UMA CARACTERIZAÇÃO DOS SUBGRUPOS VERBAIS FECHADOS DE GRUPOS PRO-P FINITAMENTE GERADOS

Lucas Corrêa Lopes

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

Orientador: Ilir Snopche Ph.D.

Rio de Janeiro
Dezembro de 2021

UMA CARACTERIZAÇÃO DOS SUBGRUPOS VERBAIS FECHADOS DE GRUPOS PRO-P FINITAMENTE GERADOS

Lucas Corrêa Lopes

DISSERTAÇÃO DE MESTRADO APRESENTADA AO PROGRAMA DE PÓS-GRADUAÇÃO DO INSTITUTO DE MATEMÁTICA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO TÍTULO DE MESTRADO EM MATEMÁTICA.

Trabalho aprovado por:

Prof. Ilir Snopche, Ph.D. (Orientador)

Prof. Slobodan Tanushevski, Ph.D. (Convidado 1)

Prof. Francesco Noseda, Ph.D. (Convidado 2)

RIO DE JANEIRO, RJ – BRASIL
NOVEMBRO DE 2021

CIP - Catalogação na Publicação

CC824c

Corrêa Lopes, Lucas
Uma caracterização dos subgrupos verbais fechados de grupos pro-p finitamente gerados / Lucas Corrêa Lopes. -- Rio de Janeiro, 2021.
75 f.

Orientador: Ilir Snopche.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-Graduação em Matemática, 2021.

1. grupos pro-p. 2. grupos livres. 3. largura verbal. 4. grupos analíticos. I. Snopche, Ilir, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

Dedicado à Alexandre Soares Lopes, meu pai.

Agradecimentos

Agradeço primeiro à Deus que me deu força e guiou meu caminho até aqui. Também quero agradecer à minha família por todo apoio e a todos os amigos que fizeram parte da minha vida nesses anos.

Agradeço ao meu orientador Ilir Snopche por todo suporte na escrita desta dissertação, assim como por tudo que me ensinou durante meu tempo na UFRJ.

Agradeço aos professores Slobodan Tanushevski, Francesco Noseda, Martino Garonzi e Aftab Pande por aceitarem compor a banca da defesa da minha dissertação e, consequentemente, dedicarem uma parte do seu tempo à leitura deste trabalho.

Agradeço à CAPES pelo suporte financeiro que possibilitou a conclusão deste trabalho.[1]

[1] O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Resumo

Seja F um grupo livre com k geradores independentes. Nós chamaremos um elemento w de F de uma palavra. Se G é um grupo, então dizemos que $g \in G$ é um w-valor de G se existem $g_1, ..., g_k \in G$ tais que $g = w(g_1, ..., g_k)^{\pm 1}$. Denotaremos o conjunto de todos os w-valores em G por G_w. Um simples argumento (veja [8]) mostra que se G é profinito, então $w(G)$ (o subgrupo abstrato gerado por G_w) é fechado se, e somente se, existe l tal que qualquer elemento de $w(G)$ é um produto de, no máximo, l elementos de G_w. O menor dentre os números l é chamado de largura de w em G. O principal objetivo deste trabalho é apresentar uma demonstração de que uma palavra não trivial w de um grupo livre F tem largura finita em todo grupo pro-p finitamente gerado se, e somente se, $w \notin (F')^p F''$. Além disso, também apresentaremos uma demonstração de que que qualquer palavra w tem largura finita em um grupo p-ádico compacto.

Este trabalho é baseado no artigo "On the verbal width of finitely generated pro-p groups", de Andrei Jaikin-Zapirain (see [9]).

Abstract

Let F be a free group on k independent generators. We will call an element w from F a word. If G is a group, then we say that $g \in G$ is a w-value in G if there are $g_1, ..., g_k \in G$ such that $g = w(g_1, ..., g_k)^{\pm 1}$. We denote the set of the all w-values in G by G_w. A simple argument (see [8]) shows that if G is profinite, then $w(G)$ (the abstract subgroup generated by G_w) is closed if and only if there exists l such that any element from $w(G)$ is a product of at most l elements from G_w. The smallest such number l is called the width of w in G. The main purpose of this work is to present a proof that a non-trivial word w from a free group F has finite width in every finitely generated pro-p group if and only if $w \notin (F')^p F''$. Also we will present a proof that any word w has finite width in a compact p-adic group.

This work is based on the article "On the verbal width of finitely generated pro-p groups", by Andrei Jaikin-Zapirain (see [9]).

Sumário

Introdução

Um alfabeto é formado por letras e a justaposição dessas letras forma as palavras. Uma letra nada mais é do que um símbolo e assim, um alfabeto é um conjunto de símbolos, então as palavras são formadas por justaposição desses símbolos. Essa é a ideia intuitiva de uma palavra, do ponto de vista da matemática. De forma mais precisa, uma palavra w é uma expressão da forma $w(x_1, ..., x_n) = \prod_{j=1}^{s} x_{i_j}^{\epsilon_{i_j}}$ onde x_{i_j} são símbolos e $\epsilon_{i_j} = \pm 1$. Se G for um grupo, então uma palavra w em G é formada de maneira que os seus símbolos sejam os elementos de G. Para cada n-upla $g_1, ..., g_n$ de elementos de G, $w(g_1, ..., g_n)$ assume um valor, o subgrupo gerado por todos os valores assumidos por w é o subgrupo verbal correspondente à palavra w. Observe que, ao fazer as justaposições dos valores assumidos por w, as palavras resultantes podem ter cada vez mais elementos em sua composição, isto é, elas podem ficar cada vez mais "largas". Pode ser que exista um limite para esse crescimento, ou seja, a largura de cada palavra é limitada por um valor. Esse é o caso que nos interessa. Quando G é um grupo arbitrário, ainda é muito difícil estabelecer critérios gerais relacionados à largura de palavras, em nosso caso trabalharemos com grupos pro-p.

No capítulo 1 se inicia uma revisão básica de alguns conceitos topológicos importantes. Definiremos grupos profinitos, grupos pro-p e grupos uniformes. Estudaremos essas estruturas de maneira direta. Apresentaremos os resultados mais importantes e daremos alguns exemplos.

O capítulo 2 introduzirá as variedades analíticas para que possamos estudar os grupos analíticos. Veremos teoremas importantes como a extensão de grupos p-ádicos analíticos abertos e uma caracterização dos grupos p-ádicos analíticos através de seus subgrupos abertos. No final do capítulo apresentaremos construções de $\mathbb{Z}_p$ e $\mathbb{Q}_p$ usando as ferramentas dos dois primeiros capítulos: construiremos $\mathbb{Z}_p$ como um grupo profinito e $\mathbb{Q}_p$ como um grupo analítico.

O capítulo 3 começa, a princípio, de maneira desconexa com os dois primeiros. Começamos fazendo uma rápida introdução as álgebras de Lie e apresentamos a série de

Campbell-Hausdorff. O motivo de estudar essas ideias aparece na última seção. Essas ideias nos permitirão conectar duas estruturas que, em uma primeira leitura, parecem distintas: grupos uniformes e álgebras de Lie.

No capítulo 4 introduzimos formalmente o que são palavras e subgrupos verbais. Além disso, veremos algumas propriedades e como os subgrupos verbais se relacionam com grupos profinitos. Definiremos uma classe de palavras, as $\mathcal{N}_p$-palavras, e apresentaremos alguns resultados que serão úteis no último capítulo.

O objetivo de capítulo 5 é concluir o trabalho demonstrando o teorema principal do artigo de A. Jaikin-Zapirain: *$w(G)$ é fechado para todo grupo pro-p finitamente gerado G se, e somente se, $w \notin (F')^p F''$ para qualquer palavra não trivial w de um grupo livre F*. A prova desse resultado será divida em duas partes. Em uma delas será apresentada uma demonstração de outro teorema importante: *se w é uma $\mathcal{N}_p$-palavra e G um grupo pro-p finitamente gerado, então $w(G)$ é fechado em G*. A demonstração desse teorema usa não só argumentos algébricos, mas analíticos e é exatamente neste ponto que se torna relevante a correspondência entre grupos uniformes e álgebras de Lie. Ao final do capítulo, veremos como é possível generalizar o teorema principal para os grupos pronilpotentes.

Os pré-requisitos para o entendimento deste trabalho são: conhecimentos avançados em teoria de grupos, teoria dos anéis, topologia geral e, além disso, conhecimentos básicos sobre álgebras, séries de potências formais e análise. É desejável que o leitor esteja familiarizado com grupos profinitos, variedades analíticas e álgebras de Lie, mas os três primeiros capítulos têm o papel de cobrir os conhecimentos necessários sobre esses assuntos.

