p-Grupos finitos com grupo de automorfismos pequeno

Daniel Alber Ninaquispe Corales

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

Orientador: Ilir Snopche

Rio de Janeiro

Fevereiro de 2018

p-Grupos finitos com grupo de automorfismos pequeno

Daniel Alber Ninaquispe Corales

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

Aprovada por:

Prof. Dr. Ilir Snopche - MAT/UFRJ (Orientador)

Prof. Dr. Aftab Pande - MAT/UFRJ (Membro)

Prof. Dr. Slobodan Tanusevski - MAT/UFF (Membro)

RESUMO

p-GRUPOS FINITOS COM GRUPO DE AUTOMORFISMOS PEQUENO

Daniel Alber Ninaquispe Corales
Orientador: Ilir Snopche

Resumo da dissertação de mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro-UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Seja p um primo. Um p-grupo finito é um grupo finito em que a ordem de todo elemento é igual a uma potência de p. Os p-grupos finitos formam uma classe importante de grupos com muitas propriedades interessantes e bonitas. Através dos teoremas de Sylow, eles são os "blocos de construção"de grupos finitos arbitrários.

Um dos tópicos mais importantes na teoria dos p-grupos finitos é o estudo dos automorfismos de p-grupos finitos; em particular, o estudo da relação entre um p-grupo finito G e o seu grupo de automorfismos $\mathrm{Aut}(G)$. A questão mais famosa nesta direção é a seguinte: É verdade que $|G|$ divide $|\mathrm{Aut}(G)|$ para cada p-grupo finito não-abeliano G? O primeiro resultado nesta direção foi publicado há mais de 60 anos. Atualmente, há uma literatura rica sobre esta questão com resultados positivos em várias classes de p-grupos finitos.

Esta dissertação baseia-se em um artigo recente de González-Sánchez e Jaikin-Zapirain [13], e o seu objetivo principal é mostrar que a resposta à questão acima em geral é negativa. Na verdade, depois de uma grande quantidade de resultados positivos durante os últimos 60 anos, recentemente González-Sánchez e Jaikin-Zapirain, usando a teoria de grupos pro-p uniformes, provaram que existe um p-grupo finito não-abeliano G tal que $|\mathrm{Aut}(G)| < |G|$.

Palavras-chave: p-Grupos finitos, Automorfismos de p-grupos finitos, Grupo de automorfismos, Grupos pro-p uniformes, Grupos profinitos, Cohomologia de grupos profinitos.

Rio de Janeiro
Fevereiro de 2018

ABSTRACT

FINITE p-GROUPS WITH SMALL AUTOMORPHISM GROUP

Daniel Alber Ninaquispe Corales
Orientador: Ilir Snopche

Abstract da dissertação de mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro-UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Let p be a prime. A p-group is a group in which the order of every element is equal to a power of p. Finite p-groups form an important class of groups with many interesting and beautiful properties. Via the Sylow theorems they are the 'building blocks' of arbitrary finite groups.

One of the most important topics in the theory of finite p-groups is the study of the automorphisms of finite p-groups; in paricular, the study of the relation between a finite p-group G and its group of automorphisms $\mathrm{Aut}(G)$. The most famous question in this direction is the following: Is it true that $|G|$ divides $|\mathrm{Aut}(G)|$ for every non-abelian finite p-group G? The first result regarding this question is more than 60 years old. Nowadays there is a rich literature concerning this question with positive results in various classes of finite p-groups.

This dissertation is based on a recent paper of González-Sánchez and Jaikin-Zapirain [13], and its main purpose is to show that the answer to the above question in general is negative. Indeed, after a huge number of positive results during the last 60 years, recently González-Sánchez and Jaikin-Zapirain, using the theory of uniform pro-p groups, proved that there exists a non-abelian finite p-group G such that $|\mathrm{Aut}(G)| < |G|$.

Key words: Finite p-groups, Automorphisms of finite p-groups, Automorphism group, Uniform pro-p groups, Profinite groups, Cohomology of profinite groups.

Rio de Janeiro
Fevereiro de 2018

Sumário

Introdução

Seja p um primo. Um p-grupo é um grupo em que a ordem de todo elemento é igual a uma potência de p. Não é difícil ver que um grupo finito G é um p-grupo se e somente se $|G| = p^k$ para algum inteiro não negativo k. Os p-grupos finitos formam uma classe importante de grupos com muitas propriedades interessantes e bonitas. Através dos teoremas de Sylow, eles são os "blocos de construção"de grupos finitos arbitrários. Por exemplo, um grupo finito G é nilpotente se e somente se é produto direto de seus p-subgrupos de Sylow.

Um dos tópicos mais importantes na teoria dos p-grupos finitos é o estudo dos automorfismos de p-grupos finitos; em particular, o estudo da relação entre um p-grupo finito G e o seu grupo de automorfismos $\mathrm{Aut}(G)$. A questão mais famosa nesta direção é a seguinte: É verdade que $|G|$ divide $|\mathrm{Aut}(G)|$ para cada p-grupo finito não-abeliano G?

O primeiro resultado nesta direção é o resultado de Schenkman, que foi publicado há mais de 60 anos. Em [7] Schenkman mostrou que essa questão sempre tem uma resposta positiva para os p-grupos finitos não-abelianos de classe 2; a demonstração de Schenkman teve um erro, que foi concertado pelo Faudree em [26]. Atualmente, há uma literatura rica sobre esta questão com resultados positivos em várias classes de p-grupos finitos. Por exemplo, a questão tem resposta positiva para os p-grupos finitos de expoente p [32], para os p-grupos finitos de classe maximal [1], para os p-grupos finitos de ordem $\leq p^7$ [23], para os p-grupos finitos modulares [27], para os p-grupos finitos com centro de ordem p, para os p-grupos metacíclicos com p ímpar, etc.

Esta dissertação baseia-se em um artigo recente de González-Sánchez e Jaikin-Zapirain [13], e o seu objetivo principal é mostrar que a resposta à questão acima em geral é negativa. Na verdade, depois de uma grande quantidade de resultados positivos durante os últimos 60 anos, recentemente González-Sánchez e Jaikin-Zapirain provaram que existe um p-grupo finito não-abeliano G tal que $|\mathrm{Aut}(G)| < |G|$. Para provar esse resultado, eles usaram a teoria de grupos pro-p e técnicas cohomológicas. A ideia principal é achar um grupo pro-p analítico p-ádico (mais precisamente, um grupo pro-p uniforme) G tal que $\dim(\mathrm{Aut}(G)) < \dim(G)$, onde $\dim(G)$ é a dimensão de G como variedade analítica p-ádica; como $\mathrm{Aut}(G)$ também é um grupo analítico p-ádico, faz sentido considerar $\dim(\mathrm{Aut}(G))$. Escrevendo esse grupo G como limite inverso de p grupos finitos $\{G_i\}_{i\geq 1}$, isto é $G = \varprojlim G_i$, temos que $\mathrm{Aut}(G)=\varprojlim \mathrm{Aut}(G_i)$. Agora basta mostrar que para algum j suficientemente grande $|\mathrm{Aut}(G_j)| < |G_j|$.

No primeiro capítulo deste trabalho fazemos uma revisão de grupos topológicos e limites inversos. No segundo capítulo introduzimos os inteiros p-ádicos e o grupo de Prüfer. Em seguida, em terceiro capítulo, fazemos uma revisão sobre os p-grupos finitos e os automorfismos de grupos finitos. O quarto capítulo aborda vários tópicos relacionados aos

grupos profinitos e pro-p. Grupos profinitos são grupos topológicos compactos e totalmente desconexos, que aparecem naturalmente como grupos de Galois de extensões de corpos. Equivalentemente, um grupo profinito é o limite inverso de um sistema inverso de grupos finitos. Um grupo pro-p é o limite inverso de um sistema inverso de p-grupos finitos. Na primeira parte do capítulo 4 apresentamos a teoria básica de grupos profinitos e grupos pro-p, incluindo a conexão de grupos profinitos com grupos de Galois. Em seguida, introduzimos os grupos pro-p powerful, grupos pro-p de posto finito e grupos pro-p uniformes. Concluímos o capítulo quatro com a introdução de Álgebras de Lie associadas aos grupos pro-p uniformes. No capítulo cinco apresentamos a conexão entre os grupos p-ádicos analíticos e a Teoria de Lie. No sexto capítulo fazemos uma breve revisão dos conceitos e resultados básicos da cohomologia de grupos profinitos, que vamos usar na demonstração do teorema principal deste trabalho. No capítulo 7 introduzimos a álgebra de Lie nilpotente de Sato; essa álgebra de Lie tem papel crucial na construção de um grupo pro-p uniforme G tal que $\dim(\mathrm{Aut}(G)) < \dim(G)$. Finalmente, no último capítulo, vamos provar o Teorema de González-Sánchez e Jaikin-Zapirain, ou mais precisamente, vamos mostrar que existe um p-grupo finito não-abeliano H tal que $|\mathrm{Aut}(H)| < |H|$.

Além do artigo [13], as principais referencias deste trabalho são os livros [11], [15], [6], [8], [20], [19], [14], [5] e os artigos [2] e [18].

Capítulo 1

Grupos Topológicos e Limites Inversos

Este primeiro capítulo analisa as noções de topologia, tais como espaços Hausdorff, espaços desconexos, grupos topológicos e limites inversos. O desenvolvimento deste capítulo foi obtido do livro de Jhon S. Wilson 'Profinite groups' [15].

1.1 Espaços Topológicos

Um *espaço topológico* é um conjunto X junto com uma família de subconjuntos chamados conjuntos *abertos*, com as seguintes propriedades:

(i) O conjunto vazio $\emptyset$ e X são abertos.

(ii) A interseção de dois conjuntos abertos é um conjunto aberto.

(iii) A união de uma coleção de conjuntos abertos é um conjunto aberto.

O conjunto formado por esses abertos é chamado uma *topologia* em X. Um subconjunto de X é chamado *fechado* se seu complemento é aberto. Se Y é um subconjunto de X o fecho $\overline{Y}$ de Y é a interseção de todos os conjuntos fechados contendo Y, em particular $\overline{Y}$ é um conjunto fechado. Um subconjunto Y de X é chamado *denso* em X se $\overline{Y} = X$. Uma *vizinhança* aberta de um elemento x de X é um conjunto aberto contendo x. Uma base para a topologia em X é uma coleção $\{U_\lambda \mid \lambda \in \Lambda\}$ de conjuntos abertos tal que cada conjunto aberto é uma união de alguns dos conjuntos U_λ (E uma base de vizinhanças abertas de x é definida similarmente). Qualquer conjunto X pode ser considerado como um espaço topológico em relação à topologia na qual cada subconjunto é aberto; esta topologia é chamada a *topologia discreta* em X, e X é chamado então um *espaço discreto.*

Se Y é um subconjunto de um espaço X, então a coleção de todos os subconjuntos da forma $Y \cap U$ com U aberto em X é uma topologia em Y; esta topologia é chamada a *topologia de subespaço*, e em relação a esta topologia Y é chamado um *subespaço de* X.

Um espaço topológico X é chamado *compacto* se, para cada família $\{U_\alpha \mid \alpha \in A\}$ de subconjuntos abertos cuja união é X existe uma subfamília finita $\{U_{\alpha_1}, ..., U_{\alpha_n}\}$ cuja união é X.

Um espaço topológico X é chamado Hausdorff se dados quaisquer dois elementos x e y em X existem duas vizinhanças U e V de x e y respectivamente tal que $U \cap V = \emptyset$.

Um espaço X é chamado *conexo* se não pode ser escrito como a união disjunta de dois subconjuntos abertos não vazios. Um espaço topológico X se diz *totalmente desconexo* se cada subespaço conexo tem no máximo um elemento.

Proposição 1.1.1 *Seja X um espaço compacto Hausdorff.*

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

(b) *Seja $x \in X$ e seja A a interseção de todos os subconjutnos de X contendo x os quais são ao mesmo tempo fechados e abertos. Então A é conexo.*

(c) *Se X é totalmente desconexo, então cada conjunto aberto é a união de conjuntos os quais são ao mesmo tempo fechados e abertos.*

Dizemos que uma aplicação $f : X \to Y$ entre dois espaços topológicos é *contínua* se a imagem inversa de um aberto em Y é um aberto em X. Um *homeomorfismo* é uma aplicação bijetiva continua onde a aplicação inversa é contínua .

Proposição 1.1.2 *Sejam X e Y dois espaços topológicos.*

(a) *Cada subconjunto fechado de um espaço compacto é compacto.*

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

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

(d) *Se $f : X \to Y$ é contínua e bijetiva com X compacto e Y Hausdorff então f é um homeomorfismo.*

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

Proposição 1.1.3 *Seja X um espaço totalmente desconexo. Então para cada x em X, $\{x\}$ é fechado em X.*

Seja ρ uma relação de equivalência sobre um espaço topológico X, e escrevemos X/ρ para o conjunto quociente e q para a aplicação quociente de X para X/ρ. A *topologia quociente* sobre X/ρ é a topologia cujos conjuntos abertos são os subconjuntos V de X/ρ tais que $q^{-1}(V)$ é aberto em X. Se X/ρ tem a topologia quociente então a aplicação quociente q é contínua.

O *produto cartesiano* (ou simplesmente *produto*) de uma família $\{X_\lambda \mid \lambda \in \Lambda\}$ de conjuntos é o conjunto $\prod_{\lambda\in\Lambda} X_\lambda$ cujos elementos são as aplicações x de Λ para $\bigcup_\lambda X_\lambda$ com a propriedade que $x(\lambda) \in X_\lambda$ para cada λ. Podemos considerar os elementos de $\prod_{\lambda\in\Lambda} X_\lambda$ como vetores com entradas ou coordenadas indexadas por elementos de Λ. Assim um elemento típico será escrito como (x_λ). A aplicação projeção $\pi_\lambda : \prod_{\lambda\in\Lambda} X_\lambda \to X_\lambda$ é a aplicação que leva um elemento $x \in \prod_{\lambda\in\Lambda} X_\lambda$ para o valor $x(\lambda)$. O produto de uma família finita $X_1, ..., X_n$ de conjuntos é denotada por $X_1 \times ... \times X_n$.

Agora suponha que cada X_λ é um espaço topológico. A *topologia produto* em $\prod_{\lambda\in\Lambda} X_\lambda$ tem como seus conjuntos abertos todas as uniões de conjuntos da forma

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

com n finito, cada λ_i em Λ e U_i abertos em X_{λ_i}. Portanto cada aplicação projeção π_λ é contínua, de fato, a topologia produto é a menor topologia que faz as aplicações projeção contínuas.

Seja Z um espaço topológico e $f : Z \to \prod_{\lambda\in\Lambda} X_\lambda$ uma aplicação, afirmamos que f é contínua se e somente se cada aplicação $\pi_\lambda f$ é contínua.

Teorema 1.1.4 *Seja $\{X_\lambda \mid \lambda \in \Lambda\}$ uma família de espaços topológicos.*

(a) *Se cada X_λ é Hausdorff então $\prod_{\lambda\in\Lambda} X_\lambda$ é Hausdorff.*

(b) *Se cada X_λ é totalmente desconexo então $\prod_{\lambda\in\Lambda} X_\lambda$ é totalmente desconexo.*

(c) (**Teorema de Tychonoff**)*Se cada X_λ é compacto então $\prod_{\lambda\in\Lambda} X_\lambda$ é compacto.*

1.2 Grupos Topológicos

Definição 1.2.1 Um *grupo topológico* é um conjunto G que é ao mesmo tempo um grupo e um espaço topológico e para o qual a aplicação $(x, y) \to xy^{-1}$ de $G \times G$ (com a topologia produto) para G é contínua.

Se G é um grupo, $g \in G$ e U, V subconjuntos de G, escrevemos $Ug = \{ug \mid u \in G\}$, $gU = \{gu \mid u \in G\}$, $U^{-1} = \{u^{-1} \mid u \in U\}$ e $UV = \{uv \mid u \in U, v \in V\}$. Escrevemos 1 para o elemento identidade de um grupo. O seguinte Lema contém alguns resultados elementares sobre os grupos topológicos.

Proposição 1.2.2 *Seja G um grupo topológico e sejam x, y elementos de G. Então*

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

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

(c) *Cada subgrupo aberto de G é fechado, e cada subgrupo fechado de índice finito é aberto. Se G é compacto então cada 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 em relação à topologia induzida e G/K é um grupo topológico em relação à topologia quociente; e a aplicação q de G para G/K leva conjuntos abertos para conjuntos abertos.*

(f) *G é 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, D são subconjuntos fechados então o conjunto CD é também 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 todos $\lambda_1, \lambda_2 \in \Lambda$ existe um elemento $\mu \in \Lambda$ para o qual $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$. Se Y é um subconjunto fechado de G, então $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y = \bigcap_{\lambda\in\Lambda} X_\lambda Y$.*

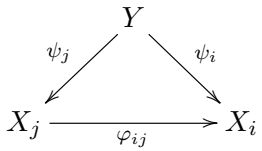
Proposição 1.2.3 *Seja G um grupo topológico compacto. Se C é um subconjunto que é ao mesmo tempo fechado e aberto e contém o conjunto $\{1\}$, então C contém um subgrupo aberto normal.*

1.3 Limites Inversos

Um conjunto *dirigido* é um conjunto parcialmente ordenado I onde para todo $i, j \in I$ existe um elemento $k \in I$ tal que $i \leq k$ e $j \leq k$.

Definição 1.3.1 Um sistema inverso (X_i, φ_{ij}) de espaços topológicos indexado por um conjunto dirigido I consiste de uma família $\{X_i \mid i \in I\}$ de espaços topológicos e uma família $\{\varphi_{ij} : X_j \to X_i \mid i, j \in J, i \leq j\}$ de aplicações contínuas tal que φ_{ii} é a aplicação identidade id_{X_i} e $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ onde $i \leq j \leq k$. Na definição não precisamos que os conjuntos X_i sejam espaços topológicos. Podemos mudar eles por grupos topológicos ou anéis dependendo de cada caso.

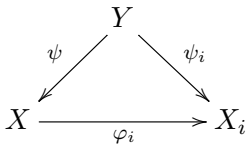
Seja (X_i, φ_{ij}) um sistema inverso de espaços topológicos e seja Y um espaço topológico. Chamaremos à família $\{\psi_i : Y \to X_i \mid i \in I\}$ de aplicações contínuas *compatível* se $\varphi_{ij}\psi_j = \psi_i$ onde $i \leq j$. Esta condição é equivalente a mostrar que o seguinte diagrama



comuta.

Definição 1.3.2 Um *limite inverso* (X, φ_i) de um sistema inverso (X_i, φ_{ij}) de espaços topológicos (resp. grupos topológicos, anéis) é um espaço (resp. grupos topológicos, anéis) topológico X junto com uma família compatível $(\varphi_i : X \to X_i)$ de aplicações contínuas (resp. homomorfismos contínuos) com a seguinte propriedade universal: sempre que $(\psi_i : Y \to X_i)$ é uma família compatível de aplicações contínuas do espaço Y (resp. de homomorfismos contínuos de um grupo ou anel Y) topológico, existe uma única aplicação contínua (resp. homomorfismo contínuo) $\psi : Y \to X$ tal que $\varphi_i\psi = \psi_i$ para cada i.

Portanto, precisamos que exista um único ψ tal que o seguinte diagrama comute



A proposição seguinte mostra que o limite inverso existe e é único.

Proposição 1.3.3 *Seja (X_i, φ_{ij}) um sistema inverso de espaços topológicos, indexado por I.*

(a) *Se (Y, φ_i) e (Z, ψ_i) são limites inversos do sistema inverso (X_i, φ_{ij}), então existe um isomorfismo $\sigma : Y \to Z$ tal que $\psi_i \sigma = \varphi_i$ para cada i.*

(b) *Denotamos por π_i a aplicação projeção de $\prod_{j \in I} X_j$ para X_i e definimos*

$$X = \{c \in \prod_{j \in I} X_j \mid \varphi_{ij}\pi_j(c) = \pi_i(c), \forall i, j \text{ com } j \geq i\} \tag{1.1}$$

e $\varphi_i = \pi_i|_X$ 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.*

Este resultado mostra que o limite inverso de um sistema inverso (X_i, φ_{ij}) existe e é único sob isomorfismos. Denotemos este limite inverso por $\varprojlim (X_i, \varphi_{ij})$, ou simplesmente por $\varprojlim X_i$.

Proposição 1.3.4 Seja (X_i, φ_{ij}) um sistema inverso indexado por I, e escrevemos $X = \varprojlim X_i$.

(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 compacto e Hausdorff, então X é compacto e Hausdorff.*

(d) *Se cada X_i é um espaço não vazio compacto Hausdorff, então X é não vazio.*

Proposição 1.3.5 *Seja (X, φ_i) um limite inverso de um sistema inverso (X_i, φ_{ij}) de espaços compactos Hausdorff não vazios indexados por I. Temos as seguintes afirmações:*

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

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

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

(d) *Se θ é uma aplicação do espaço Y para X então θ é contínua se e somente se cada aplicação $\varphi_i\theta$ é contínua.*

(e) *Se $f : X \to A$ é uma aplicação contínua, sendo A discreto. Então para algum i existe uma aplicação contínua $g : X_i \to A$ satisfazendo $f = g\varphi_i$.*

Proposição 1.3.6 *Seja X um espaço totalmente desconexo compacto Hausdorff. Então X é o limite inverso de seus espaços quocientes discretos.*

Capítulo 2

Os inteiros p-ádicos e o grupo de Prüfer

Na segunda seção do capítulo anterior desenvolvimos a teoria de limites inversos. Dos exemplos muitos importantes dentro dessa teoria são o anel de inteiros p-ádicos e o grupo de Prüfer. Os inteiros p-ádicos serão a base para definir os grupos p-ádicos analíticos no capítulo 4 e poderemos definir as álgebras de Lie que usaremos na demonstração do Teorema principal no capítulo 7. Para este capítulo, foi usado o livro "Field Arithmetic"de Michael D. Fried e Moshe Jarden [20].

2.1 Inteiros p-ádicos

Definição 2.1.1 Seja p um primo. Consideremos os aneis quocientes $\mathbb{Z}/p^i\mathbb{Z}$ e os homomorfismos canônicos $\pi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ definidos por $\pi_{ij}(x + p^j\mathbb{Z}) = x + p^i\mathbb{Z}$ para $j \geq i$. O limite inverso $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ é o *anel de inteiros p-ádicos*. Este anel satisfaz as seguintes propriedades:

(i) Cada $x \in \mathbb{Z}_p$ é uma sequência $(x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ onde $x_i \in \mathbb{Z}$ e $x_j \equiv x_i \mod p^i\mathbb{Z}$, $\forall j \geq i$.

(ii) A aplicação $\rho_i : \mathbb{Z} \to \mathbb{Z}_p$ definida por $\rho_i(a) = (a + p^i\mathbb{Z})_{i\in\mathbb{N}}$ é um homomorfismo injetivo.

(iii) A sequência $(x_i)_{i\in\mathbb{N}}$ converge para $x = (x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ na topologia p-ádica. Portanto $\mathbb{Z}$ é denso em $\mathbb{Z}_p$.

(iv) $\mathbb{Z} \neq \mathbb{Z}_p$.

(v) Um elemento $x = (x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ de $\mathbb{Z}_p$ é invertível se e somente se $p \nmid x_1$.

(vi) $\mathbb{Z}_p$ é um domínio integral.

Sejam $x \in \mathbb{Z}_p$ e os homomorfismos projeção $\pi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$, para cada $i \in \mathbb{N}$. No capítulo de grupos profinitos vamos ver que un sistema de vizinhanças para x consiste das imagens

inversas $\pi_i^{-1}(x_i + p^i\mathbb{Z})$ para cada $i \in \mathbb{N}$. Assim temos que

$$\begin{aligned}\pi_i^{-1}(x_i + p^i\mathbb{Z}) &= \{y \in \mathbb{Z}_p \mid \pi_i(y) = x_i + p^i\mathbb{Z}\} \\ &= \{y \in \mathbb{Z}_p \mid y_i + p^i\mathbb{Z} = x_i + p^i\mathbb{Z}\} \\ &= \{y \in \mathbb{Z}_p \mid y_i - x_i \in p^i\mathbb{Z}\} \\ &= \{y \in \mathbb{Z}_p \mid y_i \equiv x_i (\mathrm{mod} p^i\mathbb{Z})\}.\end{aligned}$$

Então para cada $n \in \mathbb{N}$ temos uma vizinhança básica de x dada por

$$B_n(x) = \{y \in \mathbb{Z}_p \mid y_n \equiv x_n (\mathrm{mod} p^n\mathbb{Z})\}$$

Observação 2.1.2 Os $B_n(x)$ definidos para cada $x \in \mathbb{Z}_p$ definem a *topologia p-ádica* para o anel de inteiros p-ádicos.

