo j. Assim,

$$\prod_{j=1}^{t-1}(1+p^{m_j}u^{(j)})^{\mu_j} \equiv \prod_{j=1}^{t-1}(1+\lambda_j p^{m_t}u^{(j)}) \mod p^{m_t+1}.$$

E

$$\begin{aligned}&\prod_{j=1}^{t-1}(1+\lambda_j p^{m_t}u^{(j)}) =\\ =\ & (1+\lambda_1 p^{m_t}u^{(1)})(1+\lambda_2 p^{m_t}u^{(2)})(1+\lambda_3 p^{m_t}u^{(3)})\dots(1+\lambda_{t-1}p^{m_t}u^{(t-1)})\\ =\ & (1+\lambda_1 p^{m_t}u^{(1)}+\lambda_2 p^{m_t}u^{(2)}+\lambda_1\lambda_2 p^{2m_t}u^{(1)}u^{(2)})(1+\lambda_3 p^{m_t}u^{(3)})\dots(1+\lambda_{t-1}p^{m_t}u^{(t-1)})\\ =\ & (1+\lambda_1 p^{m_t}u^{(1)}+\lambda_2 p^{m_t}u^{(2)}+\lambda_3 p^{m_t}u^{(3)}+\lambda_1\lambda_2 p^{2m_t}u^{(1)}u^{(2)}+\lambda_1\lambda_3 p^{2m_t}u^{(1)}u^{(3)}+\\ +\ & \lambda_2\lambda_3 p^{2m_t}u^{(2)}u^{(3)}+\lambda_1\lambda_2\lambda_3 p^{3m_t}u^{(1)}u^{(2)}u^{(3)})(1+\lambda_4 p^{m_t}u^{(4)})\dots(1+\lambda_{t-1}p^{m_t}u^{(t-1)})\\ =\ & 1+p^{m_t}\sum_{j=1}^{t-1}\lambda_j u^{(j)} + p^{m_t+1}(\lambda_1\lambda_2 p^{m_t-1}u^{(1)}u^{(2)}+\lambda_1\lambda_3 p^{m_t-1}u^{(1)}u^{(3)}+\dots+\\ +\ & \lambda_1\lambda_2\dots\lambda_{t-1}p^{[(t-3)m_t+(m_t-1)]}u^{(1)}u^{(2)}\dots u^{(t-1)})\\ \equiv\ & 1+p^{m_t}\sum_{j=1}^{t-1}\lambda_j u^{(j)} \mod p^{m_t+1}.\end{aligned}$$

Logo, o efeito de g' nas imagens de $a_1,\dots,a_r$ em $\frac{A}{p^{m_t+1}A}$ é descrito pela matriz inteira $\prod_{j=1}^{t-1}(1+p^{m_j}u^{(j)})^{\mu_j}$ que é congruente a $1+p^{m_t}\sum_{j=1}^{t-1}\lambda_j u^{(j)}$ modulo p^{m_t+1}. Como $u^{(t)}\equiv\sum_{j=1}^{t-1}\lambda_j u^{(j)} \mod p$, temos

$$\prod_{j=1}^{t-1}(1+\lambda_j p^{m_t}u^{(j)}) \equiv 1+p^{m_t}u^{(t)} \mod p.$$

Portanto, g' e g_t induzem a mesma aplicação em $\frac{A}{p^{m_t+1}A}$ e então $g_t^{-1}g'$ age trivialmente no módulo $\frac{A}{p^{m_t+1}A}$. Logo, temos que $m(g_t^{-1}g') \geq m_t + 1$. Mas como $\{g_1, \ldots, g_{t-1}, g_t^{-1}g', \ldots, g_d\}$ é um conjunto gerador para G, temos uma contradição com a maximalidade de $\sum_{k=1}^{d} m(g_k)$.

Logo, as imagens $u^{(1)}, \ldots, u^{(d)}$ são linearmente independentes, e consequentemente $d(G) \leq r^2$.

(b) Agora vamos mostrar que, em geral, $d(G) \leq \frac{1}{2}(5r^2 - r)$. Considere C_1 e C_2 os núcleos das ações induzidas de G em A/pA e A/p^2A. Assim, para todo $g \in C_1$, $(a+pA)g = ag+pA = a+pA$ e, para todo $g \in C_2$, $(a+p^2A)g = ag+p^2A = a+p^2A$, para todo $a \in A$.

Note que, G/C_1 age então em A/pA que é um espaço vetorial sobre $\mathbb{F}_p$, logo é isomorfo a um subgrupo de $GL_r(\mathbb{F}_p)$.

Mas temos que $|GL_r(\mathbb{F}_p)|$ é igual ao número de bases de $\mathbb{F}_p^r$, logo

$$\begin{aligned} |GL_r(\mathbb{F}_p)| &= (p^r - 1)(p^r - p)\ldots(p^r - p^{r-1}) \\ &= p^{\frac{1}{2}r(r-1)}(p^r - 1)(p^r - 1)\ldots(p^r - 1). \end{aligned}$$

Então os subgrupos p-Sylow de $GL_r(\mathbb{F}_p)$ tem ordem $p^{\frac{1}{2}r(r-1)}$.

E como G é um p-grupo, então G/C_1 tem ordem potência de p. Logo, $d(G/C_1) \leq \frac{1}{2}r(r-1)$.

Observe que, $d(G) \leq d(G/C_1)+d(C_1)$, então é suficiente mostrar que $d(C_1) \leq 2r^2$.

Para cada $g \in C_1$, temos que $ag - a \in pA$, então a aplicação

$$\begin{aligned} \gamma_g : \ A &\longrightarrow pA/p^2A \\ a &\longmapsto ag - a + p^2A \end{aligned}$$

é um homomorfismo de grupos. E como o núcleo de γ_g contém pA, induz o seguinte homomorfismo

$$\begin{aligned} \theta(g) : \ A/pA &\longrightarrow pA/p^2A \\ a + pA &\longmapsto ag - a + p^2A. \end{aligned}$$

Para todo $g_1, g_2 \in C_1$ e $a \in A$, temos

$$\begin{aligned} ag_1g_2 - a &= (ag_1 - a) + (ag_2 - a) + ((ag_1 - a)g_2 - (ag_1 - a)) \\ &\equiv (ag_1 - a) + (ag_2 - a) \mod p^2A \end{aligned}$$

e então a aplicação θ é um homomorfismo em $Hom(\frac{A}{pA}, \frac{pA}{p^2A})$, o grupo dos homomorfismos de A/pA em pA/p^2A.

Como A tem posto r então os grupos A/pA e pA/p^2A tem posto no máximo r e portanto a imagem de θ tem posto no máximo r^2. Agora observe que,

$$\theta(g)(a + pA) = 0 + p^2A \Leftrightarrow ag - a + p^2A = p^2A \Leftrightarrow ag + p^2A = a + p^2A \Leftrightarrow g \in C_2$$

então $ker\theta = C_2$.

Logo, C_1/C_2 está na imagem de θ e tal imagem tem posto no máximo r^2, então $d(C_1/C_2) \leq r^2$. Pela construção, temos também que cada elemento de C_2 age trivialmente no módulo quociente A/p^2A, então do item (a), $d(C_2) \leq r^2$.

E como

$$d(C_1) \leq d(C_1/C_2) + d(C_2) \leq r^2 + r^2 = 2r^2$$

e

$$d(G) \leq d(G/C_1) + d(C_1) \leq \frac{1}{2}r(r-1) + 2r^2 = \frac{1}{2}(5r^2 - r).$$

Portanto, $d(G) \leq \frac{1}{2}(5r^2 - r)$.

■

Lema 1.5.15 *Seja A um grupo pro-p abeliano de posto r e suponha também que A é um G-módulo profinito, onde G é um grupo pro-p, e que cada elemento não trivial de G age não trivialmente em A. Então $d(G) \leq \frac{1}{2}(5r^2 - r)$.*

Demonstração: Fixe um inteiro $i > 0$. Primeiramente verificaremos que A/p^iA é um módulo topológico finito.

Por hipótese, A é um grupo pro-p abeliano, então A/p^iA é um p-grupo abeliano finito.

Observe que, a aplicação $a \longmapsto p^i a$ de A em A é contínua, então sua imagem p^iA é fechada. E como A é um grupo topológico, então todo subgrupo fechado de índice finito é aberto, daí, p^iA também é aberto, logo A/p^iA é um módulo topológico finito.

Portanto, o núcleo K_i da ação de G em A/p^iA é um subgrupo normal aberto. E cada elemento não trivial de G/K_i age não trivialmente em A/p^iA. Além disso, como G é um grupo pro-p, então G/K_i é um p-grupo, logo pelo lema anterior $d(G/K_i) \leq t$, onde $t = \frac{1}{2}(5r^2 - r)$.

Agora seja $N \lhd_o G$. Como cada elemento não trivial de G age não trivialmente em A, e como $\bigcap_{i\in\mathbb{N}} p^iA = 0$, temos que $\bigcap_{i\in\mathbb{N}} K_i = 1$. E como as famílias de subgrupos $(K_i)_{i\in\mathbb{N}}$ e $(K_iN)_{i\in\mathbb{N}}$ são cadeias, temos que

$$\bigcap_{i\in\mathbb{N}}(K_iN) = (\bigcap_{i\in\mathbb{N}} K_i)N = N \Rightarrow N = \bigcap_{i\in\mathbb{N}}(K_iN)$$

. Logo, $K_i \leq N$ para algum i.

E segue do teorema do isomorfismo que $\frac{G}{N} \cong \frac{G/K_i}{N/K_i}$, logo $d(G/N) \leq t$, uma vez que $d(G/K_i) \leq t$.

E como tomamos N um subgrupo normal aberto arbitrário de G, essa desigualdade é válida para todo $N \lhd_o G$. E sabemos que $d(G) = \sup\{d(G/N) \mid N \lhd_o G\}$, então $d(G) \leq t = \frac{1}{2}(5r^2 - r)$. ■

Agora mostraremos a caracterização dos grupos profinitos solúveis de posto finito através dos subgrupos abelianos.

Teorema 1.5.16 *Seja G um grupo profinito solúvel. Então G tem posto finito se, e somente se, todo subgrupo abeliano de G é finitamente gerado.*

Demonstração: Se G tem posto finito, então segue da definição que todo grupo é finitamente gerado, em particular os subgrupos abelianos.

Por outro lado, mostraremos que se todo subgrupo abeliano de G é finitamente gerado então G tem posto finito.

Por hipótese G é solúvel, então G tem uma série de subgrupos normais

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

com fatores abelianos. Mostraremos por indução sobre n que G tem posto finito.

Se $n = 1$, então $1 = G_0 \leq G_1 = G$, logo $G_1/G_0 = G$ é abeliano e consequentemente, tem posto finito.Suponha que $n > 1$.

Como G é um grupo prosolúvel, e $G_{n-1} \lhd G$ tal que G/G_{n-1} é abeliano, então pelo lema 1.5.13 , existe um subgrupo H pronilpotente tal que $G = HG_{n-1}$.

Observe que,

$$\frac{G}{G_{n-1}} = \frac{HG_{n-1}}{G_{n-1}} \cong \frac{H}{H \cap G_{n-1}},$$

logo, se H tem posto finito, então G/G_{n-1} também tem posto finito. E por hipótese de indução G_{n-1} tem posto finito. E se G/G_{n-1} e G_{n-1} tem postos finito, então G tem posto finito.

Assim, é suficiente mostrar que H tem posto finito.

Escreva $A = H \cap G_1$. Como $A \leq G_1$ e G_1 tem posto finito, então A tem posto finito. E pelo mesmo argumento anterior, é suficiente mostrar que H/A tem posto finito. Como a série

$$1 = \frac{H \cap G_1}{A} \leq \frac{H \cap G_2}{A} \leq \cdots \leq \frac{H \cap G_n}{A} = \frac{H}{A}$$

para H/A tem fatores abelianos, isto segue por indução se cada subgrupo abeliano de H/A tiver posto finito.

Sejam B/A um subgrupo abeliano de H/A, $D = C_B(A)$ o centralizador de A em B e E um subgrupo finitamente gerado de D contendo A, com a propriedade de ser maximal em relação a ser abeliano. Note que, como A é um grupo abeliano, então pelo lema de Zorn, existe um subgrupo E com tal propriedade. Vamos mostrar que B/A é finitamente gerado.

Agora observe que, se o grupo quociente de um grupo profinito módulo seu centro é procíclico, então o grupo é abeliano. Portanto, se $x \in C_D(E)$ então o subgrupo gerado por E e x é abeliano. Mas E é maximal com relação a propriedade de ser abeliano, então $x \in E$, e consequentemente $E = C_D(E)$.

Sejam p um primo fixo, B_p e $B_{p'}$ os subgrupos p-Sylow e o p-complemento de Hall do grupo pronilpotente B. Então $B = B_p \times B_{p'}$. Escreva A_p, D_p e E_p as interseções de A, D e E com B_p.

Assim, A_p e $A_p \cap B_{p'}$ são os subgrupos p-Sylow e o p-complemento de Hall de A, então $A = A_p \times (A_p \cap B_{p'})$, de modo que $C_{B_p}(A_p) = C_B(A) \cap B_p = D \cap B_p = D_p$. E

similarmente, $E = E_p \times (E \cap B_{p'})$, de modo que $C_{D_p}(E_p) = C_D(E) \cap B_p = E \cap B_p = E_p$.

Como E é finitamente gerado, podemos supor que, E tem posto r. Então A_p e E_p tem posto no máximo r

Recapitulando, temos que, B_p é um subgrupo p-Sylow, $D_p = C_B(A) \cap B_p$, onde $C_B(A) = \{g \in B \mid a^g = a, \forall a \in A\}$, então B_p/D_p é um grupo pro-p. E além disso $A_p = A \cap B_p$ é um grupo pro-p abeliano de posto finito.

Assim, a ação de B_p por conjugação induz em A_p a estrutura de um $(\frac{B_p}{D_p})$-módulo tal que cada elemento não trivial de B_p/D_p age não trivialmente em A_p. Logo, pelo Lema 1.5.15, $d(B_p/D_p) \leq t$, onde $t = \frac{1}{2}(5r^2 - r)$. Analogamente, $d(D_p/E_p) \leq t$ e como E_p é finitamente gerado, então $d(E_p) = k$, para algum k, logo $d(D_p) \leq d(D_p/E_p) + d(E_p) \leq t + k$. E segue que, $d(B_p) \leq d(B_p/D_p) + d(D_p) \leq 2t + k$.

E como isso se aplica para cada p, ou seja, todo subgrupo p-Sylow de B, para cada p, pode ser gerado por um número inteiro z de elementos, então pelo Lema 1.5.8, B é finitamente gerado, e consequentemente, B/A é finitamente gerado.

E como B/A é um subgrupo arbitrário de H/A, então por hipétese de indução H/A tem posto finito. Portanto, H tem posto finito e o resultado segue. ■

A hipótese de solubilidade no teorema acima é indispensável. Por exemplo, o grupo pro-p livre em um conjunto infinito enumerável não é finitamente gerado e portanto, não pode ter posto finito. No entanto, cada um dos seus subgrupos é livre, e então cada subgrupo abeliano é procíclico, e consequentemente finitamente gerado.

A idéia de relacionar propriedades de finitude de um grupo com as de seus subgrupos abelianos remonta um importante artigo de Mal'cev [11], que contém uma prova de que um grupo solúvel abstrato cujos subgrupos abelianos são finitamente gerados devem ser policíclicos, para mais detalhes veja também [16], páginas $455 - 459$.

Para finalizar a seção, vamos fornecer uma estrutura para os grupos profinitos de posto finito. Para isso, enunciaremos três teoremas da teoria de grupos abstratos e demonstraremos alguns resultados auxiliares.

O próximo teorema foi provado por Feit e Thompson, e a demonstração pode ser encontrada no artigo [3].

Teorema 1.5.17 *Todo grupo simples finito não abeliano tem ordem par.*

Os dois resultados a seguir são o teorema de Tate e o teorema de Zassenhaus, respectivamente.

Teorema 1.5.18 *Sejam G um grupo finito, K um subgrupo normal de G e P um subgrupo p-Sylow de G. Se $P \cap K \leq \Phi(P)$, então K tem um p-complemento, isto é, tem um subgrupo normal com índice potência de p e ordem comprima com p.*

Mais detalhes desse resultado pode ser encontrado em [20].

Teorema 1.5.19 *Existe uma função de valores inteiros $f(r)$ de r tal que todo grupo solúvel de matrizes $r \times r$ sobre um corpo possui comprimento derivado no máximo $f(r)$.*

A demonstração desse resultado pode ser encontrado em [16, 15.1.3].

Definição 1.5.20 *Um fator chief de um grupo G é um subgrupo normal minimal de um grupo quociente de G.*

Observe que, se G é finito, então cada fator chief de G é um produto direto de grupos simples isomorfos não abelianos, ou um p-grupo abeliano elementar, para algum primo p.

Lema 1.5.21 *Seja G um grupo finito e suponha que $d(P) = d$, onde P é um 2-Sylow de G. Então em uma série*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

de subgrupos normais de G, podem existir no máximo d fatores chief não abelianos.

Demonstração: Vamos mostrar por indução sobre n.

Se $n = 0$, $G = 1$ e o resultado segue. Suponha que $n \geq 1$.

Suponha que G_1/G_0 não é um fator chief não abeliano, então a série

$$G_1 \leq G_2 \leq \cdots \leq G_n = G$$

tem tamanho $n - 1$, e por hipótese de indução existem no máximo d fatores chief não abelianos.

Suponha agora que G_1/G_0 é um fator chief não abeliano. E como G é finito, então G_1 é um produto direto de grupos simples não abelianos. Logo pelo teorema de

Feit-Thompson, G_1 tem ordem par, então, G_1 não pode ter um 2-complemento normal. Assim, segue do Teorema 1.5.18, que $P \cap G_1 \not\leq \Phi(P)$.