Lista de Símbolos

$\Phi(G)$	subgrupo de Frattini do grupo G
$\leq_o$	subgrupo aberto
$\lhd_o$	subgrupo normal aberto
$P_i(G)$	i-ésimo termo da p-série inferior de G
$\mathbb{F}_p$	corpo de ordem p
$\mathrm{d}(G)$	conjunto gerador de G com menor cardinalidade
$\mathrm{rk}(G)$	posto de G
$\dim(G)$	dimensão de G
$\mathbb{Z}_p$	anel dos inteiros p-ádicos
$K[[X]]$	anel das séries de potências formais sobre K
$\mathbb{Q}_p$	conjunto dos rácionais p-ádicos
T_xX	espaço tangente de X em x
$[\cdot,\cdot]_L$	colchete de Lie
$\mathbb{Q}_p\langle\langle X\rangle\rangle$	anel das séries de potências formais sobre $\mathbb{Q}_p$
G_w	conjunto dos w-valores
$w(G)$	subgrupo verbal de w em G
G_W	vocabulário de W em G
$W(G)$	subgrupo verbal de W em G
$C_p \wr \mathbb{Z}$	produto entrelaçado entre C_p e $\mathbb{Z}$
$\mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$	conjunto dos homomorfismos entre $\widehat{\mathbb{Z}}$ e $\mathbb{Q}/\mathbb{Z}$

Capítulo 1

A classe dos Grupos Profinitos

Sejam K uma extensão algébrica de Galois de um corpo F e $G = \mathrm{Gal}(K/F)$ seu grupo de Galois. Se K/F tem grau finito, então a teoria de Galois clássica nos permite obter uma correspondência entre os subgrupos de G e corpos intermediários entre K e F. Se K/F tem grau infinito, subgrupos diferentes podem corresponder a um mesmo corpo intermediário. Para solucionar esse problema, define-se uma topologia em G, chamada de *topologia de Krull* que nos permite obter uma reformulação do teorema fundamental da teoria de Galois e naturalmente introduz a ideia de grupos profinitos (veja [12]). Existem outras maneiras de observar o surgimento natural da ideia de grupo profinito, mas iremos apresentar esse conceito de forma independente e como base para o desenvolvimento deste trabalho.

Vale ressaltar que desenvolveremos os conceitos necessários para que possamos concluir nosso objetivo final, sendo assim não será viável enunciar e demonstrar todos os resultados e consequências que serão usados neste capítulo. Para uma maior profundidade, o leitor pode consultar [14].

Os principais teoremas deste capítulo foram baseados em [4] e [14].

1.1 Definições iniciais

De acordo com o que mencionamos anteriormente, grupos profinitos surgem na teoria de Galois conforme definimos uma topologia em um grupo de Galois de uma extensão infinita. No caso geral, um grupo profinito também pode ser definido puramente a partir de propriedades topológicas. Além das propriedades topológicas serem suficientes para definir um grupo profinito, conceitos de grupos topológicos desempenham um papel chave para sustentar as ideias e resultados matemáticos que estudaremos.

Definição 1.1.1. Um *grupo topológico* G é um grupo e um espaço topológico no qual o mapa $(g,h) \mapsto gh^{-1}$ de $G \times G$ em G é contínuo.

É comum encontrar a exigência de que os mapas $(g,h) \mapsto gh$ de $G \times G$ em G e $g \mapsto g^{-1}$ de G em G sejam contínuos. De fato, poderíamos usar isso também como definição, pois é equivalente a exigência feita acima.

Exemplo 1.1.1. Dado um grupo G qualquer, ao colocarmos em G a topologia discreta o tornamos um grupo topológico.

Exemplo 1.1.2. O mapa $(x,y) \mapsto x - y$, para $x, y \in \mathbb{R}$, é claramente contínuo em relação a topologia usual. Também é fácil ver que $(x,y) \mapsto \dfrac{x}{y}$, para $x, y \in \mathbb{R}$ com $y \neq 0$, é contínuo com a topologia usual de $\mathbb{R}$. Com isso, o grupo aditivo $\mathbb{R}$ e o grupo multiplicativo $\mathbb{R} - \{0\}$ são grupos topológicos com respeito à topologia euclidiana. Por esses dois exemplos, podemos ver ainda que o grupo $\mathrm{GL}_n(\mathbb{R})$ é um grupo topológico se considerarmos a topologia produto.

Exemplo 1.1.3. Seja G um grupo e $\mathcal{L}$ uma família não-vazia de subgrupos normais tais que se $K_1, K_2 \in \mathcal{L}$ e K_3 é um subgrupo normal contendo $K_1 \cap K_2$ então $K_3 \in \mathcal{L}$. Seja τ a família de todas as uniões de conjuntos de classes Kg com $K \in \mathcal{L}, g \in G$.

Podemos escrever uma coleção de conjuntos de classe de G como $\{K_I g_J\} = \{K_i g_j\}_{i \in I, j \in J}$. Assim,

$$\tau = \left\{ H : H = \bigcup_{I,J} K_I g_J \right\}.$$

Note que se $K_1, K_2 \triangleleft G$, $K_1 \cap K_2 \triangleleft G$. Então, $K_1, K_2 \in \mathcal{L}$ implica $K_1 \cap K_2 \in \mathcal{L}$. Se $K \in \mathcal{L}$ e $N \triangleleft G$ tal que $K \subset N$, tomando $K_1 = K_2 = K$, $K_1 \cap K_2 \subset N$. Logo, $N \in \mathcal{L}$.

Seja $g \in K_1 g_1 \cap K_2 g_2$. Uma vez que $K_1 g_1 = K_1 g$ e $K_2 g_2 = K_2 g$, temos

$$K_1 g_1 \cap K_2 g_2 = K_1 g \cap K_2 g = (K_1 \cap K_2) g.$$

Assim, se $K_1 g_1, K_2 g_2$ não são disjuntos, então existe $g \in G$ tal que $K_1 g_1 \cap K_2 g_2 = (K_1 \cap K_2) g$.

Além disso,

(i) Se $\{K_I g_J\}$ é uma família vazia de classes $K_i g_i$, então $\bigcup_{I,J} K_I g_J = \emptyset \in \tau$. Além disso, $G = \bigcup_{g} Kg \in \tau$.

(ii) Por definição, a união de qualquer coleção de elementos de τ pertence a τ.

(iii) Se $X, Y \in \tau$ não são disjuntos, então

$$\begin{aligned} X \cap Y &= \bigcup_{I,J} K_I g_J \cap \bigcup_{\tilde{I},\tilde{J}} K_{\tilde{I}} g_{\tilde{J}} \\ &= \bigcup_{I,\tilde{I},J,\tilde{J}} K_I g_J \cap K_{\tilde{I}} g_{\tilde{J}} \\ &= \bigcup_{I,\tilde{I}} (\underbrace{K_I \cap K_{\tilde{I}}}_{\in \mathcal{L}}) g_{I,\tilde{I}} \in \tau. \end{aligned}$$

Assim, τ é uma topologia.

Considere $\mathcal{B} = \{Kg : K \in \mathcal{L}, g \in G\}$. Não é difícil verificar que $\mathcal{B}$ é fechado para interseção finita e $G \in \mathcal{B}$. Assim, $\mathcal{B}$ é uma base para a topologia τ. Com isso, mostrar continuidade de um mapa f num espaço topológico definido pela topologia τ se resume à analisar a imagem inversa de elementos da base $\mathcal{B}$, uma vez que se $H = \bigcup Kg$ com $Kg \in \mathcal{B}$, então

$$f^{-1}(H) = \bigcup f^{-1}(Kg).$$

Considere o mapa $\varphi : G \times G \to G$ definido por $(x, y) \mapsto xy$. Uma vez que $K \triangleleft G$, $gK = Kg$ para todo $g \in G$. Assim, $Kg_1Kg_2 = Kg_1g_2$. Com isso, se $Kg \in \mathcal{B}$ então

$$Kg = Kg_1Kg_2 = Kg_2Kg_1 = Kg_1\{e\}g_2 = \{e\}g_1Kg_2,$$

consequentemente, podemos ver que a união de todos os produtos cartesiano mapeados em Kg é um conjunto envolvendo $K \in \mathcal{L}$ e algum $g \in G$. Como os abertos da topologia $\tau \times \tau$ são um produto de abertos de τ, $\varphi^{-1}(Kg) \in \tau$.

Considere o mapa $\psi : G \to G$ dado por $x \mapsto x^{-1}$. Tome $Kg \in \mathcal{B}$. Note que $\psi(x) \in Kg$ se, e somente se $\psi(x) = kg$ para algum $k \in K$ e $g \in G$. Mas

$$kg = (k^{-1})^{-1}(g^{-1})^{-1} = (g^{-1}k^{-1})^{-1},$$

isto é, $\psi^{-1}(Kg) = g^{-1}K^{-1} = Kg^{-1} \in \tau$.

Uma vez que φ e ψ são mapas contínuos, G é um grupo topológico com a topologia τ.

Com isso, dado um grupo arbitrário, podemos torná-lo um grupo topológico através dos subgrupos normais.

Definição 1.1.2. Um *homomorfismo* de grupos topológicos é um homomorfismo de grupos que é contínuo. Um *isomorfismo* de grupos topológicos é um homomorfismo bijetivo com inversa sendo um homomorfismo (de grupos topológicos).

A proposição abaixo apresenta algumas propriedades dos grupos topológicos que nos serão úteis.

Proposição 1.1.1. *Sejam G um grupo topológico e H, K subgrupos de G. Então*

(i) O fecho topológico $\overline{H}$ é um subgrupo de G. Se além disso H é normal em G, então $\overline{H}$ é normal em G;

(ii) se H é aberto em G, então H é fechado em G. Se G for compacto e H aberto, então $|G : H|$ é finito;

(iii) se H é fechado e $|G : H|$ é finito, então H é aberto;

(iv) G é Hausdorff se, e somente se $\{1\}$ é fechado em G.

A demonstração de tais propriedades pode ser feita de maneira simples e direta. Elas podem ser encontradas na maioria dos livros sobre grupos profinitos (veja [4]). Por exemplo:

(iii) Uma vez que

$$G - H = \bigcup_{g \notin H} Hg,$$

Hg é fechado pois é a imagem da translação $h \mapsto hg$ (que é um homeomorfismo) e H tem índice finito em G, isto é, existe uma quantidade finita de Hg, então H fechado implica $G - H$ fechado, ou seja, H é aberto.