O homomorfismo $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ é injetivo. Assim podemos ver $\mathbb{Z}$ como um subanel de $\mathbb{Z}_p$. Si $p \neq 2$, o elemento $(\sum_{i=0}^{n-1} p^i + p^n\mathbb{Z})_{n\in\mathbb{N}}$ está em $\mathbb{Z}_p$ mas não em $\mathbb{Z}$. Se $p = 2$, $(\sum_{i=0}^{n-1} 4^i + p^n\mathbb{Z})_{n\in\mathbb{N}}$ está em $\mathbb{Z}_2$ e não em $\mathbb{Z}$. Assim $\mathbb{Z} \subsetneq \mathbb{Z}_p$. Finalmente a sequência $(x_i)_{i\in\mathbb{N}}$ converge para $(x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ na topologia p-ádica. Então $\mathbb{Z}_p = \overline{\mathbb{Z}}$.

Lema 2.1.3 *Seja $\mathbb{Z}_p$ o anel de inteiros p-ádicos.*

(a) *Para cada i, $p^i\mathbb{Z}_p$ é o núcleo da projeção $\pi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$. Assim, $p^i\mathbb{Z}_p$ é um subgrupo aberto de $\mathbb{Z}_p$ de índice p^i.*

(b) *Se H é um subgrupo de $\mathbb{Z}_p$ de índice finito, então $H = p^i\mathbb{Z}_p$ para algum $i \in \mathbb{N}$.*

(c) *0 é o único subgrupo fechado de $\mathbb{Z}_p$ de índice infinito.*

(d) *$p\mathbb{Z}_p$ é o único subgrupo maximal fechado de $\mathbb{Z}_p$.*

(e) *Todos os subgrupos fechados não trivias de $\mathbb{Z}_p$ são isomorfos a $\mathbb{Z}_p$.*

Cada elemento $x = (x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ de $\mathbb{Z}_p$ tem uma única representação como uma série formal de potências $\sum_{i=0}^{\infty} a_i p^i$, com $0 \leq a_i < p$ para todo i. Necessariamente, $x_n \equiv \sum_{i=0}^{n-1} a_i p^i \mod p^n$, para cada $n \in \mathbb{N}$.

Lema 2.1.4 *Seja $\alpha : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ um epimorfismo com $n \geq 1$ e H um subgrupo fechado de $\mathbb{Z}_p$. Suponha $\alpha(H) = \mathbb{Z}/p^n\mathbb{Z}$. Então $H = \mathbb{Z}_p$.*

2.2 O grupo de Prüfer

Definição 2.2.1 Para cada $n \in \mathbb{N}$ consideremos o grupo quociente $\mathbb{Z}/n\mathbb{Z}$ e os homomorfismos canônicos $\sigma_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ definidos por $\sigma_{mn}(x + n\mathbb{Z}) = x + m\mathbb{Z}$, para $m|n$. O limite inverso $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ é o *grupo de Prüfer*. Este grupo satisfaz os seguintes items:

(i) A aplicação $\delta_i : \mathbb{Z} \to \hat{\mathbb{Z}}$ definida por $\delta_i(a) = (a+n\mathbb{Z})_{n\in\mathbb{N}}$ é um homomorfismo injetivo.

(ii) A sequência $(x_i)_{i\in\mathbb{N}}$ converge para $x = (x_i + n\mathbb{Z})_{n\in\mathbb{N}}$ na topologia p-ádica. Portanto $\mathbb{Z}$ é denso em $\hat{\mathbb{Z}}$.

(iii) $\hat{\mathbb{Z}}$ é o fecho do subgrupo gerado por 1.

(iv) Vamos escrever $\hat{\mathbb{Z}} = \langle 1 \rangle$ e dizemos que 1 gera $\hat{\mathbb{Z}}$.

(v) Os subgrupos $n\hat{\mathbb{Z}}$ de $\hat{\mathbb{Z}}$ formam uma base de vizinhanças de 0 na topologia induzida.

Lema 2.2.2 *Para cada $n \in \mathbb{N}$, $n\hat{\mathbb{Z}}$ é um subgrupo aberto de $\hat{\mathbb{Z}}$ de índice n e $n\hat{\mathbb{Z}} \equiv \hat{\mathbb{Z}}$. Se H é um subgrupo de $\hat{\mathbb{Z}}$ de índice n, então $H = n\hat{\mathbb{Z}}$.*

Lema 2.2.3 *O grupo $\hat{\mathbb{Z}}$ é topológicamente isomorfo ao produto cartesiano $\prod \mathbb{Z}_p$ onde p varia em todos os números primos.*

Capítulo 3

p-Grupos finitos

Neste capítulo daremos uma introdução aos p-grupos finitos que desempnham um papel fundamental na teoria de grupos finitos e na teoria de grupos pro-p. As primeiras definições são obtidas do artigo de Gustavo. A. Fernández [8] e para desenvolver a parte de automorfismos de grupos finitos usamos o trabalho de David. A. Craven [6] e os teoremas de Sylow podem ser encontrados em [18]. Ao final do presente capítulo fazemos menção aos trabalhos anteriores ao trabalho de J. González e A. Jaikin [13] que resolveram o problema para casos especiais de p-grupos finitos.

3.1 p-Grupos finitos

Definição 3.1.1 Seja p um primo. Um p-grupo finito G é um grupo finito cuja ordem é uma potência de p.

O grupo $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$ de inteiros módulo p com a operação de adição é um grupo cíclico de ordem p e portanto o primeiro exemplo de um p-grupo finito. Assim temos também que para cada $n \in \mathbb{N}$, $\mathbb{Z}/p^n\mathbb{Z}$ é um p-grupo finito.

Seja $\Gamma = \mathrm{GL}_n(\mathbb{Z}_p)$ o grupo de todas as matrizes invertíveis $n \times n$ sobre $\mathbb{Z}_p$. Definamos

$$\Gamma_i = \{\gamma \in \Gamma \mid \gamma \equiv 1_n (\mathrm{mod} p^i)\},$$

para cada i. Temos que $|\Gamma_1 : \Gamma_i| = p^{n^2(i-1)}$. Assim os grupos quocientes Γ_1/Γ_i são p-grupos finitos.

Teorema 3.1.2 *Seja G um p-grupo finito e N um subgrupo normal não trivial de G. Então $N \cap Z(G) \neq 1$. Em particular, o centro de um p-grupo finito não trivial é não trivial.*

Demonstração. Observe que G age sobre N por conjugação, pois N é normal em G. Temos que $|Orb_G(n)| = |G : C_G(n)|$ para cada $n \in \mathbb{N}$ e G é um p-grupo, portanto o comprimento de cada órbita é uma potência de p. Além disso, as órbitas de comprimento 1 se correspondem aos elementos em N os quais comutam com qualquer elemento de G, logo o número de órbitas distintas de comprimento 1 é igual a $|N \cap Z(G)|$. Como N é a união disjunta de suas orbitas, segue que

$$|N| = |N \cap Z(G)| + \sum_{i=1}^{r} |Orb_G(n_i)|$$

onde $n_1, ..., n_r$ são os representantes das orbitas de comprimento maior do que 1. Fazendo na última desigualdade módulo p e considerando que $|N| > 1$, temos que

$$|N \cap Z(G)| \equiv 0 \pmod{p}$$

e assim segue que $N \cap Z(G) \neq 1$. □

Corolário 3.1.3 *Seja G um p-grupo finito. Se H é um subgrupo normal de G de ordem p então H é central em G (i.e. $H \leq Z(G)$).*

As seguintes consequências do Teorema 3.1.2 são muito importantes na teoria de p-grupos finitos.

Teorema 3.1.4 *Seja G um p-grupo finito.*

(i) *Se $H \lneq G$ então $H \lneq N_G(H)$.* **(a condição do normalizador)**

(ii) *Se M é um subgrupo maximal de G então M é normal em G e $|G : M| = p$.*

Demonstração. (i) Provaremos isto por indução sobre $|G|$. O resultado é obvio se $|G| = p$, por isso vamos supor que $|G| > p$. Se $Z(G)$ não está contido em H então $H \lneq HZ(G) \leq N_G(H)$ e acabamos. Assim podemos supor que $Z(G) \leq H$. Como $Z(G) \neq 1$, da hipótese indutiva obtemos que $H/Z(G) \lneq N_{G/Z(G)}(H/Z(G)) = N_G(H)/Z(G)$ e consequentemente $H \lneq N_G(H)$.

(ii) Se M é maximal em G, obtemos de (i) que $N_G(M) = G$, isto é, $M \lhd G$. Então o grupo quociente G/M é um p-grupo que não possui subgrupos não triviais. Portanto G/M tem ordem p e $|G : M| = p$. □

O seguinte resultado mostra que os subgrupos de um p-grupo estão bastante bem situados.

Teorema 3.1.5 *Seja G um p-grupo finito de ordem p^m.*

(i) *Se N é um subgrupo normal de G de ordem p^k, então existe uma série*

$$1 = G_0 \leq G_1 \leq ... \leq G_k = N \leq ... \leq G_m = G \tag{3.1}$$

tal que $G_i \lhd G$ e $|G_{i+1} : G_i| = p$ para todo i. Em particular, um p-grupo tem subgrupos normais de cada ordem possível.

(ii) *Se H é um subgrupo de G de ordem p^k, então existe uma serie*

$$1 = G_0 \leq G_1 \leq ... \leq G_k = H \leq ... \leq G_m = G \tag{3.2}$$

tal que $G_i \lhd G_{i+1}$ e $|G_{i+1} : G_i| = p$ para todo i. Então cada subgrupo de um p-grupo é subnormal.

Demonstração. (i) Provaremos isto por indução sobre $|G|$. Suponha primeiro que $N \neq 1$. Então do Teorema 3.1.2 obtemos $Z = N \cap Z(G) \neq 1$. Escolhamos qualquer G_1 em Z de ordem p. Então G_1 é normal em G e o resultado segue por aplicação da hipótese indutiva para G/G_1 e para o subgrupo normal N/G_1. Finalmente, se $N = 1$ então podemos tomar qualquer uma das séries obtidas do argumento anterior.

(ii) Primeiro, lembremos que um subgrupo H de G é subnormal se existe uma cadeia finita de subgrupos do grupo G onde cada subgrupo da cadeia é normal no seguinte subgrupo começando em H e terminando em G, i.e. se existem $H_0, H_1, ..., H_k \leq G$ tal que

$$H = H_0 \leq H_1 \leq ... \leq H_k \leq G$$

e $H_i \lhd H_{i+1}$, para cada $i = 0, .., k-1$.
Para a prova usaremos indução sobre $|G|$. Se $H = G$ então podemos usar a parte (i) para obter a serie procurada. De outra forma H está contido num subgrupo maximal M de G e pela hipótese indutiva obtemos uma serie como (3.2) cujo último termo é M. Como já sabemos do Teorema 3.1.4 que $M \lhd G$, a prova está completa. □

Seja G um grupo e $H \leq G$. Então H se chama *característico* se para qualquer automorfismo σ de G, temos que $\sigma(H) \subseteq H$, denotaremos por $H \text{char} G$. Assim temos que G e o subgrupo trivial $\{e\}$ são característicos. Exemplos de subgrupos característicos são o subgrupo derivado $[G, G]$ e o centro $Z(G)$. Seja $g \in G$, um *automorfismo interior* é definido como $T_g(x) = gxg^{-1}$, para cada $x \in G$. Os subgrupos normais são característicos se consideramos somente os automorfismos interiores, mas não necessariamente se nós consideramos todos os automorfismos.

Para um grupo finito G, a interseção de seus subgrupos maximais é chamado o *subgrupo de Frattini* de G e é denotado por $\Phi(G)$. Como a imagem de um subgrupo maximal sob um automorfismo de G é também um subgrupo maximal, $\Phi(G)$ é um subgrupo característico de G. Uma razão pela qual este subgrupo tem um papel importante é o seguinte resultado.

Teorema 3.1.6 *Seja G um grupo finito e sejam $x_1, ..., x_m \in G$. Então temos que $G = \langle x_1, ..., x_n \rangle$ se e somente se $G/\Phi(G) = \langle x_1\Phi(G), ..., x_n\Phi(G) \rangle$.*

Demonstração. É suficiente mostrar a condição necessária do Teorema. Se $\langle x_1, ..., x_n \rangle$ não é igual a G então está contido num subgrupo maximal M de G. Assim $\langle x_1\Phi(G), ..., x_n\Phi(G) \rangle$ está contido em $M/\Phi(G)$, que é um subgrupo próprio de $G/\Phi(G)$, o que dá uma contradição. Portanto necessariamente $G = \langle x_1, ..., x_n \rangle$. □

Teorema 3.1.7 (**O Teorema da Base de Burnside**). *Seja G um p-grupo finito. Então*

(i) *$G/\Phi(G)$ é um p-grupo abeliano elementar e portanto pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$.*

(ii) *O conjunto $\{x_1, ..., x_d\}$ é um conjunto minimo de geradores para G se e somente se $\{x_1\Phi(G), ..., x_d\Phi(G)\}$ é uma base para $G/\Phi(G)$.*

(iii) *O minimo numero d de geradores para o grupo G coincide com a dimensão de $G/\Phi(G)$ como um $\mathbb{F}_p$-espaço vetorial, i.e. $|G : \Phi(G)| = p^d$.*

Demonstração. (i) Temos que mostrar que $x\Phi(G)y\Phi(G) = y\Phi(G)x\Phi(G)$ e $(x\Phi(G))^p = \Phi(G)$ para todo $x, y \in G$, isto é $x^{-1}y^{-1}xy, x^p \in \Phi(G)$. Pela definição de $\Phi(G)$, é suficiente mostrar que $x^{-1}y^{-1}xy, x^p \in M$ para qualquer subgrupo maximal M de G. Isto é obvio pois de acordo com o Teorema 3.1.4, G/M é um grupo de ordem p.

(ii) Do Teorema anterior temos que $S = \{x_1, ..., x_d\}$ é um conjunto de geradores para G se e somente se $\overline{S} = \{x_1\Phi(G), ..., x_d\Phi(G)\}$ é um conjunto de geradores para $G/\Phi(G)$. Portanto S é um conjunto minimo de geradores se e somente se $\overline{S}$ for, que equivale $\overline{S}$ ser uma base para $G/\Phi(G)$.

(iii) Isto segue imediatamente de (ii). □

Se G fosse um grupo finito, denotamos por $d(G)$ o número mínimo de geradores para G.

Definição 3.1.8 Seja G um grupo finito e seja p um primo. Cada subgrupo de G cuja ordem seja a maior possível potência de p dividendo $|G|$ é chamado um *p-subgrupo de Sylow* de G. Um p-subgrupo de Sylow para algum p é chamado um *p-subgrupo de Sylow*.

Nos seguintes teoremas nós consideramos G um grupo finito e p um número primo dividendo a ordem de G.

Primeiro Teorema de Sylow. *G contém um p-subgrupo de Sylow e cada p-subgrupo de G está contido num p-subgrupo de Sylow de G.*

Segundo Teorema de Sylow. *Todos os p-subgrupos de Sylow de G são conjugados.*

Terceiro Teorema de Sylow. *Seja n_p o número de p-subgrupos de Sylow de G. Escrevamos $|G| = p^k m$, onde p não divide m. Então*

$$n_p \equiv 1 \bmod p \quad \text{e} \quad n_p | m.$$

Agora vamos ver alguns exemplos de grupos de automorfismos de p-grupos finitos.

3.2 Automorfismos de grupos finitos

Dado um grupo G, um automorfismo de G é um isomorfismo de G para G, em outras palavras, é um homomorfismo que é ao mesmo tempo injetivo e sobrejetivo. Como o inverso de um automorfismo é um automorfismo e a composição de automorfismos também é um automorfismo, temos que o conjunto de todos os automorfismos de G é um grupo. Denotamos este grupo por $Aut(G)$.

Proposição 3.2.1 *Seja G um grupo nilpotente finito, e seja $G = P_1 \times P_2 \times ... \times P_n$, onde P_i são os p-subgrupos de Sylow de G. Então*

$$\mathrm{Aut}(G) = \mathrm{Aut}(P_1) \times \mathrm{Aut}(P_2) \times \cdots \times \mathrm{Aut}(P_n).$$

Essa proposição enfoca a atenção na estrutura dos p-grupos finitos e os automorfismos dos p-grupos finitos.

Lema 3.2.2 *Seja $g(n)$ o número de grupos de ordem n. Então*

(i) *$g(p) = 1$ para p primo.*

(ii) *Se* $p < q$, *então* $g(pq) = 1$ *se* $q \not\equiv 1 \bmod p$, *e* $g(pq) = 2$ *outro caso.*

(iii) $g(p^2) = 2$.

(iv) $g(p^3) = 5$.

A partir disso, podemos ver que o número de grupos de ordem n depende mais da forma de n do que de seu tamanho. Observemos a seguinte tabela onde comparamos os valores para n e $g(n)$.

n	$g(n)$	n	$g(n)$	n	$g(n)$	n	$g(n)$
1	1	11	1	21	2	31	1
2	1	12	5	22	2	32	51
3	1	13	1	23	1	33	1
4	2	14	2	24	15	34	2
5	1	15	1	25	2	35	1
6	2	16	14	26	2	36	14
7	1	17	1	27	5	37	1
8	5	18	5	28	4	38	2
9	2	19	1	29	1	39	2
10	2	20	5	30	4	40	14

(Section 1.3 - The Theory of p-Groups 2008)

O resultado $g(32) = 51$ deve fazer acreditar que, se alguém escolher um grupo G de ordem ao máximo n ao acaso, então quando n tende para o infinito, a probabilidade de que G seja um p-grupo tende para 1 e, de fato, G é um 2-grupo não abeliano com probabilidade 1.

Isto junto com os Teoremas de Sylow mostram que os p-grupos finitos tem um papel muito importante na teoria de grupos finitos.

Proposição 3.2.3 *Seja* G *um grupo abeliano elementar de ordem* p^n. *Então* $\mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{F}_p)$, *o grupo de* $n \times n$ *matrizes invertíveis sobre* $\mathbb{F}_p$.

Demonstração. Observe que existem $p^n - 1$ elementos de ordem p em G. Suponha que G é gerado por $x_1, ..., x_n$. Um automorfismo do grupo finito é determinado unicamente pela sua ação nos geradores de um grupo, então, se sabemos onde enviar o x_i, nós criamos nosso automorfismo. Escrevemos ϕ para este automorfismo.

Também precisamos ver que qualquer elemento de G pode ser expresso como um produto

$$\prod_{i=1}^{n} x_i^{b_i}.$$

onde os b_i são inteiros únicos tais que $0 \leq b_i \leq p - 1$. Então G não pode ser gerado por menos de n elementos, em outras palavras não podemos "desperdiçar"um gerador atribuindo-o para algum lugar que já podemos expressar em termos de outros geradores. Emprestando um termo da álgebra linear, nós gostaríamos que as imagens dos geradores fossem "linearmente independentes".

Notamos que x_1 pode ser enviado para qualquer elemento de ordem p, então há $p^n - 1$ escolhas para $\phi(x_1)$. Agora temos que decidir o que fazemos com x_2; não podemos envia-lo

para $\langle x_1 \rangle$, já que estaríamos desperdiçando um gerador, e por isso existem $p^n - p$ escolhas para $\phi(x_2)$. Então $\langle x_1, x_2 \rangle$ tem ordem p^2, e assim existem $p^n - p^2$ escolhas para $\phi(x_3)$, e assim por diante, até obter

$$|\mathrm{Aut}(G)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1}),$$

que é a ordem de $\mathrm{GL}_n(\mathbb{F}_p)$. Então, se pudermos encontrar um homomorfismo de $\mathrm{Aut}(G)$ para $\mathrm{GL}_n(\mathbb{F}_p)$, e mostrar que é injetivo, teremos terminado.

Usando o fato que qualquer elemento de G pode ser expresso como um múltiplo dos elementos da base, procedemos a escrever uma matriz para ϕ: seja $A_\phi = (a_{i,j}^{(\phi)})$, onde

$$\phi(x_j) = \sum_{i=1}^{n} a_{i,j}^{(\phi)} x_i.$$

Como A_ϕ é unicamente determinado, temos

$$A_\phi(x_1, x_2, ..., x_n) = (\phi(x_1), \phi(x_2), ..., \phi(x_n)).$$

A função $\Phi : \mathrm{Aut}(G) \to \mathrm{GL}_n(p)$ dada por $\phi \mapsto A_\phi$ é injetiva, como os coeficientes $a_{i,j}^{(\phi)}$ são unicamente determinados. Devemos mostrar que este é um homomorfismo. Se ϕ e ψ são dois elementos de $\mathrm{Aut}(G)$, então

$$\begin{aligned}
(\Phi\psi)(\Phi\phi)(x_1) &= \psi(\sum_{i=1}^{n} a_{i,j}^{(\phi)} x_i) \\
&= \sum_{i=1}^{n}\sum_{k=1}^{n} a_{i,j}^{(\phi)} a_{i,j}^{(\psi)} x_k \\
&= \sum_{i=1}^{n}(\sum_{i=1}^{n} a a_{i,j}^{(\phi)} a_{i,j}^{(\psi)}) x_k \\
&= \Phi(\psi\phi)(x_i).
\end{aligned}$$

assim $\Phi(\psi\phi) = (\Phi\psi)(\Phi\phi)$ como precisamos. Portanto $\mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{F}_p)$. □

Proposição 3.2.4 *Seja G um grupo cíclico de ordem n. Então o $\mathrm{Aut}(G)$ é abeliano e tem ordem $\phi(n)$, onde ϕ denota a função ϕ de Euler.*

Demonstração. Seja $G = \langle x \rangle$. Então um automorfismo G deve enviar x para outro gerador de G, o que obviamente deve ter ordem n, e assim reduz-se a descobrir quantos elementos de C_n tem ordem n. Se n e m são coprimos, com $1 \leq m \leq n$, então o primeiro inteiro k para o qual $x^{mk} = 1$ é $k = n$. Portanto, se m e n são coprimos então x^m tem ordem n. No outro lado, seja d o $\mathrm{mdc}(m, n)$ e suponha que x^m tem ordem n. Como $(x^m)^{n/d} = 1$ (pois mn/d é divisível por n), $n \leq n/d$; isto claramente implica que $d = 1$ e assim m e n são coprimos.

Temos provado que x^m tem ordem n se e somente se m e n são coprimos, e portanto $|\mathrm{Aut}(G)| = \phi(n)$, pois a função ϕ de Euler é simplesmente a quantidade de números $m \leq n$ coprimos com n.

Para ver que $\mathrm{Aut}(G)$ é abeliano, observemos que todos os automorfismos tem a forma $x \mapsto x^m$; se $\phi : x \mapsto x^m$ e $\psi : x \mapsto x^k$ são dois automorfismos, então

$$(\psi\phi)x = \psi(\phi x) = \psi x^m = x^{mk} = \phi x^k = (\phi\psi)x.$$

e assim $\mathrm{Aut}(G)$ é abeliano. □

Podemos melhorar a proposição anterior no caso em que o grupo cíclico é de ordem primo.

Proposição 3.2.5 *Seja $G \cong C_p = \langle x \rangle$. Então $\mathrm{Aut}(G)$ é cíclico de ordem $p-1$.*

Demonstração. Nós já sabemos que $\mathrm{Aut}(G)$ é abeliano de ordem $p-1$ (pois qualquer número menor que p é coprimo com p), então somente precisamos mostrar que $\mathrm{Aut}(G)$ é cíclico. Para ver isso, observemos que $\mathrm{Aut}(G)$ é o mesmo que multiplicar os inteiros diferentes de zero módulo p. Então como os inteiros módulo um primo formam um corpo, $\mathrm{Aut}(G)$ é cíclico.

Consideremos dois automorfismos $\phi_m : x \mapsto x^m$ e $\phi_k : x \mapsto x^k$, onde m e k estão entre 1 e $p-1$. Então $\phi_m\phi_k$ é dado por

$$\phi_{mk} : x \mapsto x^{mk}.$$

então obtemos um homomorfismo de $\mathrm{Aut}(G)$ para o grupo multiplicativo de inteiros módulo p por

$$\Phi : \mathrm{Aut}(G) \to (\mathbb{Z}/p\mathbb{Z})^*, \qquad \Phi : \phi_m \mapsto m.$$

[Onde, $F^* = F\backslash\{0\}$ denota o subgrupo multiplicativo de F.] Portanto $\mathrm{Aut}(G)$ é cíclico de ordem $p-1$, como queríamos. □

Observe que neste caso $|G| > |\mathrm{Aut}(G)|$ então $|G| \nmid |\mathrm{Aut}(G)|$. Em geral na maioria dos casos de p-grupos finitos, $|G|$ divide $|\mathrm{Aut}(G)|$.

De agora em diante vamos seguir o trabalho de J. González-Sánchez. e A. Jaikin-Zapirain [13].