Como P é um grupo pro-p finitamente gerado, com $p = 2$, pela Proposição 1.5.7 item (e), $P/\Phi(P)$ é um grupo abeliano elementar de ordem $2^{d(P)} = 2^d$, e

$$\Phi\left(\frac{P}{P \cap G_1}\right) = \frac{P \cap G_1\Phi(P)}{P \cap G_1}.$$

Logo,

$$\frac{P/P \cap G_1}{\Phi(P/P \cap G_1)} = \frac{P/P \cap G_1}{P \cap G_1\Phi(P)/P \cap G_1} \cong \frac{P}{P \cap G_1\Phi(P)}$$

e

$$\left|\frac{P}{P \cap G_1\Phi(P)}\right| < \left|\frac{P}{\Phi(P)}\right| = 2^d.$$

Portanto, $d(P/P \cap G_1) \leq d - 1$. Além disso, $PG_1/G_1 \cong P/P \cap G_1$ e PG_1/G_1 é um 2-Sylow de G/G_1, então $d(PG_1/G_1) \leq d - 1$. E como a série para G/G_1 tem tamanho $n-1$, então por hipótese de indução existe no máximo $d-1$ fatores chief não abelianos. Mas temos que, G_1/G_0 também é um fator chief não abeliano. Logo existe no máximo d fatores chief não abelianos. ■

Lema 1.5.22 *Seja G um grupo profinito e $(K_\lambda \mid \lambda \in \Lambda)$ é uma família de subgrupos normais satisfazendo $\bigcap K_\lambda = 1$. Suponha que, para algum inteiro m, G/K_λ é solúvel com comprimento derivado no máximo m, para cada $\lambda \in \Lambda$. Então G é solúvel com comprimento derivado no máximo m.*

Demonstração: Seja $G = G^{(0)}, G^{(1)}, G^{(2)}, \ldots, G^{(m)}$ os primeiros termos da série derivada de G, assim $G^{(i+1)} = \{[x, y] \mid x, y \in G^{(i)}\}$, para cada i. Veja que por indução sobre i o i-ésimo termo da série derivada de um grupo quociente G/K é $G^{(i)}K/K$, para $0 \leq i \leq m$. Portanto, $G^{(m)} \leq K_\lambda$, para cada λ, e então temos $G^{(m)} = 1$. ■

Com todos esses resultados em mãos estamos prontos para fornecer uma estrutura para os grupos profinitos de posto finito. Mostraremos que se G é um grupo profinito de posto finito, então G possui uma série (pronilpontente-por-solúvel)-por-finito.

Teorema 1.5.23 *Seja G um grupo profinito de posto finito. Então G tem uma série*

$$1 \leq C \leq N \leq G$$

de subgrupos normais tal que C é pronilpotente, N/C é solúvel e G/N é finito.

Demonstração: Seja G um grupo profinito de posto r. Pelo Lema 1.5.21, temos que, para cada série $G_0 \leq G_1 \leq \ldots \leq G_n = G$ de subgrupos normais abertos, no máximo r dos fatores G_{i+1}/G_i são fatores chief não abelianos. Escolha tal série com uma quantidade de fatores chief não abelianos o maior possível e $N = G_0$. E sendo $N \lhd_\circ G$, então G/N é finito.

Por nossa escolha de N, um fator chief $X = U/V$ de G com V aberto e $U \leq N$ não pode ser o produto direto de grupos simples não abelianos, uma vez que, a série já tem a quantidade maior possível de fatores chief não abelianos, e então $X = U/V$ deve ser abeliano. Assim, se M é um subgrupo normal aberto de G, com $M \leq N$, então cada série maximal de subgrupos normais de G, de M para N, tem fatores abelianos e, então N/M é solúvel.

Veja que, cada fator chief X do tipo considerado acima, é um p-grupo abeliano elementar, para algum primo p, e a conjugação de N induz um homomorfismo com o núcleo C_X, digamos de N para o grupo de automorfismo de X. Assim, o grupo solúvel é N/C_X, pela mesma justificativa dada anteriormente para N/M, e é isomorfo a um subgrupo de $GL_r(\mathbb{F}_p)$, pois $d(X) \leq r$, e então pelo Teorema 1.5.19, N/C_X tem comprimento derivado limitado independentemente de X.

Agora considere C a interseção de todos os subgrupos C_X. Como N/C_X é solúvel, com comprimento derivado limitado, então pelo Lema 1.5.22, N/C é solúvel.

Seja M novamente um subgrupo normal aberto de G, contido em N, e seja $M = N_0 \leq N_1 \leq \ldots \leq N_k = N$ uma cadeia maximal de subgrupos normais de G de M para N. Como a ação de C por conjugação em cada fator N_i/N_{i-1} é trivial, cada comutador de um elemento de C e um elemento de N_i está em $C \cap N_{i+1}$, e segue que $C \cap N_i/C \cap N_{i-1}$ está no centro de $C/C \cap N_{i-1}$, para cada i. Portanto, as imagens dos subgrupos $C \cap N_i$ em $C/C \cap M$ forma uma série central de $C/C \cap M$, e então $C/C \cap M$ é nilpotente. E aplicando para cada subgrupo normal aberto M de G contido em N, concluímos que C é pronilpotente. E com isso, concluímos que G possui uma série (pronilpontente-por-solúvel)-por-finito. ■

Capítulo 2

Grupos Pro-p Uniformes e Álgebras de Lie Powerful sobre $\mathbb{Z}_p$

Nesse capítulo vamos mostrar os resultados mais importantes da teoria dos grupos pro-p uniformes, mostraremos inclusive, como munir um grupo pro-p uniforme G com uma estrutura aditiva, e a partir daí transformá-lo em uma álgebra de Lie sobre $\mathbb{Z}_p$. Além disso, apresentaremos resultados garantindo que existe uma correspondência exata entre grupos pro-p uniformes e álgebras de Lie powerful sobre $\mathbb{Z}_p$, com o objetivo de demonstrar o resultado principal do artigo [19] de I. Snopce, que será demonstrado no próximo capítulo. As principais referências deste capítulo são J. D. Dixon; M. P. F. Du Sautoy; A. Mann; D. Segal [2], L. Ribes e P. Zalesskii [15] e J.S. Wilson [22].

2.1 Preliminares

Como vimos anteriormente, um grupo pro-p é o limite inverso de p-grupos finitos. Ou equivalentemente, um grupo pro-p é um grupo profinito no qual todo subgrupo normal aberto tem índice igual a alguma potência de p, a demonstração dessa equivalência pode ser encontrada em [2, Proposition 1.12]. Segue da definição que um grupo finito é um grupo pro-p se, e somente se, sua ordem é uma potência de p. E note que, em um grupo pro-p todo subgrupo aberto tem índice potência de p, uma vez que contém um subgrupo normal aberto.

Os resultados a seguir são de caráter introdutório e serão utilizados como ferra-

mentas nas seções seguintes, a teoria detalhada pode ser vista em [2], Capítulo 1.

No estudo dos grupos pro-p, o subgrupo de Frattini $\Phi(G)$ de G desempenha um papel particularmente útil. Relembrando que, $\Phi(G)$ é o conjunto dos não geradores de G e coincide com a interseção de todos os subgrupos maximais de G.

Proposição 2.1.1 *Se G é um grupo pro-p, então*

$$\Phi(G) = \overline{G^p[G, G]},$$

onde $[G, G]$ é o grupo derivado e $G^p = \langle g^p \mid g \in G \rangle$.

A demonstração pode ser encontrada em [2, Proposition 1.13].

Proposição 2.1.2 *Seja G um grupo pro-p. Então G é finitamente gerado se, e somente se, $\Phi(G)$ é aberto em G.*

A demonstração desse resultado pode ser encontrada em [2, Proposition 1.14].

Agora definiremos uma série de subgrupos característicos chamada *lower p-series*.

Definição 2.1.3 *Seja G um grupo pro-p. Então definimos $P_1(G) = G$, e para $i \geq 1$*

$$P_{i+1}(G) = \overline{P_i(G)^p[P_i(G), G]}.$$

Para simplificar a notação, denotaremos $P_i(G) = G_i$.

Veja que pela Proposição 2.1.1, $P_2(G) = \Phi(G)$. Além disso, $\Phi(G_i) = \overline{G_i^p[G_i, G_i]} \leq \overline{G_i^p[G_i, G]} = G_{i+1}$, para cada i, e

$$G = G_1 \geq G_2 \geq \ldots \geq G_n \geq \ldots,$$

onde cada termo é característico no termo anterior e, consequentemente, todos os termos são característicos em G. Em particular, se H é um subgrupo característico em grupo pro-p G, então $P_k(H)$ é característico em G. De fato, como $H \, char \, G$, então é suficiente mostrar que $P_k(H) \, char \, H$. Vamos mostrar por indução sobre k que $P_k(H) \, char \, H$.

Se $k = 1$, $P_1(H) = H$. Suponha que $P_k(H) \, char \, H$, para $k \geq 1$. E vamos mostrar que a afirmação é verdadeira para, $k + 1$, ou seja, $P_{k+1}(H) \, char \, H$. Seja $\varphi \in Aut(H)$. Temos que, $P_{k+1}(H) = P_k(H)^p[P_k(H), H]$ então

$$\varphi(P_{k+1}(H)) = \varphi(P_k(H))^p[\varphi(P_k(H)), \varphi(H)] = P_k(H)^p[P_k(H), H] = P_{k+1}(H),$$

por hipótese de indução. Logo, $P_k(H)\,char\,H$, para todo k e, consequentemente, $P_k(H)\,char\,G$, para todo k.

Uma das vantagens de estudar a série definida acima, é que, se G é um grupo pro-p finitamente gerado, então a série é bem comportada, uma vez que consiste de subgrupos abertos. Essa e mais algumas das propriedades da lower p-series, serão apresentadas no próximo resultado.

Proposição 2.1.4 *Seja G um grupo pro-p.*

(i) *$P_i(G/K) = P_i(G)K/K$, para todo $K \lhd_c G$ e para todo i;*

(ii) *$[P_i(G), P_j(G)] \leq P_{i+j}(G)$, para todo i e j;*

(iii) *Se G é finitamente gerado, então $P_i(G)$ é aberto em G para cada i, e o conjunto $\{P_i(G) \mid i \geq 1\}$ é uma base de vizinhança de 1 em G.*

A demonstração desse resultado pode ser encontrada em [2, Proposition 1.16]. Veja que, do item (iii), como $\{G_i \mid i \geq 1\}$ forma uma base para uma vizinhança da identidade em G, então para todo $N \lhd_o G$ existe um i tal que $G_i \leq N$.

Uma característica notável dos grupos pro-p finitamente gerados é que a topologia é completamente determinada pela estrutura de grupo. O teorema fundamental é

Teorema 2.1.5 *Se G é um grupo pro-p finitamente gerado, então todo subgrupo de índice finito em G é aberto.*

A demonstração pode ser encontrada em [2, Theorem 1.17].

Esse resultado foi provado por J. P. Serre nos anos 70, e somente em 2003 N. Nikolov e D. Segal [14] provaram o caso mais geral, que garante que todo subgrupo de índice finito é aberto em um grupo profinito finitamente gerado. Em [21] pode-se encontrar um estudo geral sobre o desenvolvimento desse resultado, bem como aspectos da prova, resultados relacionados e algumas maneiras pelas quais os resultados já foram usados.

Outra informação interessante é que, em um grupo pro-p finitamente gerado, $\Phi(G) = G^p[G, G]$, o que significa que podemos simplificar a Definição 2.1.3, removendo a 'barra', ou seja,

$$P_{i+1}(G) = P_i(G)^p[P_i(G), G],$$

esse argumento pode ser visto com mais detalhes em [2, Corollary 1.20].

E como consequência do Teorema 2.1.5, temos os seguintes corolários:

Corolário 2.1.6 **(i)** *Todo homomorfismo (abstrato) de um grupo pro-p finitamente gerado em um grupo profinito é contínuo.*

(ii) *A topologia de um grupo pro-p finitamente gerado é determinada pela sua estrutura de grupo.*

Esse resultado está demonstrado em [2, Corollary 1.21].

Corolário 2.1.7 *Se G é um grupo pro-p finitamente gerado, então todo automorfismo de G (como um grupo abstrato) é um automorfismo topológico, e todo subgrupo topologicamente característico de G é característico.*

A demonstração pode ser encontrada em [2, Corollary 1.22].

Temos também o seguinte resultado relativo à convergência de sequências de elementos na topologia profinita.

Definição 2.1.8 *Seja G um grupo abstrato e $I = (K_n \mid n \in \mathbb{N})$ uma família de subgrupos normais de índices finitos tal que $K_{n_2} \leq K_{n_1}$ sempre que $n_1 \leq n_2$. Uma sequência (g_i) de elementos de G é chamada* sequência de Cauchy *(com respeito a I) se $K_n g_m = K_n g_n$, sempre que $n \leq m$.*

Se G é um grupo profinito e I também é uma base de vizinhanças abertas de 1 então toda sequência de Cauchy em G tem limite em G, para mais detalhes veja [22], Exercício 1.6.13.

Reformulando a definição temos o seguinte resultado.

Proposição 2.1.9 *Se G é um grupo profinito, então uma sequência $(g_i) \subseteq G$ converge se, e somente se, para cada $N \lhd_\circ G$ existe $n = n(N)$ tal que $g_i^{-1} g_j \in N$, para todo $i, j \geq n$.*

A demonstração desse resultado pode ser encontrada em [18, Proposition 2.19].

Para finalizar os resultados introdutórios, apresentaremos uma proposição que é uma ferramenta muito útil, em especial, na teoria dos grupos pro-p de posto finito. Por exemplo, com essa proposição podemos provar que G é um grupo pro-p de posto finito se, e somente se, G é o produto de uma quantidade finita de subgrupos procíclicos.

Proposição 2.1.10 *Seja G um grupo pro-p. Então as seguintes afirmações são equivalentes:*

(i) *G é procíclico;*

(ii) *G pode ser gerado topologicamente por um conjunto com um único elemento;*

(iii) *$G = g^{\mathbb{Z}_p}$, para algum $g \in G$;*

(iv) *G é cíclico e finito, ou então é isomorfo topologicamente a $\mathbb{Z}_p$.*

A demonstração desse resultado pode ser vista em [2, Proposition 1.28].

2.2 Grupos Pro-p Powerful

Começaremos esta seção desenvolvendo a teoria dos grupos pro-p powerful, com o objetivo de caracterizar os grupos pro-p de posto finito como exatamente aqueles que contêm um subgrupo aberto powerful finitamente gerado.

Definição 2.2.1 *Seja p primo e G um grupo pro-p.*

(i) *Dizemos que G é powerful quando $G/\overline{G^p}$ é abeliano se p é ímpar, ou $G/\overline{G^4}$ é abeliano se $p = 2$.*

(ii) *Seja $N \leq_\circ G$. Dizemos que N é powerfully embedded em G quando $[N, G] \leq \overline{N^p}$ se p é ímpar, ou $[N, G] \leq \overline{N^4}$ se $p = 2$.*

Se N é powerfully embedded em G, denotaremos por $N\, p.e.\, G$.

Note que, se $N\, p.e.\, G$, então $N \trianglelefteq_\circ G$ e N é powerful. Um exemplo trivial de grupos pro-p powerful são os grupos pro-p abelianos.

O próximo resultado é uma ferramenta muito importante, que nos permite verificar se um grupo pro-p é powerful reduzindo-se aos p-grupos finitos.

Proposição 2.2.2 *Seja G um grupo pro-p e $N \leq_\circ G$. Então $N\, p.e.\, G$ se, e somente se, $NK/K\, p.e.\, G/K$ para todo $K \trianglelefteq_\circ G$.*

Demonstração: Suponha p um primo ímpar. Se $N\, p.e.\, G$, então $[N, G] \leq \overline{N^p}$ e pela Proposição 1.1.16, item (c), $\overline{N^p} = \bigcap_{K \lhd_o G} N^p K$. Logo, $[N, G] \leq N^p K$, para todo $K \lhd_o G$. Daí, $[NK/K, G/K] \leq N^p K/K = (NK/K)^p \leq \overline{(NK/K)^p}$, para todo $K \lhd_o G$, o que implica que $NK/K\, p.e.\, G/K$, para todo $K \lhd_o G$.

Por outro lado, se $NK/K\, p.e.\, G/K$, para todo $K \lhd_o G$, e como G/K é um p-grupo finito, então $[NK/K, G/K] \leq (NK/K)^p = N^p K/K$, para todo $K \lhd_o G$, o que implica

que, $[N, G] \leq [NK, G] \leq N^pK$, para todo $K \lhd_o G$. Logo, $[N, G] \leq \bigcap_{K \lhd_o G} N^pK = \overline{N^p}$. E portanto, $N\, p.e.\, G$. A demonstração é análoga para o caso $p = 2$. ■

No corolário a seguir, veremos que o limite inverso de um sistema inverso de p-grupos powerful produz um grupo powerful. Lembrando que, um p-grupo finito G é powerful se p é primo ímpar e G/G^p é abeliano, ou se $p = 2$ e G/G^4 é abeliano.

Corolário 2.2.3 *Um grupo topológico G é um grupo pro-p powerful se, e somente se, G é o limite inverso de um sistema inverso de p-grupos finitos powerful em que todas as aplicações são sobrejetivas.*

A demonstração desse resultado segue da definição de limite inverso, e pode ser vista com detalhes em [2, Corollary 3.3].

Veja que, os p-grupos finitos são um caso particular de grupos pro-p. E as propriedades dos grupos pro-p finitamente gerados powerful seguem, em grande parte, dos p-grupos powerful. Sendo assim, apresentaremos uma série de resultados de grupos pro-p powerful, mas na maioria dos casos, começaremos com um resultado para p-grupos powerful antes de estendê-lo ao resultado correspondente sobre grupos pro-p finitamente gerados powerful. A teoria dos p-grupos powerful pode ser vista com detalhes em [2], Capítulo 2. Lembrando que, sempre que citarmos os p-grupos powerful, de acordo com a definição de ser powerful, estamos nos referindo apenas aos p-grupos finitos.

Proposição 2.2.4 *Se G é um p-grupo powerful então todo elemento de G^p é uma potência de p de um elemento de G.*

A demonstração pode ser encontrada em [2, Proposition 2.6].

Proposição 2.2.5 *Seja G um grupo pro-p finitamente gerado powerful. Então todo elemento de G^p é uma potência de p de um elemento de G, e $G^p = \Phi(G)$ é aberto em G. E se $p = 2$, então G^4 é aberto em G.*

Demonstração: Primeiramente mostraremos que todo elemento de G^p é uma potência de p de um elemento de G. Para isso, basta mostrar que $\overline{G^p} = G^p$. Seja $g = (g_N) \in \overline{G^p} = \bigcap_{N \lhd_o G} G^pN$, então para cada $N \lhd_o G$, $g_N \in (G/N)^p$. E como G/N é um p-grupo powerful, então pela Proposição 2.2.4, g_N é uma potência de p em G/N, para cada $N \lhd_o G$. Defina $X_N = \{h_N \in G/N \mid h_N^p = g_N\}$. Note que, com respeito

a aplicação natural $\pi_{MN} : G/N \longrightarrow G/M$, sempre que $N \leq M$, $(X_N, \pi_{MN})_{N \lhd_o G}$ forma um sistema inverso de conjuntos finitos não vazios. Então $\varprojlim X_N \neq \varnothing$, o que implica que que existe $h = (h_N) \in \varprojlim X_N \subseteq G$, onde $h^p = g$ e então $\overline{G^p} \subseteq G^p$, mas $G^p \leq \overline{G^p}$, por definição. Logo, $\overline{G^p} = G^p = \{g^p \mid g \in G\}$. Agora mostraremos a segunda parte. Como G é powerful, então $G\, p.e.\, G$, o que implica que $[G, G] \leq \overline{G^p} = G^p$. Por outro lado, como G é um grupo pro-p finitamente gerado, então $\Phi(G) = G^p[G, G]$, logo $G^p = \Phi(G) = P_2(G)$ que é aberto pela Proposição 2.1.4. E se $p = 2$ com um argumento similar podemos ver que $\overline{G^4} = G^4 \geq P_3(G)$ o que implica que G^4 é aberto em G.