(iv) É imediato notar que todos os singletons são fechados em um espaço Hausdorff, em particular, $\{1\}$ é fechado em G. Reciprocamente, suponhamos que $\{1\}$ é fechado em G. Não é difícil verificar que, como consequência da definição, os mapas $x \mapsto x^{-1}$, $x \mapsto gx$ e $x \mapsto xg$ são homeomorfismos e com isso, se $a, b \in G$ são elementos distintos, então $\{a^{-1}b\}$ é imagem inversa de um conjunto fechado, isto é, $\{a^{-1}b\}$ é fechado. Assim, deve existir uma vizinhança U de 1 tal que $a^{-1}b \notin U$. Existem abertos V, W tais que $1 \in VW^{-1} \subset U$, já que a imagem inversa de U pelo mapa $(x, y) \mapsto xy^{-1}$ deve ser aberto. Consequentemente, $a^{-1}b \notin VW^{-1}$ e então $aV \cap bW = \emptyset$.

Note que se para um subconjunto X de G, $\langle X \rangle$ for denso em G, então $\overline{\langle X \rangle} = G$. Isso motiva a seguinte definição:

Definição 1.1.3. Um grupo topológico G é *gerado topologicamente* por $X \subset G$ se $G = \overline{\langle X \rangle}$. Se X é um conjunto finito, dizemos que G é *finitamente gerado*.

Considere G um grupo topológico Hausdorff tal que o conjunto dos subgrupos normais abertos de G constituem uma base para as vizinhanças abertas de 1. Uma vez que G é Hausdorff, o limite de uma sequência convergente é único. De acordo com nossas suposições sobre G podemos formular a convergência de uma sequência (g_n) da seguinte maneira: Uma sequência (g_n) *converge* para g se para todo $N \triangleleft_o G$ existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$ tem-se $g_n g^{-1} \in N$. Sendo $N \triangleleft_o G$ é evidente que podemos, de maneira equivalente, pedir que $g^{-1} g_n \in N$. Além disso, a definição de uma sequência de Cauchy pode ser escrita deste modo: Uma sequência (g_n) é de *Cauchy* se para todo $N \triangleleft_o G$ existe $n_0 \in \mathbb{N}$ tal que para todo $m, n > n_0$ tem-se $g_n g^{-1} \in N$ (ou $g^{-1} g_n \in N$). Uma sequência em G é convergente se, e só se, é uma sequência de Cauchy e, no caso em que todas as sequências de Cauchy em G são convergentes, dizemos que G é *completo*.

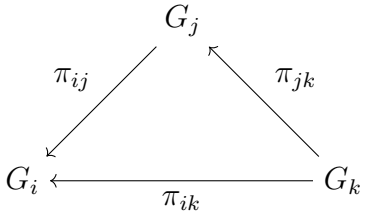
Do ponto de vista topológico já podemos definir o que é um grupo profinito: Um grupo profinito é um grupo topológico Hausdorff compacto totalmente desconexo (as componentes conexas são os conjuntos de um único ponto) ou ainda, um grupo topológico Hausdorff compacto tal que os subgrupos abertos são uma base para as vizinhanças da identidade. Contudo, existe uma maneira alternativa de definir tais grupos que, apesar de inicialmente parecer mais complicada, nos permite checar se um grupo é profinito de maneira muito mais simples. Por isso faremos uma outra construção para definir um grupo profinito que nos permitirá estudar tais estruturas com menos trabalho.

As definições e construções usadas para grupos topológicos também são válidas para anéis topológicos fazendo as devidas adaptações. O leitor interessado pode consultar [20].

Definição 1.1.4. Um *conjunto direcionado* é um conjunto não-vazio parcialmente ordenado I tal que para todo $i_1, i_2 \in I$ existe um $j \in I$ com $i_1 \leq j$ e $i_2 \leq j$.

Definição 1.1.5. Seja I um conjunto direcionado. Um *sistema inverso* de grupos topológicos sobre I é um par (G_i, π_{ij}) de grupos topológicos G_i e homomorfismos $\pi_{ij} : G_j \to G_i$ para todo $i \leq j$ de modo que $\pi_{ii} = \mathrm{id}_G$ e $\pi_{ik} = \pi_{ij}\pi_{jk}$ para todo $i \leq j \leq k$.

Podemos representar esses homomorfismos através do seguinte diagrama:



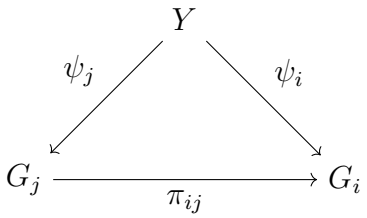
Se (G_i, π_{ij}) é um sistema inverso de grupos topológicos sobre algum conjunto direcionado I, considere o conjunto $G_I = \prod_i G_i$. Seja G o subconjunto de G_I formado pelos elementos (g_i) com $g_i \in G_i$ tais que $\pi_{ij}(g_j) = g_i$ para cada $i \leq j$, ou seja,

$$G = \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i : \pi_{ij}(g_j) = g_i, \forall i \leq j \right\}.$$

Definição 1.1.6. Seja (G_i, π_{ij}) um sistema inverso de grupos topológicos. O *limite inverso* de (G_i, π_{ij}) é o subgrupo G construído no parágrafo anterior. Escrevemos

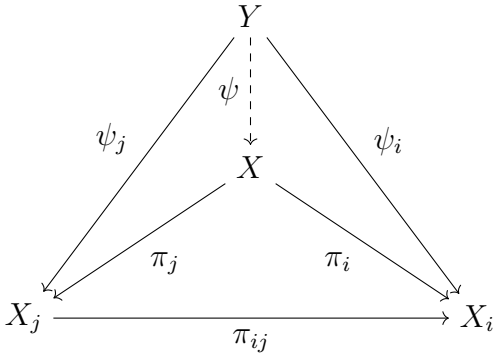
$$G = \varprojlim_i G_i.$$

Suponha que (G_i, π_{ij}) seja um sistema inverso de grupos topológicos e $\pi_i : G \to G_i$ a projeção canônica. Se Y é um espaço topológico, uma família de homomorfismos contínuos $\{\psi_i : Y \to G_i\}$ é chamado de *compatível* se $\pi_{ij}\psi_j = \psi_i$ para cada $i \leq j$. Podemos representar isso através do diagrama



que é comutativo

A definição do limite inverso implica naturalmente a seguinte **propriedade universal**: se G é o limite inverso com a família compatível $\{\pi_i : G \to G_i\}$ de homomorfismos contínuos, então sempre que $\{\psi_i : Y \to G_i\}$ é uma família compatível de homomorfismos contínuos, existe um único homomorfismo contínuo $\psi : Y \to G$ tal que $\pi_i\psi = \psi_i$ para cada i.



Exemplo 1.1.4. Seja G um grupo e considere $\mathcal{N}$ o conjunto dos subgrupos normais de índice finito em G com ordem parcial dada por $K \prec N$ se $N \subset K$. Então $\mathcal{N}$ é um conjunto direcionado. Considerando as projeções $\pi_{N,K} : G/K \to G/N$, o sistema inverso $(G/N, \pi_{N,K})$ tem um limite inverso $\varprojlim_{N} G/N$.

Definição 1.1.7. Um *grupo (anel) profinito* é um grupo (anel) topológico que é topologicamente isomorfo ao limite inverso de um sistema inverso de grupos (anéis) finitos.

Para ser mais preciso, podemos dizer que um grupo G é profinito se

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

A prova de que essa definição ser equivalente a que mencionamos no início desta seção pode ser encontrada em [20].

Exemplo 1.1.5. Veremos posteriormente que $\mathbb{Z}_p$ (o anel dos inteiros p-ádicos) é o limite inverso do sistema inverso $(\mathbb{Z}/p^i\mathbb{Z}, \pi_{ij})$

Exemplo 1.1.6. Sejam π_{ij} as projeções do exemplo anterior. Essas projeções induzem projeções $\tilde{\pi}_{ij}$ que tornam $(\mathrm{SL}_n(\mathbb{Z}/p^i\mathbb{Z}), \tilde{\pi}_{ij})$ um sistema inverso de grupos finitos com limite inverso

$$\varprojlim \mathrm{SL}_n(\mathbb{Z}/p^i\mathbb{Z}).$$

Os mapas projetivos $\pi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$ induzem um homomorfismo bijetivo entre $\mathrm{SL}_n(\mathbb{Z}_p) \to \varprojlim \mathrm{SL}_n(\mathbb{Z}/p^i\mathbb{Z})$, isto é,

$$\mathrm{SL}_n(\mathbb{Z}_p) \simeq \varprojlim \mathrm{SL}_n(\mathbb{Z}/p^i\mathbb{Z}).$$

Uma maneira mais direta de verificar que $\mathrm{SL}_n(\mathbb{Z}_p)$ é profinito, é notar que esse grupo é a imagem inversa do conjunto $\{1\}$ em relação ao mapa contínuo $\det : M_n(\mathbb{Z}_p) \to \mathbb{Z}_p$ onde $M_n(\mathbb{Z}_p)$ é compacto, Hausdorff e totalmente desconexo sendo isomorfo à $(\mathbb{Z}_p)^{n^2}$.

Exemplo 1.1.7. No exemplo 1.1.4, os conjuntos G/N são finitos e o limite inverso, comumente denotado por $\widehat{G}$, é conhecido como *completamento profinito* de G.

Proposição 1.1.2. *Se G é um grupo profinito, então as seguintes afirmações são verdadeiras:*

(i) um subconjunto de G é aberto se, e somente se, é a união de classes de subgrupos normais abertos;

(ii) para qualquer $X \subset G$, $\overline{X} = \bigcap_{N \lhd_o G} XN$;

(iii) o produto XY de subgrupos fechados é um subgrupo fechado;

(iv) um subgrupo fechado H é profinito;

(v) se N é um subgrupo normal fechado, então G/N é profinito.