Uma questão bem conhecida (ver, por exemplo, [[37], Problema 12.77]) pergunta se é verdade que $|G|$ divide $|\mathrm{Aut}(G)|$ para cada p-grupo finito não-abeliano G. Não está claro quem lançou essa pergunta pela primeira vez; o primeiro resultado nesse sentido que nós encontramos na literatura é devido a Schenkman [7], que foi publicado há mais de 60 anos. Nesse artigo, Schenkman mostrou que isso é verdade para p-grupos finitos não abelianos da classe 2 (a prova tem uma erro que foi corrigido por Faudree em [26]). Mais tarde, também foi estabelecido para p-grupos de exponente p em [32], para p-grupos de classe maximal em [1], para p-grupos com centro de ordem p em [38], para p grupos meta cíclicos quando p é ímpar em [27], para p-grupos central-meta-cíclicos quando p é ímpar em [30], para p-grupos p-abelianos em [31] (veja também [3]), para p-grupos modulares finitos em [31], para alguns produtos centrais em [10, 16], para p-grupos com centro de índice ao máximo p^4 em [29], para p-grupos com subgrupo Frattini cíclico em [34], para p-grupos de ordem ao máximo p^6 em [29, 35], para p-grupos de ordem ao máximo p^7 em [23], para p-grupos de coclasse 2 em [33] (veja também um resultado relacionado em [4]), e para p-grupos G tais que $(G, Z(G))$ é uma "Camina pair" em [21].

Todos esses resultados parciais mostraram a dificuldade de obter um contra-exemplo. O trabalho realizado por J. González-Sánchez. e A. Jaikin-Zapirain [13] utiliza técnicas pro-p, e o objetivo é mostrar o seguinte Teorema que é o resultado principal deste trabalho.

Teorema principal. *Para cada primo p existe uma família de p-grupos finitos $\{U_i\}$ tal que*

$$\lim_{i\to\infty} |U_i| = \infty \qquad \text{e} \qquad \limsup_{i\to\infty} \frac{|\mathrm{Aut}U_i|}{|U_i|^{40/41}} < \infty.$$

Em particular, para cada primo p, existe um p-grupo finito não abeliano tal que $|\mathrm{Aut}(G)| < |G|$.

A construção em [13] consiste de duas partes que vamos desenvolver neste trabalho.

(i) **Primeira parte.** Vamos considerar um grupo U pro-p infinito finitamente gerado tal que $\dim(\mathrm{Aut}(U)) < \dim(U)$, onde $\dim U$ é definida como $\dim_{\mathbb{Q}_p}\mathbf{L}(U)$, onde $\mathbf{L}(U)$ é uma $\mathbb{Q}_p$-álgebra de Lie associada a U. Podemos fazer isto pois U é um grupo pro-p p-ádico analítico e portanto $\mathrm{Aut}(U)$ é um grupo profinito p-ádico analítico.

(ii) **Segunda parte.** Escrevamos U como um limite inverso da família de p-grupos finitos $\{U_i\}$ onde $U_i = U/U^{p^i}$. Assim $U = \varprojlim U_i$, e por isso $\mathrm{Aut}U_i = \varprojlim \mathrm{Aut}U_i$, de onde esperamos que para algum i podamos ter $|\mathrm{Aut}(U_i)| < |U_i|$.

Para ter uma ideia sobre a primeira parte, como G é um grupo pro-p uniforme, temos que

$$\dim\ \mathrm{Aut}(U) = \dim_{\mathbb{Q}_p}\mathrm{Der}\mathbf{L}(U),$$

onde $\mathrm{Der}\mathbf{L}(U)$ é uma $\mathbb{Q}_p$-álgebra de derivações internas de $\mathbf{L}(U)$. Um exemplo de álgebras de Lie L com $\dim \mathrm{Der}(L) < \dim L$ é construída por Sato [36] e vamos discutir isso no capítulo 7 deste trabalho; esta álgebra é construída sobre $\mathbb{Q}$ e tem dimensão 41 com centro de dimensão 1, assim a álgebra consiste somente de derivações internas e portanto tem dimensão 40.

A segunda parte é baseada no analise da primeira cohomologia de grupos $H^1(U, L_i)$, onde $L_i = \mathbf{log}(U)/p^i\mathbf{log}(U)$ e $\mathbf{log}(U)$ é o anel de Lie correspondente ao grupo pro-p uniforme U pela correspondência de Lazard. Temos que $\mathrm{Der}(\mathbf{L}(U)) = \mathrm{Inn}(\mathbf{L}(U))$; segue que $\mathrm{Der}(\mathbf{log}(U))$ é finito e portanto

$$H^1_{cts}(U, \mathbf{log}(U)) \cong \mathrm{Der}(\mathbf{log}(U))$$

é também finito. Isto implica a existência de uma cota superior para $|H^1(U, L_i)|$. Agora se definimos $U_i = U/U^{p^i}$ teremos uma cota superior para $|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)|$ e culminamos com a prova.

Capítulo 4

Grupos Uniformes

Este é o capítulo com mais conteúdo teórico que será útil em capítulos posteriores. Na seção 4.1, falaremos sobre grupos profinitos e para o qual usaremos o conceito de limites inversos e mostraremos como um grupo de Galois é um exemplo de um grupo profinito (exemplo obtido de [5]). Na seção 4.2, daremos tratamento especial aos grupos pro-p e o resultado mais importante é que cada grupo pro-p é o limite inverso de p-grupos finitos; daremos alguns exemplos desses grupos. Na Seção 4.3, faremos uma breve menção aos grupos procíclicos e suas equivalências. Nas seções 4.4 e 4.5, mostraremos as principais propriedades dos p-grupos *powerful* e definiremos o posto de um grupo finito e um grupo pro-p. Os grupos uniformes serão tratados na seção 4.6, onde definiremos sua dimensão e mostraremos que $(G, +)$ é um $\mathbb{Z}_p$-módulo livre; além disso, vamos estudar os subgrupos pro-p de $\mathrm{GL}_n(\mathbb{Z}_p)$. Finalmente, na seção 4.7, mostraremos que o $\mathbb{Z}_p$-módulo livre $(G, +)$ se torna uma álgebra de Lie sobre $\mathbb{Z}_p$. O livro usado para todas as seções deste capítulo foi 'Analytic Pro-p Groups' [11].

4.1 Grupos Profinitos

Definição 4.1.1 Um *grupo profinito* é um grupo topológico, compacto e Hausdorff tal que seus subgrupos abertos formam uma base de vizinhanças para a unidade.

Proposição 4.1.2 *Seja G um grupo profinito.*

(i) *Cada subgrupo aberto de G é fechado, tem índice finito em G e contém um subgrupo normal aberto de G. Um subgrupo fechado de G é aberto se e somente se tem índice finito. A família de todos os subgrupos abertos de G tem como interseção o conjunto $\{1\}$.*

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

(iii) *Para qualquer subconjunto X de G,*

$$\overline{X} = \bigcap_{N \lhd_o G} XN$$

Se X é um subgrupo de G então

$$\overline{X} = \bigcap\{K \mid X \leq K \leq_o G\}$$

(iv) *Se X e Y são subconjuntos fechados de G então o conjunto $XY = \{xy \mid x \in X, y \in Y\}$ também é fechado. Se X é fechado e n é um inteiro então o conjunto $\{x^n \mid x \in X\}$ é fechado.*

(v) *Seja H um subgrupo fechado de G. Então H (com a topologia induzida) é um grupo profinito. Cada subgrupo aberto de H é da forma $H \cap K$ com $K \leq_o G$.*

(vi) *Seja N um subgrupo normal fechado de G. Então G/N (com a topologia quociente) é um grupo profinito, e o homomorfismo natural $G \to G/N$ é uma aplicação contínua aberta e fechada.*

(vii) *Uma sequência (g_i) em G converge se e somente se é uma sequência de Cauchy: i.e. para cada $N \lhd_o G$ existe $n = n(N)$ tal que $g_i^{-1}g_j \in N$ para todo $i \geq n$ e $j \geq n$.*

A demonstração desta Proposição segue das definições.

Podemos definir um grupo profinito também como um limite inverso (seção 1.3 do capítulo 1). Seja G um grupo e seja A uma família de subgrupos normais de G. Suponha que a família A está ordenada por inclusão. Então obtemos um sistema inverso $\{(G/N)_{N\in A}\}$ cujas aplicações são os epimorfismos naturais $G/N \to G/M$ sempre que $N \leq M$. Assim podemos ter a seguinte proposição.

Proposição 4.1.3 *Se G é um grupo profinito então G é isomorfo topologicamente a $\varprojlim(G/N)_{N\lhd_o G}$. No outro lado, o limite inverso de um sistema inverso de grupos finitos é um grupo profinito.*

Demonstração. Seja $L = \varprojlim(G/N)_{N\lhd_o G}$. Consideremos o homomorfismo natural $\rho : G \to \prod G/N$, dado por $\rho(g) = (gN)_{N\lhd_0 G}$. Como $\bigcap_{N\lhd_0 G} N = 1$ temos que ρ é injetiva e assim $\rho(G) \leq L$. Agora, seja $(g_N N) \in L$, então cada coleção finita de classes $g_N N$ tem interseção não vazia e como essas classes são também subconjuntos fechados do espaço compacto G, segue que $\bigcap_{N\lhd_o G} g_N N$ é não vazia. Escolhamos g nessa interseção. Então $\rho(g) = (g_N N)$, logo ρ é sobrejetiva.

Seja $P \lhd_o G$ e definamos

$$M(P) = \prod_{N\not\geq P} G/N \times \prod_{N\geq P} \{1\} \leq \prod_{N\lhd_o G} G/N,$$

assim os subgrupos $M(P) \cap L$ é uma base para as vizinhanças de 1 em L e para cada P temos que $\rho^{-1}(M(P)) = P$ é aberto em G, portanto ρ é contínuo. Mas cada isomorfismo contínuo entres grupos compactos Hausdorff é um isomorfismo topológico portanto ρ é um isomorfismo topológico.

Para a outra implicação, consideremos um sistema inverso de grupos finitos $\{G_\lambda\}_{(\lambda\in I)}$ (os grupos finitos munidos com a topologia discreta). Assim $\prod_{\lambda\in I} G_\lambda$ é Hausdorff e pelo teorema de Tychonoff (Teorema 1.1.4 (iii) Cap. 1) é compacto. Da definição de produto topológico, cada vizinhança de 1 contém um subgrupo da forma $M(S) = \prod_{\lambda\notin S} G_\lambda \times \prod_{\lambda\in S}\{1\}$

para algum subconjunto finito S de I. Portanto $\prod G_\lambda$ é um grupo profinito. Agora somente temos que mostrar que $\varprojlim G_\lambda = L$ é um subgrupo fechado. Seja $l = (g_\lambda) \in \prod G_\lambda \backslash L$, então existem $\upsilon > \mu$ em I tais que $\pi_{\upsilon\mu}(g_\upsilon) \neq g_\mu$. Temos que $lM(\upsilon, \mu)$ é uma vizinhança aberta de $l \in \prod G_\lambda$ e $lU(\upsilon, \mu) \cap L = \emptyset$. Mostrando finalmente que $\prod G_\lambda \backslash L$ é aberto em $\prod G_\lambda$ e obtemos o resultado. □

Dado um grupo topológico G, dizemos que um subconjunto X de G *gera* G *topologicamente* se $G = \overline{\langle X \rangle}$.

Proposição 4.1.4 *Sejam G um grupo profinito, H um subgrupo fechado de G, $X \subseteq H$ e d um inteiro positivo. Então*

(i) $H = \overline{\langle X \rangle}$ se e somente se $HN/N = \overline{\langle XN/N \rangle}$ para cada $N \lhd_o G$.

(ii) Se HN/N pode ser gerado por d elementos para cada $N \lhd_o G$, então H pode ser gerado topologicamente por um subconjunto de d elementos.

Demonstração. (i) Segue da Proposição 4.1.2 (iii). (ii) Para cada $N \lhd_o G$, seja Z_N o conjunto de todas as d-tuplas de elementos de G/N que geram HN/N. Cada Z_N é finito e não vazio. Se $\pi_{MN} : G/M \to G/N$ é a projeção natural para $M \leq N$, ambos subgrupos normais abertos de G, então $\pi_{MN}(Z_M) \subseteq Z_N$, e por isso $\{Z_N\}_{N \lhd_o G}$ torna-se um sistema inverso. Pela Proposição 1.3.5 do capítulo 1 o limite inverso desse sistema inverso é não vazia. Seja agora $(X_N) \in \varprojlim Z_N$. Então existem $x_1, ..., x_d$ elementos em G tais que para cada $N \lhd_o G$, $X_N = (x_1N, ..., x_dN)$ e usando a parte (i) temos que $\{x_1, ..., x_d\}$ gera H topologicamente. □

Um subgrupo de G é *topologicamente característico* se é invariante sob os automorfismos de G.

Proposição 4.1.5 *Sejam G um grupo profinito finitamente gerado e m um inteiro positivo. Então G tem somente um número finito de subgrupos abertos de índice m e cada subgrupo aberto contém um subgrupo aberto topologicamente característico.*

Para a demonstração veja [Proposição 1.6, [11]].

Proposição 4.1.6 *Se G é um grupo profinito finitamente gerado então cada subgrupo aberto de G é finitamente gerado.*

Demonstração. Seja X um conjunto de geradores topológicos para G, e assumimos sem perda de generalidade que $X^{-1} = X$. Seja $H \leq_o G$ e T um transversal (conjunto de representantes de todas as classes laterais) para as classes laterais direita de H em G tal que $1 \in T$; note que T é finito. Para cada $x \in X$ e $t \in T$ existe $s = s(t, x) \in T$ tal que $Htx = Hs$. Definamos

$$Z = \{tx.s(t, x)^{-1} \mid t \in T, x \in X\},$$

e mostramos que $H = \overline{\langle Z \rangle}$.

Consideremos o subgrupo $M = \overline{\langle Z \rangle}$ de G. Se $a \in M$, $t \in T$ e $x \in X$, então

$$at.x = atxs(t,x)^{-1}.s(t,x) \in MT;$$

assim $MTX = MT$. Como $1 \in MT$ e $X = X^{-1}$, segue que $MT \supseteq \langle X \rangle$; e como T é finito MT é fechado e portanto $MT = G$. Também $M \leq H$ e assim

$$H = MT \cap H = M(T \cap H) = M.$$

Como Z é um conjunto finito, temos que H é finitamente gerado. □

Definição 4.1.7 Seja G um grupo profinito. O *subgrupo de Frattini* de G é definido por

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

Proposição 4.1.8 *Seja G um grupo profinito.*

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

(ii) *Se $K \lhd_c G$ e $K \leq \Phi(G)$ então $\Phi(G/K) = \Phi(G)/K$.*

(iii) *Para um subconjunto X de G os seguintes são equivalentes:*

(a) *X gera G topologicamente.*

(b) *$X \cup \Phi(G)$ gera G topologicamente.*

(c) *$X\Phi(G)/\Phi(G)$ gera $G/\Phi(G)$ topologicamente.*

Para a demonstração veja [Proposição 1.9, [11]].

Claramente cada grupo finito é um grupo profinito. O grupo de inteiros p-ádicos e o grupo de Prüfer são também exemplos de grupos profinitos. Exemplos mais sofisticados de grupos profinitos vêm da teoria de Galois.

4.1.1 Grupos profinitos como grupos de Galois

Consideramos uma extensão de Galois $L|K$ (i.e. L é um corpo de decomposição separável possivelmente infinito de uma família de polinômios sobre um corpo K) então L é a união $L = \bigcup\{L_i \mid i \in I\}$ de suas subextensões finitas de Galois $L_i|K$. O conjunto $\{L_i \mid i \in I\}$ é um conjunto parcialmente ordenado por inclusão. Escrevamos $i \succeq j$ quando $L_i \supseteq L_j$. Assim para o conjunto $\{L_i \mid i \in I\}$ se $i, j \in I$ existe $k \in I$ tal que $k \succeq i$ e $k \succeq j$.

Podemos definir o grupo de Galois $\mathrm{Gal}(L|K)$ como o grupo de automorfismos de L que fixam os elementos de K. Cada automorfismo $\alpha \in \mathrm{Gal}(L|K)$ está unicamente determinado por suas restrições $\alpha|_{L_i}$ para cada $i \in I$, e a sobrejetividade de $\phi_i : \mathrm{Gal}(L|K) \to \mathrm{Gal}(L_i/K)$ vem graças a que $L|K$ e suas subextensões $L_i|K$ são normais. No caso de ter $i \succeq j$ então $(\alpha|_{L_i})|_{L_j} = \alpha|L_j$ que é chamada a *condição de compatibilidade*. Se temos $L_i \supseteq L_j$, nesse caso escrivamos $\phi_{j,i} : \mathrm{Gal}(L_i|K) \to \mathrm{Gal}(L_j|K)$ que denota a aplicação de restrição natural, assim podemos escrever a condição de compatibilidade como $\phi_i\phi_{ij} = \phi_j$ quando $i \succeq j$. Expressemos uma condição semelhante em termos de restrições, se $i \succeq j \succeq k$ então $\phi_{ij}\phi_{jk} = \phi_{ik}$.

Seja o grupo de Galois $G := \mathrm{Gal}(L|K)$. Definamos $G_i := \mathrm{Gal}(L_i|K)$ e a aplicação

$$\phi : G \to \prod_{i\in I} G_i, \qquad g \mapsto (\phi_i(g))_{i\in I}$$

induz um isomorfismo de G sobre o grupo

$$G_\phi = \{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid \phi_{ij}(g_i) = g_j \text{ quando } i \succeq j\}.$$

Agora, podemos nós fazer mais uma pergunta, que acontece com a correspondência de Galois? A resposta é que apenas certos subgrupos de G correspondem aos corpos intermediários de $L|K$. Para responder essa questão e saber quais subgrupos desempenham um papel na correspondência de Galois, vamos munir G com a *topologia de Krull*. Consideremos G_i com a topologia discreta, assim $\prod_{i\in I} G_i$ torna-se um grupo topológico totalmente desconexo, compacto e Hausdorff. Logo G_ϕ é fechado e assim G torna-se um grupo topológico totalmente desconexo, compacto e Hausdorff e portanto a estrutura de G é determinada por suas imagens finitas G_i. Além disso, G_ϕ é o limite inverso do sistema inverso $(G_i; \phi_{ij})$ de grupos finitos (Proposição 1.3.3 (1.1)) e portanto G é isomorfo a um grupo profinito.

Se M é um corpo intermediário da extensão $L|K$, então o conjunto G^M de todos os elemento de G que fixam M pode ser descrito em termos das restrições dos automorfismos para subextensões finitas de M. De fato, G^M pode ser escrito como uma interseção de subgrupos abertos-fechados de G e portanto é um subgrupo fechado para a topologia de Krull. Portanto é assim que a correspondência de Galois é generalizada.

4.2 Grupos pro-p

Definicão 4.2.1 Um grupo pro-p é um grupo profinito onde cada subgrupo normal aberto tem índice igual a uma potência de p.

Proposição 4.2.2 *Seja G um grupo profinito*

(i) *Se G é pro-p e $H \leq_c G$ então H é pro-p.*

(ii) *Seja $K \lhd_c G$. Então G é pro-p se e somente se K e G/K são grupos pro-p.*

Demonstração. Segue da definição e da Proposição 4.1.2. □

Proposição 4.2.3 *Um grupo topológico G é um grupo pro-p se e somente se G é topologicamente isomorfo a um limite inverso de p-grupos finitos.*

Demonstração. Suponha que G é pro-p, então é profinito por definição e usando a Proposição 4.1.3 temos que

$$G \cong \varprojlim (G/N)_{N \lhd_o G}$$

sendo cada G/N um p-grupo finito. Para a outra implicação, suponha que $G = \varprojlim (G_\lambda)_{\lambda\in I}$ onde cada G_λ é um p-grupo finito. Então pela Proposição 4.1.3 G é um grupo profinito e temos que cada subgrupo aberto de G contém um subgrupo da forma

$$U(M) = G \cap (\prod_{\lambda\notin M} G_\lambda \times \prod_{\lambda\in M} \{1\})$$

para algum subconjunto finito M de I. Temos que $|G : U(M)|| \prod_{\lambda \in M} |G_\lambda|$ e assim cada subgrupo de G tem índice igual a uma potência de p. □

Proposição 4.2.4 *Seja G é um grupo pro-p, $[G, G]$ o grupo derivado e $G^p = \langle g^p \mid g \in G \rangle$, então o subgrupo de Frattini de G é igual a*

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

Para a demonstração veja [Proposição 1.13, [11]].

Proposição 4.2.5 *Seja G um grupo pro-p. Então G é finitamente gerado se e somente se $\Phi(G)$ é aberto em G.*

Demonstração. Suponha que $\Phi(G)$ é aberto em G. Então pela Proposição 4.1.2.(i) o índice de $\Phi(G)$ em G é finito e assim $G/\Phi(G)$ é finito. Logo existe um subconjunto finito X de G tal que $G = X\Phi(G)$ e usando a Proposição 4.1.8.(iii) segue que $G = \overline{\langle X \rangle}$.

Para a outra implicação, suponha que $G = \overline{\langle X \rangle}$ onde $|X| = d$ é finito. Se $\Phi(G) \leq N \lhd_o G$ então G/N é um p-grupo abeliano elementar e portanto pode ser gerado por d elementos (Proposição 4.2.5); assim $|G : N| \leq p^d$. Vamos escolher um subgrupo N_0 com $\Phi(G) \leq N_0$ tal que o índice em G é o maior possível. Portanto se $\Phi(G) \leq N \lhd_o G$ temos que $N_0 \leq N$. Como $\Phi(G)$ é um subgrupo aberto e fechado em G segue que

$$\Phi = \bigcap \{N \mid \Phi(G)N \lhd_o G\} = N_o.$$

Assim $\Phi(G)$ é aberto em G. □

Definição 4.2.6 Seja G um grupo pro-p. Definimos a *série p-central inferior de G* na forma seguinte:

$$P_1(G) = G$$

e para $i \geq 1$

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

Assim $P_2(G) = \Phi(G)$ (Proposição 4.2.4). Observe que $P_{i+1}(G) \geq \Phi(P_i(G))$ para cada i.

A seguinte proposição mostra que a topologia dos grupos pro-p finitamente gerados é determinada pela sua estrutura de grupo. Veja a demonstração dessa proposição em [Proposição 1.16, [11]].

Proposição 4.2.7 *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 todo i, e o conjunto $\{P_i(G) \mid i \geq 1\}$ é uma base para as vizinhanças de 1 em G.*

Lema 4.2.8 *Se G é um grupo pro-p e K é um subgrupo de índice finito em G então $|G : K|$ é uma potência de p.*

Proposição 4.2.9 *Se G é um grupo pro-p finitamente gerado então o grupo derivado $[G,G]$ é fechado em G.*

Desses dois resultados segue o teorema seguinte.

Teorema 4.2.10 *Se G é um grupo pro-p finitamente gerado então cada subgrupo de índice finito em G é aberto.*

Demonstração. Seja G um grupo pro-p finitamente gerado. Escrevemos $G^{\{p\}} = \{g^p \mid g \in G\}$, $G^{\{p\}}$ por ser a imagem de uma função contínua ($g \mapsto g^p$) é compacto e portanto fechado. Como $G/[G,G]$ é abeliano então $G^p[G,G] = G^{\{p\}}[G,G]$ e usando a Proposição 4.2.9 $G^p[G,G]$ é fechado e é igual a $\Phi(G)$. Pela Proposição 4.2.5 segue que $G^p[G,G]$ é aberto em G.

Seja agora K um subgrupo normal próprio de índice finito de G. Então usando indução e sem perda de generalidade podemos assumir que K é aberto em M sempre que M é um grupo pro-p finitamente gerado com $K \leq M < G$. Tomando $M = G^p[G,G]K$, temos que G/K é um p-grupo finito (Lema 4.2.8); segue que $M < G$. Como $|G:M| \leq |G:\Phi(G)| < \infty$, temos que M é um subgrupo aberto em G. Portanto M é um grupo pro-p finitamente gerado (Proposição 4.1.6) e usando a hipótese indutiva; K é aberto em M. Assim K é aberto em G e como cada subgrupo de índice finito em G contém um subgrupo da forma de K; temos que cada subgrupo de índice finito tem que ser aberto. □

Uma observação importante é que no caso de um grupo pro-p *finitamente gerado* podemos suprimir a "barra"da Definição 4.2.6.

Corolário 4.2.11 *Se G é um grupo pro-p finitamente gerado, então $\Phi(G) = G^p[G,G]$ e $P_{i+1}(G) = P_i(G)^p[P_i(G),G]$ para cada i.*

Recentemente Nikolov e Segal mostraram que em um grupo profinito finitamente gerado cada subgrupo de índice finito é aberto (veja [24]); logo a topologia de um grupo profinito finitamente gerado é determinado por sua estrutura de grupo.

Corolário 4.2.12 *Cada homomorfismo (abstrato) de um um grupo pro-p finitamente gerado para um grupo profinito é continuo.*

Proposição 4.2.13 *Se $H = \langle a_1, ...a_d\rangle$ é um grupo nilpotente então cada elemento de $[H,H]$ é igual a um produto da forma $[x_1,a_1]...[x_d,a_d]$ com $x_1, ...x_d \in H$.*

Agora vamos mencionar alguns exemplos de grupos pro-p.