■

Proposição 2.2.6 *Seja G um p-grupo finito e $N \leq G$. Se $N\, p.e.\, G$ então $N^p\, p.e.\, G$.*

A demonstração pode ser encontrada em [2, Proposition 2.3].

Corolário 2.2.7 *Seja G um grupo pro-p finitamente gerado powerful. Então para cada $i \geq 1$,*

$$G^{p^i} = (G^{p^{i-1}})^p = \{x^{p^i} \mid x \in G\}\, p.e.\, G^{p^{i-1}}.$$

Demonstração: Mostraremos por indução sobre i que $G^{p^i}\, p.e.\, G^{p^{i-1}}$.

Se $i = 1$, então $G^{p^i} = G^p$. Assim para o caso $i = 1$ mostraremos que $\overline{G^p} = G^p\, p.e.\, G$. Mas pela Proposição 2.2.2 é suficiente mostrar que $G^pK/K\, p.e.\, G/K$, para todo $K \lhd_o G$. Por hipótese, G é um grupo powerful, então G/K é powerful e, consequentemente, $G/K\, p.e.\, G/K$, para todo $K \lhd_o G$. Como G/K é um p-grupo finito, então pela Proposição 2.2.6, $(G/K)^p\, p.e.\, G/K$, mas $(G/K)^p = G^pK/K$. Logo, $G^p\, p.e.\, G$.

Agora suponha que $G^{p^i}\, p.e.\, G^{p^{i-1}}$, e vamos mostrar que a afirmação é verdadeira para $i + 1$, ou seja, $G^{p^{i+1}}\, p.e.\, G^{p^i}$.

Por hipótese de indução $G^{p^i}\, p.e.\, G^{p^{i-1}}$, então G^{p^i} é powerful, o que implica que, $G^{p^i}\, p.e.\, G^{p^i}$, e pela Proposição 2.2.2, $G^{p^i}/K\, p.e.\, G^{p^i}/K$, para todo $K \lhd_o G^{p^i}$. Segue que, pela Proposição 2.2.6, $(G^{p^i}/K)^p\, p.e.\, G^{p^i}/K$, para todo $K \lhd_o G^{p^i}$, mas $(G^{p^i}/K)^p = (G^{p^i})^p/K = G^{p^{i+1}}/K$. Logo, $G^{p^{i+1}}/K\, p.e.\, G^{p^i}/K$, o que implica que, $G^{p^{i+1}}\, p.e.\, G^{p^i}$.

■

O próximo resultado de grupos pro-p nos dá as principais características da lower p-series em um grupo pro-p powerful.

Teorema 2.2.8 *Seja $G = \langle a_1, \ldots, a_d \rangle$ um p-grupo powerful, e escreva $G_i = P_i(G)$, para cada i. Então*

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

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

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

(iv) *A aplicação $x \longmapsto x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} em G_{i+k}/G_{i+k+1} para cada i e cada k.*

A demonstração pode ser encontrada em [2, Theorem 2.7].

Teorema 2.2.9 *Seja $G = \overline{\langle a_1, \ldots, a_d \rangle}$ um grupo pro-p powerful finitamente gerado e escreva $G_i = P_i(G)$ para cada i. 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) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \overline{\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle}$;*

(iv) *A aplicação $x \longmapsto x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} em G_{i+k}/G_{i+k+1} para cada i e cada k.*

Demonstração: Pela Proposição 2.2.5, temos que $G_2 = \Phi(G_1) = G^p = \{g^p \mid g \in G\} \lhd_\circ G$. Como $N \lhd_\circ G$, então G/N é um p-grupo finito powerful e, consequentemente pelo Teorema 2.2.8, $G^{p^{i-1}}N/N$ p.e. G/N, para todo i. E como isso vale para todo $N \lhd_\circ G$, então pela Proposição 2.2.2, $G_i = G^{p^{i-1}}$ p.e. G. Assim,

$$G_i = \Phi(G_{i-1}) = G^{p^{i-1}} = \{g^{p^{i-1}} \mid g \in G\} \lhd_\circ G.$$

Agora, tomando G_i no lugar de G e $k+1$ no lugar de i, temos

$$P_{k+1}(G_i) = G_i^{p^k} = \{y^{p^k} \mid y \in G_i\} = (G^{p^{i-1}})^{p^k} = G^{p^{(i+k)-1}} = G_{i+k}.$$

E sendo $\Phi(G_i) = G_{i+1} = \{g^p \mid g \in G_i\}$, segue que, a aplicação $x \longmapsto x^p$ é um homomorfismo sobrejetivo de G_i/G_{i+1} em G_{i+1}/G_{i+2}, e compondo essas aplicações, assim como é feito na prova do Teorema 2.2.8, temos que, $x \longmapsto x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} em G_{i+k}/G_{i+k+1} para cada i e cada k. E essa aplicação implica que

$G_2 = \langle a_1^p, \ldots, a_d^p \rangle G_3$ e por indução, $G_i = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle G_{i+1}$. E como $\Phi(G_i) = G_{i+1}$ é o conjunto dos não geradores de G_i, então $G_i = \overline{\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle}$. ■

Corolário 2.2.10 *Se $G = \langle a_1, \ldots, a_d \rangle$ é um p-grupo powerful então $G = \langle a_1 \rangle \ldots \langle a_d \rangle$, ou seja, G é o produto de seus subgrupos cíclicos $\langle a_i \rangle$.*

A demonstração pode ser encontrada em [2, Corollary 2.8].

Proposição 2.2.11 *Se $G = \overline{\langle a_1, \ldots, a_d \rangle}$ é um grupo pro-p powerful então $G = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$, isto é, G é o produto de seus subgrupos procíclicos $\overline{\langle a_1 \rangle}, \ldots, \overline{\langle a_d \rangle}$.*

Demonstração: Tome $A = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$, vamos mostrar que $G = A$. Como um produto de uma quantidade finita de fechados é fechado, então A é um subconjunto fechado de G. Assim, $A = \overline{A} = \bigcap_{N \lhd_o G} AN$. Por hipótese, $G = \overline{\langle a_1, \ldots, a_d \rangle}$ é finitamente gerado, então $G/N = \overline{\langle a_1, \ldots, a_d \rangle}/N$ é finitamente gerado, para cada $N \lhd_o G$. E como G é um grupo pro-p powerful, G/N é um p-grupo powerful, então pelo Corolário 2.2.10, $G/N = AN/N$, para cada $N \lhd_o G$. Logo $G = A$. ■

Lembrando que, para qualquer grupo topológico G, $d(G)$ denota a cardinalidade mínima de um conjunto de geradores topológicos para G.
Se G é um grupo pro-p finitamente gerado, temos que

$$d(G) = dim_{\mathbb{F}_p}(G/\Phi(G)),$$

ou seja, $d(G)$ é a dimensão de $G/\Phi(G)$ visto como espaço vetorial sobre um corpo com p elementos.

O próximo resultado dá condições sobre um grupo pro-p para garantir que a quantidade minimal de geradores de um subgrupo próprio é menor do que a quantidade minimal de geradores do grupo. Veja que esse resultado é de suma importância para a teoria dos grupos pro-p powerful, pois através dele podemos garantir que todo grupo pro-p powerful finitamente gerado tem posto finito.

Teorema 2.2.12 *Se G é um p-grupo powerful e $H \leq G$, então $d(H) \leq d(G)$.*

A demonstração pode ser encontrada em [2, Theorem 2.9].

Teorema 2.2.13 *Seja G um grupo pro-p powerful finitamente gerado e H um subgrupo fechado de G. Então $d(H) \leq d(G)$.*

Demonstração: Por hipótese G é um grupo pro-p powerful, então G/N é um p-grupo powerful e pelo Teorema 2.2.12, $d(HN/N) \leq d(G/N)$, para cada $N \lhd_o G$. E como HN/N e G/N são finitamente gerados, existem $X \subseteq H$ e $Y \subseteq G$ tais que XN/N gera HN/N, para cada $N \lhd_o G$, e YN/N gera G/N, para cada $N \lhd_o G$. Então X gera H topologicamente e Y gera G topologicamente, e $|X| \leq |Y|$. Logo, $d(H) \leq d(G)$.

■

Nosso próximo passo é construir um subgrupo aberto powerful em um grupo pro-p finitamente gerado, com o intuito de obter informações mais gerais do que o teorema acima. Por exemplo, provaremos mais adiante que, se G é um grupo pro-p finitamente gerado e tem um subgrupo aberto powerful, então G tem posto finito.

Definição 2.2.14 *Seja G um grupo pro-p finitamente gerado. Definimos $V(G,r)$ como sendo a interseção dos núcleos de todos os homomorfismos de G em $GL_r(\mathbb{F}_p)$.*

Como G é finitamente gerado e $GL_r(\mathbb{F}_p)$ é finito, então pelo Corolário 2.1.6, os homomorfismos de G em $GL_r(\mathbb{F}_p)$ são contínuos. Logo, existe uma quantidade finita de homomorfismos de G em $GL_r(\mathbb{F}_p)$, e consequentemente, $V(G,r)$ é aberto em G, pois é a interseção finita de abertos.

Proposição 2.2.15 *Seja G um p-grupo finito, p primo e r um inteiro positivo. Considere $V = V(G,r)$ e seja $W = V$ se p é ímpar e $W = V^2$ se $p = 2$. Se $N \lhd G$, $d(N) \leq r$ e $N \leq W$, então N p.e. W.*

A demonstração pode ser encontrada em [2, Proposition 2.12].

Proposição 2.2.16 *Seja G um grupo pro-p finitamente gerado, p primo e r um inteiro positivo. Considere $V = V(G,r)$. E seja $N \trianglelefteq_o G$ satisfazendo $d(N) \leq r$ e $N \leq V$ se p é ímpar, e $N \leq V^2$ se $p = 2$. Então N p.e. V se p é ímpar, e N p.e. V^2 se $p = 2$.*

Demonstração: Por hipótese G é um grupo pro-p, então G/K é um p-grupo, para todo $K \lhd_o G$ e $NK/K \lhd_o G/K$, para todo $K \lhd_o G$, uma vez que $N \lhd_o G$. Além disso, como $d(N) \leq r$, então $d(NK/K) \leq r$, para todo $K \lhd_o G$. Agora considere $V(G/K,r)$ a interseção dos núcleos de todos os homomorfismos de G/K em $GL_r(\mathbb{F}_p)$.

E veja que, $V(G,r)K/K \leq V(G/K,r)$, pois um homomorfismo de G em $GL_r(\mathbb{F}_p)$ é a composição das funções $G \longrightarrow G/K$ e $G/K \longrightarrow GL_r(\mathbb{F}_p)$.

Suponha que p é ímpar. Como $NK/K \leq V(G,r)K/K \leq V(G/K,r)$, para todo $K \lhd_o G$, então pela Proposição 2.2.15, $NK/K\, p.e.\, V(G/K,r)$, o que implica que, $[NK/K, V(G/K,r)] \leq (NK/K)^p$, mas $[NK/K, V(G,r)K/K] \leq [NK/K, V(G/K,r)]$, então $[NK/K, V(G,r)K/K] \leq (NK/K)^p$, logo $NK/K\, p.e.\, V(G,r)K/K$, para todo $K \lhd_o G$, e pela Proposição 2.2.2, $N\, p.e.\, V(G,r)$. Analogamente, se $p = 2$, então $N\, p.e.\, V^2$, o que completa a prova da proposição. ■

Definição 2.2.17 *Dado $r \in \mathbb{N}$, definimos $\lambda(r)$ como sendo um inteiro que satisfaz*

$$2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}.$$

Lema 2.2.18 *Se G é um p-grupo finito, então $G/V(G,r)$ possui uma série de comprimento $\lambda(r)$, de subgrupos normais com todos os fatores abelianos elementares.*

A demonstração desse resultado pode ser encontrada em [2, Lemma 2.11].

Teorema 2.2.19 *Seja G um grupo pro-p finitamente gerado e p primo. Suponha que $r = sup\{d(N) \mid N \trianglelefteq_\circ G\}$ é finito, então G tem um subgrupo característico powerful de índice no máximo $p^{r\lambda(r)}$ se p é ímpar e $2^{r+r\lambda(r)}$ se $p = 2$.*

Demonstração: Considere $V = V(G,r)$. Por definição V é a interseção dos núcleos de todos os homomorfismos de G em $GL_r(\mathbb{F}_p)$, e como o núcleo de cada homomorfismo é característico, então V é característico em G. Por hipótese G é um grupo pro-p, então G/K é um p-grupo finito, para todo $K \lhd_o G$, e pelo Lema 2.2.18, $\frac{G/K}{VK/K}$ possui uma série

$$G/K = N_0/K \geq N_1/K \geq \ldots \geq N_s/K = VK/K$$

de subgrupos normais em G/K tais que $s \leq \lambda(r)$ e todos os fatores $\frac{N_i/K}{N_{i+1}/K}$ são abelianos elementares com $0 \leq i \leq s-1$. E pelo teorema do isomorfismo $VK/K \cong V/V \cap K$ e $\frac{N_i/K}{N_{i+1}/K} \cong \frac{N_i}{N_{i+1}}$, com $0 \leq i \leq s-1$. Então, G/V possui uma série

$$G = N_0 \geq N_1 \geq \ldots \geq N_s = V$$

de subgrupos normais de G tais que $s \leq \lambda(r)$ e todos os fatores N_i/N_{i+1} são abelianos elementares com $0 \leq i \leq s-1$. E como $r = sup\{d(N) \mid N \trianglelefteq_\circ G\}$ é finito, cada um desses fatores tem ordem no máximo p^r e então $|G : V| \leq p^{r\lambda(r)}$.

Suponha que p é ímpar. Como V é a interseção finita de subgrupos normais abertos, então $V \triangleleft_\circ G$. Além disso, $d(V) \leq r = sup\{d(N) \mid N \trianglelefteq_\circ G\}$, então pela Proposição 2.2.16, $V\, p.e.\, V$ e, consequentemente, V é powerful. Assim, se p é ímpar, V é um subgrupo aberto característico powerful, com índice no máximo $p^{r\lambda(r)}$.

Agora suponha que $p = 2$. Note que, dado ϕ um automorfismo de V, $\phi(v^2) = \phi(v)^2$, para todo $v \in V$, então V^2 é característico em V, logo V^2 é característico em G, e como $r = sup\{d(N) \mid N \trianglelefteq_\circ G\}$ e $V^2 \triangleleft_\circ G$, então $d(V^2) \leq r$. E pela Proposição 2.2.16, $V^2\, p.e.\, V^2$ e, consequentemente, V^2 é powerful. Além disso, $|V/V^2| = 2^t \leq |V| \leq 2^r$, então $|V/V^2| \leq 2^r$. E como a série de V em G tem tamanho no máximo $\lambda(r)$, então a série de V^2 em G tem tamanho no máximo $\lambda(r)+1$, assim $|G : V^2| \leq 2^{r+r\lambda(r)}$. Logo, se $p = 2$, V^2 é um subgrupo característico powerful com índice no máximo $2^{r+r\lambda(r)}$, o que completa a prova do teorema. ■

Relembrando que um grupo profinito de posto finito é por definição finitamente gerado. E se G é um grupo pro-p powerful finitamente gerado, então pelo Teorema 2.2.13, G tem posto finito e $rk(G) = d(G)$. Tendo em mãos os resultados acima, podemos provar que, se G é um grupo pro-p finitamente gerado e tem um subgrupo aberto powerful, então G tem posto finito.

Teorema 2.2.20 *Seja G um grupo pro-p. Então G tem posto finito se, e somente se, G é finitamente gerado e tem um subgrupo aberto powerful; neste caso, G tem um subgrupo característico aberto powerful.*

Demonstração: Suponha que G tem posto finito, digamos $rk(G) = r$, então G é finitamente gerado, e pelo Teorema 2.2.19, G tem um subgrupo aberto característico powerful, mais precisamente, tal subgrupo é $V = V(G, r)$ se p é ímpar e V^2 se $p = 2$.

Reciprocamente, suponha que G é finitamente gerado e tem um subgrupo H aberto powerful. Então H tem índice finito e contém um subgrupo normal aberto de G, digamos N. Sabemos que, $rk(G) \leq rk(N) + rk(G/N)$. E por hipótese, G é um grupo pro-p, então G/N é um p-grupo finito e, consequentemente, tem posto finito.

Além disso, sendo G um grupo pro-p finitamente gerado, então H é um grupo pro-p finitamente gerado, $d(H) = d$. Assim, H é um grupo pro-p powerful finitamente gerado, então pelo Teorema 2.2.13, $d(K) \leq d(H) = d$, para todo $K \leq_c H$. Logo, $rk(H) \leq d(H) = d$. E como $N \leq H$, então N tem posto no máximo d. E portanto, $rk(G) \leq rk(N) + rk(G/N)$ é finito. ■

Corolário 2.2.21 *Seja G um grupo pro-p e r um inteiro positivo. Suponha que todo subgrupo aberto de G contém um subgrupo normal aberto N de G, com $d(N) \leq r$. Então G tem posto finito.*

Demonstração: Como $d(G/N)$ é finito, com $N \lhd_o G$ e $d(N) \leq r$, então G é finitamente gerado, pois $d(G) \leq d(G/N) + d(N)$.

Considere $W = V(G, r)$ se p é ímpar e $W = V(G, r)^2$ se $p = 2$. Como W é aberto em G, então contém um subgrupo N normal aberto r-gerado de G e pela Proposição 2.2.16, $N\, p.e.\, W$ e, consequentemente, N é powerful. E pelo teorema anterior, G tem posto finito. ■

E para finalizar essa seção apresentaremos dois teoremas nos quais são adicionados condições em um grupo pro-p para o mesmo ter posto finito.