A verificação dos fatos acima é relativamente simples. Podem ser encontradas demonstrações dessas propriedades em [4]. Façamos, por exemplo:

(iv) Seja (G_i, π_{ij}) um sistema inverso de grupos finitos com limite inverso G e projeção $\pi_i : G \to G_i$. Se H é um subgrupo de G, denote então $\pi_i(H) = H_i$. Uma vez que $\pi_{ij}\pi_j = \pi_i$,

$$\pi_{ij}(H_j) = (\pi_{ij}\pi_j)(H) = \pi_i(H) \subset H_i.$$

Defina $\tilde{\pi}_{ij}$ como sendo a restrição de π_{ij} a H_j. Com isso, $(H_i, \tilde{\pi}_{ij})$ é um sistema inverso com limite inverso L e a projeção $\tilde{\pi}_i = \pi_i|_H$ torna H compatível. Então $H \leq L$ satisfazendo $\tilde{\pi}_i(H) = H_i$ o que nos permite verificar que H é denso em L (veja [20, proposição 1.1.6]), ou seja, $\overline{H} = L$. Sendo H fechado e L profinito, então H é profinito.

(v) Podemos usar uma construção muito semelhante a do item anterior. Contudo, lembrando da definição topológica de grupos profinitos, exista uma maneira puramente topológica de justificar esse item. Se N é qualquer subespaço topológico de um espaço Hausdorff compacto G, então o quociente G/N também será Hausdorff compacto com a topologia quociente. Além disso, o quociente de dois espaços totalmente desconexos é totalmente desconexo. Assim, G/N é, de fato, um grupo profinito.

Em um sistema inverso (G_i, π_{ij}), considerando cada G_i como um grupo finito, damos a eles a topologia discreta. Então G_I, com a topologia produto, induz uma topologia no limite inverso G, o que o torna um grupo topológico. Além disso, é relevante que G não seja vazio, senão não seria útil estudar sua estrutura. Uma vez que o sistema inverso é de grupos, então a identidade sempre deve fazer parte do limite inverso, logo, G nunca será vazio.

A partir de agora iremos concentrar nosso estudo apenas em grupos topológicos, salvo menção contrária.

Proposição 1.1.3. *Se G é um grupo profinito finitamente gerado então todo subgrupo aberto de G é finitamente gerado.*

Demonstração. Seja X um conjunto finito que gera G topologicamente. Para cada $x \in X$, podemos adicionar seu inverso x^{-1} ao conjunto gerador e o conjunto resultante

ainda será um gerador topológico de G. Podemos supor então, sem perda de generalidade, que $X = X^{-1}$.

Sejam H um subgrupo aberto de G e T um transverso à direita de H em G com $1 \in T$. Sendo H aberto, então T é finito. Defina

$$Y = \{t_1 x t_2^{-1} : t_1, t_2 \in T, x \in X, t_1 x t_2^{-1} \in H\}.$$

Sejam $y \in \overline{\langle Y \rangle}$, $t \in T$ e $x \in X$. Sendo T um transverso à direita, podemos escolher $\tilde{t} \in T$ tais que $tx \in H\tilde{t}$ e assim, $tx\tilde{t}^{-1} \in H$ e, consequentemente, $tx\tilde{t}^{-1} \in Y$. Portanto,

$$(yt)x = y(tx\tilde{t}^{-1})\tilde{t},$$

logo, $(yt)x \in \overline{\langle Y \rangle}T$. Assim, $\overline{\langle Y \rangle}T$ é invariante em relação a multiplicação por elementos de X. Uma vez que $1 \in \overline{\langle Y \rangle}T$, então

$$\langle X \rangle \subset \overline{\langle Y \rangle}T$$

É imediato notar que $\overline{\langle Y \rangle}T$ é fechado, pois T é finito, logo, $G = \overline{\langle X \rangle} \subset \overline{\langle Y \rangle}T$, isto é, $G = \overline{\langle Y \rangle}T$. Como $|G : \overline{\langle Y \rangle}| \leq |T| = |G : H|$ e $\overline{\langle Y \rangle} \leq H$, então $\overline{Y} = H$. □

Sendo G um grupo profinito, um elemento $g \in G$ não é um gerador de G sempre que $G = \overline{\langle X, g \rangle}$ implica $G = \overline{X}$.

Definição 1.1.8. Seja G um grupo profinito. O *subgrupo de Frattini* de G é o subgrupo

$$\Phi(G) = \bigcap_{M <_{m,o} G} M$$

onde M é um subgrupo maximal aberto próprio de G.

Se G é um grupo profinito não-trivial, então $\Phi(G) < G$, uma vez que G possui subgrupos maximais próprios. No caso em que $G = \{1\}$ convencionamos $\Phi(G) = G$.

Antes de provar algumas propriedades relevantes sobre o subgrupo de Frattini, precisaremos de alguns lemas.

Lema 1.1.1. *Sejam H um subgrupo fechado de um grupo profinito G e $\mathcal{U} = \{U_i\}_{i \in I}$ uma família de subconjuntos fechados de G. Suponha que, se $U_1, U_2 \in \mathcal{U}$ então existe $U_3 \in \mathcal{U}$ tal que $U_3 \leq U_1 \cap U_2$. Então*

$$\bigcap_i HU_i = H\left(\bigcap_i U_i\right).$$

Demonstração. Se I é finito, então existe U_j tal que $U_j \subset U_1 \cup \cdots \cup U_n$. Daí,

$$\bigcap_i HU_i = HU_j = H\left(\bigcap_i U_i\right).$$

Seja agora I infinito. Se $x \in H\left(\bigcap_i U_i\right)$, então $x = hu$ com $u \in \bigcap_i U_i$. Mas então $u \in U_i$ para todo i, isto é, $x \in HU_i$ para todo i, e assim,

$$H\left(\bigcap_i U_i\right) \subset \bigcap_i HU_i.$$

Reciprocamente, sejam $x \in \bigcap_i HU_i$ e $J = \{J_k\}_{k\in K}$ o conjunto de todos os subconjuntos finitos de I tais que $\tilde{\mathcal{U}} = \{U_j\}_{j\in J_k}$ satisfaz a mesma propriedade que $\mathcal{U}$. Assim, para cada $k \in K$, vale

$$\bigcap_{j\in J_k} HU_j = H\left(\bigcap_{j\in J_k} U_j\right) \ni x,$$

logo, existe $u_k \in \bigcap_{j\in J_k} U_j$ tal que $x = h_1 u_k$, equivalentemente, $h_2 x = u_k$, isto é, $Hx \cap \left(\bigcap_{j\in J_k} U_k\right) \neq \emptyset$. Uma vez que G é compacto,

$$\bigcap_{k\in K}\left(Hx \cap \left(\bigcap_{j\in J_k} U_k\right)\right) \neq \emptyset,$$

isto é,

$$Hx \cap \left(\bigcap_i U_i\right) \neq \emptyset$$

e assim, $x \in H\left(\bigcap_i U_i\right)$, ou seja,

$$H\left(\bigcap_i U_i\right) = \bigcap_i HU_i.$$

□

Lema 1.1.2. *Seja H um subgrupo fechado de um grupo profinito G. Então todo subgrupo aberto de G que contém H contém um subgrupo da forma HU para algum subgrupo normal aberto U de G.*

Demonstração. Seja K um subgrupo aberto de G tal que $H \subset K$. Tome $U = \bigcap_g gKg^{-1}$, que é um subgrupo normal aberto de G. Além disso, $HU \leq K$. □

Segue desses resultados que se H é um subgrupo fechado de um grupo profinito, então H é a interseção de todos os subgrupos abertos que contém H.

Considere um conjunto X e suponha que $G = \langle X \rangle$. Claramente, $G = \langle X \cup \Phi(G) \rangle$ o que implica $G/\Phi(G) = \langle X\Phi(G)/\Phi(G) \rangle$. Supondo inicialmente que $G/\Phi(G) = \langle X\Phi(G)/\Phi(G) \rangle$, escolha algum subgrupo aberto H de G que contém X. Se $G \neq H$, então H está contido em algum subgrupo (próprio) maximal aberto M de G. Então

$$\langle X \rangle \, \Phi(G)/\Phi(G) \neq G/\Phi(G)$$

uma contradição com o nossa suposição. Logo, $G = H$. Além disso,

$$\overline{\langle X \rangle} = \bigcap_{\langle X \rangle \leq K \leq_o G} K,$$

devemos ter $\langle X \rangle = G$. Com isso, podemos enunciar que se G é um grupo profinito, então as seguintes afirmações são equivalentes:

(i) X gera G topologicamente,

(ii) $X \cup \Phi(G)$ gera G topologicamente,

(iii) $X\Phi(G)/\Phi(G)$ gera $G/\Phi(G)$ topologicamente.

1.2 Grupos Pro-p

Dentro da classe dos grupos profinitos, existe uma subclasse composta pelos grupos pro-p. Esta classe de grupos é uma "ponte" entre os grupos profinitos e os grupos uniformes, que apresentaremos por último neste capítulo. Nesta seção iremos introduzir o conceito de grupo pro-p e estudaremos algumas de suas propriedades.

Definição 1.2.1. Um *grupo pro-p* é um grupo profinito que é isomorfo ao limite inverso de um sistema inverso de p-grupos finitos.

Exemplo 1.2.1. Veremos posteriormente, com bastante detalhes, que o grupo aditivo dos inteiros p-ádicos $\mathbb{Z}_p$ pode ser construído como um grupo pro-p.