(1) Todo p-grupo finito é um grupo pro-p.

(2) Seja G o grupo de Galois de uma extensão de Galois (possivelmente infinita) de um corpo, se todo subgrupo normal de G de índice finito tem índice uma potência de p então G é um grupo pro-p.

(3) O grupo aditivo dos inteiros p-ádicos também é um grupo pro-p.

4.3 Grupos procíclicos

Vamos ver a importância de definir a potência p-ádica em um grupo pro-p e notamos qual papel desempenha os inteiros p-ádicos neste sentido.

Lema 4.3.1 *Seja G um grupo pro-p e $g \in G$. Consideremos as sequencias (a_i) e (b_i) de inteiros convergentes na topologia p-ádica e tendo para o mesmo limite em $\mathbb{Z}_p$. Então as sequências (g^{a_i}) e (g^{b_i}) convergem em G para o mesmo limite.*

Demonstração. Seja N um subgrupo normal e aberto em G, então $|G/N| = p^j$ para algum j. Se consideramos inteiros i e k suficientemente grandes temos que $a_i \equiv a_k \ (\mathrm{mod} p^j)$ e assim $g^{a_i} \equiv g^{a_k} (\mathrm{mod} N)$. Temos que (g^{a_i}) é uma sequencia de Cauchy em G e pela Proposição 4.1.2 é convergente para um elemento em G, digamos g_1. Analogamente (g^{b_i}) converge para um elemento g_2 em G. Se k é um inteiro suficientemente grande então $b_k \equiv a_k \ (\mathrm{mod} p^j)$, $g^{b_k} \equiv g_2 \ (\mathrm{mod} N)$, assim obtemos

$$g_1 g_2^{-1} \equiv g^{a_k - b_k} \equiv 1 \ (\mathrm{mod} N),$$

e por ser N arbitrário temos que $g_1 = g_2$. □

Com o Lema 4.3.1 temos a unicidade do Limite e portanto podemos fazer a seguinte definição.

Definição 4.3.2 Seja G um grupo pro-p, $g \in G$ e $\lambda \in \mathbb{Z}_p$. Então

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

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

A definição de "exponenciação p-ádica"que nós terminamos de definir tem as seguintes propriedades que podem ser demonstradas a partir de sua própria definição.

Proposição 4.3.3 *Seja G um grupo pro-p, sejam $g, h \in G$, e sejam $\lambda, \mu \in \mathbb{Z}_p$. Então temos que*

(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 $\upsilon \to g^{\upsilon}$ define um homomorfismo contínuo de $\mathbb{Z}_p$ para G. Sua imagem $g^{\mathbb{Z}_p}$ é o fecho em G de $\langle g \rangle$.*

Para a demonstração veja [Proposição 1.26, [11]].

Definição 4.3.4 Um grupo G é *procíclico* se é profinito e G/N é um grupo cíclico para cada subgrupo normal aberto N de G.

Proposição 4.3.5 *Seja G um grupo pro-p. Então as seguintes afirmações são equivalentes.*

(a) *G é procíclico;*

(b) *G pode ser gerado topologicamente por um subconjunto de 1-elemento;*

(c) *$G = g^{\mathbb{Z}_p}$ para algúm $g \in G$;*

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

Demonstração. $((a) \Rightarrow (b))$. Suponha que G é um grupo procíclico e suponha que ele tem dois subgrupos próprios maximais diferentes M e N. Então $M \cap N \geq \Phi(G) \geq G^p[G,G]$, assim M e N são subgrupos normais de índice p em G e $G/(M \cap N)$ é um grupo abeliano elementar de ordem p^2, mas não é um grupo cíclico. Então $G = 1$ ou G tem um único subgrupo próprio maximal aberto; de qualquer forma em ambos casos $\Phi(G)$ é aberto em G e $G/\Phi(G)$ é cíclico. Portanto G pode ser gerado topológicamente por um conjunto de um elemento (Proposição 4.1.8). $((b) \Rightarrow (c))$ Proposição 4.3.3 (iii). $((c) \Rightarrow (d))$ Suponha que $G = g^{\mathbb{Z}_p}$ para algum $g \in G$ e seja K o núcleo do homomorfismo $\theta : \mathbb{Z}_p \to G$ dado por $\theta(\lambda) = g^{\lambda}$, assim θ é sobrejetivo por definição e pelo Corolário 4.2.12 é contínua. Como $\mathbb{Z}_p/K$ e G são grupos compactos Hausdorff e assim G é topológicamente isomorfo a $\mathbb{Z}_p/K$. $((d) \Rightarrow (a))$ Simplesmente temos que observar que cada grupo quociente próprio de $\mathbb{Z}_p$ é cíclico. □

Todos os grupos cíclicos finitos são grupos pro-cíclicos. Da definição 4.3.4 obtemos que o grupo de Prüfer e os inteiros p-ádicos são exemplos de grupos pro-cíclicos.

4.4 p-Grupos powerful

Nesta seção prestamos mais atenção aos p-grupos finitos. Para nós entender a estrutura dos grupos pro-p analíticos devemos olhar nas propriedades de uma classe especial de grupos finitos.

Definição 4.4.1

(i) Um p-grupo finito G é *powerful* se p é ímpar e G/G^p é abeliano, ou se $p = 2$ e G/G^4 é abeliano.

(ii) Um subgrupo N de um p-grupo finito G é *powerfully embedded* em G, escrevemos N p.e. G, se p é ímpar e $[N,G] \leq N^p$, ou se $p = 2$ e $[N,G] \leq N^4$.

Portanto G é powerful se e somente se G p.e. G; e se N p.e. G então $N \lhd G$ e N é powerful. Quando p é ímpar G é powerful se e somente se $G^p = \Phi(G)$.

Lema 4.4.2 *Seja G um p-grupo finito e sejam N, K e W subgrupos normais de G tais que $N \leq W$.*

(i) *Se N p.e. G então NK/K p.e. G/K.*

(ii) *Se p é ímpar e $K \leq N^p$, ou se $p = 2$ e $K \leq N^4$, então N p.e. G se e somente se N/K p.e. G/K.*

(iii) *N p.e. G e $x \in G$ então $\langle N, x\rangle$ é powerful.*

(iv) *Se N não é powerfully embedded em W, então existe um subgrupo normal J de G tal que*

- *se p é ímpar,*

$$N^p[N,W,W] \leq J \leq N^p[N,W] \qquad \text{e} \qquad |N^p[N,W] : J| = p;$$

- *se $p = 2$,*

$$N^4[N,W]^2[N,W,W] \leq J \leq N^4[N,W] \qquad \text{e} \qquad |N^4[N,W] : J| = 2.$$

Demonstração. (i), (ii) Usar só a definição. (iii) Definimos $H = \langle N, x\rangle$. Como $N \lhd H$ temos $[H,H] = [N,H]$, por hipótese temos que N p.e. G e portanto $[H,H] \leq N^p \leq H^p$ (respectivamente $[H,H] \leq H^4$ se $p = 2$). (iv) Suponha que p é ímpar e que $[N,W] \not\leq N^p$, então $N^p \lneq N^p[N,W] = M$. Sabemos que G é um p-grupo e M e N são normais em G então existe um $J \lhd G$ tal que $N^p \leq J \lneq M$ e $|M : J| = p$. Portanto M/J é central em G/J e temos o resultado (proceder da mesma forma para o caso $p = 2$). □

Proposição 4.4.3 *Seja G um p-grupo finito e $N \leq G$. Se N p.e. G então N^p p.e. G.*
Para a demonstração veja [Proposição 2.3, [11]].

Observe que se G fosse um p-grupo finito, então:

$$P_1(G) = G, \quad P_{i+1}(G) = P_i(G)^p[P_i(G), G] \ \text{ para cada } \ i \geq 1.$$

Para o resto da seção vamos escrever simplesmente $G_i = P_i(G)$.

Lema 4.4.4 *Seja G um p-grupo finito powerful.*

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

(ii) *Para cada i, a aplicação $x \to x^p$ induz um epimorfismo de G_i/G_{i+1} para G_{i+1}/G_{i+2}.*

Demonstração. (i) Temos que $G = G_1$ é powerful, assim G_1 p.e. G. Suponha que G_i p.e G para algum $i \geq 1$. Então $G_{i+1} = G_i^p[G_i, G] = G_i^p$, e G_{i+1} p.e. G (Proposição 4.4.3) mas $G_i^p \leq \Phi(G_i) = G_i^p[G_i, G_i] \leq G_{i+1}$ e assim $G_{i+1} = \Phi(G_i)$. Então aplicando indução temos o resultado.

(ii) Pela parte (i) podemos mostrar que G_i é powerful, $G_{i+1} = P_2(G_i)$ e $G_{i+2} = P_3(G_i)$. Vamos supor que $i = 1$ e fazemos a mudança de G por G/G_3; aqui podemos supor que $G_3 = 1$. Portanto $[G,G] \leq G_2 \leq Z(G)$, assim para $x, y \in G$ temos que

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

Se p é ímpar temos que $p|(p(p-1)/2)$, assim

$$[y,x]^{p(p-1)/2} \in G_2^p = G_3 = 1,$$

Se $p = 2$ então $[G,G] \leq G^4 \leq G_3 = 1$. Assim no qualquer caso temos que $(xy)^p = x^p y^p$. Como $G_2^p = G_3 = 1$ e $G^p = G_2$, isto mostra que $x \mapsto x^p$ induz um homomorfismo de G/G_2 para G_2/G_3. □

Lema 4.4.5 *Se $G = \langle a_1, ..., a_d \rangle$ é um p-grupo finito powerful, então $G^p = \langle a_1^p, ..., a_d^p \rangle$.*

Para a demonstração veja [Lema 2.5, [11]].

Proposição 4.4.6 *Se G é um p-grupo finito powerful então cada elemento de G^p é uma p-ésima potência em G.*

Demonstração. A prova é por indução sobre $|G|$. Seja $g \in G^p$. Então existem $x \in G$ e $y \in G_3$ tais que $g = x^p y$ (Lema 4.4.4). Definamos $H = \langle G^p, x \rangle$. Pelo Lema 4.4.4, $G^p = G_2$ p.e. G e pelo Lema 4.4.2 (iii) H é powerful. Além disso, como $y \in G_3 = G_2^p$; temos que $g \in H^p$. Suponha que $H \neq G$. Então pela hipótese indutiva g é uma p-ésima potência em H. Suponha agora que $H = G$. Como $G = \langle G^p, x \rangle = \Phi(G)\langle x \rangle$, temos que G é cíclico. Nesse caso é claro que G é uma p-ésima potência em G. Isso termina a prova.□

Podemos agora resumir a principal característica de uma série p-inferior em um p-grupo powerful.

Teorema 4.4.7 *Seja $G = \langle a_1, ..., a_d \rangle$ um p-grupo finito powerful e seja $G_i = P_i(G)$ 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) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}} \rangle$;*

(iv) *a aplicação $x \to x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} para G_{i+k}/G_{i+k+1}, isto é para cada i e k.*

Para a demonstração veja [Proposição 2.7, [11]].

Corolário 4.4.8 *Se $G = \langle a_1, ..., a_d \rangle$ é um p-grupo finito powerful então $G = \langle a_1 \rangle, ..., \langle a_d \rangle$, i.e. G é o produto de seus subgrupos cíclicos $\langle a_i \rangle$.*

Para a demonstração veja [Proposição 2.8, [11]].

Para um p-grupo finito G, definimos por $d(G)$ a menor cardinalidade de um conjunto de geradores de G. Assim $d(G)$ é também a dimensão de $G/\Phi(G)$ como um espaço vetorial sobre $\mathbb{F}_p$.

Teorema 4.4.9 *Se G é um p-grupo powerful e $H \leq G$ então $d(H) \leq d(G)$.*

Demonstração. Provaremos isto por indução sobre $|G|$. Suponha que o resultado é válido para os p-grupos powerful com a ordem menor que a ordem de G. Definamos d=d(G) e m =d(G_2). Então G_2 é powerful (Lema 4.4.4 (i)) e usando a hipótese indutiva temos que o subgrupo $K = H \cap G_2$ satisfaz d$(K) \leq m$. Consideramos a aplicação $\pi : G/G_2 \to G_2/G_3$ dada por $x \mapsto x^p$, esta aplicação é um epimorfismo (Lema 4.4.4 (ii)) e dim(kerπ)=$d - m$. Assim dim(ker$\pi \cap HG_2/G_2) \leq d - m$. Logo

$$\dim(\pi(HG_2/G_2)) \geq \dim(HG_2/G_2) - (d - m) = m - (d - r);$$

onde r =dim(HG_2/G_2). Sejam $h_1, ..., h_r$ elementos em H tais que $HG_2 = \langle h_1, ..., h_r\rangle G_2$. Sabemos que $\Phi \leq K^p \leq G_3$. Então o subespaço formado pelas classes laterais $h_1^p, ..., h_r^p$ tem dimensão ao menos dim$((HG_2/G_2)\pi) \geq m - (d - r)$ e como d$(K) \leq m$ podemos encontrar $d - r$ elementos $y_1, ..., y_{d-r} \in K$ tais que

$$K = \langle h_1^p, ..., h_r^p, y_1, ..., y_{d-r}\rangle\Phi(K).$$

Então $K = \langle h_1^p, ..., h_r^p, y_1, ..., y_{d-r}\rangle$ e assim temos que

$$H = H \cap \langle h_1, ..., h_r\rangle G_2 = \langle h_1, ..., h_r\rangle K = \langle h_1, ..., h_r, y_1, ..., y_{d-r}\rangle$$

Portanto d$(H) \leq d$. □

O *posto* de um grupo finito G é definido por:

$$rk(G) = \sup\{d(H) \mid H \leq G\}. \tag{4.1}$$

Por (1.1) e usando o Teorema 4.4.9 podemos dizer que se *G é um p-grupo powerful então* $rk(G) = d(G)$.

Definição 4.4.10 Para um p-grupo finito G e um inteiro positivo r, $V(G, r)$ denota a interseção dos núcleos de todos os homomorfismos de G para $GL_r(\mathbb{F}_p)$.

Definição 4.4.11 Um grupo G é metacíclico se contém um subgrupo cíclico N, tal que G/N é também cíclico.

Proposição 4.4.12 *Se p é ímpar então cada p-grupo metacíclico finito é powerful.*

Demonstração. Seja G um p-grupo metacíclico finito. Então contém um subgrupo cíclico $N = \langle x\rangle$ tal que $G/N = \langle yN\rangle$ é cíclico. Se $b \in G$ ele pode ser escrito como $y = x^n y^m$. Então $G = \langle x, y\rangle$. Como N é cíclico então $N \lhd G$ e G/N é abeliano por ser cíclico. Logo $[G, G] \subseteq N$. Como $\{x, y\}$ gera G então $[x, y]$ gera $[G, G]$. Assim $\langle[x, y]\rangle = [G, G] \subseteq N$ e portanto $[x, y] = x^{p^e}$ para algum inteiro não negativo e. Logo $[G, G] \subseteq G^p$ e G é powerful.□

Observação 4.4.13 Na verdade podemos considerar os p-grupos "powerful"como generalizações de p-grupos finitos abelianos.

Alguns exemplos de grupos powerful.

(i) Todo p-grupo finito abeliano é um p-grupo powerful.

(ii) Consideremos o grupo $\mathbb{Z}/10\mathbb{Z}$. Ele contém um subgrupo isomorfo ao grupo cíclico $\mathbb{Z}/2\mathbb{Z}$ e o subgrupo quociente é isomorfo a $\mathbb{Z}/5\mathbb{Z}$, que é também cíclico. Pela Proposição 4.4.12, $\mathbb{Z}/10\mathbb{Z}$ é um p-grupo metacíclico finito e assim um p-grupo powerful.

(iii) O primeiro exemplo de um grupo powerful não cíclico é o grupo de Klein Dih_2. E o grupo powerful não abeliano mais pequeno é Dih_3 (a prova disso é usando a Proposição 4.4.12).

4.5 Grupos pro-p de posto finito

Definição 4.5.1 Seja G um grupo pro-p.

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

(ii) Seja $N \leq_o G$. Então N é *powerfully embedded* em G, escrevemos N p.e. G, se p é ímpar e $[N, G] \leq \overline{N^p}$, ou se $p = 2$ e $[N, G] \leq \overline{N^4}$.

Observe que se N p.e. G então $N \lhd_o G$ e N é powerful. Como $\overline{N^p}$ (resp. $\overline{N^4}$) é a interseção de todos os subgrupos normais abertos de G nos quais N^p (resp. N^4) está contido.

Proposição 4.5.2 *Seja G um grupo pro-p e N um subgrupo normal aberto em G. Então N p.e. G se e somente se NK/K p.e. G/K para cada K subgrupo normal aberto em G.*

Corolário 4.5.3 *Seja G um grupo topológico. Então 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 onde todas as aplicações são sobrejetivas.*

Lema 4.5.4 *Seja G um grupo pro-p finitamente gerado powerful. Então cada elemento de G^p é uma p-ésima potência em G, e $G^p = \Phi(G)$ é aberto em G. Se $p = 2$, então G^4 é aberto em G.*

Para a demonstração veja [Proposição 3.4, [11]].

Corolário 4.5.5 *Seja G como no Lema acima. Então para cada i temos*

$$G^{p^i} = (G^{p^{i-1}})^p = \{x^{p^i} \mid x \in G\} \quad p.e. \quad G^{p^{i-1}} \tag{4.2}$$

Teorema 4.5.6 *Seja $G = \overline{\langle a_1, ..., a_d \rangle}$ um grupo pro-p finitamente gerado powerful e definamos $G_i = P_i(G)$ 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) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \overline{\langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}} \rangle}$;*

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

Proposição 4.5.7 *Se* $G = \overline{\langle a_1 \cdots a_d \rangle}$ *é um grupo pro-p powerful então* $G = \overline{\langle a_1 \rangle} ... \overline{\langle a_d \rangle}$, *i.e.* G *é o produto de seus subgrupos procíclicos* $\overline{\langle a_1 \rangle}, ..., \overline{\langle a_d \rangle}$.

Demonstração. O conjunto $A = \overline{\langle a_1 \rangle}, ..., \overline{\langle a_d \rangle}$ é compacto (pois é o produto de um número finito de conjuntos fechados e portanto compactos), e por isso é fechado em G. Assim $A = \bigcap_{N \lhd_o G} AN$. Também temos que $AN/N = G/N$ (Corolário 4.4.8) para cada N subgrupo normal aberto em G e portanto $A = G$. □

Para cada grupo topológico G, $d(G)$ denota a menor cardinalidade de um conjunto de geradores topológicos de G. Se G é um grupo pro-p finitamente gerado, então temos

$$d(G) = \dim_{\mathbb{F}_p}(G/\Phi(G)). \tag{4.3}$$

Usando o Teorema 4.4.9 e a Proposição 4.1.4, obtemos o seguinte teorema

Teorema 4.5.8 *Seja* G *um grupo pro-p finitamente gerado powerful e* H *um subgrupo fechado de* G. *Então* $d(H) \leq d(G)$.

Na seguinte proposição mostramos as equivalentes definições de "posto".
Proposição 4.5.9 *Seja* G *um grupo profinito, e sejam:*

$$\begin{aligned} r_1 &= sup\{d(H) \mid H \leq_c G\} \\ r_2 &= sup\{d(H) \mid H \leq_c G \text{ e } d(H) < \infty\} \\ r_3 &= sup\{d(H) \mid H \leq_o G\} \\ r_4 &= sup\{rk(G/N) \mid N \lhd_o G\} \end{aligned}$$

Então $r_1 = r_2 = r_3 = r_4$.

Para a demonstração veja [Proposição 3.11, [11]].

Definição 4.5.10 Seja G um grupo profinito. O *posto* $rk(G)$ de G é quaisquer dos r_i dados na Proposição 4.5.9.

Observe que por definição um grupo profinito de posto finito é finitamente gerado. Se G é um grupo pro-p finitamente gerado powerful, então o Teorema 4.5.8 mostra que rk(G) =d(G) e assim G tem posto finito. Generalizando, se G é finitamente gerado e possui um subgrupo powerful aberto então G tem posto finito. O seguinte resultado é o principal desta seção.

Teorema 4.5.11 *Seja* G *um grupo pro-p. Então* G *tem posto finito se e somente se* G *é finitamente gerado e* G *possui um subgrupo powerful aberto. Nestas condições,* G *possui um subgrupo característico powerful aberto.*

Para a demonstração veja [Proposição 3.13, [11]].

Corolário 4.5.12 *Seja G um grupo pro-p e seja r um inteiro positivo. Suponha que cada subgrupo aberto de G contém um subgrupo aberto normal N de G com $d(N) \leq r$. Então G tem posto finito.*

Teorema 4.5.13 *Seja G um grupo pro-p. Então as seguintes propriedades 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.

Demonstração. $((c) \Rightarrow (b))$. Suponha que G tem posto finito r. Então G possui um subgrupo normal aberto powerful H. Definamos $H_i = P_i(H)$ para cada i. Então temos que $|H : H_2| \leq p^r$ e $|H : H_{k+1}| \leq p^{kr}$ para todo k (Proposição 4.5.6 (iv)). Além disso $H_{k+1} = H^{p^k}$ (Teorema 4.5.6 (iii)) e assim temos que

$$|G : G^{p^k}| \leq |G : H^{p^k}| \leq |G : H|p^{kr}.$$

$((b) \Rightarrow (a))$ É simplesmente notar que $|G : \overline{G^{p^k}}| \leq |G : G^{p^k}|$ e o resultado é obvio. $((a) \Rightarrow (c))$ Suponha que temos (a). Então $|G : \Phi(G)| \leq |G : \overline{G^p}| \leq cp^s$ é finito e portanto G é finitamente gerado. Definimos $W = V(G, s)$ se p é ímpar e $W = V(G, s)^2$ se $p = 2$. Escrevamos $G_i = \overline{G^{p^i}}$ para cada i. Como W é um subgrupo normal aberto de G existe um m tal que $G_m \leq W$ e pela nossa hipótese indutiva temos que $|G_k : G_{k+1}| \leq p^s$ para algum $k \geq m$. Se não fosse assim, então existiria um n suficientemente grande tal que

$$|G : G_{m+n}| \geq |G_m : G_{m+n}| \geq p^{s+1}n > cp^{ms}p^{ns} = cp^{(m+n)s},$$

contradizendo a nossa hipótese. Escolhendo um k e definindo $K = G_k$ temos que $\Phi(K) \geq \overline{K^p} \geq G_{k+1}$, assim $|K/\Phi(K)| \leq p^s$ e $\mathrm{d}(K) \leq s$. Finalmente K é powerful e $\mathrm{rk}(K)$=$\mathrm{d}(K) \leq s$ (Teorema 4.5.8).

Teorema 4.5.14 *Seja G um grupo pro-p. Então as seguintes afirmações são equivalentes:*

(a) *G é o produto de um número finito de subgrupos procíclicos;*

(b) *G é o produto de um número finito de subgrupos fechados de posto finito;*

(c) *G tem posto finito;*

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

Exemplo. Consideremos ao grupo $\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. Esse grupo munido com a topologia discreta é um grupo de posto finito pois é finitamente gerado e contém um subgrupo isomorfo a $\mathbb{Z}/10\mathbb{Z}$ que na seção anterior mostramos que é um p-grupo powerful.

4.6 Grupos Uniformes

Definição 4.6.1 Um grupo pro-p G se diz *uniforme* ou *uniformemente powerful* se:

(i) G é finitamente gerado

(ii) G é powerful, e

(iii) $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$, para cada i.

Podemos supor que um grupo pro-p G satisfaz (i) e (ii) e repensar (iii). Assim no seu lugar podemos escrever "a aplicação $f_i : P_i(G)/P_{i+1}(G) \to P_{i+1}(G)/P_{i+2}(G)$ induzida pela aplicação $x \mapsto x^p$ é um isomorfismo para cada i".

Teorema 4.6.2 *Seja G um grupo pro-p finitamente gerado powerful. Então existe um k suficientemente grande tal que $P_k(G)$ é uniforme.*

Demonstração. Definamos $G_i = P_i(G)$ e suponha que $|G_i : G_{i+1}| = p^{d_i}$ então temos que $d_1 \geq d_2 \geq ... \geq d_i \geq d_{i+1} \geq ...$ (Teorema 4.5.6 (iv)). Assim existe m tal que $d_k = d_m$ para todo $k \geq m$. Além disso $P_i(G_k) = G_{k+i-1}$ para todo i e k (Teorema 4.5.6 (ii)) e portanto G_k é uniforme (Teorema 4.5.6 (i)). □

Corolário 4.6.3 *Um grupo pro-p de posto finito tem um subgrupo característico aberto uniforme.*

Com ajuda do Teorema 4.5.6 e do Teorema 4.5.8 temos que um grupo powerful G é uniforme se e somente se $d(G_i/G_{i+1}) = d(G_1/G_2) = d$ para todo i.