Teorema 2.2.22 *Seja G um grupo pro-p. Então as seguintes afirmações são equivalentes:*

(a) *Existe $s \in \mathbb{N}$ e $c > 0$ tal que $|G : \overline{G^{p^k}}| \leq cp^{ks}$, para todo k;*

(b) *Existe $s \in \mathbb{N}$ e $c > 0$ tal que $|G : G^{p^k}| \leq cp^{ks}$, para todo k;*

(c) *G tem posto finito.*

Além disso, se em (c) G tem posto r, então podemos tomar $s = r$ em (a) e (b). E dado s como em (a), G tem um subgrupo normal aberto K, com $rk(K) \leq s$.

A demonstração desse resultado pode ser encontrada em [2, Theorem 3.16].

Teorema 2.2.23 *Seja G um grupo pro-p. Então as seguintes afirmações são equivalentes:*

(a) *G é o produto de uma quantidade finita de subgrupos procíclicos;*

(b) *G é o produto de uma quantidade finita de subgrupos fechados de posto finito;*

(c) *G tem posto finito;*

(d) *G é finitamente gerado como um grupo '$\mathbb{Z}_p$-powered', isto é, G tem um subconjunto X finito tal que todo elemento de G é igual a um produto da forma $x_1^{\lambda_1} \dots x_s^{\lambda_s}$, com $x_j \in X$ e $\lambda_j \in \mathbb{Z}_p$.*

(e) *G é gerado como um grupo '$\mathbb{Z}_p$-powered' por um subconjunto enumerável.*

A demonstração desse teorema pode ser encontrada em [2, Theorem 3.17].

2.3 Grupos Pro-p Uniformes e Teoria de Lie

Na seção anterior, mostramos que todo grupo pro-p de posto finito tem um subgrupo normal aberto que é powerful. Agora mostraremos que este subgrupo pode ser escolhido de modo a satisfazer uma condição ligeiramente mais forte, a de ser uniformly powerful. Além disso, mostraremos que nos grupos pro-p uniformly powerful a operação do grupo pode ser 'suavizada', para dar uma nova estrutura de grupo abeliano, e esse novo grupo abeliano é de forma natural um $\mathbb{Z}_p$- módulo livre finitamente gerado. E por fim, estabeleceremos a correspondência entre grupos pro-p uniformes e álgebras de Lie.

Definição 2.3.1 *Seja G um grupo pro-p. Dizemos que G é uniformly powerful quando*

(i) *G é finitamente gerado,*

(ii) *G é powerful, e*

(iii) *Para todo i, $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$.*

Para simplificar, abreviaremos 'uniformly powerful' denotando apenas por 'uniforme'.

Veja que, se G é um grupo pro-p satisfazendo os itens (i) e (ii) da definição acima, então pelo Teorema 2.2.9, a aplicação $x \longmapsto x^p$ induz um epimorfismo

$$f_i : P_i(G)/P_{i+1}(G) \longrightarrow P_{i+1}(G)/P_{i+2}(G)$$

para cada i, e pelo item (iii) da definição acima $|P_i(G) : P_{i+1}(G)|$ é constante, assim,

$$|P_i(G)/P_{i+1}(G)| = |P_{i+1}(G)/P_{i+2}(G)| = |G/P_2(G)|.$$

Logo, a condição (iii) da definição acima é equivalente a:

(iii)' Para cada $i \geq 1$, a aplicação f_i é um isomorfismo.

Teorema 2.3.2 *Seja G um grupo pro-p powerful finitamente gerado. Então $P_k(G)$ é uniforme, para todo k suficientemente grande.*

Demonstração: Escreva $P_i(G) = G_i$, para todo i. Como G é finitamente gerado e G_i é aberto em G para cada i, então pela Proposição 2.1.4, G_i é finitamente gerado, para cada i. Além disso, pelo Teorema 2.2.9, item (i), $G_i\, p.e.\, G$, para todo i e, consequentemente, G_i é powerful, para todo i.

Resta verificar que $|P_i(G_k) : P_{i+1}(G_k)| = |G_k : P_2(G_k)|$. Sendo G_i um grupo pro-p, então $|G_i : G_{i+1}| = p^{d_i}$, para algum $d_i \in \mathbb{N}$. E pelo Teorema 2.2.9 item (iv), a aplicação $x \longmapsto x^{p^k}$ induz um homomorfismo sobrejetor de G_i/G_{i+1} em G_{i+k}/G_{i+k+1}, assim $p^{d_i} = |G_i/G_{i+1}| \geq |G_{i+k}/G_{i+k+1}|$, em particular, para $k = 1$, $p^{d_i} = |G_i/G_{i+1}| \geq |G_{i+1}/G_{i+2}| = p^{d_{i+1}}$, então $d_1 \geq d_2 \geq \ldots \geq d_i \geq d_{i+1} \geq \ldots$, o que implica que existe m tal que $d_k = d_m$, para todo $k > m$, logo,

$$p^{d_k} = |G_k/G_{k+1}| = |G_{k+1}/G_{k+2}| = \ldots = |G_{k+j}/G_{k+j+1}|.$$

E pela Proposição 2.2.9 item (ii), $P_i(G_k) = G_{k+i-1}$, para todo i e para todo k. Logo,

$$p^{d_k} = |G_k/G_{k+1}| = |G_k/P_2(G_k)| = |G_{k+i-1}/G_{k+i}| = |P_i(G_k)/P_{i+1}(G_k)|,$$

para todo i, o que implica que $|P_i(G_k) : P_{i+1}(G_k)| = |G_k : P_2(G_k)|$. E portanto, $P_k(G) = G_k$ é uniforme para todo k suficientemente grande. ■

Corolário 2.3.3 *Um grupo pro-p de posto finito tem um subgrupo uniforme aberto característico.*

Demonstração: Seja G um grupo pro-p de posto finito, então pelo Teorema 2.2.20, G tem um subgrupo H aberto, powerful e característico. E como G tem posto finito, então H é finitamente gerado. Assim, H é um grupo pro-p, powerful finitamente gerado, então pelo Teorema 2.3.2, $P_k(H)$ é uniforme, para k suficientemente grande. E sendo $P_k(H)$ aberto em H, então tem índice finito em H, e como H tem índice finito em G, o índice de $P_k(H)$ em G também é finito, o que implica que $P_k(H)$ é aberto em

G. Agora veja que, $P_k(H)$ *char* G, para todo k, pois por hipótese, H *char* G. Portanto, para k suficientemente grande, $P_k(H)$ é um subgrupo uniforme aberto e característico de G. ■

O próximo resultado estabelece condições sobre um grupo pro-p finitamente gerado powerful para que ele possa ser um grupo uniforme.

Proposição 2.3.4 *Seja G um grupo pro-p finitamente gerado powerful. Então as seguintes afirmações são equivalentes:*

(a) *G é uniforme;*

(b) *$d(P_i(G)) = d(G)$, para todo $i \geq 1$;*

(c) *$d(H) = d(G)$, para todo H subgrupo aberto powerful de G.*

Demonstração: Escreva $G_i = P_i(G)$.

(a) ⇒ (b) Suponha G uniforme. Segue do item (iii)' da definição, que um grupo pro-p finitamente gerado powerful é uniforme se, e somente se, $d(G_i/G_{i+1}) = d(G_1/G_2)$, para todo i. E pelo Teorema 2.2.9, $G_{i+1} = \Phi(G_i)$, para todo $i \geq 1$,

$$d(G_i) = d(G_i/\Phi(G_i)) = d(G_i/G_{i+1}) = d(G_1/G_2) = d(G/\Phi(G)) = d(G),$$

uma vez que $\Phi(G)$ é o conjunto dos não geradores de G. Logo, $d(P_i(G)) = d(G)$, para todo $i \geq 1$.

(b) ⇒ (a) Suponha que $d(P_i(G)) = d(G)$, para todo $i \geq 1$. Por hipótese, temos que G é um grupo pro-p, powerful e finitamente gerado, então resta mostrar $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$. Como, $G_{i+1} = \Phi(G_i)$, para todo $i \geq 1$, é o conjunto dos não geradores de G_i, então

$$d(G_i/G_{i+1}) = d(G_i) = d(G) = d(G/\Phi(G)) = d(G/P_2(G)),$$

para todo i, logo $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$. E portanto, G é uniforme.

(c) ⇒ (b) Como G é um grupo pro-p finitamente gerado, então $P_i(G)$ é aberto em G. Além disso, $P_i(G)$ é powerful, então por hipótese $d(P_i(G)) = d(G)$.

(b) $\Rightarrow$ (c) Suponha que $d(P_i(G)) = d(G)$. E seja $H \leq_\circ G$ tal que H é powerful, então para algum i, $G_i \leq H$, assim $d(P_i(G)) = d(G_i) \leq d(H) \leq rk(G) = d(G)$, o que implica que $d(H) = d(G)$.

■

O próximo teorema é uma caracterização muito útil de grupos uniformes. Lembre que um grupo G é dito *livre de torção* se G não possui elementos de ordem finita.

Teorema 2.3.5 *Um grupo pro-p powerful finitamente gerado é uniforme se, e somente se, é livre de torção.*

Demonstração: Seja G um grupo pro-p powerful finitamente gerado e escreva $G_i = P_i(G)$, para cada i.

Suponha que G não é livre de torção. Então G contém um elemento de ordem finita. Veja que, um elemento de ordem finita em G coprima com p está em G_i, para todo i, consequentemente, é igual a 1. Sendo assim, G contém um elemento x de ordem p. Temos que $x \in G_i \setminus G_{i+1}$, para algum i, então $1 \neq xG_{i+1} \in G_i/G_{i+1}$. E considerando o epimorfismo $f_i : G_i/G_{i+1} \longrightarrow G_{i+1}/G_{i+2}$, temos que, $f_i(xG_{i+1}) = (xG_{i+1})^p = x^pG_{i+2} = G_{i+2}$, assim $f_i(xG_{i+1}) = 1$, o que implica que, $xG_{i+1} \in ker(f_i)$. Logo, f_i não é injetiva. E portanto, pelo item (iii)' da definição, G não é uniforme.

Por outro lado, suponha que G não é uniforme, e vamos mostrar que G não é livre de torção. A ideia é encontrar um elemento de ordem finita a partir da construção de uma sequência de Cauchy. Como G não é uniforme, então para algum i, o epimorfismo $f_i : G_i/G_{i+1} \longrightarrow G_{i+1}/G_{i+2}$ não é injetivo, então existe $x \in G_i \setminus G_{i+1}$ tal que $f_i(xG_{i+1}) = (xG_{i+1})^p = 1$, com $1 \neq xG_{i+1} \in G_i/G_{i+1}$, o que implica que, $x^p \in G_{i+2}$.

Escreva $x_2 = x$. Suponha que existe uma sequência de elementos $x_2, x_3, \ldots, x_n$ satisfazendo $x_j^p \in G_{i+j}$ e $x_j \equiv x_{j-1}\ (mod\, G_{i+j-2})$, para $2 < j \leq n$. Existe $z \in G_{i+n-1}$ tal que $z^p = x_n^p$, pois $x_n^p \in G_{i+n} = (G_{i+n-1})^p$. Agora escreva $x_{n+1} = z^{-1}x_n$. Então $x_{n+1} \equiv x_n\ (mod\, G_{i+n-1})$. Além disso, $x_{n+1}^p \in G_{i+n+1}$: Se p ímpar, temos que

$$x_{n+1}^p = (z^{-1}x_n)^p \equiv z^{-p}x_n^p[x_n, z^{-1}]^{p(p-1)/2} \equiv 1\ (mod\, G_{i+n+1}),$$

uma vez que, $[G_{i+n-1}, G, G][G_{i+n-1}, G]^p \leq G_{i+n+1}$. E se $p = 2$, temos que

$$x_{n+1}^p = z^{-2}[z^{-1}, x_n^{-1}]x_n^2 \equiv z^{-2}x_n^2 \equiv 1\ (mod\, G_{i+n+1}),$$

pois $[G_{i+n-1}, G] \leq G_{i+n-1}^4 = G_{i+n+1}$, já que, $G_{i+n-1}\, p.e.\, G$. Assim, a sequência $x_2, x_3, \ldots, x_n, \ldots$ pode ser construida recursivamente. Tal sequência é uma sequência de Cauchy e converge para um elemento $x_\infty \in G$, uma vez que $\{G_i \mid i \geq 1\}$ forma uma base para uma vizinhança da identidade em G. Então $x_\infty \equiv x \not\equiv 1 \ (mod\, G_{i+1})$ e $x_\infty^p \equiv x_n^p \equiv 1 \ (mod\, G_{i+n-1})$, para todo n, então $x_\infty^p = 1$. Logo, G não é livre de torção. ■

Nosso próximo passo é definir a dimensão de um grupo pro-p G de posto finito, mas para isso precisaremos do seguinte lema:

Lema 2.3.6 *Se A e B são subgrupos abertos uniformes de algum grupo pro-p, então $d(A) = d(B)$.*

Demonstração: Sejam G um grupo pro-p e, A e B subgrupos abertos uniformes de G. Sendo A e B abertos, então $A \cap B$ é um subgrupo aberto de B. Além disso, para i suficientemente grande, $P_i(A) \leq A \cap B \leq B$. Agora observe que, $P_i(A)$ é aberto em A e em B. E sendo $P_i(A)$ powerful e B uniforme, então pela Proposição 2.3.4, $d(P_i(A)) = d(B)$. Por outro lado, como A é uniforme então pela Proposição 2.3.4, $d(P_i(A)) = d(A)$. Portanto, $d(A) = d(B)$. ■

Definição 2.3.7 *Seja G um grupo pro-p de posto finito. A dimensão de G é*

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

onde H é um subgrupo uniforme aberto de G.

Lembrando que o Corolário 2.3.3 garante que sempre existe H subgrupo aberto uniforme de G. E pela Proposição 2.3.6, $dim(G)$ independe da escolha de H.

Teorema 2.3.8 *Seja G um grupo pro-p de posto finito e N um subgrupo normal fechado de G. Então*

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

Veja que, a afirmação do teorema faz sentindo pois N e G/N tem posto finito.

Demonstração: Primeiramente vamos mostrar que a afirmação é verdadeira para o caso particular em que G, N e G/N são uniformes e usaremos tal resultado para mostrar o caso geral.

Caso particular: Suponha que G, N e G/N são uniformes. Pelo Lema 2.2.5, $\Phi(G) = \{g^p \mid g \in G\}$ e $\Phi(N) = \{g^p \mid g \in N\}$. Agora observe que, $\Phi(N) = \Phi(G) \cap N$. De fato, por definição, $\Phi(N) \subseteq \Phi(G) \cap N$. Por outro lado, se $y \in \Phi(G) \cap N$, então $y \in \Phi(G)$ e daí, $y = g^p$, para algum $g \in G$, e $y = g^p \in N$, entã $g^pN = N$, o que implica que $(gN)^p = N = \overline{1}$. Mas, como G/N é uniforme, então G/N é livre de torção, logo não existe $x \in G\backslash N$ tal que $\circ(xN) < +\infty$. Sendo assim, $g \in N$. Logo $y \in \Phi(N)$, o que implica que $\Phi(G) \cap N \subseteq \Phi(N)$. E portanto, $\Phi(N) = \Phi(G) \cap N$.

Agora observe que, como G é um grupo pro-p finitamente gerado, então pela Proposição 1.5.7,

$$\Phi(G/N) = \Phi(G)N/N \cong N/\Phi(G) \cap N = N/\Phi(N).$$

Além disso, $G/\Phi(G)$, $N/\Phi(N)$ e $\frac{G/N}{\Phi(G/N)}$ são espaços vetoriais sobre $\mathbb{F}_p$, assim

$$dim_{\mathbb{F}_p}(\Phi(G/N)) + dim_{\mathbb{F}_p}\left(\frac{G/N}{\Phi(G/N)}\right) = dim_{\mathbb{F}_p}(G/\Phi(G)).$$

Logo,

$$d(G) = dim_{\mathbb{F}_p}(G/\Phi(G)) = dim_{\mathbb{F}_p}(\Phi(G/N)) + dim_{\mathbb{F}_p}\left(\frac{G/N}{\Phi(G/N)}\right) = d(N) + d(G/N).$$

E portanto, $d(G) = d(N) + d(G/N)$.

Caso geral: De acordo com o caso particular é suficiente encontrar um subgrupo aberto uniforme H em G tal que $H \cap N$ e $H/H \cap N$ também são uniformes, pois nessas condições teremos, $dim(G) = d(H)$, $dim(N) = d(H \cap N)$ e $dim(G/N) = d(H/H \cap N)$, uma vez que, $H/H \cap N \cong HN/N$. E como $d(H) = d(H \cap N) + d(H/H \cap N)$, então $dim(G) = dim(N) + dim(G/N)$.

Considere $rk(G) = r$ e $G_0 = V(G, r)$, se p é ímpar, e $G_0 = V(G, r)^2$, se $p = 2$, onde $V(G, r)$ é a interseção dos núcleos de todos os homomorfismos de G em $GL_r(\mathbb{F}_p)$. Pela Proposição 2.2.16, todo subgrupo normal aberto G contido em G_0 é powerful. (I)

E sendo G_0 um grupo pro-p powerful, finitamente gerado, então pelo Teorema 2.3.2, $P_k(G_0) = G_1$ é uniforme, para todo k suficientemente grande. Logo, pelo

Teorema 2.3.5, G_1 é livre de torção, daí, todo subgrupo normal aberto de G_1 também é livre de torção. Mas note que, todo subgrupo normal aberto de G_1 é também um subgrupo normal aberto de G_0, pois $G_1\, char\, G_0$, então por (I), todo subgrupo normal aberto de G contido em G_1 é powerful. E sendo G um grupo pro-p, finitamente gerado, então todo subgrupo normal aberto de G contido em G_1 é um grupo pro-p, finitamente gerado. Assim, todo subgrupo normal aberto de G contido em G_1 é um grupo pro-p, finitamente gerado, powerful e livre de torção, logo, pelo Teorema 2.3.5, é uniforme. (II)

Similarmente, como N tem posto finito, então N tem um subgrupo aberto característico N_1 tal que todo subgrupo normal aberto de N contido em N_1 é uniforme.

E finalmente, pelo mesmo argumento, como $G_1/G_1 \cap N_1$ tem posto finito, então tem um subgrupo normal aberto uniforme $H/G_1 \cap N_1$. Assim, $H/G_1 \cap N_1$ é livre de torção e $N/G_1 \cap N_1$ é finito, pois $G_1 \cap N_1$ é aberto, então $H \cap N = G_1 \cap N_1$. Logo, $H/H \cap N$ é uniforme e como $H \cap N = G_1 \cap N_1 \lhd_\circ N_1$, então $H \cap N$ também é uniforme.