Proposição 1.2.1. *Seja G um grupo topológico. Então G é pro-p se, e somente se, G é profinito e $|G : N| = p^k$ para todo $N \lhd_o G$.*

Demonstração. Suponha que $G \simeq \varprojlim(G_i)_{i\in I}$ onde G_i é um p-grupo finito. Então G é profinito. Usando argumentos de topologia geral, é fácil ver que um subgrupo aberto N de G contém um subgrupo da forma

$$G^J = G \cap \left(\prod_{i \notin J} G_j \times \prod_{i \in J} \{1\} \right)$$

onde J é algum subconjunto finito de I. Além disso,

$$|G : G^J| = p^r$$

para algum r. Assim, $|G : N| = p^k$ para algum k.

Reciprocamente, temos que

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

e cada G/N é um p-grupo finito. □

Exemplo 1.2.2. Seja $p \neq 2$ primo e considere os grupos

$$\Gamma_j = \{g \in \mathrm{SL}_n(\mathbb{Z}_p) : g \equiv 1_n \pmod{p^j}\}.$$

Se $\varphi_j : \mathrm{SL}_n(\mathbb{Z}_p) \to \mathrm{SL}_n(\mathbb{Z}/p^j\mathbb{Z})$ é o homomorfismo natural, então $\Gamma_j = \ker \varphi_j$ e assim, Γ_j é um subgrupo normal fechado de $\mathrm{SL}_n(\mathbb{Z}_p)$. O conjunto Γ_1/Γ_j é isomorfo ao subgrupos das matrizes com entradas em $\mathbb{Z}/p^j\mathbb{Z}$ tais que $a_{ii} - 1 \in p\mathbb{Z}$, que é um p-grupo, logo,

$$|\Gamma_1 : \Gamma_j| = p^k.$$

Além disso, $\{\Gamma_j\}_j$ formam uma base para as vizinhanças de identidade em Γ_1, logo, se $N \lhd_o \Gamma_1$, então $N \leq \Gamma_j$ para algum j e assim, $|\Gamma_1 : N| = p^l$. Portanto, Γ_1 é um grupo pro-p.

Os subgrupos de Frattini, vistos na seção anterior, desempenham um papel importante na teoria dos grupos pro-p.

Proposição 1.2.2. *Se G é um grupo pro-p, então*

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

Demonstração. Seja M um subgrupo aberto maximal próprio de G. Então existe um subgrupo N de M normal aberto em G e M/N é um subgrupo maximal de G/N. Como G/N é um p-grupo finito, então $|G : M| = p$ e $M \lhd G$. Assim G/M é um grupo cíclico

de ordem p, logo, $G^p[G,G] \leq M$ o que implica $G^p[G,G] \leq \Phi(G)$. Como $\Phi(G)$ é, por definição, fechado, seque que $\overline{G^p[G,G]} \leq \Phi(G)$.

Tome $H = G/\overline{G^p[G,G]}$. Como H é um grupo pro-p, se $N \lhd_o H$, então H/N é um grupo cíclico finito de ordem p e disso é fácil concluir que $\Phi(H/N) = 1$ o que implica $\Phi(H) \leq N$. Note que

$$\bigcap_{N \lhd_o H} N = \{1\},$$

logo, $\Phi(H) = \{1\}$. Como consequência imediata da definição do subgrupo de Frattini, temos que

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

isto é,

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

□

Esses resultados conseguem determinar quando um grupo pro-p é finitamente gerado por meios de propriedades do subgrupo de Frattini.

Proposição 1.2.3. *Um grupo pro-p G é finitamente gerado se, e somente se, $\Phi(G)$ é aberto em G.*

Demonstração. Suponha que exista um conjunto finito X tal que $G = \langle X \rangle$. Seja qualquer $N \lhd_o G$ tal que $\Phi(G) \leq N$. Uma vez que $\Phi(G) = \overline{G^p[G,G]}$, então G/N é um p-grupo abeliano elementar e, portanto, $|G : N|$ é, no máximo, $p^{|X|}$. Seja N_0 o subgrupo que tem o maior índice em G entre todos os subgrupos N. Então $\Phi(G) \leq N$ implica $N_0 \leq N$. Portanto,

$$\Phi(G) = \bigcap_{\Phi(G) \leq N \lhd_o G} N = N_0$$

é aberto em G.

Reciprocamente, se $\Phi(G)$ é aberto em G, então $G/\Phi(G)$ é finito. Assim existe um conjunto finito X tal que $G/\Phi(G) = X\Phi(G)/\Phi(G)$. Logo, $G = \overline{\langle X \rangle}$ (veja a última parte da seção 1.1). □

Definiremos agora uma série de grupos que será de extrema importância no estudo dos grupos uniformes.

Definição 1.2.2. Seja G um grupo pro-p. A *p-série central inferior* é definida, indutivamente, para ser

$$P_1(G) = G$$

e

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

Vimos que se G é um grupo pro-p, então $\Phi(G) = \overline{G^p[G,G]}$. Se G é finitamente gerado, $\Phi(G) = G^p[G,G]$ (veja [4, Proposição 1.19]). Disso segue que $P_2(G) = \Phi(G)$ e, em geral,

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

isto é, $P_{i+1}(G) \geq \Phi(P_i(G))$.

O teorema abaixo é fundamental na justificativa de que a topologia dos grupos pro-p finitamente gerados é determinada pela sua estrutura de grupo.

Teorema 1.2.1. *Se G é um grupo pro-p finitamente gerado então todo subgrupo de índice finito em G é aberto.*

Uma demonstração pode ser vista em [4, Teorema 1.7].

Seja G um grupo pro-p finitamente gerado e defina $G_i = P_i(G)$ para cada i. Então $G_1 = G$ é finitamente gerado e aberto em G. Suponha que G_n seja finitamente gerado e aberto em G. Pela Proposição 1.2.3 temos que $\Phi(G_n)$ é aberto em G_n. Além disso, $\Phi(G_n) \leq G_{n+1}$ e $G_{n+1} \leq G_n$, logo, G_{n+1} é aberto em G_n e, portanto, em G. Então, pela Proposição **??**, G_{n+1} é finitamente gerado. Assim, G_i é um grupo pro-p finitamente gerado e $\Phi(G_i)$ é aberto em G_i para cada i. Note que

$$\Phi(G_i) \leq [G_i, G]G_i^p,$$

consequentemente, $[G_i, G]G_i^p$ é aberto em G. Portanto,

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

Obtemos então duas consequências para p-série central inferior quando G é pro-p finitamente gerado:

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

e

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

Denotaremos de agora em diante $G_i = P_i(G)$.

A fim de estabelecer uma definição de posto que se assemelha essencialmente a que conhecemos para espaços vetoriais, estudaremos uma subclasse dos grupos pro-p.

Definição 1.2.3. Seja G um p-grupo finito. Dizemos que G é *poweful* se $[G,G] \leq G^4$ caso $p = 2$ e $[G,G] \leq G^p$ caso p seja um primo ímpar.

Note que se p é ímpar, então $[G,G] \leq G^p$ implica $\Phi(G) = G^p[G,G] = G^p$. Reciprocamente, se $G^p[G,G] = \Phi(G) = G^p$ então $[G,G] \leq G^p$. Assim, G é powerful se, e só se, $\Phi(G) = G^p$.

Exemplo 1.2.3. Todo p-grupo abeliano é, evidentemente, powerful.

Exemplo 1.2.4. Dado p um primo ímpar, considere p-grupo não abeliano representado por:

$$\left\langle x, y, z : x^p = y^p = z^{p^2} = 1, z^p = [x,y], [x,z] = [y,z] = 1 \right\rangle.$$

Segue da definição do grupo que $[G,G] \leq G^p$, o que torna G powerful que não é abeliano.

Exemplo 1.2.5. Considere o grupo 2-grupo

$$D_4 = \left\langle r, s : r^4 = s^2 = 1, srs^{-1} = r^{-1} \right\rangle,$$

isto é,

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

Temos que

$$[D_4, D_4] = \left\langle r^2 \right\rangle = \{1, r^2\}.$$

Uma vez que

$$r^2 \notin D_4^4 = \{1\},$$

então

$$[D_4, D_4] \not\leq D_4^4.$$

Assim, D_4 é um exemplo de um 2-grupo finito que não é powerful. Lembrando que todo grupo cíclico e todo grupo de ordem p^2 são abelianos, podemos concluir então que a menor ordem possível para um grupo finito que não seja powerful é exatamente 8.

Existem dois resultados particularmente importantes sobre geradores de grupos powerful que apresentaremos aqui.

Teorema 1.2.2. *Se $G = \langle g_1, ..., g_n \rangle$ é um p-grupo powerful, então $G = \langle g_1 \rangle \cdots \langle g_n \rangle$.*

A demonstração desse resultado segue diretamente por indução em G_i considerando que $G_i = \left\langle g_1^{p^{i-1}}, ..., g_n^{p^{i-1}} \right\rangle$ (veja [4, Teorema 2.7 (iii)]).

Se p for um primo ímpar e $G = \langle g_1 \rangle \cdots \langle g_n \rangle$, então $g \in G$ implica $g = g_1^{r_1} \cdots g_n^{r_n}$. Note que $a \equiv b \pmod{G^p}$ se $ab^{-1} \in G^p$ o que implica, módulo G^p, em g ser escrito como $g_1^{s_1} \cdots g_n^{s_n}$ com $0 \leq s_i \leq p-1$. Assim,

$$p^d \geq [G : G^p] = [G : \Phi(G)] = p^d,$$

logo, $G^p = \Phi(G)$ e disse segue que $[G, G] \leq G^p$. Isso nos dá uma recíproca do teorema acima quando p for ímpar. No caso em que $p = 2$, o grupo dos quatérnios

$$Q_8 = \left\langle i, j : i^4 = 1, i^2 = j^2, j^{-1}ij = i^{-1} \right\rangle.$$

satisfaz

$$|\langle i \rangle \langle j \rangle| = \frac{|\langle i \rangle || \langle j \rangle|}{|\langle i \rangle \cap \langle j \rangle|} = 8 = |Q_8|,$$

ou seja, $Q_8 = \langle i \rangle \langle j \rangle$. No entanto, não é difícil verificar que Q_8 não é powerful.