Proposição 4.6.4 *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 cada $i \geq 1$*;

(c) *$d(H) = d(G)$ para cada subgrupo powerful aberto H em G.*

Uma caracterização de um grupo uniforme é a seguinte.

Teorema 4.6.5 *Seja G um grupo pro-p finitamente gerado powerful. Então G é uniforme se e somente se é livre de torsão.*

Demonstração. Seja G um grupo pro-p finitamente gerado powerful e definamos $G_i = P_i(G)$ para todo i. Vamos supor que G não é livre de torsão. Então G contém um elemento x de ordem p. Se $x \in G_i \backslash G_{i+1}$ então $1 \neq xG_{i+1} \in G_i/G_{i+1}$ e $1 = x^pG_{i+2} \in G_{i+1}/G_{i+2}$. Portanto a aplicação $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ não é injetiva e assim G não é uniforme.

Para a outra implicação, suponha que G não é uniforme. Então f_i não é injetivo para algum i e assim existe $x \in G_i \backslash G_{i+1}$ tal que $x^p \in G_{i+2}$. Definamos $x_2 = x$ e suponha que para algum $n \geq 2$ podemos encontrar $x_2, ..., x_n$ satisfazendo $x_j^p \in G_{i+j}$ e

$x_j \equiv x_{j-1} \,(\mathrm{mod} G_{i+j-2})$ para $2 < j \leq n$. Então existe $y \in G_{i+n-1}$ tal que $x_n^p = y^p$. Definamos $x_{n+1} = y^{-1}x_n$. Então $x_{n+1} \equiv x_n \,(\mathrm{mod} G_{i+n-1})$ e também $x_{n+1}^p \in G_{i+n+1}$. Portanto $x_{n+1}^p \equiv 1 \,(\mathrm{mod} G_{i+n+1})$. Assim podemos construir uma sequência $x_2, ..., x_n, ...$ de Cauchy convergente para algum $\overline{x} \in G$. Portanto $\overline{x} \equiv x \not\equiv 1 \,(\mathrm{mod} G_{i+1})$ e $\overline{x}^p \equiv x_n^p \equiv 1 \,(\mathrm{mod} G_{i+n-1})$ para todo n, e assim $\overline{x}^p = 1$, o que mostra que G não é livre de torsão. □

Lema 4.6.6 *Se A e B são subgrupos abertos uniformes de algum grupo pro-p G. Então $d(A) = d(B)$.*

Demonstração. Seja i um número suficientemente grande tal que $P_i(B) \leq A \cap B \leq A$ e usando a Proposição 4.6.4 temos que d(A)=d$(P_i(B))$ =d(B). □

Definição 4.6.7 Seja G um grupo pro-p de posto finito e seja H um subgrupo uniforme aberto arbitrário em G. A *dimensão* de G é definida por

$$\dim(G) = d(H). \tag{4.4}$$

Teorema 4.6.8 *Seja G um grupo pro-p de posto finito e N um subgrupo normal fechado de G. Então*

$$\dim(G) = \dim(N) + \dim(G/N) \tag{4.5}$$

(Observe que N e G/N tem posto finito.)

Para a demonstração veja [Proposição 4.8, [11]].

Teorema 4.6.9 *Seja G um grupo pro-p uniforme e $d = d(G)$. Suponha que G é gerado topológicamente pelo conjunto finito $\{a_1, ..., a_d\}$. Então a aplicação*

$$\begin{aligned} \psi : \mathbb{Z}_p^d &\longrightarrow G \\ (\lambda_1, ..., \lambda_d) &\longmapsto a_1^{\lambda_1} ... a_d^{\lambda_d} \end{aligned}$$

é um homeomorfismo.

Demonstração. Seja $\{a_1, \cdots, a_d\}$ um conjunto de geradores topológicos de G. Assim $G = \overline{\langle a_1, \cdots, a_d \rangle}$. Então $G = \overline{\langle a_1 \rangle} \cdots \overline{\langle a_d \rangle}$ (Proposição 4.5.7). Se $a \in G$ temos que $a = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$ com $\lambda_1, \cdots, \lambda_d \in \mathbb{Z}_p$. Seja k fixo e arbitrário. O grupo G/G_{k+1} tem ordem p^{kd} e $G/G_{k+1} = \langle a_1 G_{k+1} \rangle \cdots \langle a_d G_{k+1} \rangle$, onde cada subgrupo cíclico tem ordem p^k. Então cada elemento de G/G_{k+1} pode ser escrito como $a_1^{e_1} \cdots a_d^{e_d} G_{k+1}$ onde $e_1, \cdots, e_d$ são inteiros unicamente determinados módulo p^k. Isso implica que $\lambda_1, \cdots, \lambda_d$ são unicamente determinados módulo p^k,para cada k. Assim $\lambda_1, \cdots, \lambda_d$ são inteiros p-ádicos unicamente determinados. Obtemos que a aplicação $\theta : G \to \mathbb{Z}_p^d$ dada por $\theta(a) = (\lambda_1, \cdots, \lambda_d)$ é uma bijeção e pelo Corolário 4.2.12 é continua. Temos que $\psi : \mathbb{Z}_p^d \to G$ é a bijeção recíproca, onde $\psi(\lambda_1, \cdots, \lambda_d) = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$. Como a multiplicação em G é continua. Então ψ é continua. Assim ψ é homeomorfismo. □

Lema 4.6.10 *Seja G um grupo pro-p uniforme e para cada $n \in \mathbb{N}$ a aplicação $x \mapsto x^{p^n}$ é um homeomorfismo de G para G_{n+1}. Além disso, para cada k e m em $\mathbb{N}$, a restrição desse homeomorfismo é uma bijeção de G_k para G_{k+n} e induz uma bijeção de G_k/G_{k+m}*

para G_{n+k}/G_{n+k+m}.

Para a demonstração veja [Proposição 4.10, [11]].

A importância desse lema é que cada elemento $x \in G_{n+1}$ tem uma única p^n-ésima raiz em G, que vamos denotar por $x^{p^{-n}}$. Vamos aproveitar a bijeção entre G e G_{n+1}. Assim podemos usar a operação de grupo de G_{n+1} em G. Nessa forma definimos uma nova estrutura de grupo em G.

Para $x, y \in G$ definimos:

$$x +_n y = (x^{p^n} y^{p^n})^{p^{-n}}.$$

Assim, a aplicação $x \to x^{p^{-n}}$ torna-se um homomorfismo de grupos entre G_{n+1} e $(G, +_n)$.

Lema 4.6.11 Se $n > 1$, $x, y \in G$, e $u, v \in G$ então:

$$xu +_n yv \equiv x +_n y \equiv x +_{n-1} y \pmod{G_n},$$

e para todo $m > n$

$$x +_m y \equiv x +_n y \pmod{G_{n+1}}.$$

Para a demonstração veja [Proposição 4.11, [11]].

Definição 4.6.12 Seja G é um grupo pro-p uniforme e sejam $x, y \in G$. Definimos uma nova operação (soma em G) por

$$x + y = \lim_{n\to\infty} x +_n y \tag{4.6}$$

A partir dessa definição temos que $x + y \equiv x +_n y \pmod{G_{n+1}}$ e se $u, v \in G_n$ então $xu + yv \equiv x + y \pmod{G_n}$

Observemos que um grupo pro-p uniforme G com a operação $+$ é um grupo abeliano com elemento identidade 1 e o elemento inverso é dado por $x \mapsto x^{-1}$.

Lema 4.6.13 *Seja G um grupo pro-p uniforme e sejam x, y elementos de G. Então:*

(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 $x + y \equiv xy \pmod{G_{n+1}}$*

Para a demonstração veja [Proposição 4.14, [11]].

Agora vamos listar rapidamente alguns outros resultados importantes; para as demonstrações veja [11].

(i) Seja G um grupo pro-p uniforme e $n \in \mathbb{N}$, então G_n é um subgrupo aditivo de G, e as classes laterais aditivas de G_n em G são as mesmas que as classes laterais multiplicativas de G_n em G. Também a aplicação identidade $G_n/G_{n+1} \to G_n/G_{n+1}$ é um isomorfismo do grupo aditivo G_n/G_{n+1} para o grupo multiplicativo G_n/G_{n+1}, e o índice de G_n no grupo aditivo $(G,+)$ é igual a $|G : G_n|$.

(ii) $(G,+)$ é um grupo pro-p uniforme de dimensão $d = d(G)$ (com a topologia inicial). Além disso, qualquer conjunto de geradores topológicos para G é um conjunto de geradores topológicos para $(G,+)$.

(iii) Seja G um grupo pro-p uniforme de dimensão d, e seja $\{a_1, ..., a_d\}$ um conjunto de geradores topológicos para G. Então, com as operações acima definidas, $(G,+)$ é um $\mathbb{Z}_p$-módulo livre com a base $\{a_1, ..., a_d\}$.

(iv) Seja G um grupo pro-p uniforme de dimensão d. Então a ação de $Aut(G)$ sobre G é $\mathbb{Z}_p$-linear com respeito à estrutura de $\mathbb{Z}_p$-módulo sobre $(G,+)$. Portanto $Aut(G)$ pode ser definido como um subgrupo de $GL_d(\mathbb{Z}_p)$.

(v) *Seja G um grupo pro-p de posto finito de dimensão d. Então para algum $e \leq d$ e algum p-grupo finito F existe uma sequência exata*

$$1 \to \mathbb{Z}_p^e \to G \to GL_d(\mathbb{Z}_p) \times F.$$

(vi) Seja G um grupo pro-p powerful finitamente gerado. Então os elementos de ordem finito de G formam um subgrupo característico T de G. Também T é um p-grupo finito powerful e G/T é uniforme.

Exemplos de grupos uniformes

(1) O grupo aditivo de inteiros p-ádicos é um grupo uniforme. Além disso, todo grupo abeliano pro-p finitamente gerado e livre de torsao é um grupo pro-p uniforme; em outras palavras $\mathbb{Z}_p^n$ onde n é um inteiro positivo é um grupo pro-p uniforme.

(2) Agora vamos mostrar que o grupo $\mathrm{GL}_n(\mathbb{Z}_p)$ contém vários exemplos não triviais de grupos pro-p uniformes.

O grupo $\mathrm{GL}_d(\mathbb{Z}_p)$

Seja d um inteiro positivo e seja $M_d(\mathbb{Z}_p)$ o espaço topológico das matrizes $d \times d$ sobre $\mathbb{Z}_p$. Definimos $\Gamma = \mathrm{GL}_d(\mathbb{Z}_p)$ o subespaço topológico de $M_d(\mathbb{Z}_p)$ de todas as matrizes $d \times d$ invertíveis. Então Γ é um grupo topológico Hausdorff com a topologia p-ádica (Observação 2.1.2). Dado um elemento a em $M_d(\mathbb{Z}_p)$, temos que $a \in \Gamma$ se e somente se $\det a \not\equiv 0 \pmod{p}$. Então Γ é ao mesmo tempo um subespaço fechado e aberto de $M_d(\mathbb{Z}_p)$ pois cada matriz $b \equiv a \pmod{p}$ satisfaz $b \in \Gamma$ se e somente se $a \in \Gamma$; isto mostra que Γ é a união de ao máximo p^{d^2} classes aditivas de $pM_d(\mathbb{Z}_p)$. Portanto Γ é compacto. Uma base para as vizinhanças de 1 em Γ é dada pelos "subgrupos de congruência"

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

para $i \geq 0$. Como $\Gamma/\Gamma_i \cong \mathrm{GL}_d(\mathbb{Z}/p^i\mathbb{Z})$ para $i \geq 1$, temos que

$$\begin{aligned} |\Gamma : \Gamma_1| &= (p^d - 1)(p^d - p)...(p^d - p^{d-1}) \quad \text{e} \\ |\Gamma_1 : \Gamma_i| &= p^{d^2(i-1)} \text{ para } i \geq 1. \end{aligned}$$

Assim Γ é profinito e Γ_1 é um grupo pro-p.

Quando vamos definir o conceito de grupo p-ádico analítico no capítulo 5 notaremos que Γ é um grupo p-ádico analítico compacto; uma propriedade fundamental de tais grupos é que eles contém um subgrupo pro-p powerful aberto finitamente gerado e agora verificamos isso diretamente para $\Gamma = \mathrm{GL}_d(\mathbb{Z}_p)$.

Lema. *Seja p primo; se $p > 2$ e $n \geq 2$, ou se $p = 2$ e $n \geq 3$, então todo elemento de Γ_n é uma p-ésima potência de um elemento em Γ_{n-1}.*

Demonstração. Temos que mostrar que para qualquer $a \in M_d(\mathbb{Z}_p)$ podemos resolver

$$1 + p^n a = (1 + p^{n-1}x)^p \tag{4.7}$$

com $x \in M_d(\mathbb{Z}_p)$. A solução é por aproximação sucessiva. Começamos com $(1 + p^{n-1}a)^p \equiv 1 + p^n a (\mathrm{mod}\ p^{n+1})$ (sempre que n esteja no lugar indicado). Faça $x_1 = a$ e suponha indutivamente que encontramos para $r \geq 1$, uma matriz x_r comutando com a, tal que $(1 + p^{n-1}x_r)^p \equiv 1 + p^n a (\mathrm{mod}\ p^{n+r})$. Digamos

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

Agora seja

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

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

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

Assim obtemos uma sequencia convergente (x_r) em $M_d(\mathbb{Z}_p)$, cujo limite x satisfaz (4.7). □

Teorema. *Para cada i seja $\Gamma_i = \{\gamma \in \mathrm{GL}_d(\mathbb{Z}_p) \mid \gamma \equiv 1_d (\mathrm{mod}\ p^i)\}$. Definamos $G = \Gamma_1$ se p é impar, $G = \Gamma_2$ se $p = 2$. Então G é um grupo pro-p uniforme e $\dim(G) = \mathrm{rk}(G) = \mathrm{d}(G) = d^2$. Também $P_i(G) = \Gamma_{i+\epsilon}$ para todo i, onde $\epsilon = 0$ se $p \neq 2$, $\epsilon = 1$ se $p = 2$.*

Demonstração. Temos $P_1(G) = G = \Gamma_{1+\epsilon}$ por definição. Suponha que $r \geq 1$ e $P_r(G) = \Gamma_{r+\epsilon}$. Então um cálculo fácil mostra que $P_r(G)^p[P_r(G), G] \leq \Gamma_{r+1+\epsilon}$ e pelo Lema 3.2.1 mostramos que $\Gamma_{r+1+\epsilon} \leq \Gamma_{r+\epsilon}^p = P_r(G)^p$. Como $\Gamma_{r+1+\epsilon}$ é um subgrupo fechado de G, temos que $P_{r+1}(G) = \Gamma_{r+1+\epsilon}$. Assim por indução segue que $P_i(G) = \Gamma_{i+\epsilon}$ para todo i, e no caminho mostramos que $P_{i+1}(G) = P_i(G)^p$ para todo i. Tomando $i = 1$, vemos que G é powerful (quando $p = 2$ notamos que $[\Gamma_2, \Gamma_2] \leq \Gamma_4 \leq \Gamma_2^4$); e como $P_2(G) = \Gamma_{2+\epsilon}$ é aberto em G, o Teorema 3.1.14 mostra que G é finitamente gerado. Como $|\Gamma_i : \Gamma_{i+1}| = p^{d^2}$ é constante para todo

$i \geq 1$, G é uniforme. Finalmente, como $G/\Phi(G) = \Gamma_{1+\epsilon}/\Gamma_{2+\epsilon}$ é abeliano elementar de ordem p^{d^2}, este tem necessariamente d^2 geradores, de onde segue que $\dim(G)$=rk(G)=d$(G) = d^2$. □

A teoria dos grupos powerful mostra que $\mathrm{GL}_d(\mathbb{Z}_p)$ tem posto finito sem a necessidade de fazer cálculo pesado de matrizes. Se conseguimos mostrar que cada grupo pro-p de posto finito tem uma representação linear fiel sobre $\mathbb{Z}_p$, então isto proporcionará mais uma caracterização para os grupos pro-p de posto finito.

Teorema. *Um grupo pro-p é p-ádico analítico se e somente se é um subgrupo fechado de $GL_d(\mathbb{Z}_p)$ para algum inteiro positivo d.*

4.7 Álgebras de Lie

Seja G um grupo pro-p uniforme. Lembremos que $G_n = P_n(G) = G^{p^{n-1}}$ para cada $n \geq 1$. Sejam $x, y \in G$ e $n \in \mathbb{N}$. Então $[x^{p^n}, y^{p^n}] \in [G_{n+1}, G_{n+1}] \leq G_{2n+2}$. Assim faz sentido definir uma nova operação na forma seguinte:

$$(x, y)_n = [x^{p^n}, y^{p^n}]^{p^{-2n}}$$

Lema 4.7.1 *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 $m > n$

$$(x, y)_m \equiv (x, y)_n \pmod{G_{n+2}}.$$

Para a demonstração veja [Proposição 4.28, [11]].

Definição 4.7.2 Para cada $x, y \in G$ definimos:

$$(x, y) = \lim_{n\to\infty} (x, y)_n. \tag{4.8}$$

Teorema 4.7.3 *Com a operação $(,)$, o $\mathbb{Z}_p$-módulo $(G, +)$ torna-se uma álgebra de Lie sobre $\mathbb{Z}_p$.*

Proposição 4.7.4 *Seja H um subgrupo fechado uniforme de G, e seja $N \lhd_c G$ tal que G/N é uniforme. Então:*

(i) A aplicação inclusão $H \to G$ é um monomorfismo de álgebras de Lie $(H, +, (,)) \to (G, +, (,))$; em particular, H é uma subálgebra 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 aditivas de N em G são as mesmas que as classes multiplicativas, assim $(G/N, +, (,)) = (G, +, (,))/(N, +, (,))$; além disso, o epimorfismo natural $* : G \to G/N$ é um epimorfismo de $\mathbb{Z}_p$-álgebras de Lie de $(G, +, (,))$ para $(G/N, +, (,))$.

Para a demonstração veja [Proposição 4.31, [11]].

Obervação 4.7.5 Com as operações definidas em (4.6) e (4.8) o grupo pro-p uniforme G torna-se uma $\mathbb{Z}_p$-álgebra de Lie. Denotando essa álgebra por $\mathbf{log}(G)$. Seja $f : U \to V$ um homomorfismo entre dois grupos pro-p uniformes. Então $\mathbf{log}(f) = f$ é um homomorfismo de $\mathbb{Z}_p$-álgebras de Lie. Em particular a ação de conjugação faz de $\mathbf{log}(G)$ um G-módulo.

Lema 4.7.6 *Seja G um grupo pro-p uniforme e sejam $i, j \in \mathbb{N}$ tais que $i \leq \jmath \leq 2i + 1$. Então G^{p^i}/G^{p^j} é abeliano e temos que*

$$G^{p^i}/G^{p^j} \cong \mathbf{log}(G)/p^{j-i}\mathbf{log}(G).$$

como G-módulos, onde G age por conjugação sobre G^{p^i}/G^{p^j}.

Demonstração. Pela Proposição 4.2.7 (ii) temos que $[P_i(G), P_j(G)] \leq P_{i+j}(G)$ para todo i e j. Então disso temos que $[P_{i+1}(G), P_{i+1}(G)] \leq P_{2i+2}(G)$. Logo obtemos $[G^{p^i}, G^{p^i}] \leq G^{p^{2i+1}}$ e assim $[G^{p^i}, G^{p^i}] \leq G^{p^{2i+1}} \leq G^{p^{2i}} \leq \cdots \leq G^{p^i}$. Resulta disso que $[G^{p^i}, G^{p^i}] \leq G^{p^j}$, onde $i \leq j \leq 2i + 1$. Assim obtemos que G^{p^i}/G^{p^j} é abeliano para $i \leq j \leq 2i + 1$.

Para a outra parte. Pelo Lema 4.6.13 (iii), $G_n = G^{p^{n-1}} = p^{n-1}\mathbf{log}(G)$. Logo temos que $G^{p^i}/G^{p^j} = p^i\mathbf{log}(G)/p^j\mathbf{log}(G) \cong \mathbf{log}(G)/p^{j-i}\mathbf{log}(G)$. □

Capítulo 5

Grupos p-ádicos analíticos e teoria de Lie

Neste capítulo, lidaremos com alguns resultados dos grupos p-ádicos analíticos e da teoria de Lie, basicamente, para estabelecer um isomorfismo entre as categorias de grupos pro-p uniformes e as álgebras de Lie em $\mathbb{Z}_p$, também mostraremos uma bijeção entre a categoria de grupos p-ádicos analíticos e álgebras de Lie em $\mathbb{Q}_p$, tais bijecções, mantêm a dimensão, que é fundamental para a demonstração do teorema principal desenvolvido no capítulo 7. Tanto a teoria dos grupos p-ádicos analíticos quanto a teoria de Lie podem ser encontradas em J. Dixon [11], de onde obtivemos.

5.1 Variedades p-ádicas analíticas

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

$$\begin{aligned} B(\mathbf{y}, p^{-h}) &= \{\mathbf{z} \in \mathbb{Z}_p^r \mid |z_i - y_i| \leq p^{-h}, \forall i = 1, ..., r\} \\ &= \{\mathbf{y} + p^h\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}_p^r\}. \end{aligned}$$

Definição 5.1.1 Seja V um subconjunto aberto não vazio de $\mathbb{Z}_p^r$ e seja

$$\mathbf{f} = (f_1, ..., f_s)$$

uma função de V em $\mathbb{Z}_p^s$.

(i) Seja $\mathbf{y} \in V$. Então $\mathbf{f}$ é *analítica* em $\mathbf{y}$ se existe $h \in \mathbb{N}$ com $B(\mathbf{y}, p^{-h}) \subseteq V$ e uma série formal de potências $F_i(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ $(i = 1, ..., s)$ tal que

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

(ii) A função $\mathbf{f}$ é *analítica sobre* V se é analítica em cada ponto de V.

Lema 5.1.2 *Suponha que $F(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ pode ser avaliado em $\mathbf{x}$ para todo $\mathbf{x} \in \mathbb{Z}_p^r$. Seja $\mathbf{a} \in \mathbb{Z}_p^r$. Então existe $G(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ tal que $F(\mathbf{x} + \mathbf{a}) = G(\mathbf{x})$ para todo $\mathbf{x} \in \mathbb{Z}_p^r$.*

Corolário 5.1.3 *Suponha que $V \subseteq \mathbb{Z}_p^r$ pode ser escrito como uma união $\bigcup\{B(\mathbf{y}(i), p^{-h(i)}) \mid i \in I\}$ de bolas e que $\mathbf{f} = (f_1, ..., f_s)$ é uma função de V em $\mathbb{Z}_p^s$ tal que, para cada $i \in I$, as*

funções $\mathbf{x} \to f_j(\mathbf{y}(i) + p^{h(i)}\mathbf{x})$ *são estritamente analíticas sobre* $\mathbb{Z}_p^r$ *para* $j = 1, ..., s$. *Então* $\mathbf{f}$ *é analítica sobre* V.

Lema 5.1.3 *Sejam* $\mathbf{f} : U \to V$ *e* $\mathbf{g} : V \to W$ *duas funções analíticas, onde* $U \subseteq \mathbb{Z}_p^r$, $V \subseteq \mathbb{Z}_p^s$ *e* $W \subseteq \mathbb{Z}_p^t$ *são conjuntos abertos não vazios. Então* $\mathbf{g} \circ \mathbf{f}$ *é analítica sobre* V.

Definição 5.1.5 (i) Seja X um espaço topológico e U um subconjunto aberto não vazio de X. Um triplo (U, ϕ, n) é um *carta* sobre X se ϕ é um homeomorfismo de U sobre um subconjunto aberto de $\mathbb{Z}_p^n$ para algum $n \in \mathbb{N}$. A *dimensão* da carta é n. A carta (U, ϕ, n) é uma *carta global* se $U = X$.

(ii) Duas cartas (U, ϕ, n) e (V, ψ, m) sobre um espaço topológico X são *compatíveis* se as aplicações $\psi \circ \phi^{-1}|_{\phi(U \cap V)}$ e $\phi \circ \psi^{-1}|_{\psi(U \cap V)}$ são funções analíticas sobre $\phi(U \cap V)$ e $\psi(U \cap V)$ respectivamente.

(iii) Um *atlas* sobre um espaço topológico X é um conjunto de pares compatíveis de cartas que cobrem X, i.e. é um conjunto da forma

$$A = \{(U_i, \phi_i, n_i) \mid i \in I\}$$

com as seguintes propriedades

- Para cada $i \in I$, (U_i, ϕ_i, n_i) é uma carta sobre X.
- para cada $i, j \in I$, (U_i, ϕ_i, n_i) e (U_j, ϕ_j, n_j) são compatíveis.
- $X = \bigcup_{i \in I} U_i$.

A é um *atlas global* se para algum $i \in I$ a carta (U_i, ϕ_i, n_i) é global.