E sendo $H \lhd_\circ G_1$, então por (II), H é uniforme. Assim, $dim(G) = d(H)$, $dim(N) = d(H \cap N)$ e $dim(G/N) = d(H/H \cap N)$. Portanto, $dim(G) = dim(N) + dim(G/N)$.

■

De agora em diante, denote G um grupo pro-p uniforme, com $d(G) = d$. E para cada n denote $G_n = P_n(G)$.

O próximo resultado estabelece um homeomorfismo entre $\mathbb{Z}_p^d$ e G.

Teorema 2.3.9 *Seja G um grupo pro-p uniforme e $\{a_1, a_2, \ldots, a_d\}$ um conjunto de geradores topológicos para G, onde $d = d(G)$. Então a aplicação*

$$(\lambda_1, \ldots, \lambda_d) \longmapsto a_1^{\lambda_1} \ldots a_d^{\lambda_d}$$

de $\mathbb{Z}_p^d$ em G é um homeomorfismo.

Demonstração: Como o conjunto $\{a_1, a_2, \ldots, a_d\}$ gera G topologicamente, então pela Proposição 2.2.11, $G = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$. Segue que, pela Proposição 2.2.23 cada

elemento $a \in G$ pode ser expresso da forma

$$a = a_1^{\lambda_1} \dots a_d^{\lambda_d}$$

com $\lambda_1, \dots, \lambda_d \in \mathbb{Z}_p$.

Considere a aplicação $\theta : G \longrightarrow \mathbb{Z}_p^d$ definida por

$$a_1^{\lambda_1} \dots a_d^{\lambda_d} \longmapsto (\lambda_1, \dots, \lambda_d).$$

Agora fixe um inteiro k, e considere o p-grupo finito G/G_{k+1}. Como G é uniforme, então $|G_k : G_{k+1}| = |G : G_2| = p^d$, para todo k. Assim,

$$|G/G_{k+1}| = |G : G_{k+1}| = |G : G_2||G_2 : G_3| \dots |G_k : G_{k+1}| = p^{kd}.$$

E sendo G/G_{k+1} um p-grupo powerful, então $G/G_{k+1} = \langle a_1 G_{k+1} \rangle \dots \langle a_d G_{k+1} \rangle$. E como $G_{k+1} = \{g^{p^k} \mid g \in G\}$, então para cada i, $|\langle a_i G_{k+1} \rangle| \leq p^k$. Mas $|G/G_{k+1}| = p^{kd}$, então $|\langle a_i G_{k+1} \rangle| = p^k$. Consequentemente, cada elemento de G/G_{k+1} pode ser expresso na forma $a_1^{e_1} \dots a_d^{e_d} G_{k+1}$, onde os inteiros $e_1, \dots, e_d$ são unicamente determinados módulo p^k, isso implica que, na expressão $a = a_1^{\lambda_1} \dots a_d^{\lambda_d}$, os inteiros p-ádicos $\lambda_1, \dots, \lambda_d$ são unicamente determinados módulo p^k. E como isso vale para todo k, segue que, $\lambda_1, \dots, \lambda_d$ são inteiros p-ádicos unicamente determinados. Portanto, θ está bem definida e é uma bijeção.

Seja $\psi : \mathbb{Z}_p^d \longrightarrow G$ definida por $((\lambda_1, \dots, \lambda_d))\psi = a_1^{\lambda_1} \dots a_d^{\lambda_d}$ a inversa bijetiva de θ. Veja que, ψ é a composição das aplicações $\alpha : \mathbb{Z}_p^d \longrightarrow G \times G \times \dots \times G$ e $\beta : G \times G \times \dots \times G \longrightarrow G$ dadas por $((\lambda_1, \dots, \lambda_d))\alpha = (\phi_{a_1}(\lambda_1), \dots, \phi_{a_d}(\lambda_d))$ e $(g_1, \dots, g_d)\beta = g_1 \dots g_d$, onde a aplicação $\phi_g : \mathbb{Z}_p \longrightarrow G$ é definida da seguinte maneira $\lambda \longmapsto g^\lambda$. Pelo Corolário 2.1.6, cada ϕ_{a_i} é contínua, então α também é contínua. E como a multiplicação em G é contínua, então β é contínua e, portanto, ψ é contínua. E sendo, G e $\mathbb{Z}_p$ espaços Hausdorff e compactos, então pelo Lema 1.1.8 ψ é um homeomorfismo. ■

O homeomorfismo definido no teorema acima tem muitas propriedades analíticas, entretanto, suas propriedades algébricas não são particularmente boas, sendo assim, definiremos em G duas novas operações de modo a obter todas as propriedades que

procuramos. A primeira operação a ser definida cria uma estrutura aditiva em G, com o objetivo de torná-lo um $\mathbb{Z}_p$-módulo livre. Mas esse procedimento envolve "esquecer" muitas informações sobre a estrutura de G, já que todos $\mathbb{Z}_p$-módulos livres de um dado posto são isomorfos. Então com o objetivo de salvar mais informações definiremos em G uma segunda operação, que tornará o $\mathbb{Z}_p$-módulo livre em uma álgebra de Lie sobre $\mathbb{Z}_p$.

Relembrando que, uma *álgebra de Lie* sobre uma anel comutativo K é um K-módulo L com uma operação binária (comumente chamada de colchete de Lie)

$$[\cdot,\cdot] : L \times L \longrightarrow L$$

que é K-bilinear e satisfaz as seguintes propriedades:
(i) $[a, a] = 0$,
(ii) $[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$,
para todo $a, b, c \in L$.

A identidade (ii) é chamada *identiade de Jacobi*. E veja que, de (i) temos que, $[a, b] = -[b, a]$, para todo a, $b \in L$. De fato,

$$0 = [a + b, a + b] = [a, a] + [a, b] + [b, a] + [b, b] = [a, b] + [b, a],$$

o que significa que o colchete de Lie é uma aplicação K-bilinear antissimétrica.

Um anel não associativo sem unidade, cuja multiplicação é denotada pelo colchete de Lie e que satisfaz as condições (i) e (ii) é chamado *anel de Lie*. Assim, se um anel de Lie é também um K-módulo, onde a multiplicação por qualquer elemento de K é um homomorfismo de L, então L é uma K-álgebra de Lie.

Se R é um anel e K é um subanel de R, então o R-módulo $L \otimes_K R$ (fazendo as extensões de escalares de K para R) pode ser considerado de maneira natural uma R-álgebra de Lie com a multiplicação (colchete) de Lie dada por

$$[l_1 \otimes r_1, l_2 \otimes r_2] = [l_1, l_2] \otimes r_1 r_2,$$

com l_1, $l_2 \in L$ e r_1, $r_2 \in R$. E veja que, como uma K-álgebra de Lie, L pode ser isomorficamente imerso em $L \otimes_K R$ pela aplicação $l \longmapsto l \otimes 1$, uma leitura detalhada sobre esse assunto pode ser feita em [5], capítulo 1.

E um resultado relevante que vale a pena mencionar é o seguinte: Se os elementos $a_1, a_2, \ldots, a_s$ geram um K-módulo A e os elementos $b_1, b_2, \ldots, b_t$ geram um K-módulo B, então os st elementos $a_i \otimes b_j$ geram o K-módulo $A \otimes_K B$.

O lema a seguir mostra que cada elemento $x \in G_{n+1}$ tem uma única p^n-ésima raiz em G, que denotaremos por $x^{p^{-n}}$.

Lema 2.3.10 *Seja $n \in \mathbb{N}$. A aplicação $x \longmapsto x^{p^n}$ é um homeomorfismo de G em G_{n+1}. Para cada k e m, ele restringe a uma bijeção $G_k \longrightarrow G_{k+n}$ e induz uma bijeção $G_k/G_{k+m} \longrightarrow G_{n+k}/G_{n+k+m}$.*

Demonstração: Escreva $f(x) = x^{p^n}$. Pelo Teorema 2.2.9, temos que $G_{n+k} = G_k^{p^n}$, assim, $f(G_k) = G_{n+k}$ e $f(G_{k+m}) = G_{n+k+m}$. Segue que, se $x \equiv y \ (mod\, G_{k+m})$, então $f(x) \equiv f(y) \ (mod\, G_{n+k+m})$. De fato, se $x \equiv y \ (mod\, G_{k+m})$, então $x = ya$, onde $a \in G_{k+m}$, e como f está bem definida então $f(x) = f(ya) = f(y)f(a)$, onde $f(a) \in f(G_{k+m}) = G_{n+k+m}$, logo, $f(x) \equiv f(y) \ (mod\, G_{n+k+m})$. Tal afirmação implica que a aplicação $G_k/G_{k+m} \longrightarrow G_{n+k}/G_{n+k+m}$ está bem definida. Assim, f induz uma aplicação sobrejetiva de G_k/G_{k+m} em G_{n+k}/G_{n+k+m}.

Como G é uniforme, $p^d = |G : G_2| = |G_i : G_{i+1}|$, para todo i. Assim,

$$|G_k : G_{k+m}| = |G_k : G_{k+1}||G_{k+1} : G_{k+2}| \ldots |G_{k+(m-1)} : G_{k+m}| = p^{d(m-1)}$$

e

$$|G_{n+k} : G_{n+k+m}| = |G_{n+k} : G_{n+k+1}| \ldots |G_{n+k+(m-1)} : G_{n+k+m}| = p^{d(m-1)}.$$

Logo, $|G_k : G_{k+m}| = |G_{n+k} : G_{n+k+m}|$ e, consequentemente, a aplicação sobrejetiva de G_k/G_{k+m} em G_{n+k}/G_{n+k+m} é uma bijeção. Veja que, se $x, y \in G_k$ e $f(x) = f(y)$ então $x \equiv y \ (mod\, G_{k+m})$, para todo m. De fato, suponha que $x \not\equiv y \ (mod\, G_{k+m})$, para algum m, então $f(x) \not\equiv f(y) \ (mod\, G_{n+k+m})$, mas $f(x) = f(y)$ e $1 \in G_{n+k+m}$, logo $f(x) = f(y)1$, o que é uma contradição e, portanto, $x \equiv y \ (mod\, G_{k+m})$, para todo m. E como $\bigcap_m G_{k+m} = 1$, então $x = y$, o que implica que, $f|_{G_k}$ é injetiva.

E para finalizar, temos que, pelo Corolário 2.1.6, f é contínua, então $f|_{G_k}$ é uma bijeção e como, tanto o domínio quanto o contradomínio são espaços Hausdorff e compactos, segue do Lema 1.1.8 que $f|_{G_k}$ é um homeomorfismo de G_k em G_{k+n}. E observe que, a primeira afirmação é caso em que $k = 1$. ■

Podemos usar a bijeção entre G e G_{n+1} para transferir a operação do grupo G_{n+1} para G, definindo assim uma nova estrutura de grupo em G. Para $x, y \in G$ defina

$$x +_n y = (x^{p^n} y^{p^n})^{p^{-n}}.$$

Assim, a aplicação $x \longmapsto x^{p^{-n}}$ se torna um isomorfismo de G_{n+1} para o grupo $(G, +_n)$.

Lema 2.3.11 *Se $n > 1$, $x, y \in G$ e $u, v \in G_n$, então*

$$xu +_n yv \equiv x +_n y \equiv x +_{n-1} y \pmod{G_n},$$

e para todo $m > n$,

$$x +_m y \equiv x +_n y \pmod{G_{n+1}}.$$

Demonstração: Seja $x, y \in G$, então pelo Teorema 2.2.9, $x^{p^{n-1}}, y^{p^{n-1}} \in G_n$. E pela Proposição 2.1.4, $[G_n, G_n] \leq G_{2n}$. Assim, $[y^{p^{n-1}}, x^{p^{n-1}}] \in [G_n, G_n] \leq G_{2n}$, o que implica que, $[y^{p^{n-1}}, x^{p^{n-1}}]^{p(p-1)/2} \in [G_n, G_n] \leq G_{2n}$. Por outro lado,

$$(x^{p^{n-1}} y^{p^{n-1}})^p \equiv (x^{p^{n-1}})^p (y^{p^{n-1}})^p [y^{p^{n-1}}, x^{p^{n-1}}]^{p(p-1)/2} \pmod{\gamma_3(G_n)},$$

onde $\gamma_3(G_n) = [[G_n, G_n], G_n] \leq [G_{2n}, G_n] \leq G_{2n}$. Logo,

$$(x^{p^{n-1}} y^{p^{n-1}})^p \equiv x^{p^n} y^{p^n} \pmod{G_{2n}}.$$

Mas observe que, $x +_{(n-1)} y = (x^{p^{n-1}} y^{p^{n-1}})^{p^{-(n-1)}}$, o que implica que $(x +_{(n-1)} y)^{p^n} = [(x^{p^{n-1}} y^{p^{n-1}})^{p^{-(n-1)}}]^{p^n} = (x^{p^{n-1}} y^{p^{n-1}})^p$. Assim,

$$x^{p^n} y^{p^n} \equiv (x +_{(n-1)} y)^{p^n} \pmod{G_{2n}}.$$

Agora considere $k = 1$ e $m = n - 1$ no Lema 2.3.10, então temos que o homeomorfismo $x \longmapsto x^{p^n}$ de G em G_{n+1} induz a seguinte bijeção

$$\begin{array}{ccc} G/G_n & \longrightarrow & G_{n+1}/G_{2n} \\ xG_n & \longmapsto & x^{p^n} G_{2n}. \end{array} \tag{2.1}$$

E como $x^{p^n} y^{p^n} \equiv (x +_{(n-1)} y)^{p^n} \pmod{G_{2n}}$, então extraindo a p^n-ésima raiz obtemos que

$$x +_n y = (x^{p^n} y^{p^n})^{p^{-n}} \equiv x +_{(n-1)} y \pmod{G_n}.$$

E como $(xu)^{p^n} \equiv x^{p^n} \ (mod\, G_{2n})$ e $(yv)^{p^n} \equiv y^{p^n} \ (mod\, G_{2n})$, então novamente pelo Lema 2.3.10, o mesmo argumento nos dar que

$$xu +_n yv \equiv x +_n y \ (mod\, G_n),$$

uma vez que, $xu +_n yv = ((xu)^{p^n}(yv)^{p^n})^{p-n}$ e $x +_n y = (x^{p^n}y^{p^n})^{p^n}$. Logo,

$$xu +_n yv \equiv x +_n y \equiv x +_{n-1} y \ \ (mod\, G_n).$$

Resta verificar a última afirmação. A mesma segue por indução sobre $m - n$, onde $m > n$.

Suponha que $m - n = 1$, então $n = m - 1$ e, pelo caso anterior $x +_m y \equiv x +_{m-1} y \ \ (mod\, G_m)$, o que implica que, $x +_m y \equiv x +_n y \ \ (mod\, G_{n+1})$.

Suponha que a afirmação é verdadeira para $m - n = r$, ou seja, $x +_m y \equiv x +_{m-r} y \ \ (mod\, G_{n+1})$. E mostraremos que é verdade para $m - n = r + 1$. Pelo caso anterior, $x +_{m-r} y \equiv x +_{(m-r)-1} y \ \ (mod\, G_{m-r})$, e por hipótese de indução $x +_m y \equiv x +_{m-r} y \ \ (mod\, G_{n+1})$. Logo,

$$x +_m y \equiv x +_n y \ \ (mod\, G_{n+1}),$$

para todo $m > n$. ■

Assim, para um dado par (x, y), a sequência $(x +_n y)$ é uma sequência de Cauchy, e podemos fazer a seguinte definição:

Definição 2.3.12 *Para $x, y \in G$, defina*

$$x + y = \lim_{n \longrightarrow \infty} x +_n y.$$

Pelo Lema 2.3.11, temos que

$$x + y \equiv x +_n y \ \ (mod\, G_{n+1})$$

e que, se $u, v \in G_n$, então

$$xu + yv \equiv x + y \ \ (mod\, G_n).$$

Proposição 2.3.13 *O conjunto G com a operação $+$ definida acima é um grupo abeliano, com elemento identidade 1 e a inversão dada por $x \longmapsto x^{-1}$.*

Demonstração: Para cada n, $x +_n 1 = (x^{p^n}1^{p^n})^{p^{-n}} = x$ e $x +_n x^{-1} = 1$. Consequentemente, $x + 1 = x$ e $x + x^{-1} = 1$.

Para verificar a associatividade, considere x, y, $z \in G$ e $n > 1$. Pela definição anterior $x + y \equiv x +_n y \pmod{G_{n+1}}$, então $x + y = (x +_n y)u$, para algum $u \in G_{n+1}$, daí

$$\begin{aligned}(x + y) + z &\equiv (x +_n y) + z \pmod{G_{n+1}} \\ &\equiv (x +_n y) +_n z \pmod{G_{n+1}}.\end{aligned}$$

Similarmente, $x+(y+z) \equiv x+_n(y+_n z) \pmod{G_{n+1}}$. Como a operação $+_n$ é associativa, segue que,

$$(x + y) + z \equiv x + (y + z) \pmod{G_{n+1}}.$$

E como tomamos n arbitrário, a associatividade segue. Resta verificar que $+$ é comutativa. Veja que, $[x^{p^n}, y^{p^n}] \in [G_{n+1}, G_{n+1}] \leq G_{2n+2}$, então $x^{p^n}y^{p^n} \equiv y^{p^n}x^{p^n} \pmod{G_{2n+2}}$. Extraindo a p^n-ésima raiz e usando o Lema 2.3.10 obtemos que $x +_n y \equiv y +_n x \pmod{G_{n+2}}$. Assim, $x + y \equiv y + x \pmod{G_{n+1}}$, e como isso vale para cada n, o resultado segue. ■

De agora em diante, usaremos a notação 'aditiva' para as operações do grupo em $(G, +)$, sendo assim, escreveremos 0 para representar a identidade, $-x$ para representar o elemento inverso, $x - y$ para representar $x + (-y)$ e mx para representar $x + \ldots + x$ (m vezes) se m for positivo, ou mx para representar $|m| \cdot (-x)$ se m for negativo.

Nosso próximo passo é tornar claro a estrutura desse grupo aditivo.

Lema 2.3.14 **(i)** *Se $xy = yx$ então $x + y = xy$.*

(ii) *Para cada inteiro m, $mx = x^m$.*

(iii) *Para cada $n \geq 1$, $p^{n-1}G = G^n$.*

(iv) *Se x, $y \in G_n$, então $x + y \equiv xy \pmod{G_{n+1}}$.*

Demonstração:

(i) Suponha que $xy = yx$. Por definição

$$\begin{aligned} x+y &= \lim_{n\longrightarrow\infty} x +_n y = \lim_{n\longrightarrow\infty}(x^{p^n}y^{p^n})^{p^{-n}} = \lim_{n\longrightarrow\infty}(\underbrace{xx\ldots x}_{p^n\ vezes}\underbrace{yy\ldots y}_{p^n\ vezes})^{p^{-n}} \\ &= \lim_{n\longrightarrow\infty}(\underbrace{(xy)(xy)\ldots(xy)}_{p^n\ vezes})^{p^{-n}} = \lim_{n\longrightarrow\infty}((xy)^{p^n})^{p^{-n}} = \lim_{n\longrightarrow\infty} xy = xy. \end{aligned}$$

Logo, $x + y = xy$.