Dado um p-grupo finito G, denotamos por $\mathrm{d}(G)$ a menor cardinalidade dentre os conjuntos de geradores de G. Uma vez que o subgrupo de Frattini é composto pelos não geradores, $\mathrm{d}(G)$ é a dimensão de $G/\Phi(G)$ sobre $\mathbb{F}_p$ (como espaço vetorial). Usando indução em $|G|$, podemos mostrar o seguinte resultado usando algumas propriedades (veja [4, Teorema 2.9]) de p-grupos powerful:

Teorema 1.2.3. *Se G é um p-grupo powerful e $H \leq G$, então* $\mathrm{d}(H) \leq \mathrm{d}(G)$.

Esse teorema nos dá uma informação importante sobre o posto de um p-grupo powerful, que definiremos agora.

Definição 1.2.4. Seja G um grupo finito. O *posto* de G é definido para ser

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

Então se G é um p-grupo powerful, $\mathrm{rk}(G) = \sup\{\mathrm{d}(H) : H \leq G\} = \mathrm{d}(G)$.

Para finalizar esta seção, iremos estender esses conceitos à categoria dos grupos pro-p.

Definição 1.2.5. Seja G um grupo pro-p. Dizemos que G é *powerful* se $[G, G] \leq \overline{G^4}$ caso $p = 2$ e $[G, G] \leq \overline{G^p}$ caso p seja um primo ímpar.

Exemplo 1.2.6. Considere o grupo Γ_1 definido no exemplo 1.2.2. Se $g, h \in \Gamma_1$, então

$$gh \equiv hg \pmod{\Gamma_2},$$

logo, $[\Gamma_1, \Gamma_1] \leq \Gamma_2$. Dado $a \in \mathcal{M}_n(\mathbb{Z}_p)$, por indução podemos construir uma sequência de elementos x_r comutando com a tais que

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

e $1 + p^{n-1}x_r$ é invertível, definida por

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

Além disso, podemos verificar que a sequência é convergente para um limite x. Isso mostra que a equação

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

tem solução para todo $a \in \mathcal{M}_n(\mathbb{Z}_p)$. Sendo x o limite de (x_r), então $1 + p^{n-1}x$ deve ser invertível, já que $1 + p^{n-1}x_r$ é. Note então que

$$\det(1 + p^{j-1}x)^p = \det(1 + p^j a) = 1,$$

para cada j, de modo que $1 + p^{j-1}x \in \Gamma_{j-1}$. Assim, qualquer elemento de Γ_i é uma p-ésima potência de um elemento em Γ_{j-1}. Esses argumentos nos mostram que $\Gamma_j = \Gamma_{j-1}^p$ o que implica

$$[\Gamma_1, \Gamma_1] \leq \Gamma_1^p,$$

logo, Γ_1 é powerful.

Usando a projeção canônica $\pi : G \to G/K$ segue imediatamente da definição que G é powerful se, e somente se, G/K é powerful para todo $K \lhd_o G$. Como uma consequência disso podemos enunciar o seguinte resultado:

Teorema 1.2.4. *Seja G um grupo topológico. Então G é um grupo pro-p poweful se, e somente se, G é o limite inverso de um sistema inverso de p-grupos finitos powerful onde os homomorfismos são sobrejetivos.*

Assim como ocorre no caso dos p-grupos powerful, temos os seguintes resultados:

Teorema 1.2.5. *Se $G = \overline{\langle g_1, ..., g_n \rangle}$ é um grupo pro-p powerful, então $G = \overline{\langle g_1 \rangle} \cdots \overline{\langle g_n \rangle}$.*

Dado um grupo pro-p G, denotamos por $\mathrm{d}(G)$ a menor cardinalidade dentre os conjuntos de geradores de G. Se G é finitamente gerado, assim como no caso dos p-grupos finitos, $\mathrm{d}(G)$ é a dimensão de $G/\Phi(G)$ sobre $\mathbb{F}_p$.

Teorema 1.2.6. *Se G é um grupo pro-p powerful e $H \leq_c G$, então $\mathrm{d}(H) \leq \mathrm{d}(G)$.*

As demonstrações de ambos usam truques simples de forma a resumir a veracidade de ambos ao caso de p-grupos powerful.

Seja G um grupo profinito e considere agora os seguintes conjuntos:

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

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

$$r_3 = \sup\{\mathrm{d}(H) : H \leq_o G\},$$

$$r_4 = \sup\{\mathrm{rk}(G/N) : N \lhd_o G\}.$$

Temos o seguinte resultado

Proposição 1.2.4. *Se G é um grupo profinito, então*

$$r_1 = r_2 = r_3 = r_4.$$

Uma demonstração simples desse fato pode ser vista em [4, Proposição 3.11].

Definição 1.2.6. Seja G um grupo profinito. O *posto* de G é definido para ser

$$\mathrm{rk}(G) = \sup\{\mathrm{d}(H) : H \leq_c G\}.$$

Assim como para grupos finitos, se G for um grupo pro-p powerful finitamente gerado, então segue diretamente pela definição de posto que, $\mathrm{rk}(G) = \mathrm{d}(G)$.

1.3 Grupos Uniformes

O leitor pode notar que os grupos profinitos, de certo modo, podem ser visto como uma generalização dos grupos finitos já que compartilham muitas propriedades em comum. Dentro da classe dos grupos profinitos, os grupos powerful podem ser pensados como uma generalização dos grupos abelianos. Um certo tipo de grupo powerful nos permite redefinir sua operação a fim de dá-lo uma estrutura de grupo abeliano e, além disso, uma estrutura de módulo sobre $\mathbb{Z}_p$. Nesta seção iremos apresentar estes tipos de grupos e suas propriedades.

Relembre que a p-série inferior é a série definida indutivamente que satisfaz

$$P_1(G) = G$$

e

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

Denotaremos $P_i(G)$ por G_i.

Definição 1.3.1. Um grupo pro-p G é *uniforme* se é finitamente gerado, powerful e $|G_i : G_{i+1}| = |G : P_2(G)|$ para cada $i \geq 1$.

Exemplo 1.3.1. Uma vez que $\Gamma_2 = \Gamma_1^p$, podemos concluir que

$$\Phi(\Gamma_1) = \Gamma_2.$$

Seja

$$\tilde{\Gamma}_j = \{g \in \mathrm{GL}_n(\mathbb{Z}_p) : g \equiv 1_n \pmod{p^j}\}.$$

Podemos ver $\tilde{\Gamma}_j$ como um produto de n^2 bolas de raio p^{-j} em $\mathbb{Z}_p^{n^2}$. Logo, os conjuntos $\tilde{\Gamma}_2$ são abertos em $\mathrm{GL}_n(\mathbb{Z}_p)$. Além disso, $\Gamma_2 = \tilde{\Gamma}_2 \cap \mathrm{SL}_n(\mathbb{Z}_p)$ e então Γ_2 é aberto em $\mathrm{SL}_n(\mathbb{Z}_p)$. Pela Proposição **??**, Γ_1 é finitamente gerado. Além disso, por indução em i, podemos verificar que $P_i(\Gamma_1) = \Gamma_i$. Com a notação G_i para $P_i(G)$, vemos então que

$$|G_i : G_{i+1}| = |\Gamma_i : \Gamma_{i+1}|$$

e como

$$\Gamma_i/\Gamma_{i+1} \simeq (\mathbb{Z}/p\mathbb{Z})^{n^2},$$

concluímos que $|G_i : G_{i+1}|$ é constante, logo, Γ_1 é uniforme.

No caso de grupos pro-p que são finitamente gerados (que serão particularmente relevantes), podemos simplificar essa definição (veja [4, Teorema 4.5]).

Proposição 1.3.1. *Seja G um grupo pro-p powerful finitamente gerado. Então G é uniforme se, e somente se, G é livre de torção.*

Com isso podemos escrever: "Um grupo pro-p powerful finitamente gerado G é uniforme se G é livre de torção."

Se G é um grupo pro-p, então para quaisquer dois subgrupos abertos uniformes H, K temos $\mathrm{d}(H) = \mathrm{d}(K)$ (por [4, Lema 4.6]). Além disso, um grupo pro-p de posto finito sempre possui um subgrupo aberto uniforme (por [4, Corolário 4.3]). Se G é um grupo pro-p de posto finito, então $\mathrm{d}(H) < \infty$ para todo subgrupo H de G.

Definição 1.3.2. Seja G um grupo pro-p de posto finito. A *dimensão* de G é definida para ser

$$\dim(G) = \mathrm{d}(H)$$

onde H é um subgrupo aberto uniforme de G.

Esta definição de dimensão é, de fato, a dimensão de G como uma variedade analítica (um objeto que será definido no próximo capítulo).

Se G é um grupo pro-p uniforme de dimensão finita, através de uma estrutura aditiva natural de G, podemos introduzir um "sistema de coordenadas" que nos permitirá trabalhar com uma estrutura de módulo em G.