(iv) Sejam A e B dois atlas sobre um espaço topológico X. Então A e B são *compatíveis* se cada carta em A é compatível com cada carta em B; isto é, se $A \cup B$ é um atlas sobre X.

com X_A nós denotamos o espaço topológico dotado de um atlas A. Uma função $f : X_A \to Y_B$ se diz *analítica* se para cada par de cartas $(U, \phi, n) \in A$ e $(V, \psi, m) \in B$, se satisfaz o seguinte:

(i) $f^{-1}(V)$ é aberto em X, e

(ii) a composição $\psi \circ f \circ \phi^{-1}|_{\phi(u \cap f^{-1}(V))}$ é uma função analítica do conjunto aberto $\phi(U \cap f^{-1}(V)) \subseteq \mathbb{Z}_p^n$ em $\mathbb{Z}_p^m$.

Lema 5.1.6 *Sejam* X, Y *e* Z *espaços topológicos e* A, B, C *atlas sobre* X, Y, Z *respectivamente. Se* $f : X_A \to Y_B$ *e* $g : Y_B \to Z_C$ *são analíticas, então* $g \circ f : X_A \to Z_C$ *é analítica.*

A compatibilidade é uma relação de equivalência sobre a classe de todas os atlas sobre X. Portanto temos

Definição 5.1.7 Seja X um espaço topológico. Uma *estrutura de variedade p-ádica*

analítica sobre X é uma classe de equivalência de atlas compatíveis sobre X. Se tal estrutura existe, X é uma *variedade p-ádica analítica*. Qualquer atlas pertencendo a essa classe de equivalência é chamado um atlas de (a variedade) X; qualquer carta pertencendo para este atlas é uma carta de (a variedade) X.

De agora em diante, vamos escrever "variedade analítica"ou "variedade"no lugar de "variedade p-ádica analítica".

Definição 5.1.8 Sejam X e Y variedades analíticas e $f : X \to Y$ uma função, f é *analítica* se existem dois atlas A e B de X e Y respectivamente tal que $f : X_A \to Y_B$ é analítica.

Lema 5.1.9 *Suponha que $f : X \to Y$ e $g : Y \to Z$ são funções analíticas onde X, Y e Z são variedades analíticas. Então $g \circ f : X \to Z$ é uma função analítica.*

Lema 5.1.10 *Seja $f : X \to Y$ uma função, onde X e Y são variedades. Suponha que $X = \bigcup_{i\in I} X_i$ tal que os X_i são subconjuntos abertos em X e que $f|_{X_i} : X_i \to Y$ são analíticas em relação à estrutura de variedade induzida sobre X_i, para cada $i \in I$. Então f é uma função analítica.*

Lema 5.1.11 *Seja $f : X \to Y$ uma função analítica. Então f é contínua.*

5.2 Grupos p-ádicos analíticos

Definição 5.2.1 Um grupo topológico G é um grupo p-ádico analítico se G tem uma estrutura de variedade p-ádica analítica com as propriedades

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

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

Proposição 5.2.2 *Seja G um grupo topológico contendo um subgrupo aberto H. Suponha que H tem estrutura de grupo p-ádico analítico, e que: para cada $g \in G$, existe uma vizinhança aberta V_g da identidade em H tal que*

(i) *$gVgg^{-1} \subseteq H$ e*

(ii) *a função $k_g : V_g \to H$ definida por $x \mapsto gxg^{-1}$ é analítica.*

Então existe uma única estrutura de variedade analítica sobre G estendendo a estrutura de variedade sobre H e tornando-se G um grupo p-ádico analítico.

Lema 5.2.3 *Sejam G e G' grupos p-ádicos analíticos e seja $\phi : G \to G'$ um homomorfismo de grupos. Suponha que $\phi|_H$ é analítica para um subgrupo aberto H de G. Então ϕ é uma função analítica.*

O seguinte resultado fica dentro dos grupos pro-p uniformes

Teorema 5.2.4 *Seja G um grupo topológico contendo um subgrupo aberto que é um grupo pro-p uniforme. Então G é um grupo p-ádico analítico.*

5.3 Grupos Standard

Nesta seção vamos mostrar o inverso do Teorema 5.2.4.

Sejam $X_1, X_2, ..., Y_1.Y_2, ...$ indeterminadas, então o seguinte

$$\mathbb{Z}_p[[X_1, ..., X_n]] = \mathbb{Z}_p[[\mathbf{X}]]$$

denota o subanel de $\mathbb{Q}_p[[\mathbf{X}]]$ consistente das séries formais de potências

$$F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X_1^{\alpha_1} ... X_n^{\alpha_n} = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \mathbf{X}^\alpha$$

onde $a_\alpha \in \mathbb{Z}_p$ para cada $\alpha \in \mathbb{N}^n$. Notemos que $F(\mathbf{X}) \in \mathbb{Z}_p[[\mathbf{X}]]$ então $F(\mathbf{X})$ existe para todo $\mathbf{x} \in p\mathbb{Z}_p^n$.

Definição 5.3.1 Seja G um grupo p-ádico analítico. Então G é um *grupo standard* (de dimensão r sobre $\mathbb{Q}_p$) se

(i) a estrutura de variedade analítica sobre G é definida por um atlas global da forma $\{(G, \psi, r)\}$ onde ψ é um homeomorfismo de G sobre $p\mathbb{Z}_p^r$ (se $p > 2$) ou sobre $4\mathbb{Z}_2^r$ (se $p = 2$), com $\psi(1) = 0$, e

(ii) para $j = 1, ..., r$ existe $P_j(\mathbf{X}, \mathbf{Y}) \in \mathbb{Z}_p[[\mathbf{X}, \mathbf{Y}]]$ tal que

$$\psi_j(xy^{-1}) = P_j(\psi(x), \psi(y))$$

para todo $x, y \in G$, onde $\psi = (\psi_1, ..., \psi_r)$

Lema 5.3.2 *Seja $G[Y_1, ..., Y_m] \in \mathbb{Z}_p[\mathbf{Y}]$ e sejam $F_i[\mathbf{X}] \in \mathbb{Z}_p[\mathbf{X}]$ para $i = 1, ..., m$. Suponha que cada uma das séries $F_i[\mathbf{X}]$ tenha termo constante 0. Então $G \circ \mathbf{F} \in \mathbb{Z}_p[\mathbf{X}]$ e $(G \circ \mathbf{F})(\mathbf{x}) = G(F_1(\mathbf{x}), ..., F_m(x))$ para todo $\mathbf{x} \in p\mathbb{Z}_p^m$.*

Lema 5.3.3 *Seja G um grupo standard de dimensão r. Seja $\omega(x_1, ..., x_n)$ uma palavra de grupo nas variáveis $x_1, ..., x_n$. Então existe*

$$F_j[X_{11}, ..., X_{1r}, ..., X_{n1}, ..., X_{nr}] \in \mathbb{Z}_p[[\mathbf{X}_1, ..., \mathbf{X}_n]]$$

$(j = 1, ..., r)$ tal que para todo $x_1, ..., x_n \in G$

$$\psi_j(\omega(x_1, ..., x_n)) = F_j(\psi(x_1), ..., \psi(x_n))$$

Lema 5.3.4 *Seja $F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \mathbf{X}^\alpha \in \mathbb{Q}_p[[\mathbf{X}]]$. Suponha que existe uma vizinhança aberta V de 0 em $\mathbb{Q}_p$ tal que, para todos $\lambda_1, ..., \lambda_n \in V^n$,*

$$F(\lambda_1, ..., \lambda_n) = 0$$

Então $a_\alpha = 0$ *para todo* $\alpha \in \mathbb{N}^n$.

Agora estamos prontos para mostrar o primeiro resultado desta seção

Teorema 5.3.5 *Seja* G *um grupo p-ádico analítico. Então* G *tem um subgrupo aberto* H *que é um grupo standard em relação à estrutura de variedade induzida por* G.

Precisamos mais um Lema antes de completar a prova do resultado principal

Lema 5.3.6 *Seja* G *um grupo standard sobre* $\mathbb{Q}_p$ *com um atlas global* $\{(G, \psi, r)\}$. *Então existem séries de potências* $F_1(\mathbf{X}), ..., F_r(\mathbf{X}) \in \mathbb{Z}_p[[\mathbf{X}_1, ..., \mathbf{X}_r]]$ *tal que*

$$\begin{aligned} \psi(x^p) &= F(\psi(x)) \text{ para todo } x \in G \\ F_k(\mathbf{X}) &= pX_k + \sum_{\langle\alpha\rangle>1} c_{k,\alpha}\mathbf{X}^\alpha \text{ para cada } k, \end{aligned}$$

onde $c_{k,\alpha} \in \mathbb{Z}_p$ *para cada* α *e* k. *Também cada* $c_{k,\alpha} \equiv 0(\mod p)$ *onde* $\langle\alpha\rangle = 2$, *sempre que* $p \neq 2$.

Teorema 5.3.7 *Seja* G *um grupo standard de dimensão* r *sobre* $\mathbb{Q}_p$. *Então* G *é um grupo pro-p uniforme de dimensão* r.

Teorema 5.3.8 *Seja* G *um grupo topológico. Então* G *tem estrutura de um grupo p-ádico analítico se e somente se* G *contém um subgrupo aberto que é um grupo pro-p uniforme.*

Corolário 5.3.9 *Um grupo topológico* G *é p-ádico analítico se e somente se* G *tem um subgrupo aberto que é um grupo pro-p de posto finito.*

Corolário 5.3.10 *As seguintes são equivalentes para um grupo topológico* G

(i) G *é um grupo compacto p-ádico analítico.*

(ii) G *contém um subgrupo aberto normal pro-p uniforme de índice finito.*

(iii) G *é um grupo profinito contendo um subgrupo aberto que é um grupo pro-p de posto finito.*

Corolário 5.3.11 *Seja* G *um grupo compacto p-ádico analítico. Então* $\mathrm{Aut}(G)$ *é um grupo compacto p-ádico analítico.*

Definamos a *dimensão* para um grupo p-ádico analítico.

Teorema 5.3.12 *Seja* G *um grupo p-ádico analítico. Então existe um único inteiro não negativo* n *com as seguintes propriedades:*

- *cada carta pertencendo um atlas definindo a estrutura de variedade sobre* G *tem dimensão* n, *no sentido da Definição 5.1.5.*

- *cada subgrupo aberto pro-p de G tem posto finito e dimensão n, no sentido da Definição 4.6.7.*

Definição 5.3.13 Seja G um grupo p-ádico analítico. Então a *dimensão*

$$\dim(G)$$

de G é o número n especificado no Teorema 5.3.12.

5.4 Teoria de Lie

Lema 5.4.1 *Seja G um grupo standard, em relação à carta global (G, ψ, d). Seja $G_2 = P_2(G)$, e seja $\{u_1, ..., u_d\}$ um conjunto de geradores topológicos para G, definamos $\phi : G \to \mathbb{Z}_p^d$ por $\phi(u_1^{\lambda_1}, ..., u_d^{\lambda_d}) = \lambda$ para cada $\lambda = (\lambda_1, ..., \lambda_d) \in \mathbb{Z}_p^d$ Então as cartas $(G, \psi|_{G_2}, d)$ e $(G, \phi|_{G_2}, d)$ são compatíveis.*

Um resultado importante é o seguinte

Teorema 5.4.2 *Sejam G_1 e G_2 grupos p-ádicos analíticos. Então cada homomorfismo contínuo $G_1 \to G_2$ é analítico.*

Corolário 5.4.3 *Seja G um grupo topológico. Então G tem como máximo uma estrutura de grupo p-ádico analítico; e a menos que G seja discreto, o primo p é unicamente determinado.*

Teorema 5.4.4 *Seja G um grupo p-ádico analítico. Sejam H um subgrupo fechado de G e N um subgrupo normal fechado de G.Então*

(i) *H é p-ádico analítico, e a aplicação inclusão $H \to G$ é um homomorfismo analítico.*

(ii) *G/N com a topologia quociente é p-ádico analítico, e a projeção natural $G \to G/N$ e um homomorfismo analítico.*

Teorema 5.4.5 *Seja G um grupo topológico Hausdorff, e N um subgrupo normal fechado. Se ambos N e G/N são p-ádico analíticos (com a topologia induzida e quociente respectivamente), então G é p-ádico analítico.*

5.5 Álgebras de Lie powerful

Nesta seção vamos mostrar como a correspondência que atribui uma álgebra de Lie a cada grupo pro-p uniforme pode ser revertida.

Fixemos

$$\epsilon = 1 \text{ se } p \text{ é ímpar, } \epsilon = 2 \text{ se } p = 2$$

Uma álgebra de Lie L sobre $\mathbb{Z}_p$ é chamada *powerful* se $L \cong \mathbb{Z}_p^d$ para algum inteiro positivo d e

$$(L, L) \subseteq p^{\epsilon} L.$$

A fórmula seguinte é chamada a *fórmula de Campbell-Hausdorff*

$$\begin{aligned} \Phi(X,Y) &= \sum_{n=1}^{\infty} u_n(X,Y) \\ u_1(X,Y) &= X+Y, \;\; u_2 = \frac{1}{2}(X,Y) \\ u_n(X,Y) &= \sum_{\mathbf{e}} q_{\mathbf{e}}(X,Y)_{\mathbf{e}} \;\; (n \geq 3) \end{aligned} \tag{5.1}$$

onde $(X,Y)_{\mathbf{e}} = (X, Y, ..., Y, X, ..., X, ...)$ denota um colchete de Lie esquerda-normado de comprimento $\langle \mathbf{e} \rangle + 1$, e a soma em (5.1) é sobre os vetores $\mathbf{e}$ de inteiros positivos satisfazendo $\langle \mathbf{e} \rangle = n - 1$. Os coeficientes $q_{\mathbf{e}}$ são números racionais satisfazendo

$$p^{\epsilon \langle \mathbf{e} \rangle} q_{\mathbf{e}} \in p^{\epsilon} \mathbb{Z}_p, \; |p^{\epsilon \langle \mathbf{e} \rangle} q_{\mathbf{e}}| \longrightarrow 0 \text{ quando } \langle \mathbf{e} \rangle \longrightarrow \infty$$

Como cada $u_n(X,Y)$ é uma soma finita, podemos avaliar em qualquer álgebra de Lie sobre $\mathbb{Q}_p$; L é uma $\mathbb{Z}_p$-algebra de Lie *powerful*, então de fato $u_n(X,Y)$ pode ser avaliado em L, e para $x, y \in L$ a série

$$\tilde{\Phi}(X,Y) = \sum_{n=1}^{\infty} u_n(X,Y)$$

converge em L. podemos portanto definir uma operação binária $* : L \times L \to L$ por

$$x * y = \tilde{\Phi}(x,y).$$

Teorema 5.5.1 *Seja L uma álgebra de Lie powerful. Então a operação $*$ faz de L um grupo pro-p uniforme. Se $\{a_1, ..., a_d\}$ é uma base para L sobre $\mathbb{Z}_p$ então $\{a_1, ..., a_d\}$ é um conjunto de geradores topológicos para o grupo $(L, *)$, e tem dimensão d.*

Lema 5.5.2 *A operação $*$ sobre uma álgebra de Lie powerful é associativa.*

Teorema 5.5.3 *As aplicações*

$$G \mapsto L_G, \; L \mapsto (L, *)$$

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

Consideremos o grupo p-ádico analítico G. Pelo Teorema 5.3.8 G tem um subgrupo que é um grupo pro-p uniforme. Se H_1 e H_2 são ambos subgrupos abertos uniformes de G, então $H = H_1 \cap H_2$ tem índice finito em H_1 e H_2, assim L_H tem índice finito em L_{H_i} para $i = 1, 2$. Portanto

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_{H_1} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_H = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_{H_2}.$$

Podemos portanto inequivocamente definir

$$\mathcal{L}(G) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_H \tag{5.2}$$

onde H é qualquer subgrupo aberto uniforme de G. Portanto temos

$$\begin{array}{rcll} \dim_{\mathbb{Q}_p}\mathcal{L}(G) & = & \dim_{\mathbb{Z}_p}L_H & \text{(por (5.2))} \\ & = & \mathrm{d}(H) & \text{(Teorema 5.5.1)} \\ & = & \dim(G) & \text{(Definição 4.6.7)} \end{array}$$

e assim $\mathcal{L}(G)$ é a álgebra de Lie sobre $\mathbb{Q}_p$; de dimensão igual a $\dim(H)$=$\dim(G)$.

Agora suponha que $f : G_1 \to G_2$ é um morfismo de grupos analíticos. Escolhemos um subgrupo aberto uniforme H_2 em G_2; como f é contínuo, o subgrupo $f^{-1}(H_2)$ é aberto em G_1, portanto contém um subgrupo aberto uniforme H_1. O homomorfismo de grupos $f_0 = f|_{H_1} : H1 \to H_2$ é ao mesmo tempo um homomorfismo de álgebras de Lie de L_{H_1} para L_{H_2}, como observamos no Teorema 5.5.3; e portanto este induz um homomorfismo de álgebras de Lie

$$f^* = 1 \otimes f_0 : \mathcal{L}(G_1) \to \mathcal{L}(G_2);$$

Claramente f^* não depende da escolha de H_2 e H_1. Também, se $f : G_1 \to G_2$ e $g : G_2 \to G_3$ são morfismos, então

$$(g \circ f)^* = g^* \circ f^*;$$

e $(Id_G)^* = Id_{\mathcal{G}}$ são morfismos. Assim obtemos a primeira parte de

Teorema 5.5.4 *(i) A aplicação $G \mapsto \mathcal{L}(G)$, $f \to f^*$ é um functor da categoria de grupos p-ádicos analíticos(de dimensão d) para a categoria de álgebras de Lie sobre $\mathbb{Q}_p$ (de dimensão d).*

(ii) *Sejam $f_1, f_2 : A \to B$ morfismos de grupos p-ádicos analíticos. Então $f_1^* = f_2^* : \mathcal{L}(A) \to \mathcal{L}(B)$ se e somente se $f_1|_U = f_2|_U$ para algum subgrupo aberto U de A.*

(ii) *Seja G um grupo p-ádico analítico, identificar $\mathcal{L}(G)$ com $\mathbb{Q}_p^d$ escolhendo uma base. Então G tem um subgrupo aberto uniforme H tal que a composição*

$$\phi : H \xrightarrow{Id} L_H \xrightarrow{1\otimes -} \mathcal{L}(G) = \mathbb{Q}_p^d$$

da uma carta (H, ϕ, d) de G.

Capítulo 6

Cohomologia de Grupos Profinitos

Neste capítulo, abordaremos o conceito de Cohomologia de grupos profinitos e, para isso, usaremos teoremas importantes obtidos de J. Neukirch, A. Schmidt and K. Wingberg, "Cohomology of Number Fields"[14] e J. S. Wilson, "Profinite Groups"[15]. O resultado mais importante deste capítulo é o Lemma 6.3.6 que afirma que partir de uma sequência exata curta, obtemos uma sequência exata longa do Grupos de Cohomologia de um grupo profinito G sobre G-módulos topológicos.

6.1 Cohomologia de grupos

Seja G um grupo. Um *G-módulo a direita* é um grupo abeliano A junto com uma aplicação $\sigma : A \times G \to A$. Escrivamos $\sigma(a, g) = ag$. Esta aplicação tem que satisfazer as seguintes condições.

(i) $(a_1 + a_2)g = a_1g + a_2g$, para todos $a_1, a_2 \in A$ e para todo $g \in G$.

(ii) $a(g_1g_2) = (ag_1)g_2$, para todo $a \in A$ e todos os $g_1, g_2 \in G$.

(iii) $a1 = a$, para todo $a \in A$.

Um *G-módulo a esquerda* é definido de forma análoga. Qualquer G-módulo a esquerda pode ser visto como um G-módulo a direita definindo $ag = g^{-1}a$, para todo $a \in A$ e $g \in G$. A partir de agora somente usaremos G-módulos a direita. Então não vamos considerar a palavra *direita* e somente chamaremos de *G-módulo*. Chamaremos A um *G-módulo topológico* se a aplicação σ é contínua.

Definição 6.1.1 Seja G um grupo profinito. Para cada G-módulo topológico A e cada subgrupo H de G escrevemos

$$A^H = \{a \mid ah = a \text{ para todo } h \in H\}$$

Definição 6.1.2 Seja G um grupo profinito e A um G-módulo topológico. Para cada $n \in \mathbb{N}$ e $n > 0$ definimos o conjunto

$$C^n(G, A) = \{f \mid f : G^n \to A \text{ é uma aplicação contínua}\}.$$

Definição 6.1.3 Seja G um grupo profinito e A um G-módulo topológico. Para cada $n \in \mathbb{N}$ e $n > 0$ definimos a aplicação $\partial_n : C^{n-1}(G, A) \to C^n(G, A)$ dada por

$$(\partial_n f)(x_1, ..., x_n) = f(x_2, ..., x_n) + \sum_{i=1}^{n-1} (-1)^i f(x_1, ..., x_i x_{i+1}, ..., x_n) + (-1)^n f(x_1, ..., x_{n-1}) x_n$$

- Se $n = 0$, então $G^{(0)} = 1$.
- $C^0(G, A) = A$.
- $\partial_1 : C^0(G, A) \to C^1(G, A)$ é a aplicação $(\partial_1 a)x = a - ax$
- $\partial_0 : 0 \to C^0(G, A)$ é a aplicação $\partial_0 \equiv 0$.

Lema 6.1.4 *$\partial_{n+1}\partial_n$ é a aplicação 0 de $C^{n-1}(G, A)$ para $C^{n+1}(G, A)$ para cada $n > 0$.*

Definimos

$$B^n(G, A) = \text{im } \partial_n \qquad \text{e} \qquad Z^n(G, A) = \ker \partial_{n+1}.$$

Podemos mostrar por indução sobre n que $B^n(G, A) \lhd Z^n(G, A)$. Assim temos a seguinte definição.

Definição 6.1.5 Seja G um grupo profinito e A um G-módulo topológico. Então $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ é o *n-ésimo grupo de cohomologia de G* com coeficientes no módulo A.
Se $n = 0$, temos

$$\begin{aligned} H^0(G, A) &= \frac{Z^0(G, A)}{B^0(G, A)} = \frac{Z^0(G, A)}{\{0\}} \cong Z^0(G, A) = \{a \in A \mid \partial_1 a = 0\} \\ &= \{a \in A \mid x \mapsto a - ax \text{ é a aplicação 0 sobre } G\} \\ &= A^G \end{aligned}$$

Seja p um primo e G um grupo profinito. O *subgrupo p-Frattini* $\Phi_p(G)$ de G é o fecho do subgrupo abstrato gerado pelo conjunto

$$\{x^{-1}y^{-1}xy \mid x, y \in G\} \cup \{x^p \mid x \in G\}.$$

Lema 6.1.6 *Seja G um grupo profinito. Então $H^1(G, A) = \text{Hom}(G, A)$ para cada G-módulo topológico A sobre o qual G age trivialmente, e*

$$H^1(G, \mathbb{F}_p) = \text{Hom}(G/\Phi_p(G), \mathbb{F}_p),$$

onde $\mathbb{F}_p$ é visto como um módulo sobre o qual G age trivialmente.

6.2 Pares compatíveis de aplicações

Definição 6.2.1 Seja $\theta : G_1 \to G_2$ um homomorfismo contínuo de grupos profinitos, sejam A_i uns G_i-módulos para cada $i = 1, 2$ e $\varphi : A_2 \to A_1$ um homomorfismo contínuo

de grupos topológicos abelianos. O par (θ, φ) é chamado *compatível* se para todo $x \in G_1$ e $a \in A_2$ temos $\varphi(a\theta(x)) = \varphi(a)x$.

Lema 6.2.2 *Sejam $\theta : G_1 \to G_2$ e $\varphi : A_2 \to A_1$ um par compatível.*

(a) *Para cada $n \geq 0$ existe um homomorfismo induzido*

$$(\theta, \varphi)^* : C^n(G_2, A_2) \to C^n(G_1, A_1)$$

definido por $((\theta, \varphi)^* f) = \varphi f(\theta x_1, ..., \theta x_n)$.

(b) *O diagrama*

$$\begin{array}{ccc} C^n(G_2, A_2) & \xrightarrow{\partial} & C^{n+1}(G_2, A_2) \\ \downarrow & & \downarrow \\ C^n(G_1, A_1) & \xrightarrow{\partial} & C^{n+1}(G_1, A_1) \end{array}$$

com as aplicações verticais $(\theta, \varphi)^*$ é comutativa para cada $n \geq 0$.

(c) Para cada $n \geq 0$ existe uma aplicação induzida $H^n(G_2, A_2) \to H^n(G_1, A_1)$ definida por $f + B^n(G_2, A_2) \mapsto (\theta, \varphi)^* f + B^n(G_1, A_1)$ (esta aplicação também é denotada por $(\theta, \varphi)^*$).