(ii) Suponha m positivo. Vamos mostrar por indução sobre m que $mx = x^m$. Se $m = 1$ o resultado é imediato. Suponha que a afirmação é verdadeira para m, ou seja, $mx = x^m$. Mostraremos que é verdade para $m + 1$. Temos que,

$$(m+1)x = \underbrace{x + x + \ldots x}_{m+1\,vezes} = x^m + x.$$

E como $x^m x = xx^m$, então pelo item anterior $x^m + x = x^m x = x^{m+1}$, logo, $(m + 1)x = x^{m+1}$. E portanto, $mx = x^m$, para todo m inteiro positivo.

Agora suponha que m é um inteiro negativo. Temos que, $mx = |m|(-x) = |m|x^{-1}$. E sendo $|m| > 0$, então pelo caso anterior $|m|x^{-1} = x^{-|m|} = x^m$.

(iii) Pelo Corolário 2.2.9, $G_n = G^{p^{n-1}} = \{x^{p^{n-1}} \mid x \in G\}$. Sendo assim, mostraremos que $p^{n-1}G = G^{p^{n-1}}$. Seja $g \in G^{p^{n-1}}$, então existe $y \in G$ tal que $g = y^{p^{n-1}}$. Mas pelo item anterior, $y^{p^{n-1}} = p^{n-1}y \in p^{n-1}G$. Logo, $G^{p^{n-1}} \subseteq p^{n-1}G$.

Agora tome $x \in p^{n-1}G$, então existe $y \in G$ tal que $x = p^{n-1}y = y^{p^{n-1}} \in G^{p^{n-1}}$. Logo, $p^{n-1}G \subseteq G^{p^{n-1}}$. E portanto, $p^{n-1}G = G^{p^{n-1}} = G_n$.

(iv) Sabemos que, a aplicação $x \longmapsto x^{p^n}$ induz um homomorfismo de G_n/G_{n+1} em G_{2n}/G_{2n+1}. Assim, para $x, y \in G_n$ temos $xG_{n+1} \longmapsto x^{p^n}G_{2n+1}$ e $yG_{n+1} \longmapsto y^{p^n}G_{2n+1}$, e como tal aplicação é bem definida e $xG_{n+1}yG_{n+1} = (xy)G_{n+1}$ então $x^{p^n}G_{2n+1}y^{p^n}G_{2n+1} = (xy)^{p^n}G_{2n+1}$, o que implica que $x^{p^n}y^{p^n}G_{2n+1} = (xy)^{p^n}G_{2n+1}$. Logo, $(xy)^{p^n} \equiv x^{p^n}y^{p^n}\ (mod\, G_{2n+1})$. Segue que, extraindo a p^n-ésima raiz e usando o Lema 2.3.10, temos que, $xy \equiv x +_n y\ (mod\, G_{n+1})$. E por definição $x + y \equiv x +_n y\ (mod\, G_{n+1})$, portanto $x + y \equiv xy\ (mod\, G_{n+1})$.

■

O próximo resultado garante que o conjunto quociente G/G_n é o mesmo, quer consideremos o grupo aditivo $(G, +)$ ou o grupo multiplicativo G. Sendo assim a notação G/G_n não é ambígua.

Corolário 2.3.15 *Para cada n, G_n é um subgrupo aditivo de G, as classes laterais aditivas de G_n em G são as mesmas que as classes laterais multiplicativas de G_n em G. Além disso, a aplicação identidade $G_n/G_{n+1} \longrightarrow G_n/G_{n+1}$ é um isomorfismo do grupo aditivo G_n/G_{n+1} no grupo multiplicativo G_n/G_{n+1}, e o índice de G_n no grupo aditivo $(G, +)$ é igual a $|G : G_n|$.*

Demonstração: Segue do Lema 2.3.14 item (iii) que $G_n = p^{n-1}G$ é um subgrupo aditivo de $(G, +)$. Agora mostraremos que as classes laterais aditivas de G_n em G são as mesmas que as classes laterais multiplicativas de G_n em G.

Seja $a \in G$ e $u \in G_n$, segue da Definição 2.3.12 que

$$a + u = a + 1 \cdot u \equiv a + 1 = a \ (mod\, G_n),$$

o que implica que $a + u \in aG_n$. Logo, $a + G_n \subseteq aG_n$. Por outro lado, tome $au \in aG_n$. Então $au - a = au + (-a) \equiv a + (-a) = 0 \ (mod\, G_n)$, o que implica que, $au - a \in G_n$, logo, $au \in a + G_n$, e portanto, $aG_n \subseteq a + G_n$. Assim, $aG_n = a + G_n$. Em particular, o índice $|G : G_n|$ é o mesmo quando calculado em qualquer grupo. E a última afirmação segue do Lema 2.3.14, item (iv) que a restrição da aplicação identidade de G_n/G_{n+1} em G_n/G_{n+1} é um isomorfismo entre a estrutura aditiva e a estrutura multiplicativa.

■

Lembre que desde o Teorema 2.3.9 fixamos G como um grupo pro-p uniforme com $d(G) = d$.

Proposição 2.3.16 *Com a topologia original de G, $(G, +)$ é um grupo pro-p uniforme de dimensão $d = d(G)$. Além disso, qualquer conjunto de geradores topológicos para G é um conjunto de geradores topológicos para $(G, +)$.*

Demonstração: Temos que G é um espaço Hausdorff e compacto. Além disso, sabemos que a aplicação $x \longmapsto -x = x^{-1}$ é contínua. E segue da Definição 2.3.12 que a aplicação $(x, y) \longmapsto x + y$, de $G \times G$ em G é contínua. Daí a aplicação $(x, y) \longmapsto x + y^{-1} = x + (-y)$ é contínua. Logo, $(G, +)$ é um grupo topológico. Vimos que, a

família $\{G_n\}_{n\in\mathbb{N}}$ é uma base para a vizinhança de $0 = 1$ em G. E como cada G_n é um subgrupo de índice potência de p no grupo aditivo $(G, +)$, pelo Corolário 2.3.15, segue que, $(G, +)$ é um grupo pro-p.

Como $(G, +)$ é um grupo abeliano, então $(G, +)$ é powerful. E pelo mesmo motivo, os subgrupos $p^{n-1}G = G_n$ são exatamente os termos da lower p-series de $(G, +)$. E como G é uniforme com a estrutura multiplicativa, então $|G_n : G_{n+1}| = |G : G_2| = p^d$, para todo n, e sendo as classes laterais aditivas de G_n em G iguais às classes laterais multiplicativas de G_n em G então $(G, +)$ é uniforme de dimensão d.

Resta provar que, qualquer conjunto de geradores topológicos para G é um conjunto de geradores topológicos para $(G, +)$. Suponha que X é um conjunto de geradores topológicos para G. Então $G/G_2 = \langle X\rangle G_2/G_2$, como um grupo multiplicativo. Mas pelo Lema 2.3.14, item (iv), o grupo aditivo G/G_2 é idêntico ao grupo multiplicativo, então $(G, +)/G_2 = \langle X\rangle_+ + G_2/G_2$, onde $\langle X\rangle_+$ denota o subgrupo aditivo gerado por X. E como $\Phi(G) = G_2 = pG$ é o conjunto dos não geradores de $(G, +)$, então X é um conjuto de geradores topológicos para $(G, +)$. ■

Como $(G, +)$ é um grupo pro-p, ele admite uma ação natural de $\mathbb{Z}_p$. E como $(G, +)$ é abeliano, pela Proposição 1.4.11 isso faz com que ele seja um $\mathbb{Z}_p$-módulo. Logo, estamos prontos para mostrar o resultado que dá a estrutura desse módulo.

Teorema 2.3.17 *Seja G um grupo pro-p uniforme de dimensão d e $\{a_1, \ldots, a_d\}$ um conjunto de geradores topológicos para G. Então, com a operação definida acima, $(G, +)$ é um $\mathbb{Z}_p$-módulo livre na base $\{a_1, \ldots, a_d\}$.*

Demonstração: Pela Proposição 2.3.16, o conjunto $\{a_1, \ldots, a_d\}$ gera topologicamente o grupo pro-p uniforme $(G, +)$ e $d(G) = d$. Sendo assim, $(G, +)$ satisfaz as hipóteses do Teorema 2.3.9, na notação aditiva. Então pelo Teorema 2.3.9, cada elemento de $(G, +)$ tem uma única expressão na forma $a = \lambda_1 a_1 + \ldots + \lambda_d a_d$, com $\lambda_1, \ldots \lambda_d \in \mathbb{Z}_p$. Note que para cada $x \in G$ e $\lambda \in \mathbb{Z}_p$, temos que $x^\lambda = \lambda x$, como segue do Lema 2.3.14, item (ii), ao tomar limites. Mas esta é exatamente a afirmação do teorema. ■

Como já foi dito, o procedimento de tornar G um $\mathbb{Z}_p$-módulo livre envolve "esquecer" muitas informações sobre a estrutura de G. Então com o objetivo de salvar

mais informações definiremos em G uma segunda operação, que tornará o $\mathbb{Z}_p$-módulo livre em uma álgebra de Lie sobre $\mathbb{Z}_p$, mas para isso precisamos da definição e do lema a seguir:

Definição 2.3.18 *Para $x, y \in G$ e $n \in \mathbb{N}$, defina*

$$(x, y)_n = [x^{p^n}, y^{p^n}]^{p^{-2n}}.$$

Veja que essa definição faz sentido, pois $[x^{p^n}, y^{p^n}] \in [G_{n+1}, G_{n+1}] \leq G_{2n+2}$.

Lema 2.3.19 *Se $n > 1$, $x, y \in G$ e $u, v \in G_n$, então*

$$(xu, yv)_n \equiv (x, y)_n \equiv (x, y)_{n-1} \pmod{G_{n+1}},$$

e para todo $m > n$

$$(x, y)_m \equiv (x, y)_n \pmod{G_{n+2}}.$$

Demonstração: Observando que, $[G_{2n}, G_{n+1}] \leq G_{3n+1}$ e usando o Lema 2.3.10 vemos, assim como na prova do Lema 2.3.11, que

$$(xu, yv)_n = (x, y)_n \pmod{G_{n+1}}.$$

Agora, se $a \in G_i$ e $b \in G_j$, então $[a^p, b] \equiv [a, b]^p \pmod{G_{2i+j}}$ e $[a, b^p] \equiv [a, b]^p \pmod{G_{i+2j}}$. Segue que, tomando $a = x^{p^n}$ e $b = y^{p^{n-1}}$, temos que

$$[x^{p^n}, y^{p^n}] \equiv [x^{p^n}, y^{p^{n-1}}]^p \pmod{G_{3n+1}}.$$

E tomando $a = x^{p^{n-1}}$ e $b = y^{p^{n-1}}$, temos que

$$[x^{p^n}, y^{p^{n-1}}] \equiv [x^{p^{n-1}}, y^{p^{n-1}}]^p \pmod{G_{3n}}.$$

Portanto,

$$\begin{aligned} [x^{p^n}, y^{p^n}] &\equiv [x^{p^{n-1}}, y^{p^{n-1}}]^{p^2} \pmod{G_{3n+1}} \\ &= (x, y)_{n-1}^{p^{2n}}. \end{aligned}$$

Extraindo a p^{2n}-ésima raiz e usando novamente o Lema 2.3.10, obtemos

$$(x, y)_n \equiv (x, y)_{n-1} \pmod{G_{n+1}}.$$

E veja que a última afirmação segue por indução sobre $m - n$, a idéia é a mesma da demonstração da última afirmação do Lema 2.3.10. ■

Assim, dado $x, y \in G$, $((x, y)_n)$ é uma sequência de Cauchy, e podemos fazer a seguinte definição:

Definição 2.3.20 *Dado $x, y \in G$*

$$(x, y) = \lim_{n \longrightarrow \infty} (x, y)_n.$$

Teorema 2.3.21 *Com a operação $(\ ,\ )$, o $\mathbb{Z}_p$-módulo $(G, +)$ torna-se uma álgebra de Lie sobre $\mathbb{Z}_p$.*

A prova desse teorema segue no mesmo espírito da prova da Proposição 2.3.13 e está delineada em [2, Exercise 4.4].

O próximo resultado nos diz como subgrupos e quocientes adequados de G correspondem a subalgebras e quocientes da $\mathbb{Z}_p$-álgebra de Lie $(G, +, (\ ,\ ))$.

Proposição 2.3.22 *Seja H um subgrupo fechado uniforme de G, e N um subgrupo normal fechado de G tal que G/N é uniforme. Então*

(i) *A aplicação inclusão de H em G é um monomorfismo de álgebras de Lie de $(H, +, (\ ,\ ))$ em $(G, +, (\ ,\ ))$. Em particular, H é uma subalgebra da álgebra de Lie G;*

(ii) *N é uniforme;*

(iii) *N é um ideal na $\mathbb{Z}_p$-álgebra de Lie $(G, +, (\ ,\ ))$. E as classes laterais aditivas de N em G são as mesmas que as classes laterais multiplicativas, então $(G/N, +, (\ ,\ )) = (G, +, (\ ,\ ))/(N, +, (\ ,\ ))$. Além disso, o epimorfismo natural $* : G \longrightarrow G/N$ é um epimorfismo de $\mathbb{Z}_p$-álgebras de Lie de $(G, +, (\ ,\ ))$ em $(G/N, +, (\ ,\ ))$.*

Demonstração:

(i) Segue da definição, uma vez que a topologia em H é a topologia do subespaço induzida de G.

(ii) Se $x \in G$ e $x^{p^n} \in N$, então $x \in N$, uma vez que, sendo G/N uniforme então pelo Teorema 2.3.5, G/N é livre de torção. Como G^p consiste das p-ésimas potências,

então $G^p \cap N = N^p$, o que implica que N/N^p é abeliano, logo, se p é ímpar, N é powerful. Dessa forma, N é um grupo pro-p, finitamente gerado, powerful e livre de torção, então pelo Teorema 2.3.5, N é uniforme. Se $p = 2$ considere N/N^4 e o mesmo argumento se aplica, concluindo assim que N é uniforme.

(iii) Seja $a, b \in G$ e escreva $c_n = a +_n b$. Então $(c_n^*)^{p^n} = a^{*p^n} b^{*p^n}$, daí temos que $a^* +_n b^* = c_n^*$ em G/N. Segue por continuidade que

$$a^* + b^* = \lim_{n \longrightarrow \infty} c_n^* = (\lim_{n \longrightarrow \infty} c_n)^* = (a+b)^*.$$

E com argumento similar, podemos mostrar que $*$ respeita a operação comutador, ou seja, $(x,y)_n^* = ([x^{p^n}, y^{p^n}]^{p^{-2n}})^* = [x^{*p^n}, y^{*p^n}]$. E respeita também a operação de $\mathbb{Z}_p$. Assim, $*$ é um homomorfismo de álgebras de Lie como queríamos. E como N é o núcleo de $*$, então N é um ideal em $(G, +, (\ ,\ ))$.

Agora, observe que, para $a, b \in G$, temos que,

$$a + N = b + N \Leftrightarrow a - b \in N \Leftrightarrow (a-b)^* = 0 \Leftrightarrow a^* = b^* \Leftrightarrow aN = bN.$$

Logo, $(G, +)/(N, +) = G/N$, o que completa a prova da proposição.

■

Já o resultado a seguir estabelece a correspondência inversa.

Denotaremos por L_G a $\mathbb{Z}_p$-álgebra de Lie $(G, +, (\ ,\ ))$.

Proposição 2.3.23 *Seja N uma subalgebra da $\mathbb{Z}_p$-álgebra de Lie L_G tal que L_G/N é livre de torção. Então*

(i) *N é um subgrupo uniforme fechado de G;*

(ii) *Se N é um ideal de L_G então N é normal em G e G/N é uniforme.*

Não demonstraremos essa proposição, uma vez que a teoria usada segue por um caminho diferente da que está sendo abordada nesse trabalho até agora, embora também parte do mesmo ponto que são os grupos pro-p uniformes, em resumo, a ideia é definir adequadamente uma aplicação injetiva $log(G)$ em uma $\mathbb{Q}_p$-álgebra associativa $\widehat{A}$ (onde, $\widehat{A}$ é o completamento de uma $\mathbb{Q}_p$-álgebra normada A), satisfazendo algumas

propriedades, de modo que permita construir uma $\mathbb{Z}_p$-álgebra de Lie. Tal teoria pode ser estudada com detalhes em [2], Capítulo 7, nesse mesmo capítulo o resultado [2, Corollary 7.14], garante que a $\mathbb{Z}_p$-álgebra de Lie L_G e a $\mathbb{Z}_p$-álgebra de Lie $log(G)$ são isomorfas. Logo, a proposição acima é verdadeira para qualquer $\mathbb{Z}_p$-álgebra de Lie que satisfaça as hipóteses. E a demonstração da proposição acima pode ser encontrada em [2, Corollary 7.15].

Outro resultado importante que também não será demonstrado pelas mesmas razões acima é:

Corolário 2.3.24 *Seja G um grupo pro-p uniforme e L_G a álgebra de Lie correspondente.*

(a) *G é abeliano se, e somente se, L_G é abeliano;*

(b) *G é solúvel se, e somente se, L_G é solúvel.*

A demonstração pode ser encontrada em [2, Corollary 7.16].

Agora, pensando no sentido inverso do que foi feito, mostraremos como a correspondência que atribui uma álgebra de Lie a cada grupo pro-p uniforme pode ser revertida. Para isso, precisaremos das seguintes definições:

Definição 2.3.25 *Fixe, $\epsilon = 1$ se p é primo ímpar e $\epsilon = 2$ se $p = 2$. A álgebra de Lie L sobre $\mathbb{Z}_p$ é powerful se $L \cong \mathbb{Z}_p^d$, para algum d finito e $(L, L)_{Lie} \subseteq p^{\epsilon}L$.*

A outra definição é a fórmula de Campbell-Hausdorff definida de seguinte maneira:

$$\Phi(X, Y) = \sum_{n=1}^{\infty} u_n(X, Y)$$

com $u_1(X, Y) = X + Y$, $u_2(X, Y) = \frac{1}{2}(X, Y)$, onde $(X, Y) = XY - YX$ tal que X e Y são variáveis não comutativas, e para $(n \geq 3)$,

$$u_n(X, Y) = \sum_{e} q_e(X, Y)_e$$

tal que cada $q_e \in \mathbb{Q}$ satifaz $p^{\epsilon(n-1)}q_e \in p^{\epsilon}\mathbb{Z}_p$ e $\lim_{\langle e\rangle \longrightarrow \infty} |p^{\epsilon\langle e\rangle}q_e| = 0$, onde estamos considerando o somatório sobre todos os vetores e de inteiros positivos satisfazendo $\langle e\rangle = n - 1$.