Sejam $\{g_1, ..., g_n\}$ um conjunto de geradores topológicos do grupo pro-p uniforme G e k um inteiro positivo. Note que $G = \overline{\langle g_1 \rangle} \cdots \overline{\langle g_n \rangle}$ e então se $g \in G$, $g = g_1^{r_1} \cdots g_n^{r_n}$ onde $r_1, ..., r_n \in \mathbb{Z}_p$. Como $|G_i : G_{i+1}| = |G : G_2|$, o grupo finito G/G_{k+1} tem ordem p^{kd} e é o produto $\langle g_1 G_{k+1} \rangle \cdots \langle g_n G_{k+1} \rangle$ e cada um desses subgrupos cíclicos tem ordem, no máximo, p^k. Além disso, como o produto tem ordem p^{kd}, nenhum desses subgrupos pode ter ordem menor que p^k, isto é, cada subgrupo cíclico tem ordem p^k. Com isso, se $b \in G/G_{k+1}$ então $b = g_1^{e_1} \cdots g_n^{e_n}$ onde cada e_i é determinado de modo único módulo p^k e então, cada r_i é determinado de modo único módulo p^k, para todo k. Logo, o mapa $\varphi : \mathbb{Z}_p^n \to G$ dado por $\varphi(r) = g_1^{r_1} \cdots g_n^{r_n}$ é uma bijeção. Uma vez que multiplicação é um mapa contínuo, segue que φ é contínuo. Mas toda bijeção contínua entre espaços compactos Hausdorff é um homeomorfismo, ou seja, G e $\mathbb{Z}_p^n$ são isomorfos como grupos profinitos.

Essa é uma maneira de identificar G com $\mathbb{Z}_p^n$, contudo não é suficiente para atingir certos objetivos e assim, faremos essa identificação de uma maneira menos intuitiva.

Dado $n \in \mathbb{N}$, o mapa $x \mapsto x^{p^n}$ é um homeomorfismo entre G e $G_{n+1} = G^{p^n}$. Este mapa induz uma operação de grupo em G. Para $x, y \in G$, definamos

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

Além disso, a sequência $(x +_n y)_n$ é uma sequência de Cauchy e, portanto, tem um limite. Para $x, y \in G$, definamos

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

Não é difícil mostrar que essa operação torna $(G, +)$ um grupo abeliano com identidade 1 e inverso dado por $x \mapsto x^{-1}$, contudo a verificação de tais fatos é feita por meios de alguns cálculos utilizando algumas propriedades modulares dessa operação definida, o que não é o objetivo principal deste trabalho. De fato, além disso, usando tais propriedades podemos concluir a seguinte proposição:

Proposição 1.3.2. *O par $(G, +)$ é um grupo abeliano. Além disso, com a topologia original de G, $(G, +)$ é um grupo pro-p uniforme com a mesma dimensão de G e qualquer conjunto de geradores de G também gera $(G, +)$ topologicamente.*

Como consequência desse teorema, por [4, Proposição 1.26], é fácil ver que $(G, +)$ é um $\mathbb{Z}_p$-módulo. Ainda podemos obter um resultado mais forte.

Seja $\{g_1, ..., g_n\}$ um conjunto de geradores topológicos do grupo pro-p uniforme $(G, +)$ e $\mathrm{d}((G, +)) = n$. Como vimos anteriormente, usando a notação aditiva, cada $g \in G$ pode ser escrito, de maneira única, como

$$g = r_1 g_1 + \cdots + r_n g_n$$

com $r_i \in \mathbb{Z}_p$ para $i = 1, ..., n$. Isso nos mostra que $(G, +)$ tem uma estrutura de módulo livre sobre $\mathbb{Z}_p$. Então podemos enunciar o seguinte teorema:

Teorema 1.3.1. *Sejam G um grupo pro-p uniforme de dimensão n e $\{g_1, ..., g_n\}$ um conjunto que gera G topologicamente. Então $(G, +)$ é um $\mathbb{Z}_p$-módulo livre sobre $\{g_1, ..., g_n\}$.*

Capítulo 2

Conexão entre Variedades e os Números p-ádicos

O primeiro contato que, provavelmente, se tem com ideias topológicas e de diferenciabilidade é através de $\mathbb{R}^n$ e suas propriedades. O que talvez não se saiba de imediato é que podemos estender alguns conceitos que caracterizam $\mathbb{R}^n$ para obter espaços com propriedades que este não possui. Para isso introduziremos as variedades analíticas p-ádicas. Sendo um pouco mais específico, nós daremos um foco às variedades analíticas p-ádicas com base nos conhecidos números p-ádicos. Além disso, apresentaremos construções dos números p-ádicos usando as ferramentas estudadas aqui.

Os principais teoremas deste capítulo foram baseados em [18].

2.1 Variedades Analíticas

Toda a matemática que surge com a definição de variedade analítica é muito significativa e complexa. Não teremos espaço suficiente aqui para apresentar tudo o que a envolve, por isso falaremos apenas dos pontos principais que serão usados ao longo do trabalho. Como sugestão para uma leitura mais completa, o leitor pode consultar [18].

Neste capítulo vamos considerar K um corpo completo com respeito a um valor absoluto não-trivial e X uma n-upla de variáveis não necessariamente comutativas.

Os teoremas não demonstrados nesta seção podem ser consultados em [18, parte II] com as devidas demonstrações.

Definição 2.1.1. Seja $U \subset K^n$ um aberto. Uma função $\varphi : U \to K$ é *analítica* em U se, para cada $x \in U$, existe uma série de potências formal

$$f(X) = \sum_{a \in \mathbb{N}^r} c_a X^a \in K[[X]]$$

tal que $B_r(x) \subset U$, f é convergente em $B_r(0)$ e $\varphi(x+y) = f(y)$ para todo $y \in B_r(0)$ para algum $r > 0$ onde

$$B_r(x) = \{y : |x - y| < r\}.$$

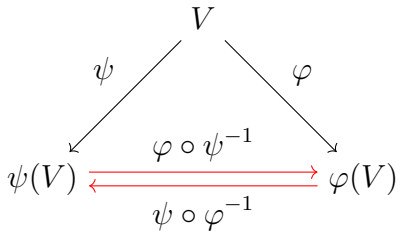
Definição 2.1.2. Seja X um espaço topológico. Sejam $U \subset X$ um aberto, n um inteiro positivo e $\varphi : U \to K^n$ é contínua com inversa contínua com $\varphi(U)$ aberto. Uma *carta local* c em X é a tripla (U, φ, n). Dizemos que uma carta $c = (U, \varphi, n)$ é *global* se $U = X$.

Exemplo 2.1.1. Se $X = V$ onde V é qualquer espaço vetorial n-dimensional sobre K com a topologia usual gerada pelas bolas abertas e $\varphi : X \to K^n$ é um isomorfismo linear, então $c = (V, \varphi, n)$ é uma carta local em X que também é global.

Uma carta local descreve o comportamento de uma parte do que definiremos a seguir como variedade. Para que possamos descrever o comportamento de toda a variedade, precisamos de alguma maneira de transitar de forma suave entre essas cartas.

Definição 2.1.3. Sejam X um espaço topológico e $c = (U, \varphi, n)$, $\tilde{c} = (\tilde{U}, \psi, \tilde{n})$ duas cartas locais em X. As cartas c e $\tilde{c}$ são *compatíveis* se os mapas $\varphi \circ \psi^{-1}|_{U \cap \tilde{U}}$ e $\psi \circ \varphi^{-1}|_{U \cap \tilde{U}}$ são analíticos.

O diagrama



onde $V = U \cap \tilde{U}$, nos permite ver que essa definição trabalha justamente a transição entre essas cartas. Fica mais claro o motivo da exigência de que esses mapas sejam analíticos quando se estuda a diferenciabilidade entre variedades.

Exemplo 2.1.2. Quaisquer duas cartas c e $\tilde{c}$ definidas de acordo com o Exemplo 2.1.1 são compatíveis.

Definição 2.1.4. Seja X um espaço topológico. Um *atlas* $\mathcal{A}$ em X é uma família de cartas locais $c_i = (U_i, \varphi_i, n_i)$ tais que $X \subset \bigcup U_i$ e qualquer par de cartas c_i e c_j são compatíveis. Dois atlas $\mathcal{A}$ e $\tilde{\mathcal{A}}$ são *compatíveis* se c e $\tilde{c}$ são compatíveis para quaisquer $c \in \mathcal{A}$ e $\tilde{c} \in \tilde{\mathcal{A}}$. Dizemos que um atlas $\mathcal{A}$ é *global* se existe alguma carta global em $\mathcal{A}$.

Exemplo 2.1.3. De acordo com as notações do Exemplo 2.1.1, defina o conjunto $\mathcal{A}$ das cartas $c = (V, \varphi, n)$ onde φ é um isomorfismo linear. Uma vez que quaisquer duas cartas locais em $\mathcal{A}$ são compatíveis, então $\mathcal{A}$ é um atlas. Além disso, como qualquer carta c é uma carta global, $\mathcal{A}$ é um atlas global.

Note que qualquer atlas $\mathcal{A}$ é compatível com si mesmo. Além disso, se $\mathcal{A}_1$ e $\mathcal{A}_2$ são compatíveis, então $\mathcal{A}_2$ e $\mathcal{A}_1$ são compatíveis, uma vez que a compatibilidade de cartas locais é claramente simétrica. Se $\mathcal{A}_1$, $\mathcal{A}_2$ e $\mathcal{A}_3$ são atlas e c_1, c_2 e c_3 respectivas cartas locais, então $\varphi_3 \circ \varphi_2^{-1}$ e $\varphi_2 \circ \varphi_1^{-1}$ são analíticas, logo, $\varphi_3 \circ \varphi_1^{-1}$ é analítica (considerando os domínios apropriados), pois a composição de mapas analíticos é claramente analítica. Analogamente vemos que $\varphi_1 \circ \varphi_3^{-1}$ é analítica. Assim, a compatibilidade de atlas é uma relação de equivalência.