Lema 6.2.3

(a) *Se θ, φ são aplicações identidades, então $(\theta, \varphi)^*$ é a aplicação identidade.*

(b) *Se $G_1 \xrightarrow{\theta_1} G_2 \xrightarrow{\theta_2} G_3$ e $A_3 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_1} A_1$ são tais que as aplicações (θ_1, φ_1) e (θ_2, φ_2) são compatíveis, então a aplicação induzida satisfaz $(\theta_2\theta_1, \varphi_1\varphi_2)^* = (\theta_1, \varphi_1)^*(\theta_2, \varphi_2)^*$.*

6.3 A sequência exata longa

Seja G um grupo profinito e sejam A e B de G-módulos. Para cada aplicação $\varphi : A \to B$ existe um homomorfismo $\varphi_n : H^n(G, A) \to H^n(G, B)$ definida por $f + B^n(G, A) \mapsto \varphi f + B^n(G, B)$. Além disso, podemos ver que $H^n(G, -)$ é um functor covariante da categoria de G-módulos para a categoria de grupos abelianos.

(i) Dado um homomorfismo de G-módulos $A \xrightarrow{i} B \xrightarrow{j} C$ temos $j_n i_n = (ji)_n$, e

(ii) se $\varphi : A \to A$ é a aplicação identidade então $\varphi_n : H^n(G, A) \to H^n(G, A)$ é a aplicação identidade.

Uma *sequência exata* de grupos é uma sequência (finita ou infinita)

$$\cdots \longrightarrow G_{n-1} \xrightarrow{f_{n-1}} G_n \xrightarrow{f_n} G_{n+1} \longrightarrow \cdots \tag{6.1}$$

de grupos e homomorfismos tais que $\ker f_n = \text{im } f_{n-1}$ para cada $n \geq 0$.

A sequência em (6.1) se diz *exata em G_n se ker $f_n = \text{im } f_{n-1}$*.

Uma *sequência exata curta* é uma sequência da forma

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 1,$$

ou equivalentemente é uma sequência exata com a propriedade adicional que i é injetiva e j é sobrejetiva.

Definição 6.3.1 Dizemos que a sequência exata curta $1 \to A \xrightarrow{i} B \xrightarrow{j} C \to 1$ de grupos topológicos abelianos é *bem ajustada* ou *split* se

(i) A aplicação i induz um homeomorfismo de A para sua imagem.

(ii) Existe uma função contínua τ (que não é necessariamente um homomorfismo) tal que $j\tau = \mathrm{id}_C$.

Notemos que uma sequência exata curta de grupos abelianos discretos é bem ajustada, assim é também uma sequência exata curta de grupos profinitos abelianos.

Lema 6.3.2

(a) *Seja* $L \xrightarrow{r} M \xrightarrow{s} N$ *uma sequência exata de* G*-módulos, e suponha que existe uma função contínua* $\kappa : \mathrm{im}\, r \to L$ *tal que* $r\kappa$ *é a aplicação identidade em* $\mathrm{im}\, r$*. Então a sequência*

$$C^n(G, L) \xrightarrow{r^*} C^n(G, M) \xrightarrow{s^*} C^n(G, N)$$

de grupos abelianos é exata.

(b) *Se* $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ *é uma sequência exata curta bem ajustada de* G*-módulos, então as sequências*

(i) $0 \to C^n(G, A) \xrightarrow{i^*} C^n(G, B) \xrightarrow{j^*} C^n(G, C) \to 0$ *e*

(ii) $H^n(G, A) \xrightarrow{i_n} H^n(G, B) \xrightarrow{j_n} H^n(G, C)$

são exatas.

No seguinte Lema vamos a construir o homomorfismo de conexão

Lema 6.3.3 *Seja* $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ *uma sequência exata curta bem ajustada de* G*-módulos. Para cada* $n \geq 0$ *existe um homomorfismo*

$$d : H^n(G, C) \to H^{n+1}(G, A)$$

tal que a sequência

$$H^n(G, B) \xrightarrow{j_n} H^n(G, C) \xrightarrow{d} H^{n+1}(G, A) \xrightarrow{i_{n+1}} H^{n+1}(G, B)$$

é exata. Tal homomorfismo d *é chamado o homomorfismo de conexão.*

Teorema 6.3.4 *Para cada sequência exata curta bem ajustada*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

de G*-módulos, existe uma correspondente sequência exata longa*

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G,A) \longrightarrow \cdots$$
$$\cdots \longrightarrow H^n(G,B) \longrightarrow H^n(G,C) \longrightarrow H^{n+1}(G,A) \longrightarrow \cdots$$

de grupos de cohomologia.

Teorema 6.3.5 *Seja $\theta : G_2 \to G_1$ um homomorfismo contínuo de grupos profinitos e*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0 \end{array}$$

um diagrama comutativo onde a linha superior é uma sequência exata curta bem ajustada de G_1 módulos e a linha inferior é uma sequência exata curta bem ajustada de G_2-módulos. Se (θ,α), θ,β e (θ,γ) são pares compatíveis então o seguinte diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1^{G_1} & \longrightarrow & B_1^{G_1} & \longrightarrow & C_1^{G_1} & \longrightarrow & H^1(G_1,A_1) \longrightarrow \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A_2^{G_2} & \longrightarrow & B_2^{G_2} & \longrightarrow & C_2^{G_2} & \longrightarrow & H^1(G_2,A_2) \longrightarrow \cdots \end{array}$$

$$\begin{array}{ccccccc} \cdots \longrightarrow & H^n(G_1,B_1) & \longrightarrow & H^n(G_1,C_1) & \longrightarrow & H^{n+1}(G_1,A_1) & \longrightarrow \cdots \\ & \downarrow & & \downarrow & & \downarrow & \\ \cdots \longrightarrow & H^n(G_2,B_2) & \longrightarrow & H^n(G_2,C_2) & \longrightarrow & H^{n+1}(G_2,A_2) & \longrightarrow \cdots \end{array}$$

comuta.

Seja G um grupo pro-p uniforme finitamente gerado e A um G-módulo topológico. Definimos $C^i_{cts}(G,A) = \{f : G^{(i)} \to A \mid f \text{ é uma função contínua}\}$ e a aplicação fronteira $\partial^{i+1}_A : C^i(G,A) \to C^{i+1}_{cts}(G,A)$ dada por

$$(\partial^{i+1}_A f)(g_1,...,g_{i+1}) = g_1.f(g_2,...,g_{i+1}) + \textstyle\sum_{j=1}^{i}(-1)^j f(g_1,...,g_{j-1},g_j,g_{j+1},g_{j+2},...,g_{i+1}) + (-1)^{i+1} f(g_1,...,g_i).$$

Sejam $Z^i_{cts}(G,A) = \ker\partial^{i+1}_A$ e $B^i_{cts}(G,A) = \mathrm{im}\partial^i_A$. Então

$$H^i_{cts}(G,A) = Z^i_{cts}(G,A)/B^i_{cts}(G,A)$$

é o **i-ésimo grupo de cohomologia contínuo** de G com coeficientes em A.

Usando os mesmos argumentos como na prova do Teorema 6.3.4, obtemos o seguinte Lema.

Lema 6.3.6 *Seja G um grupo profinito, e seja*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

uma sequência exata curta de G-módulos topológicos tal que a topologia de A é induzida pela topologia de B e tal que β é uma seção contínua (somente uma aplicação contínua, não precisa ser um homomorfismo). Então existe um homomorfismo de conexão

$$d : H^n_{cts}(G,C) \to H^{n+1}_{cts}(G,A)$$

e obtemos uma sequência exata

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{d} H^1_{cts}(G,A) \longrightarrow \cdots$$
$$\cdots \longrightarrow H^n_{cts}(G,A) \longrightarrow H^n_{cts}(G,B) \longrightarrow H^n_{cts}(G,C) \xrightarrow{d} H^{n+1}_{cts}(G,A) \longrightarrow \cdots.$$

Agora um resultado sobre a cohomologia de grupos pro-p uniformes.

Proposição 6.3.7 *Seja G um grupo pro-p uniforme tal que $\mathbf{L}(G)$ tem somente derivações internas. Então $|H^1_{cts}(G, \mathbf{log}(G))| < \infty$.*

Demonstração. Temos que G é um grupo pro-p finitamente gerado e $\mathbf{L}(G)$ é uma $\mathbb{Z}_p$-módulo finitamente gerado. Então temos que $H^1_{cts}(G, \mathbf{log}(G))$ é um $\mathbb{Z}_p$-módulo finitamente gerado. Temos também que $H^1_{cts}(G, \mathbf{log}(G)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = H^1_{cts}(G, \mathbf{L}(G))$ (veja [[25], Teorema 3.8.2]). Assim $H^1_{cts}(G, \mathbf{L}(G)) \cong H^1_{cts}(\mathbf{L}(G), \mathbf{L}(G))$ (veja [[25], Teorema 5.2.4]). Então $H^1(\mathbf{L}(G), \mathbf{L}(G)) = \mathrm{Der}(\mathbf{L}(G))/\mathrm{Inn}(\mathbf{L}(G)) = 0$. Logo $H^1_{cts}(G, \mathbf{log}(G)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = 0$ e assim $H^1_{cts}(G, \mathbf{log}(G))$ é um módulo de torsão. Como $H^1_{cts}(G, \mathbf{log}(G))$ é um $\mathbb{Z}_p$-módulo finitamente gerado. Então $H^1_{cts}(G, \mathbf{log}(G))$ é finito. □

Proposição 6.3.8 *Seja G um grupo pro-p uniforme. Suponha que a álgebra de Lie $\mathbf{L}(G)$ consiste somente de derivações internas. Então existe uma constante C tal que*

$$|H^i_{cts}(G, \mathbf{log}(G)/p^i\mathbf{log}(G))| \leq C, \qquad \forall i \geq 1.$$

Demonstração. Seja $\varphi : H^2_{cts}(G, \mathbf{log}(G)) \to H^2_{cts}(G, \mathbf{log}(G))$ uma aplicação definida por $\varphi(\sigma) = p^i\sigma$. Assim $\ker\varphi$ está contido no subgrupo de torsão de $H^2_{cts}(G, \mathbf{log}(G))$.

Por outra parte temos que G é FP_∞ e $\mathbf{log}(G)$ é um $\mathbb{Z}_p$-módulo finitamente gerado. Então $H^2_{cts}(G, \mathbf{log}(G))$ é um $\mathbb{Z}_p$-módulo finitamente gerado. Logo o subgrupo de torsão de $H^2_{cts}(G, \mathbf{log}(G))$ é finito, chamaremos de P esse grupo. Pela Proposição 6.3.7 $H^1_{cts}(G, \mathbf{log}(G))$ é finito e usando o Lema 6.3.6 temos que

$$|H^2_{cts}(G, \mathbf{log}(G))/p^i\mathbf{log}(G))| \leq |H^1_{cts}(G, \mathbf{log}(G))||P| < \infty.$$

□

Capítulo 7

A álgebra de Lie nilpotente de Sato

Este capítulo é essencial para obter o resultado exigido no capítulo 8. O conteúdo na sua totalidade é obtido do trabalho de T. Sato, "The derivations of the Lie algebras"[36], neste artigo Sato consegue obter uma álgebra de Lie de dimensão 41 com coeficientes em um corpo de característica 0. O teorema principal deste capítulo é o Teorema 7.2.1, que mostra que existe uma álgebra de Lie que não possui derivações externas e possui um centro diferente de zero.

7.1 Preliminares e notações

Ao longo desse capítulo vamos supor que as álgebras de Lie tem seus coeficientes em um corpo de característica 0. Para um subconjunto M de um espaço vetorial, denotamos por $\{M\}$ o subespaço gerado pelos elementos de M. Quando M é um subconjunto de uma álgebra de Lie L e k é um número natural, denotamos por M^k o subespaço gerado pelos elementos da forma

$$[m_1, [m_2, [\dots [m_{k-1}, m_k] \dots] \quad (m_1, m_2, \dots, m_k \in M).$$

Uma derivação de uma álgebra de Lie L é uma transformação linear de D para D tal que

$$D[x, y] = [Dx, y] + [x, Dy] \qquad x, y \in L$$

Sejam D_1 e D_2 duas derivações de L. Então $[D_1, D_2] = D_1D_2 - D_2D_1$ define um colchete de Lie. Assim o conjunto de todas as derivações de L formam uma álgebra de Lie. Vamos denotar essa álgebra por $\mathfrak{D}(L)$.

Seja $x \in L$. A aplicação $ad(x) : L \to L$ definida por $(ad(x))(y) = [x, y]$, para todo $y \in L$ é chamada uma *derivação interior de* L. O ideal gerado por todas as derivações interiores é denotado por $\mathfrak{J}(L)$. Seja $Z(L)$ o centro da álgebra de Lie L então $\mathfrak{J}(L) \cong L/Z(L)$. Uma derivação que não é interior será chamada de *derivação exterior*.

Uma álgebra de Lie L é solúvel se sua série derivada termina na subálgebra zero, i.e si existe um $n \in \mathbb{N}$ tal que

$$0 \lhd [L^n, L^n] \lhd \cdots \lhd [L, L] \lhd L$$

O radical de uma álgebra de Lie L é o maior ideal solúvel de L. Denotaremos o radical de $\mathfrak{D}(L)$ por $\mathfrak{R}(L)$. Uma álgebra de Lie é *simples* se ela é uma álgebra de Lie não abeliana

cujos únicos ideais são o ideal zero e a mesma álgebra. Uma álgebra de Lie se chama *semi-simples* se ela é a soma direta de álgebras de Lie simples. Denotamos por $\mathfrak{G}(L)$ á subálgebra semi-simples maximal de $\mathfrak{D}(L)$.

Definição 7.1.1 Seja $\mathfrak{D}(R)$ a álgebra de derivações de um álgebra de Lie solúvel R, e $\mathfrak{G}(R)$ sua subálgebra semi-simples maximal. Se existe uma derivação externa que é comutável com todos os elementos de $\mathfrak{G}(R)$, diremos que R *pertence à classe* $\mathfrak{D}$. Não é difícil mostrar que a definição é independente de $\mathfrak{G}(R)$.

Seja L uma álgebra de Lie real finito-dimensional. Uma *decomposição de Levi* de L é poder escrever L como produto semi-direto de um ideal solúvel e uma subálgebra semi-simples. O ideal solúvel no produto direto é o radical de L. A subálgebra semi-simples no produto direto vamos chamar *subálgebra de Levi.*

Seja L uma álgebra de Lie com as condições antes mencionadas. Seja $L = S + R$ uma decomposição Levi de L. Vamos denotar a restrição de $ad(s)$ para R como $ad_R(s)$. Assim $ad_R S = \{ad_R(s) \mid s \in S\}$.

Proposição 7.1.2 . *Uma álgebra de Lie R não possui derivações externas se e somente se qualquer derivação de R que é comutável com todos os elementos de $ad_R S$ é uma derivação interna.*

Proposição 7.1.3 *Se o radical R da álgebra de lie L pertence à classe $\mathfrak{D}$, então L possui uma derivação externa.*

Proposição 7.1.4 *Se a álgebra de Lie solúvel R é escrito como soma direta de dois ideais R_1 e R_2, e R_1 pertence à classe $\mathfrak{D}$, então R também pertence à classe $\mathfrak{D}$.*

Proposição 7.1.5 *Se a álgebra de Lie possui centro diferente de zero e não possui derivações externas, então L não é solúvel e seu radical é nilpotente; além disso, $L = [L, L]$.*

Então, podemos encontrar muitos exemplos de álgebras de Lie com derivações externas. Mas não foi encontrada uma álgebra de Lie com centro diferente de zero que não possui derivações externas. Na seguinte seção daremos um exemplo de tal álgebra de Lie. Para isso, precisamos construir uma álgebra de Lie nilpotente que não pertence à classe $\mathfrak{D}$.

7.2 Exemplo de uma álgebra de Lie nilpotente que não pertence à classe $\mathfrak{D}$

Teorema 7.2.1 (**Sato**) *Existe uma álgebra de Lie que não possui derivações externas e tem centro diferente de zero.*

Para provar o teorema, vamos a construir uma álgebra de Lie nilpotente N de dimensão 38, e, além disso, uma álgebra de Lie de dimensão 41 cujo radical é N. Sejam $x_1, x_2, ..., x_{38}$ uma base de N, e seja N gerado como álgebra de Lie pelos elementos x_1, x_2, x_3 e x_4. O colchete de Lie em N é dada pela seguinte tabela, mas quando o colchete de Lie não

aparece na tabela consideramos que o mesmo é zero.

$$
\begin{array}{lll}
[x_1,x_2]=x_5 & [x_1,x_4]=x_7 & [x_2,x_4]=x_8 \\
[x_1,x_3]=x_6 & [x_2,x_3]=x_7-x_5 & [x_3,x_4]=x_5
\end{array}
$$

$$
\begin{array}{lll}
[x_1,x_6]=x_9 & [x_2,x_7]=x_{11} & [x_3,x_8]=x_{15} \\
[x_1,x_7]=x_{10} & [x_2,x_8]=x_{12} & [x_4,x_6]=x_{14} \\
[x_1,x_8]=x_{11} & [x_3,x_6]=x_{13} & [x_4,x_7]=x_{15} \\
[x_2,x_6]=x_{10} & [x_3,x_7]=x_{14} & [x_4,x_8]=x_{16}
\end{array}
$$

$$
\begin{array}{lll}
[x_1,x_9]=x_{17} & [x_2,x_{11}]=x_{20} & [x_4,x_{13}]=30x_{35} \\
[x_1,x_{10}]=x_{18} & [x_2,x_{12}]=x_{21} & [x_4,x_{14}]=20x_{36} \\
[x_1,x_{11}]=x_{19} & [x_3,x_{13}]=60x_{34} & [x_4,x_{15}]=15x_{37} \\
[x_1,x_{12}]=x_{20} & [x_3,x_{14}]=30x_{35} & [x_4,x_{16}]=12x_{38} \\
[x_2,x_9]=x_{18} & [x_3,x_{15}]=20x_{36} & \\
[x_2,x_{10}]=x_{19} & [x_3,x_{16}]=15x_{37} &
\end{array}
$$

$$
\begin{array}{lll}
[x_1,x_{17}]=x_{22} & [x_3,x_{18}]=x_{29} & [x_6,x_{11}]=-x_{30} \\
[x_1,x_{18}]=x_{23} & [x_3,x_{19}]=x_{30} & [x_6,x_{12}]=-x_{31} \\
[x_1,x_{19}]=x_{24} & [x_3,x_{20}]=x_{31} & [x_7,x_9]=-x_{29} \\
[x_1,x_{20}]=x_{25} & [x_3,x_{21}]=x_{32} & [x_7,x_{10}]=-x_{30} \\
[x_1,x_{21}]=x_{26} & [x_4,x_{17}]=x_{29} & [x_7,x_{11}]=-x_{31} \\
[x_2,x_{17}]=x_{23} & [x_4,x_{18}]=x_{30} & [x_7,x_{12}]=-x_{32} \\
[x_2,x_{18}]=x_{24} & [x_4,x_{19}]=x_{31} & [x_8,x_9]=-x_{30} \\
[x_2,x_{19}]=x_{25} & [x_4,x_{20}]=x_{32} & [x_8,x_{10}]=-x_{31} \\
[x_2,x_{20}]=x_{26} & [x_4,x_{21}]=x_{33} & [x_8,x_{11}]=-x_{32}
\end{array}
$$

$$
\begin{array}{lll}
[x_2,x_{21}]=x_{27} & [x_6,x_9]=-x_{28} & [x_8,x_{12}]=-x_{33} \\
[x_3,x_{17}]=x_{28} & [x_6,x_{10}]=-x_{29} &
\end{array}
$$

$$
\begin{array}{lll}
[x_1,x_{29}]=x_{34} & [x_3,x_{26}]=-x_{37} & [x_7,x_{20}]=(1/2)x_{37} \\
[x_1,x_{30}]=x_{35} & [x_3,x_{27}]=-x_{38} & [x_7,x_{21}]=(4/5)x_{38} \\
[x_1,x_{31}]=x_{36} & [x_4,x_{22}]=5x_{34} & [x_8,x_{17}]=-4x_{35} \\
[x_1,x_{32}]=x_{37} & [x_4,x_{23}]=2x_{35} & [x_8,x_{18}]=-2x_{36} \\
[x_1,x_{33}]=x_{38} & [x_4,x_{24}]=x_{36} & [x_8,x_{19}]=-x_{37} \\
[x_2,x_{28}]=-5x_{34} & [x_4,x_{25}]=(1/2)x_{37} & [x_8,x_{20}]=(-2/5)x_{38} \\
[x_2,x_{29}]=-2x_{35} & [x_4,x_{26}]=(1/5)x_{38} & [x_9,x_{10}]=-3x_{34} \\
[x_2,x_{30}]=-x_{36} & [x_6,x_{18}]=2x_{34} & [x_9,x_{11}]=-3x_{35} \\
[x_2,x_{31}]=(-1/2)x_{37} & [x_6,x_{19}]=2x_{35} & [x_9,x_{12}]=-3x_{36} \\
[x_2,x_{32}]=(-1/5)x_{38} & [x_6,x_{20}]=2x_{36} & [x_{10},x_{11}]=-x_{36} \\
[x_3,x_{23}]=-x_{34} & [x_6,x_{21}]=2x_{37} & [x_{10},x_{12}]=(-3/2)x_{37} \\
[x_3,x_{24}]=-x_{35} & [x_7,x_{17}]=-4x_{34} & [x_{11},x_{12}]=(-3/5)x_{38} \\
[x_3,x_{25}]=-x_{36} & [x_7,x_{18}]=-x_{35} &
\end{array}
$$

Definimos $U=\{x_1,x_2,x_3,x_4\}$. Podemos verificar que o colchete de Lie definido satisfaz a identidade de Jacobi. Usando o fato $U^7=0$, $[U^2,U^2]=0$ e que x_5 pertence ao centro

de N, podemos também reduzir um pouco o cálculo.

Agora vamos tomar os seguintes endomorfismos lineares de U:

$$\begin{array}{lcl} s_0 & : & x_1 \mapsto x_1,\ \ x_2 \mapsto -x_2,\ \ x_3 \mapsto x_3,\ \ x_4 \mapsto -x_4 \\ s_1 & : & x_1 \mapsto x_2,\ \ x_2 \mapsto 0,\ \ x_3 \mapsto x_4,\ \ x_4 \mapsto 0 \\ s_2 & : & x_1 \mapsto 0,\ \ x_2 \mapsto x_1,\ \ x_3 \mapsto 0,\ \ x_4 \mapsto x_3 \end{array}$$

Então $\mathfrak{G} = \{s_0, s_1.s_2\}$ forma uma álgebra de Lie simples. Vamos ampliar s_0, s_1, s_2 para derivações de N. Isto é possível pois N é decomposto numa soma direta de $\mathfrak{G}$-módulos invariantes irredutíveis como segue

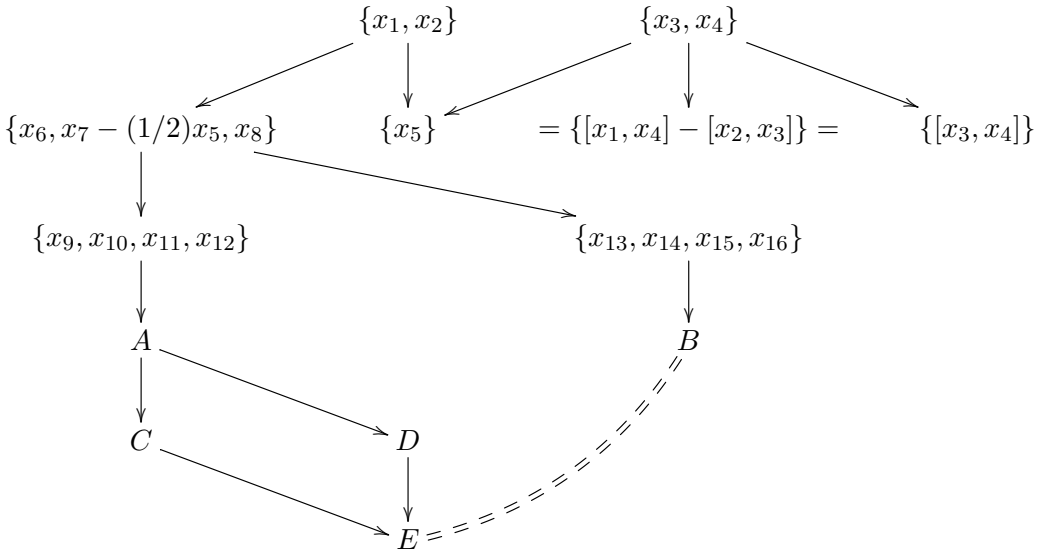
$$\begin{array}{rcl} N & = & \{x_1, x_2\} \oplus \{x_3, x_4\} \oplus \{x_5\} \oplus \{x_6.x_7 - (1/2)x_5, x_8\} \oplus \\ & & \{x_9, x_{10}, x_{11}, x_{12}\} \oplus \{x_{13}, x_{14}, x_{15}, x_{16}\} \oplus \{x_{17}, x_{18}, x_{19}, x_{20}, x_{21}\} \\ & & \oplus\{x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}\} \oplus \{x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}\} \\ & & \oplus\{60x_{34}, 30x_{35}, 20x_{36}, 15x_{37}, 12x_{38}\} \end{array}$$

Em relação à operação de $\mathfrak{G}$, N possui a estrutura indicada no seguinte diagrama. Aqui $\{\quad\}$ é um subespaço $\mathfrak{G}$-irredutível, e denotamos por '$\longrightarrow$' o processo de geração de ideais, e por '===' a identificação de subespaços.