Um estudo detalhado sobre esse assunto pode ser feito em [2], Capítulo 6.

Agora, para x, $y \in L$, considere a série

$$\widetilde{\Phi}\,(x,y) = \sum_{n=1}^{\infty} u_n(x,y),$$

quando L é powerful, $u_n(x,y) \in L$ para todo $n \in \mathbb{N}$ e além disso a série $\widetilde{\Phi}\,(x,y)$ converge em L. Tais resultados podem ser visto com detalhes em [2, Corollary 6.38]. Podemos então definir uma operação binária $* : L \times L \longrightarrow L$ tal que $x * y = \widetilde{\Phi}\,(x,y)$.

Tendo em mãos tais definições, estamos prontos para apresentar o resultado que garante que, dado uma álgebra de Lie, ela pode se tornar um grupo pro-p uniforme.

Teorema 2.3.26 *Seja L uma álgebra de Lie powerful. Então a operação $*$ torna L um grupo pro-p uniforme. E se $\{a_1, \ldots, a_d\}$ é uma base para L sobre $\mathbb{Z}_p$, então $\{a_1, \ldots, a_d\}$ é um conjunto de geradores topológicos para o grupo $(L, *)$, que tem dimensão d.*

A demonstração desse teorema pode ser encontrada em [2, Theorem 9.8].

Como $[G, G]$ consiste das p^{ϵ}-ésimas potências em G, segue que a álgebra de Lie L_G é powerful. E com isso podemos apresentar o último resultado desta seção, que garante a existência da correspondência exata entre grupos pro-p uniformes e álgebras de Lie powerful sobre $\mathbb{Z}_p$.

Teorema 2.3.27 *As aplicações*

$$G \longmapsto L_G, \quad L \longmapsto (L, *)$$

são isomorfismos mutuamente inversos entre a categoria de grupos pro-p uniformes e a categoria de álgebras de Lie powerful sobre $\mathbb{Z}_p$.

A demonstração desse resultado pode ser encontrada em [2, theorem 9.10]. No enunciado do teorema não é especificado o que acontece com os morfismos, o que é importante especificar, uma vez que um isomorfismo de categorias é um functor. Mas veja que cada morfismo é enviado em si próprio, como uma aplicação entre os conjuntos subordinados em cada categoria.

A título de curiosidade um resultado em Lazard [6, Theorem 3.2.6, Chapter IV] estabelece um isomorfismo entre a categoria de grupos p-saturáveis e uma certa categoria de álgebras de Lie sobre $\mathbb{Z}_p$, o teorema acima é nossa versão desse resultado.

Também vale a pena mencionar que, outra teoria que não está sendo estudada nesse trabalho é a teoria dos grupos pro-p analíticos, embora é facilmente relacionada

aos grupos pro-p uniformes, uma vez que um grupo G é pro-p analítico se, e somente se, G tem um subgrupo aberto característico que é uniforme, ou ainda, G é um grupo pro-p analítico se, e somente se, G tem posto finito. Para um estudo detalhado dessa teoria veja [2], Capítulo 8.

Capítulo 3

Grupos Pro-p Uniformes Finitamente Aprensentados

Neste capítulo apresentamos o resultado principal deste trabalho, o teorema de I. Snopce do artigo [19], "Uncountably many non-commensurable finitely presented pro-p groups". O teorema garante a existência de uma quantidade não enumerável de grupos pro-p uniformes, metabelianos, não comensuráveis de dimensão m. As principais referências deste capítulo são I. Snopce [19], J. D. Dixon; M. P. F. Du Sautoy; A. Mann; D. Segal [2] e L. Ribes; P. Zalesskii [15].

3.1 Resultados Preliminares

Um dos objetivos desta seção é mostrar que cada grupo pro-p de posto finito tem uma apresentação finita por "geradores e relações", no sentido apropriado para grupos pro-p, assim como limitar a quantidade de suas relações. Tais resultados serão usados fortemente na demonstração do teorema principal que será demonstrado na próxima seção.

Com esse intuito, nesta seção nos restringiremos apenas aos grupos pro-p livres, mas para um estudo detalhado dos grupos pro-$\mathcal{C}$ livres veja os livros J.S. Wilson [22] e L. Ribes; P. Zalesskii [15].

Para cada conjunto finito X existe um 'grupo pro-p livre em X', a saber, o completamento pro-p do grupo livre (ordinário) em X. O resultado que prova a existência

do 'grupo pro-p livre em X' pode ser encontrado em [22, Proposition 5.1.3]. Denotaremos esse 'grupo pro-p livre' por $F(X)$. E para qualquer subconjunto R de $F(X)$, escrevemos

$$\langle X; R\rangle = F(X)/\overline{\langle R^{F(X)}\rangle}$$

onde $\langle R^{F(X)}\rangle$ denota o fecho normal de R em $F(X)$.

Dizemos que $\langle X; R\rangle$ é uma *apresentação* para um grupo pro-p G se G é isomorfo a $\langle X; R\rangle$.

A apresentação é finita se R, assim como X, é finito, e nesse caso, dizemos que G é finitamente apresentado. Agora veja que, se G é um grupo pro-p e X é um gerador topológico finito para G, a aplicação identidade em X induz um epimorfismo $\pi : F(X) \longrightarrow G$. Para cada subconjunto R do núcleo $Ker(\pi)$ e cada $r \in R$, dizemos que 'a relação $r = 1$ se mantém em G'. Neste caso, π induz um epimorfismo π^* do grupo $\langle X; R\rangle$ em G. Se R satisfaz a condição $\overline{\langle R^{F(X)}\rangle} = Ker(\pi)$, então π^* é um isomorfismo e $\langle X; R\rangle$ é uma apresentação para G.

O primeiro resultado dessa seção garante que todo grupo pro-p uniforme tem uma apresentação finita que pode ser dada explicitamente.

Proposição 3.1.1 *Seja G um grupo pro-p uniforme de dimensão d e $\{x_1, \ldots, x_d\}$ um conjunto de geradores topológicos para G. Então G tem uma apresentação $\langle x_1, \ldots, x_d; R\rangle$, onde*

$$R = \{[x_i,\, x_j]x_1^{\lambda_1(i,j)} \ldots x_d^{\lambda_d(i,j)} \mid 1 \leq i < j \leq d\},$$

e para cada m, i e j, $\lambda_m(i,\, j) \in p\mathbb{Z}_p$ se p é primo ímpar, e $\lambda_m(i,\, j) \in 4\mathbb{Z}_2$ se $p = 2$.

Demonstração: Como G é powerful, então $G' \leq \overline{G^p}$, logo $[x_j, x_i] \in \overline{G^p}$, se p é ímpar ou $[x_j, x_i] \in \overline{G^4}$ se $p = 2$. Lembrando que, $\overline{G^p} = G^p$, uma vez que G é um grupo pro-p powerful finitamente gerado. E pelo Teorema 2.2.9, $G^p = G_2 = \overline{\langle x_1^p, \ldots, x_d^p\rangle}$, então segue da Proposição 2.2.11 que G^p é produto dos subgrupos procíclicos $\overline{\langle x_1^p\rangle}, \ldots, \overline{\langle x_d^p\rangle}$. Mas pela Proposição 2.1.10, sendo $\overline{\langle x_k^p\rangle}$ procíclico, para cada $k \in \{1, \ldots, d\}$, então $\overline{\langle x_k^p\rangle} = g^{\mathbb{Z}_p}$, para algum $g \in \overline{\langle x_k^p\rangle}$. Logo, $[x_j, x_i] = \prod_{m=1}^{d} x_m^{\lambda_m(i,j)}$, onde cada $\lambda_m(i,j)$ está em $p\mathbb{Z}_p$ se p é ímpar, ou está em $4\mathbb{Z}_2$ se $p = 2$. Assim, as relações $R = 1$ se mantêm em G.

Seja $H = \langle x_1, \ldots, x_d; R\rangle$ e defina $H_i = P_i(H)$, para cada i. Vamos mostrar que G é isomorfo a H. Seja $\pi^* : H \longrightarrow G$ o epimorfismo natural. Então $H_i\pi^* \leq G_i$,

para cada i. De fato, se $i = 1$, $H_1\pi^* = (H^p[H,H])\pi^* = (H\pi^*)^p[H\pi^*, H\pi^*] \leq G^p[G,G] = G_1$. Suponha que a afirmação é verdadeira para $i-1$, ou seja, $H_{i-1}\pi^* = (H_{i-2}\pi^*)^p[H_{i-2}\pi^*, H\pi^*] \leq G^p_{i-2}[G_{i-2}, G] = G_{i-1}$. E vamos mostrar que é verdade para i, $H_i\pi^* = (H_{i-1}\pi^*)^p[H_{i-1}\pi^*, H\pi^*] \leq (G^p_{i-2}[G_{i-2}, G])^p[G^p_{i-2}[G_{i-2}, G], G] = G^p_{i-1}[G_{i-1}, G] = G_i$. Logo, $H_i\pi^* \leq G_i$, para cada i. Agora, das relações $R = 1$ que se mantêm em H implica que H é powerful. E do Teorema 2.2.9, temos que $|H_i/H_{i+1}| \leq |H/H_2| \leq p^d$, uma vez que $d = d(G)$, daí $|H/H_{n+1}| \leq p^{nd} = |G/G_{n+1}|$, para cada n, pois G é uniforme. E como π^* é um epimorfismo e $H_{n+1}\pi^* \leq G_{n+1}$, então $ker\pi^* \leq H_{n+1}$, para cada n. Mas $\bigcap_{n=1}^{\infty} H_{n+1} = 1$, então π^* é injetiva. Assim, G é isomorfo a H. E portanto, $\langle x_1, \ldots, x_d; R\rangle$ é uma apresentação para G. ■

O lema a seguir é uma ferramenta muito útil para lidar com grupos pro-p de posto finito em geral.

Lema 3.1.2 *Seja G um grupo pro-p e K um subgrupo normal aberto de G. Se K é finitamente apresentado, então G é finitamente apresentado.*

Demonstração: Seja K um subgrupo normal aberto de G, então $|G : K| = p^m$, para algum m. Suponha que K é finitamente apresentado. Como $|G : K| = p^m$, então G/K contém um subgrupo normal de ordem p^i, para cada $i \leq m$, ou seja, existe uma série

$$K_1/K \lhd K_2/K \lhd \ldots \lhd K_{m-1}/K \lhd K_m/K = G/K$$

tal que $|K_i/K| = p^i$, para $1 \leq i \leq m$. E pelo teorema da correspondência

$$K \lhd K_1 \lhd K_2 \lhd \ldots \lhd K_{m-1} \lhd K_m = G.$$

Veja que, como G é um grupo pro-p, então K_i também é um grupo pro-p, para todo $i \leq m$. Assim, se usarmos o fato que $|K_1/K| = p$ e provarmos que $G = K_1$ é finitamente apresentado, então por indução, G é finitamente apresentado, uma vez que $|K_i : K_{i-1}| = p$. Suponha então que, $|G : K| = p$. Assim, $G = K\langle y\rangle$ onde $y^p \in K$. Agora suponha que $\langle X; R\rangle$ é uma apresentação finita de K, vindo de um epimorfismo $\pi : F(X) \longrightarrow K$. Então existe $v \in F(X)$ tal que $y^p = v\pi$, e sendo $K \lhd G$, então para cada $x \in X$ existe $w_x \in F(X)$ tal que $(x\pi)^y = w_x\pi$. Agora tome $Y = X \cup \{t\}$, onde $t \notin X$ e defina um epimorfismo $\overline{\pi} : F(Y) \longrightarrow G$ por $x\overline{\pi} = x\pi$, para $x \in X$ e $t\overline{\pi} = y$.

Coloque

$$S = \{t^p v^{-1}\} \cup \{x^t w_x^{-1} \mid x \in X\} \subseteq F(Y),$$

seja N o fecho em $F(Y)$ de $\langle (R \cup S)^{F(Y)} \rangle$ e defina $M = ker\overline{\pi}$. Note que, $N \leq M$, pois $(t^p v^{-1})\overline{\pi} = 1$ e $(x^t w_x^{-1})\overline{\pi} = 1$. Veja que, da relação $S = 1$ que se mantém em $F(Y)/N$ temos que $F(X)N \lhd F(Y)$ e que $|F(Y) : F(X)N| \leq p$, estamos identificando $F(X)$ com sua imagem em $F(Y)$, uma vez que $X \subseteq Y$. Como $F(Y)\overline{\pi} = G$ e $(F(X)N)\overline{\pi} = K$, então $ker\overline{\pi} = M \leq F(X)N$, o que implica que $M = (M \cap F(X))N$. Mas $M \cap F(X) = ker\pi = \overline{\langle R^{F(X)} \rangle} \leq N$. Logo, $M = N$. E portanto, $\langle Y; R \cup S \rangle$ é uma apresentação finita para G. ■

Tendo em mãos o lema acima, estamos prontos a demonstrar que todo grupo pro-p de posto finito tem uma apresentação finita.

Teorema 3.1.3 *Todo grupo pro-p de posto finito é finitamente apresentado.*

Demonstração: Seja G um grupo pro-p de posto finito. Pelo Corolário 2.3.3, G tem um subgrupo K que é uniforme, aberto e característico. E sendo K caracteristíco em G, então $K \lhd G$. Assim, K é um grupo pro-p, uniforme de dimensão finita, então pela Proposição 3.1.1, K tem uma apresentação finita. Dessa forma, K é um subgrupo normal aberto de G que é finitamente apresentado, então pelo lema anterior, G é finitamente apresentado. ■

Uma pergunta natural é: Qual é o número mínimo de relações requer a apresentação de um determinado grupo pro-p? O próximo teorema é uma resposta para essa pergunta.

Para um grupo pro-p finitamente gerado G, defina

$$t(G) = inf\{|R| \mid G \text{ tem uma apresentação } \langle X; R \rangle, \text{ com } |X| = d(G)\}.$$

Teorema 3.1.4 *Seja G um grupo pro-p powerful finitamente gerado, com $d = dim(G)$ e $r = d(G) = rk(G)$. Então*

$$\binom{r}{2} \leq t(G) \leq \binom{r}{2} + r - d.$$

Em particular, se G é um grupo pro-p uniforme, então $\begin{pmatrix} r \\ 2 \end{pmatrix} = t(G)$.

Demonstração: Considere primeiro a segunda desigualdade. Escreva $G_i = P_i(G)$ para cada i, e defina d_i por $p^{d_i} = |G_i : G_{i+1}|$. Pelo Teorema 2.3.2, G_k é uniforme, para algum k e $r = d_1 \geq d_2 \geq \ldots \geq d_k = d$. Segue do Teorema 2.2.9 que G tem um conjunto de geradores $\{x_1, \ldots, x_r\}$ tal que, para cada i, G_i é gerado por $\{x_1^{p^{i-1}}, \ldots, x_{d_i}^{p^{i-1}}\}$. Agora, sempre que $d_i \geq m > d_{i+1}$, temos que, $x_m^{p^i} = x_1^{\mu_1(m)} \ldots x_{d_{i+1}}^{\mu_{d_{i+1}}(m)} = x^{\mu(m)}$, com $\mu_n(m) \in p^i\mathbb{Z}_p$, para cada n. Além disso, como na prova da Proposição 3.1.1, sempre que $1 \leq i < j \leq r$, existe uma relação $[x_j, x_i] = x_1^{\lambda_1(i,j)} \ldots x_r^{\lambda_r(i,j)} = x^{\lambda(i,j)}$, com $\lambda_n(i,j) \in p\mathbb{Z}_p$ (ou $\lambda_n(i,j) \in 4\mathbb{Z}_2$, se $p = 2$), para cada n.

Seja H um grupo com a seguinte apresentação

$$\langle x_1, \ldots, x_r; [x_i, x_j]x^{\lambda(i,j)} (1 \leq i < j \leq r), x_m^{-p^i} x^{\mu(m)} (d_i \geq m > d_{i+1}, 1 \leq i < k) \rangle.$$

Escreva $H_i = P_i(H)$, e análogo a demonstração da Proposição 3.1.1, temos que H é powerful, $|H : H_n| \leq |G : G_n|$, para cada n, e $H \cong G$.

Como existem $\begin{pmatrix} r \\ 2 \end{pmatrix}$ relações da forma $[x_i, x_j]x^{\lambda}$ e $r-d$ relações da forma $x_m^{-p^i}x^{\mu}$, então $t(G) \leq \begin{pmatrix} r \\ 2 \end{pmatrix} + r - d$.

Para a outra desigualdade, suponha que temos uma apresentação $\langle X; R \rangle$ para G, com $|X| = r$ e $|R| = t$. Então G/G_2 tem uma apresentação $\langle X; R, x_1^p, \ldots, x_r^p \rangle$, onde $X = \{x_1, \ldots, x_r\}$. Mas G/G_2 é um p-grupo abeliano elementar de posto r, então $t(G/G_2) = r(r+1)/2$. Consequentemente, $t + r \geq t(G/G_2) = r(r+1)/2$, onde $t + r$ é o número de relações de $\langle X; R, x_1^p, \ldots, x_r^p \rangle$, daí

$$t \geq \frac{r(r+1) - 2r}{2} = \frac{r(r-1)}{2} = \begin{pmatrix} r \\ 2 \end{pmatrix}.$$

E portanto, $\begin{pmatrix} r \\ 2 \end{pmatrix} \leq t(G) \leq \begin{pmatrix} r \\ 2 \end{pmatrix} + r - d$.

■

3.2 Resultado Principal

Como já foi dito, nesta seção nos dedicaremos exclusivamente a demonstrar que existe uma quantidade não enumerável de grupos pro-p uniformes, metabelianos não comensuráveis de dimensão m, e que existe uma quantidade não enumerável de grupos pro-p finitamente apresentados não comensuráveis com um número minimal de geradores igual a m. Para isso, apresentaremos dois resultados que serão aplicados diretamente no teorema principal, tais resultados também fazem parte do artigo "Uncountably many non-commensurable finitely presented pro-p groups", de I. Snopce [19].