Sejam

- $A = \{x_{17}, x_{18}, x_{19}, x_{20}, x_{21}\}$
- $B = \{[x_3, x_{13}], [x_3, x_{14}], [x_3, x_{15}], [x_3, x_{16}], [x_4, x_{16}]\}$
- $C = \{x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}\}$
- $D = \{x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}\}$
- $E = \{60x_{34}, 30x_{35}, 20x_{36}, 15x_{37}, 12x_{38}\}$

Então



Agora vamos provar que a álgebra de Lie nilpotente N não pertence à classe $\mathfrak{D}$. Seja D uma derivação de N comutável com todos os elementos de $\mathfrak{G}$. Não existe um somando direto de N que seja $\mathfrak{G}$-isomorfo a $\{x_1, x_2\}$ ou $\{x_3, x_4\}$ aparte de eles mesmos. Portanto pelo Lema de Schur, D deve ter a seguinte forma:

$$\begin{aligned} Dx_1 &= \alpha x_1 + \gamma x_3 & \qquad Dx_3 &= \beta x_3 + \delta x_1 \\ Dx_2 &= \alpha x_2 + \gamma x_4 & \qquad Dx_4 &= \beta x_4 + \delta x_2 \end{aligned}$$

Então D age sobre N como segue:

$$\begin{aligned} x_5 &= [x_1, x_2] \to [\alpha x_1 + \gamma x_3, x_2] + [x_1, \alpha x_2 + \gamma x_4] = (2\alpha + \gamma)x_5 \\ x_5 &= [x_3, x_4] \to [\beta x_3 + \delta x_1, x_4] + [x_3, \beta x_4 + \delta x_2] = (2\beta + \delta)x_5 \\ x_5 &= [x_1, x_4] - [x_2, x_3] \to [\alpha x_1 + \gamma x_3, x_4] + [x_1, \beta x_4 + \delta x_2] \\ &\quad -[\alpha x_2 + \gamma x_4, x_3] - [x_2, \beta x_3 + \delta x_1] = (\alpha + \beta + 2\gamma + 2\delta)x_5 \\ x_6 &= [x_1, x_3] \to [\alpha x_1 + \gamma x_3, x_3] + [x_1, \beta x_3 + \delta x_1] = (\alpha + \beta)x_6 \\ x_9 &= [x_1, x_6] \to [\alpha x_1 + \gamma x_3, x_6] + [x_1, (\alpha + \beta)x_6] \\ &\quad = (2\alpha + \beta)x_9 + \gamma x_{13} \\ 0 &= [x_3, x_9] \to [\beta x_3 + \delta x_1, x_9] + [x_3, (2\alpha + \beta)x_9 + \gamma x_{13}] \\ &\quad = \delta x_{17} + 60\gamma x_{34} \end{aligned}$$

Portanto temos

$$\begin{gathered} 2\alpha + \gamma = 2\beta + \delta = \alpha + \beta + 2\gamma + 2\delta \\ \gamma = \delta = 0, \end{gathered}$$

isto implica que $\alpha = \beta$. Então,

$$\begin{gathered} x_{13} = [x_3, x_6] \to [\alpha x_3, x_6] + [x_3, 2\alpha x_6] = 3\alpha x_{13} \\ [x_3, x_{13}] \to [\alpha x_3, x_{13}] + [x_3, 3\alpha x_{13}] = 4\alpha [x_3, x_{13}] \\ x_{34} = [x_1, x_{29}] = [x_1, [x_3, [x_1, [x_1, x_4]]]] \to 6\alpha x_{34}. \end{gathered}$$

Como $[x_3, x_{13}] = 60x_{34}$, conseguimos

$$\alpha = \beta = \gamma = \delta = 0, \text{ assim } D = 0$$

Portanto a derivação de N que é comutável com todos os elementos de $\mathfrak{G}$ é somente 0, e assim N não pertence a $\mathfrak{D}$. Quando tomamos a soma semi direta $\mathfrak{G} + N$, temos o centro $\{x_5\}$ que é diferente de zero, e não temos derivações externas pela Proposição 7.1.2. Portanto o teorema está provado. Observamos que $[\mathfrak{G} + N, \mathfrak{G} + N] = \mathfrak{G} + N$, como menciona a Proposição 7.1.5.

Capítulo 8

Teorema principal

Neste capítulo desenvolveremos o trabalho realizado por González-Sánchez e Jaikin-Zapirain, "Finite p-groups with small automorphism group"[13]. Para isso vamos usar a álgebra de Lie de dimensão 41 discutida na seção 7.2 e do Teorema 5.5.3 para obter um grupo pro-p uniforme também de dimensão 41. Nessa forma vamos encontrar um exemplo de um p-grupo finito não abeliano de ordem maior do que a ordem de seu grupo de automorfismos.

8.1 Teorema principal

Consideramos a álgebra de Lie $M = \mathfrak{G}+N$ de dimensão 41 construída na seção 7.2. Vamos considerar que a álgebra tem seus coeficientes no corpo $\mathbb{Q}$ que tem característica 0. Assim M é uma $\mathbb{Q}$-álgebra de Lie. A álgebra M possui um subanel M_0 tal que $M = M_0 \otimes_{\mathbb{Z}} \mathbb{Q}$. Seja $L = p^2(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. Então $L \cong \mathbb{Z}_p^{41}$ como $\mathbb{Z}_p$-módulo e $[M, M] = [\mathfrak{G} + N, \mathfrak{G} + N] = \mathfrak{G} + N$. Note que

$$\begin{aligned}[L, L] = [p^2(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p), p^2(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p)] &\subseteq p^4(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p) = p^2(p^2 M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p) \\ &= p^2 L.\end{aligned}$$

Assim pela la seção 5.5 do Capítulo 5 temos que L é uma $\mathbb{Z}_p$-álgebra de Lie powerful.

Seja $U = \mathbf{exp}(L)$. Então U é um grupo pro-p uniforme (Teorema 5.5.1) e $L = \mathbf{log}(U)$ (Observação 4.7.5). Além disso

$$\begin{aligned}\mathbf{L}(U) &\cong L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \\ &\cong M \otimes_{\mathbb{Q}} \mathbb{Q}_p.\end{aligned}$$

Assim obtemos o seguinte Lema.

Lema 8.1.1 *A $\mathbb{Q}_p$-álgebra de Lie $\mathbf{L}(U)$ tem dimensão 41, seu centro tem dimensão 1 e $\mathrm{Der}(\mathbf{L}(U))$ consiste somente de derivações internas.*

Seja $U_i = U/U^{p^i}$. Denotemos por $\rho_{i,j} : \mathrm{Aut}(U_i) \to \mathrm{Aut}(U_j)$ (para $i \geq j$), as aplicações

$$\rho_{i,j}(\alpha)(uU^{p^j}) = \alpha(uU^{p^i})U^{p^j}, \text{ para todo } \alpha \in \mathrm{Aut}(U_i),\ u \in U.$$

Proposição 8.1.2 *Existe uma constante $k \in \mathbb{N}$ tal que, para todo $i \geq 2k$.*

$$\ker\rho_{i,k} \leq \mathrm{Inn}(U_i)\ker\rho_{i,i-k}. \tag{8.1}$$

Demonstração. Pela Proposição 6.3.8 existe uma constante C tal que

$$|H^1_{cts}(U, \mathbf{log}(U)/p^i\mathbf{log}(U))| \leq C$$

por isso existe $k \in \mathbb{N}$ tal que $p^k H^1_{cts}(U, \mathbf{log}(U)/p^i\mathbf{log}(U)) = 0$ para todo i provaremos a proposição por indução sobre i.

Se $i = 2k$, então $\ker\rho_{2k,k} \leq \mathrm{Inn}(U_{2k})\ker\rho_{2k,k}$. Agora suponha que a proposição seja válida para i. Provaremos a mesma para $i+1$. Seja $\phi \in \ker\rho_{i+1,k}$. Do diagrama comutativo

$$\begin{array}{ccc} \mathrm{Aut}(U_{i+1}) & \xrightarrow{\rho_{i+1,k}} & \mathrm{Aut}(U_k) \\ {\scriptstyle \rho_{i+1,i}}\downarrow & \nearrow_{\rho_{i,k}} & \\ \mathrm{Aut}(U_i) & & \end{array}$$

segue que $\rho_{i,k} \circ \rho_{i+i,i}(\phi) = \rho_{i+1,k}(\phi) = id_{U_k}$, assim $\rho_{i+i,i}(\phi) \in \ker\rho_{i,k}$. Pela hipótese indutiva temos que $\ker\rho_{i,k} \leq \mathrm{Inn}(U_i)\ker\rho_{i,i-k}$, segue que $\rho_{i+i,i}(\phi) \in \mathrm{Inn}(U_i)\ker\rho_{i,i-k}$ e portanto $\phi \in \ker\rho_{i+1,i-k}\mathrm{Inn}(U_{i+1})$. Sem perda de generalidade, vamos supor que $\phi \in \ker\rho_{i+1,i-k}$. Definamos a seguinte função

$$\begin{aligned} s : U &\to U^{p^{i-k}}/U^{p^{i+1}} \\ u &\mapsto \phi(uU^{p^{i+1}})u^{-1}. \end{aligned}$$

Então

$$\begin{aligned} s(u_1, u_2) &= \phi(u_1, u_2U^{p^{i+1}})u_2^{-1}u_1^{-1} \\ &= \phi(u_1U^{p^{i+1}})u_1^{-1}u_1\phi(u_2U^{p^{i+1}})u_2^{-1}u_1^{-1} \\ &= s(u_1)u_1s(u_2)u_1^{-1}. \end{aligned}$$

Assim $s \in \mathcal{Z}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$. Pelo Lema 4.7.6, $U^{p^{i-k}}/U^{p^{i+1}}$ é abeliano, pois $i-k \leq i+1 \leq 2(i-k)+1$ e

$$U^{p^{i-k}}/U^{p^{i+1}} \cong \mathbf{log}(U)/p^{k+1}\mathbf{log}(U)$$

como U-módulo. Em particular;

$$p^k H^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}}) = 0 \qquad (\text{para } i = k+1)$$

Consideramos a seguinte sequência exata de U-módulos:

$$1 \longrightarrow U^{p^{i-k+1}}/U^{p^{i+1}} \xrightarrow{\alpha} U^{p^{i-k}}/U^{p^{i+1}} \xrightarrow{\beta} U^{p^i}/U^{p^{i+1}} \longrightarrow 1$$

onde $\alpha(uU^{p^{i+1}}) = uU^{p^{i+1}}$ e $\beta(uU^{p^{i+1}}) = u^{p^k}U^{p^{i+1}}$. Então temos que a sequência

$$H^1_{cts}(U, U^{p^{i-k+1}}/U^{p^{i+1}}) \xrightarrow{\alpha^*} H^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}}) \xrightarrow{\beta^*} H^1_{cts}(U, U^{p^i}/U^{p^{i+1}})$$

é exata pelo Lema 6.3.6. Assim $\mathrm{im}\,\alpha^* = \ker\beta^* = H^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$. Logo existe $s' \in \mathcal{Z}^1_{cts}(U, U^{p^{i-k+1}}/U^{p^{i+1}})$ tal que $\alpha^*(s'\mathcal{B}^1_{cts}(U, U^{p^{i-k+1}}/U^{p^{i+1}})) = s\mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$. Daqui segue que

$s'\mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}}) = s\mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$ e portanto $(s')^{-1}s \in \mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$. Assim podemos obter um v em $U^{p^{i-k}}/U^{p^{i+1}}$ tal que para todo $u \in U$ temos que $(s')^{-1}(u)s(u) = [v, u]$ ou de igual forma $s(u) = s'(u)vuv^{-1}u^{-1}$. Logo obtemos que

$$\begin{aligned}\phi(uU^{p^{i+1}}) &= s(u)u = s'(u)vuv^{-1} \\ &= (s'(u)u)u^{-1}vuv^{-1} \\ &= (s'(u)u)[u^{-1}, v].\end{aligned}$$

Se definimos $\psi(u) = c'(u)u$. Não é difícil mostrar que $\psi \in \rho_{i+1.i+1-k}$. Assim $\phi \in \ker\rho_{i+1,i+1-k}\mathrm{Inn}(U_{i+1})$. □

Corolário 8.1.3 *Existe uma constante D tal que*

$$|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)| \leq D \text{ para todo } i.$$

Demonstração. Pela proposição anterior e usando o fato que $\mathrm{Inn}(U_i) \cap \ker\rho_{i,i-k} = id_{U_i}$ temos que

$$\begin{aligned}|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)| &\leq |\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)\ker\rho_{i,i-k}||\mathrm{Inn}(U_i)\ker\rho_{i,i-k} : \mathrm{Inn}(U_i)| \\ &\leq |\mathrm{Aut}(U_i) : \ker\rho_{i,k}||\ker\rho_{i,i-k}| \leq |\mathrm{Aut}(U_k)||\ker\rho_{i,i-k}|.\end{aligned}$$

Agora, como $\mathbf{L}(U)$ tem dimensão 41 segue que $\mathrm{d}(U) = 41$ e sabendo que $U_i = U/U^{p^i}$ obtemos $\mathrm{d}(U_i) = 41$. Além disso, por (4.3), $|U^{p^{i-k}}/U^{p^i}| = p^{41k}$.

Consideramos $\alpha \in ker\rho_{i,i-k}$ e $uU^{p^i} \in U_i$ então $\rho_{i,i-k}(\alpha)(uU^{p^{i-k}}) = \alpha(uU^{p^i})U^{p^{i-k}} = uU^{p^{i-k}}$, assim $\alpha(uU^{p^i})U^{p^{i-k}} = uU^{p^{i-k}}$. Seja $\alpha(uU^{p^i}) = vU^{p^i}$ para algum $v \in U$ temos que $(vU^{p^i})U^{p^{i-k}} = uU^{p^{i-k}}$ e portanto $v^{-1}u \in U^{p^{i-k}}$. Logo $v^{-1}u = \overline{u} \in U^{p^{i-k}}$ e

$$\alpha(uU^{p^i}) = vU^{p^i} = u\overline{u}^{-1}U^{p^i}, \qquad \text{onde } \overline{u}^{-1}U^{p^i} \in U^{p^{i-k}}/U^{p^i}.$$

Assim temos que as possibilidades de $\alpha(uU^{p^i})$ são no máximo $|U^{p^{i-k}}/U^{p^i}| = p^{41k}$ e sabendo que a base tem 41 elementos obtemos que $|ker\rho_{i,i-k}| \leq p^{(41)^2k}$ e portanto

$$|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)| \leq p^{(41)^2k}.|\mathrm{Aut}(U_k)| = D. \tag{8.2}$$

o que queríamos provar. □

O principal resultado que queremos alcançar é o seguinte teorema que afirma que existe um p-grupo finito não abeliano cuja ordem é maior do que a ordem do grupo de seus automorfismos.

Teorema 8.1.4 *Para cada primo p existe uma família de p-grupos finitos $\{U_i\}$ tal que*

$$\lim_{i\to\infty} |U_i| = \infty \qquad \text{e} \qquad \limsup_{i\to\infty} \frac{|\mathrm{Aut}U_i|}{|U_i|^{40/41}} < \infty.$$

Em particular, para cada primo p, existe um p-grupo finito não abeliano G tal que $|\mathrm{Aut}(G)| < |G|$.

Demonstração. Pela Definição 4.6.1 e a Proposição 4.6.4,

$$|U_i| = |U : U^{p^i}| = |U : U^p||U^p : U^{p^2}| \cdots |U^{p^{i-1}} : U^{p^i}| = p^{41}p^{41} \cdots p^{41} = p^{41i}.$$

Assim temos que

$$\lim_{i\to\infty} |U_i| = p^{41i} = \infty \tag{8.3}$$

Definimos o seguinte homomorfismo

$$\begin{aligned} \sigma : Z(U) &\to Z(U_i) \\ u &\mapsto uU^{p^i} \end{aligned}$$

Seja $v \in \ker\sigma$. Então $v \in Z(U)$ e $v \in U^{p^i}$. Assim $\ker\sigma \subseteq Z(U) \cap U^{p^i}$. Agora consideramos w na interseção $Z(U) \cap U^{p^i}$. Logo $Z(U) \cap U^{p^i} \subseteq \ker\sigma$. Então pelo primeiro teorema de isomorfismo de grupos temos que

$$\frac{Z(U)}{Z(U) \cap U^{p^i}} \leq Z(U_i),$$

e pelo segundo teorema de isomorfismo de grupos $Z(U)/Z(U) \cap U^{p^i} \cong U^{p^i}Z(U)/U^{p^i}$. Por outro lado $\mathrm{Inn}U_i \cong U_i/Z(U_i)$. Assim temos que

$$|\mathrm{Inn}(U_i)| = |U_i/Z(U_i)| = \frac{|U/U^{p^i}|}{|Z(U_i)|} \leq \frac{|U/U^{p^i}|}{|U^{p^i}Z(U)/U^{p^i}|} = |U/U^{p^i}Z(U)|. \tag{8.4}$$

A última igualdade é usando o terceiro teorema de isomorfismo de grupos.

Como $\dim(Z(U))=1$ e $\dim(U) = 41$, então $\dim(U/Z(U))=40$. Assim Temos que

$$|(U/Z(U))/(U/Z(U))^{p^i}| = p^{40i}$$

E usando os teoremas de isomorfismo obtemos

$$|U/U^{p^i}Z(U)| = |(U/Z(U))/(U/Z(U))^{p^i}| = p^{40i} \tag{8.5}$$

De (8.4) e (8.5) obtemos que

$$|\mathrm{Inn}U_i| \leq |U/U^{p^i}Z(U)| = p^{40i}$$

Pelo Corolário 8.1.3 temos que

$$\begin{aligned} |\mathrm{Aut}(U_i)| &= |\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)||\mathrm{Inn}(U_i)| \\ &\leq Dp^{40i} \end{aligned}$$

sendo D a constante em (8.2). Disso segue que

$$\frac{|\mathrm{Aut}(U_i)|}{|U_i|^{40/41}} \leq \frac{Dp^{40i}}{p^{40i}} = D,$$

Vamos supor que para todo i temos que $|U_i| \leq |\mathrm{Aut}(U_i)|$. Então

$$|U_i|^{1/41} = \frac{|U_i|}{|U_i|^{40/41}} \leq \frac{|\mathrm{Aut}(U_i)|}{|U_i|^{40/41}} \leq D, \tag{8.6}$$

o que contradiz (8.3). Isso termina a demonstração. □

Referências Bibliográficas

[1] A. D. Otto, "Central automorphisms of a finite p-group", *Trans. Amer. Math. Soc.* **125** (1966), 280-287.

[2] A. Lubotzky and A. Mann, "Powerful p-Groups. II. p-Adic Analytic Groups", *Journal of Algebra* **105**, 506-515 (1987).

[3] A. Thillaisundaram, "The automorphism group for p-central p-groups", *Int. J. Group Theory* **1** (2012), 59-71.

[4] B. Eick, "Automorphism groups of 2-groups", *J. Algebra* **300** (2006), 91 -101.

[5] B. Klopsch, "Five lectures on analytic pro-p groups: a meeting-ground between finite p-groups and Lie theory", *University of Oxford*, september (2007).

[6] D. A. Craven, "The Theory of p-Groups", *Hilary Term*, 2008.

[7] E. Schenkman, "The existence of outer automorphisms of some nilpotent groups of class 2", *Proc. Amer. Math. Soc.* **6** (1955), 6 -11.

[8] G. A. Fernández-Alcober, "An introduction to finite p-groups: regular p-groups and groups of maximal class", *Matematika Saila, Euskal Herriko Unibersitatea* 48080 Bilbao (Spain)

[9] G. C. Cook, "On Profinite Groups of Type FP_∞", *Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK*, 2010.

[10] J. Buckley, "Automorphism groups of isoclinic p-groups", *J. Lond. Math. Soc.* (2) **12** (1975/76), 37 -44.

[11] J. Dixon, M. du Sautoy, A. Mann and D. Segal, "Analytic Pro-p Groups", 2nd edn (Cambrifge University Press. Cambridge, 1999).

[12] J. D. V. Caicedo, "La conjetura de Serre sobre la multiplicidad de la intersección de dos módulos", *Revista de la Facultad de Ciencias, Universidad Nacional de Colombia, Seccional Medellín. No. 3* (1993).

[13] González-Sánchez e Jaikin-Zapirain, "Finite p-groups with small automorphism group", in *Forum of Mathematics, Sigam* (2015), Vol.3, e7, 11 pages.

[14] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd edn, Grundlehren der Mathematischen Wissenschaften, 323 (Springer, Berlin, 2008).

[15] J. S. Wilson, "Profinite Groups", *School of Mathematics and Statistics. University of Birmingham*, 1997.

[16] K. G. Hummel, "The order of the automorphism group of a central product", *Proc. Amer. Math. Soc.* 47 (1975), 37 -40.

[17] K. S. Brown, "Finiteness properties of groups", *Journal of Pure and Applied Algebra* 44 (1987) 45-75, North Holland.

[18] L. Sylow, "Théorèmes sur les groupes de subtitutions", *Methamtische Annalen* **5** (1872), 584-594. Translation into English by Robert Wilson.

[19] M. d. Sautoy, D. Segal, A. Shalev, "New Horizons in pro-p Groups", *Progress in Mathematics*, Vol. 184, (Springer, 2000).

[20] M. D. Fried and M. Jarden, "Field Arithmetic", *A Series of Modern Surveys in Mathematics*. Second Edition.

[21] M. K. Yadav, "On automorphisms of finite p-groups", *J. Group Theory* **10** (2007), 859 -866.

[22] M. Lazard, "Groupes analytiques p-adiques", *Publ. Math. Inst. Hautes Études Sci.* **26**(1965), 389-603.

[23] N. Gavioli, "The number of automorphisms of groups of order p^7", *Proc. R. Irish Acad. Sect.* A **93** (1993), 177 -184.

[24] N. Nikolov and D. Segal, "On finitely gerated profinite groups, I: strong completeness and uniform bounds", *Annals of Mathematics*, **165** (2007), 171-238.

[25] P. Symonds and T. Weigel, "Cohomology of p-adic analytic groups", in *New Horizons in Pro-p Groups*, Progress in Mathematics, 184 (Birkhäuser, Boston, MA, 2000), 349-410.

[26] R. Faudree, "A note on the automorphism group of a p-group", *Proc. Amer. Math. Soc.* **19** (1968), 1379 -1382.

[27] R. M. Davitt, "The automorphism group of a finite metacyclic p-group", *Proc. Amer. Math. Soc.* **25** (1970), 876 -879.

[28] R. M. Davitt, "The automorphism group of finite p-abelian p-groups", *Illinois J. Math.* **16** (1972), 76 -85.

[29] R. M. Davitt, "On the automorphism group of a finite p-group with a small central quotient", *Canad. J. Math.* **32** (1980), 1168 -1176.

[30] R. M. Davitt and A. D. Otto, "On the automorphism group of a finite p-group with the central quotient metacyclic", *Proc. Amer. Math. Soc.* **30** (1971), 467 -472.

[31] R. M. Davitt and A. D. Otto, "On the automorphism group of a finite modular p-group", *Proc. Amer. Math. Soc.* **35** (1972), 399 -404

[32] R. Ree, "The existence of outer automorphisms of some groups II", *Proc. Amer. Math. Soc.* **9** (1958), 105 -109.

[33] S. Fouladi, A. R. Jamali and R. Orfi, "Automorphism groups of finite p-groups of coclass 2", *J. Group Theory* **10** (2007), 437 -440.

[34] T. Exarchakos, "LA-groups", *J. Math. Soc. Japan* **33** (1981), 185 -190.

[35] T. Exarchakos, "On p-groups of small order",*Publ. Inst. Math. (Beograd) (N.S.)* **45**(59) (1989), 73 -76.

[36] T. Sato, "The derivations of the Lie algebras", *Tôhoku Math. J.***23**(1971),21-36. Volume 11, 2000.

[37] V. D. Mazurov and E. I. Khukhro, *The Kourovka Notebook. Unsolved Problems in Group Theory*, 17th augmented edn (Russian Academy of Sciences Siberian Division, Institute of Mathematics, 2010).

[38] W. Gaschütz, "Kohomologische Trivialitäten und äussere Automorphismen von p-Gruppen", *Math. Z.* **88** (1965), 432 -433.