A idéia da prova é construir uma quantidade não enumerável de $\mathbb{Q}_p$- álgebras de Lie metabelianas não isomórficas e aplicar a teoria de Lie estudada no capítulo anterior. Para isso usaremos a aplicação adjunta que é definida da seguinte maneira: Seja L uma K-álgebra de Lie. Para qualquer elemento $x \in L$ fixado, defina o K-endomorfismo

$$\begin{aligned} ad\, x : L &\longrightarrow L \\ y &\longmapsto ad\, x(y) = [x, y], \end{aligned}$$

onde a operação $[x, y]$ é o colchete Lie.

O próximo resultado mostrará sob quais condições duas álgebras de Lie, com a operação colchete de Lie definida de maneira adequada, serão isomorfas.

Veja que, quando fixada uma base de uma álgebra de Lie, os colchetes (de Lie) entre quaisquer dois elementos dessa base podem ser escritos como combinação linear. E os coeficientes dessa combinação, são chamados de *constantes de estrutura* da álgebra em relação à base e determinam a álgebra a menos de isomorfismo. Para mais detalhes, bem como a demonstração dessa afirmação veja [12]. Mas observe que, ao trocar a base, as constantes de estruturas não necessariamente serão as mesmas, para obter as mesma álgebra de Lie ou álgebras isomorfas. Porém, no caso específico que apresentaremos a seguir, as álgebras de Lie serão isomorfas se, e somente se, tiverem as mesmas constantes de estrutura.

constantes de estruturas são unicamente determinadas.

Vamos denotar $\mathbb{Z}_p^*$ o grupo das unidades dos inteiros p-ádicos, ou seja, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

Proposição 3.2.1 *Seja $d \in \mathbb{Z}_p^*$ e para $n \geq 1$, sejam $L_{2n+1}(d)$ e $L_{2n+2}(d)$ $\mathbb{Z}_p$- álgebras de Lie definidas da seguinte maneira:*

(i) *$L_{2n+1}(d)$ é o $\mathbb{Z}_p$- módulo livre na base $\{x, e_2, \ldots, e_{2n+1}\}$ e o colchete de Lie é dado da seguinte forma:*

$$\begin{aligned}
&[e_i, e_j] = 0 && \text{para } 2 \leq i, j \leq 2n+1,\\
&[e_i,\, x] = e_{2n-i+3} && \text{para } 3 \leq i \leq 2n,\\
&[e_2,\, x] = de_{2n+1},\\
&[e_{2n+1}, x] = e_2 + e_{2n+1}.
\end{aligned}$$

(ii) *$L_{2n+2}(d)$ é o $\mathbb{Z}_p$- módulo livre na base $\{x, e_2, \ldots, e_{2n+2}\}$ e o colchete de Lie é dado da seguinte forma:*

$$\begin{aligned}
&[e_i, e_j] = 0 && \text{para } 2 \leq i, j \leq 2n+2,\\
&[e_i,\, x] = e_{2n-i+4} && \text{para } 3 \leq i \leq 2n+2,\\
&[e_2,\, x] = de_{2n+2}.
\end{aligned}$$

Suponha $k \geq 3$ e $l \in \mathbb{Z}_p^*$. Então $L_k(d) \cong L_k(l)$ se, e somente se, $d = l$. Além disso, d é um invariante da $\mathbb{Q}_p$- álgebra de Lie $L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Demonstração: A idéia da demonstração é usar a aplicação adjunta $ad\,x$ para encontrar propriedades invariantes que envolvam as constantes de estruturas d e l e com isso concluir que, $L_k(d) \cong L_k(l)$ se, e somente se, $d = l$.

Seja $k \geq 3$ e $L = L_k(d)$. Veja que, $L' = [L, L]$ é um ideal abeliano gerado por $e_2, e_3, \ldots, e_k$, pois basta observar que, se y, $z \in L$, então são escritos da seguinte forma $y = \lambda_1 x + \lambda_2 e_2 + \ldots + \lambda_k e_k$ e $z = \mu_1 x + \mu_2 e_2 + \ldots + \mu_k e_k$, com $\lambda_i, \mu_i \in \mathbb{Z}_p$, $i = \{1, 2, \ldots, k\}$, assim para $k = 2n+1$, temos que

$$\begin{aligned}
[y, z] &= [\lambda_1 x + \lambda_2 e_2 + \ldots + \lambda_k e_k, \mu_1 x + \mu_2 e_2 + \ldots + \mu_k e_k]\\
&= [\lambda_1 x, \mu_1 x] + [\lambda_2 e_2, \mu_1 x] + \ldots + [\lambda_{2n+1} e_{2n+1}, \mu_1 x] +\\
&\quad [\lambda_1 x, \mu_2 e_2] + \ldots + [\lambda_{2n+1} e_{2n+1}, \mu_2 e_2] + \ldots +\\
&\quad [\lambda_1 x, \mu_{2n+1} e_{2n+1}] + \ldots + [\lambda_{2n+1} e_{2n+1}, \mu_{2n+1} e_{2n+1}]\\
&= \lambda_2\mu_1 de_{2n+1} + \ldots + \lambda_{2n+1}\mu_1(e_2 + e_{2n+1}) + (-\lambda_1\mu_2)de_{2n+1} +\\
&\quad (-\lambda_1\mu_3)e_{2n} + \ldots + (-\lambda_1\mu_{2n+1})(e_2 + e_{2n+1}),
\end{aligned}$$

ou seja, $[y,z]$ é escrito como combinação linear dos elementos $e_2, e_3, \ldots, e_{2n+1}$ e o mesmo acontece para $k = 2n+2$. E consequentemente $[L', L'] = 0$, logo, L' é abeliano, o que implica que L é metabeliano.

Considere $A(x)$ a restrição de $ad\,x$ a L', e $A_k(d)$ a matriz associada a essa transformação linear com respeito a base $e_2, e_3, \ldots, e_k$. Assim se $k = 2n+1$, temos que

$$\begin{pmatrix} e_2 \\ e_3 \\ \vdots \\ e_{2n} \\ e_{2n+1} \end{pmatrix} \overset{ad\,x}{\longmapsto} \begin{pmatrix} de_{2n+1} \\ e_{2n} \\ \vdots \\ e_3 \\ e_2 + e_{2n+1} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 & 0 & d \\ 0 & \cdots & 0 & 1 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} e_2 \\ e_3 \\ \vdots \\ e_{2n} \\ e_{2n+1} \end{pmatrix}$$

onde,

$$A_{2n+1}(d) = \begin{pmatrix} 0 & \cdots & 0 & 0 & d \\ 0 & \cdots & 0 & 1 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

uma matriz de tamanho $2n \times 2n$.

Analogamente, se $k = 2n+2$, temos que

$$A_{2n+2}(d) = \begin{pmatrix} 0 & \cdots & 0 & 0 & d \\ 0 & \cdots & 0 & 1 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

uma matriz de tamanho $(2n+1) \times (2n+1)$.

Note que $tr(A_k(d)) = 1$, para todo $k \geq 3$. Além disso, $det(A_{2n+1}(d)) = (-1)^n d$ e $det(A_{2n+2}(d)) = (-1)^n d$, para todo $n \geq 1$, ou seja, $det(A_k(d)) = (-1)^{\lfloor \frac{k-1}{2} \rfloor} d$, para $k \geq 3$.

E note também que podemos escrever L como uma soma direta $L = L' \oplus x\mathbb{Z}_p$.

Agora, considerando outra base, temos que $L = L' \oplus y\mathbb{Z}_p$, para algum $y \in L$, então $y = ux + e$, com $u \in \mathbb{Z}_p^*$ e $e \in L'$, e

$$[e_i,\, y] = [e_i,\, ux + e] = u[e_i, x] + [e_i,\, e] = u[e_i,\, x],$$

pois como $e \in L'$ então $[e_i,\, e] = 0$.

Assim, $A(y) = ad\, y_{|_{L'}} = uA(x)$, então $tr\, A(y) = u\, tr\, A(x)$ e $det\, A(y) = u^{k-1} det\, A(x)$, onde $k - 1 = dim\, L'$. Como $tr\, A(x) = tr\,(A_k(d)) = 1$, para todo $k \geq 3$, segue que

$$(tr\, A(y))^{-(k-1)} \cdot det\, A(y) = u^{1-k} \cdot det\, A(y) = det\, A(x) = (-1)^{\lfloor \frac{k-1}{2} \rfloor} d.$$

Veja que, para qualquer $y \in L$, quando aplicamos na adjunta e calculamos o determinante, o resultado será sempre o mesmo, inclusive para $y = x$ (nesse caso $u = 1$), independente de qual base escolhermos, portanto d é um invariante da álgebra L. Sendo assim, se as álgebras são isomorfas, então temos um isomorfismo entre bases que 'leva' base em base, logo, $d = l$. E por outro lado, se $l = d$, então temos o isomorfismo das álgebras, uma vez que ambas tem o produto de Lie definido com as mesmas constantes de estrutura. E portanto, $L_k(d) \cong L_k(l)$ se, e somente se, $d = l$.

E veja que a demonstração funciona igualmente bem com $\mathbb{Q}_p$ no lugar de $\mathbb{Z}_p$. Assim, d é um invariante de $\mathbb{Q}_p$-álgebra de Lie $L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, e o resultado segue.

■

Corolário 3.2.2 *Seja $k \geq 3$ e $d, l \in \mathbb{Z}_p^*$. A $\mathbb{Z}_p$-álgebra de Lie $p^2L_k(d)$ é powerful e, $p^2L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong p^2L_k(l) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ se, e somente se, $d = l$. Em particular, existe uma quantidade não enumerável de $\mathbb{Z}_p$-álgebras de Lie (powerful) não isomórficas de posto k.*

Demonstração: Como a $\mathbb{Z}_p$-álgebra de Lie $p^2L_k(d)$ é um $\mathbb{Z}_p$-módulo livre, então $p^2L_k(d) \cong \mathbb{Z}_p^k$. Além disso,

$$[p^2L_k(d),\, p^2L_k(d)] = p^4[L_k(d),\, L_k(d)] \subseteq p^2(p^2L_k(d)) \subseteq p(p^2L_k(d)).$$

Logo, por definição, $p^2L_k(d)$ é uma $\mathbb{Z}_p$-álgebra de Lie powerful.

Agora suponha que $\{e_1, e_2, \ldots, e_k\}$ é uma base de $L_k(d)$. Como $L_k(d)$ é um

$\mathbb{Z}_p$-módulo livre, então cada elemento a de $L_k(d)$ tem uma expressão única da forma

$$a = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_k e_k,$$

com $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{Z}_p$. E seja $w \in p^2 L_k(d)$, então $w = p^2 v$, para algum $v \in L_k(d)$. Daí,

$$w = p^2 v = p^2 \sum_{i=1}^{k} (\lambda_i e_i) = \sum_{i=1}^{k} \lambda_i (p^2 e_i).$$

Logo, temos que $p^2 e_1, p^2 e_2, \ldots, p^2 e_k$ é uma base de $p^2 L_k(d)$, uma vez que w é escrito de forma única como combinação linear de elementos com coeficientes em $\mathbb{Z}_p$. Reciprocamente, suponha que $p^2 e_1, p^2 e_2, \ldots, p^2 e_k$ é uma base de $p^2 L_k(d)$. Dado $v \in L_k(d)$, existe $w \in p^2 L_k(d)$ tal que $w = p^2 v$, daí

$$w = \sum_{i=1}^{k} \lambda_i (p^2 e_i) = \sum_{i=1}^{k} p^2 (\lambda_i e_i) = p^2 \sum_{i=1}^{k} (\lambda_i e_i) = p^2 v,$$

logo, $v = \sum_{i=1}^{k} \lambda_i e_i$ e $\{e_1, e_2, \ldots, e_k\}$ é uma base de $L_k(d)$. Segue que, considerando as extensões de escalares de $\mathbb{Z}_p$ para $\mathbb{Q}_p$, $L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ e $p^2 L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, temos que, $\{f_1, f_2, \ldots, f_k\}$ é uma base de $L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ se, e somente se, $p^2 f_1, p^2 f_2, \ldots, p^2 f_k$ é uma base de $p^2 L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Consequentemente, $p^2 L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong p^2 L_k(l) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ se, e somente se, $L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong L_k(l) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. E pela proposição anterior, $L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong L_k(l) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ se, e somente se, $d = l$.

A última parte do corolário segue diretamente do fato que, duas álgebras de Lie $L_k(d)$ e $L_k(l)$, com $d, l \in \mathbb{Z}_p^*$, são isomorfas se, e somente se, $d = l$, e que $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$ é um conjunto não enumerável. Logo, existe uma quantidade não enumerável de $\mathbb{Z}_p$-álgebras de Lie (powerful) não isomóficas de posto k. ■

Agora demonstraremos o resultado principal desse trabalho. Lembrando que, dois grupos são *comensuráveis* se eles tem subgrupos de índices finitos que são isomórficos.

Teorema 3.2.3 *Seja $m \geq 3$ um inteiro positivo. Existe uma quantidade não enumerável de grupos pro-p uniformes, metabelianos, não comensuráveis de dimensão m. Consequentemente, existe uma quantidade não enumerável de grupos pro-p finitamente apresentados não comensuráveis com um número minimal de geradores igual a m (e o número minimal de relações igual a $\begin{pmatrix} m \\ 2 \end{pmatrix}$).*

Demonstração: Seja $m \geq 3$ um inteiro positivo. Pelo corolário anterior, $p^2L_m(d)$ é uma $\mathbb{Z}_p$-álgebra de Lie powerful de posto m, para todo $d \in \mathbb{Z}_p^*$. Agora pelo Teorema 2.3.26, podemos associar à $\mathbb{Z}_p$-álgebra de Lie $p^2L_m(d)$ um grupo pro-p uniforme $G_m(d)$ que tem o mesmo conjunto subordinado que $p^2L_m(d)$ e tal que $d(G_m(d)) = m$. E pelo Teorema 2.3.27, $G_m(d) \cong G_m(l)$ se, e somente se, $p^2L_m(d) \cong p^2L_m(l)$. Além disso, $G_m(d)$ e $G_m(l)$ são dois a dois não comensuráveis sempre que $d \neq l$, uma vez que, $p^2L_k(d) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong p^2L_k(l) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ se, e somente se, $d = l$. E o Corolário 2.3.24 nos garante que, um grupo pro-p uniforme é solúvel se, e somente se, a álgebra de Lie correspondente é solúvel, e como a $\mathbb{Z}_p$-álgebra de Lie é metabeliana, como vimos na demonstração da Proposição 3.2.1, então o grupo pro-p uniforme $G_m(d)$ é metabeliano.

E novamente pelo corolário anterior, temos uma quantidade não enumerável de grupos pro-p uniformes G tal que $d(G) = m$ e segue da Proposição 3.1.1 que todos esses grupos são finitamente apresentados. E do Teorema 3.1.4 segue que o número minimal de relações de $G_m(d)$ é $\begin{pmatrix} m \\ 2 \end{pmatrix}$. ■

Com isso demonstramos o resultado principal do artigo [19] "Uncountably many non-commensurable finitely presented pro-p groups" de I. Snopce. E para finalizar este trabalho forneceremos um exemplo que mostra que podermos dar uma apresentação explícita de $G_m(d)$.

Exemplo 3.2.4 *Considere $m = 4$. O grupo pro-p uniforme $G_4(d)$ associado a $\mathbb{Z}_p$-álgebra de Lie powerful $p^2L_4(d)$ é dado pela seguinte apresentação*

$$\begin{aligned} G_4(d) \;=\; & \langle y, z_2, z_3, z_4 : [z_2,\, z_3] = 1, [z_3,\, z_4] = 1, [z_4,\, z_2] = 1, \\ & [z_2,\, y] = z_4^{dp^2}, [z_3,\, y] = z_3^{p^2}, [z_4,\, y] = z_2^{p^2} \rangle. \end{aligned}$$

Bibliografia

[1] Y. Chow, *General Theory Of Lie Algebras*, vol. 1, Gordon and Breach Science Publishers, 1978.

[2] J. D. Dixon; M. P. F. Du Sautoy; A. Mann; D. Segal *Analytic Pro-p Groups*, 2nd Edition, Cambridge University Press, 1999.

[3] W. Feit; J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math, **13** (1963), 775-787.

[4] R. M. Guralnick, *On the number of generators of a finite group*, Arch. Math. (Basel) **53** (1989), 521-523.

[5] E. I. Khukhro, *Nilpotent Groups and their Automorphisms*, Walter de Gruyter, Berlim, 1993.

[6] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. Inst. Haustes Études Scientifiques **26** (1965), 389-603.

[7] E. L. Lima, *Curso de Análise*, vol. 1, Décima segunda edição, Projeto Euclides, IMPA, 2010.

[8] A. Lubotzky; A. Mann, *Powerful p-Groups. I. Finite Groups*, J. Algebra **105** (1987), 484-505.

[9] A. Lubotzky; A. Mann, *Powerful p-Groups. II. p-Adic Analytic Groups*, J. Algebra **105** (1987), 506-515.

[10] A. Lucchini, *A bound on the number of generators of a finite group*, Arch. Math. (Basel) **53** (1989), 313-317.

[11] A. I. Mal'cev, *On some classes of infinite soluble groups*, Mat. Sbornik N.S. **28** (1951), 567-588.

[12] L. A. B. Martin, *Álgebras de Lie*, 2º ed, Editora da Unicamp, 2010.

[13] J. R. Munkres, *Topology*, 2nd Edition, Prentice Hall, Upper Saddle River, 2000.

[14] N. Nikolov; D. Segal, *Finite index subgroups in profinite groups*, C. R. Acad. Sci. Paris Ser. I **337** (2003), 303-308.

[15] L. Ribes; P. Zalesskii, *Profinite Groups*, 2nd Edition, Springer, 2010.

[16] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd Ed., Springer-Verlag, 1996.

[17] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th Edition, Springer-Verlag, 1994.

[18] D. C. Smyth, *Finitely Generated Powerful Pro-p Groups*, 2010, http://web.maths.unsw.edu.au/ danielch/thesis/smyth.pdf.

[19] I. Snopce, *Uncountably Many Non-commensurable Finitely Presented Pro-p Groups*, J. Group Theory **19** (2016), 512-521.

[20] J. Tate, *Nilpotent quotient groups*, Topology, **3** (1964), 109-111.

[21] J. S. Wilson, *Finite index subgroups and verbal subgroups in profinite groups*, Séminaire Bourbaki. Volume 2009/2010. Exposés 1012-1026, Astérisque 339, Société Mathématique de France, Paris (2011), Exposés 1026, 387–408.

[22] J. S. Wilson, *Profinite Groups*, Clarendon Press, Oxford, 1998.

[23] R. A. Wilson, *The Finite Simple Groups*, Springer-Verlag, 2010.