Definição 2.1.5. Seja X um espaço topológico. Uma *estrutura de variedade analítica* é uma classe de equivalência de atlas compatíveis em X. Quando tal estrutura existe, dizemos que X é uma *variedade analítica*. Se $K = \mathbb{Q}_p$, dizemos que X é uma *variedade analítica p-ádica*.

Exemplo 2.1.4. O atlas definido no Exemplo 2.1.3 dá um estrutura de variedade analítica ao K-espaço vetorial V definido no Exemplo 2.1.1.

Exemplo 2.1.5. Seja X uma variedade analítica e $Y \subset X$ um aberto. Se $\mathcal{A} = \{c_i = (U_i, \varphi_i, n_i)\}$ é um atlas de X, tome $\tilde{\mathcal{A}} = \{\tilde{c}_i = (U_i \cap Y, \varphi_i|_{U_i \cap Y}, n_i)\}$. Então $\tilde{\mathcal{A}}$ é um atlas que dá a Y uma estrutura de variedade analítica. Nesse caso dizemos que Y possui uma estrutura de variedade analítica induzida por X e X estende a estrutura de variedade de Y.

Sejam X, Y variedades analíticas, c_x, c_y respectivas cartas locais e $\mathcal{A}_x, \mathcal{A}_y$ respectivos atlas. Defina

$$c = (U_x \times U_y, \varphi_x \times \varphi_y, n_x + n_y)\,.$$

Temos que $X \times Y$ é um espaço topológico e $\mathcal{A} = \{c_x \times c_y : c_x \in X, c_y \in Y\}$ é um atlas. Assim, está determinada uma estrutura de variedade em $X \times Y$ e, portanto, o produto cartesiano de variedades analíticas é uma variedade analítica.

Definição 2.1.6. Sejam X e Y variedades analíticas. Uma função $f : X \to Y$ é *analítica* se é contínua e existe um atlas $\mathcal{A}$ de X, um atlas $\tilde{A}$ de Y tais que se $c = (U, \varphi, n) \in \mathcal{A}$ e $\tilde{c} = (\tilde{U}, \tilde{\varphi}, \tilde{n}) \in \tilde{\mathcal{A}}$, então tomando $V = U \cap f^{-1}(\tilde{U})$ a composição

$$\varphi(V) \xrightarrow{\varphi^{-1}} U \xrightarrow{f} U \xrightarrow{\tilde{\varphi}} \tilde{\varphi}(V)$$

é analítica no sentido da definição 2.1.1.

Uma vez que uma carta em um atlas descreve o comportamento local da variedade, podemos dizer que $f : X \to Y$ é analítica se é contínua e é localmente dada por funções analíticas.

Definição 2.1.7. Sejam X uma variedade analítica e $x \in X$. Seja F_x o conjunto dos pares (U, φ) onde U é uma vizinhança aberta de x e φ é uma função analítica em U. Dois elementos (U, φ) e $(\tilde{U}, \tilde{\varphi})$ em F_x são *equivalentes* se existe uma vizinhança V de x com $V \subset U \cap \tilde{U}$ tal que $\varphi|_V = \tilde{\varphi}|_V$. O conjunto das classes de equivalência de F_x é denotado por H_x e é chamado de *anel local* em x.

Sejam $f, g \in H_x$. Como f e g são classes de equivalência de elementos de F_x, escolha $(U, \varphi) \in f$ e $(\tilde{U}, \psi) \in g$. Seja $V = U \cap \tilde{U}$. Definimos $f + g$ para ser a classe de $(V, f|_V + g|_V)$ e fg para ser a classe de $(V, (f|_V)(g|_V))$. Uma vez que escolhemos elementos de classes de equivalência, é fácil ver que as definições de soma e produto independem dos elementos escolhidos.

O mapa canônico $K \ni \alpha \mapsto (X, c_\alpha) \in F_x$ onde c_α é a função constante igual a α induz uma inclusão $i : K \to H_x$. Além disso, o mapa canônico $F_x \ni (U, \varphi) \mapsto \varphi(x) \in K$ induz um homomorfismo sobrejetor $h : H_x \to K$. Sendo K um corpo, $\ker h$ é um ideal maximal. Denotando $i(K)$ por K e $\ker h$ por $\mathfrak{m}_x$, podemos decompor $H_x = K \oplus \mathfrak{m}_x$.

Podemos ver por [18, p. 80] que H_x é, de fato, um anel local.

Definição 2.1.8. Seja X uma variedade analítica e $x \in X$. O *espaço tangente* T_xX de X em x é o dual de $\mathfrak{m}_x/\mathfrak{m}_x^2$, ou seja,

$$T_xX = (\mathfrak{m}_x/\mathfrak{m}_x^2)^*.$$

Se $f \in H_x$, então $f - f(x) \in \mathfrak{m}_x$, já que h mapeia $f - f(x)$ em 0.

Definição 2.1.9. Sejam X uma variedade analítica, $x \in X$ e $f \in H_x$. A *diferencial* de f em x, denotada por df_x, é a imagem de $f - f(x)$ em $\mathfrak{m}_x/\mathfrak{m}_x^2$. Para $v \in T_xX$, a *derivada* de f na direção v, denotada por $\langle v, df_x \rangle$, é v aplicado à df_x.

Seja $\varphi : X \to Y$ é uma função analítica entre duas variedades analíticas. Defina $T_x\varphi : T_xX \to T_{\varphi(x)}Y$ por

$$\left\langle T_x\varphi(v), df_{\varphi(x)} \right\rangle = \langle v, d(f \circ \varphi)_x \rangle$$

para cada $v \in T_xX$ e $f \in H_x$.

Dado $x \in X$, sejam $f_1, ..., f_m$ funções analíticas em uma vizinhança U de x. Tomando $F(y) = (f_1(y), ..., f_m(y))$ para $y \in U$. Dizemos que $\{f_i\}_i$ define um sistema de

coordenadas em x se existe uma vizinhança $\tilde{U}$ de x, contida em U, tal que $(\tilde{U}, F|_{\tilde{U}}, m)$ define uma carta em X. Podemos mostrar que $\{f_i\}_i$ define um sistema de coordenadas em x se, e somente se, $\{d(f_i)_x\}_i$ formam uma base para $\mathfrak{m}_x/\mathfrak{m}_x^2$.

A aplicação $d(f_i)_x$ é comumente denotada por $(\partial_i f)(x)$ e chamada de *derivada parcial*.

Definição 2.1.10. O mapa $T_x\varphi$ definido no parágrafo anterior é chamado *mapa tangente* de φ.

Conhecendo o conceito de espaço tangente, podemos obter uma espécie de generalização do Teorema da Função Inversa.

Teorema 2.1.1. *Sejam X e Y variedades analíticas, $x \in X$, $y \in Y$ e uma função analítica $\varphi : X \to Y$ tal que $\varphi(x) = y$. Então φ é um isomorfismo local em x se, e somente se, $T_x\varphi$ é um isomorfismo.*

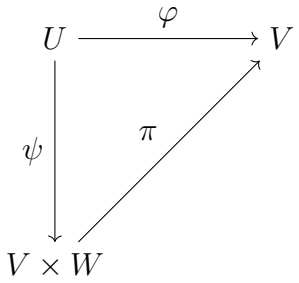
O Teorema da Função Inversa nos fornece um resultado que será particularmente útil no último capítulo.

Sejam X e Y variedades analíticas, $x \in X$ e $y \in Y$. Seja $\varphi : X \to Y$ uma função analítica tal que $\varphi(x) = y$. Sejam $m = \dim_K x$ e $n = \dim_K y$. Relembre que $\dim_K x$ é a dimensão de qualquer carta c que descreva uma vizinhança de x.

Teorema 2.1.2. *As seguintes afirmações são equivalentes:*

(i) *$T_x\varphi$ é sobrejetiva.*

(ii) *Existem vizinhanças abertas U de x, V de y e W de 0 em K^{m-n} e um isomorfismo $\psi : U \to V \times W$ tal que $\psi(U) = V$ e comuta o diagrama*



onde $\pi : V \times W \to V$ é a projeção canônica.

(iii) *Existem coordenadas $\{f_i\}$ em x e $\{g_i\}$ em y tais que $f_i = g_i \circ \varphi$ para $1 \leq i \leq n$.*

(iv) *Existem vizinhanças abertas U de x e V de y e uma função analítica $\sigma : V \to U$ tal que $\varphi(U) \subset V$ e $\varphi \circ \sigma = \mathrm{id}_V$.*

Definição 2.1.11. Uma *submersão* em x é uma função analítica φ satisfazendo alguma das condições equivalentes do Teorema 2.1.2 em x. Uma *submersão* φ em X é uma submersão em cada $x \in X$.

2.2 Grupos Analíticos

Nos últimos séculos ficou claro que as áreas da Matemática, por mais diferentes que pareçam, se conectam a medida que nos aprofundamos nela. No final do último século, a demonstração do Teorema de Fermat-Wiles se tornou um ótimo exemplo disso. Certamente não é diferente do que ocorre na relação entre grupos e variedades. Nossa ideia para esta seção é estudar um tipo de grupo que começará a unir todos os conceitos que estudamos anteriormente.

Definição 2.2.1. Um *grupo p-ádico analítico* é um grupo topológico G que também é uma variedade p-ádica analítica e o mapa $(g, h) \mapsto gh^{-1}$ em G é analítico.

De forma similar ao caso dos grupos topológicos, pedir que $(g, h) \mapsto gh^{-1}$ seja analítico é equivalente a pedir que os mapas $(g, h) \mapsto gh$ e $g \mapsto g^{-1}$ sejam analíticos.

Exemplo 2.2.1. Se G é um grupo equipado com a topologia discreta, o conjunto $\mathcal{A} = \{c = (\{g\}, \varphi, 0)\}$ com $\varphi : \{g\} \to 0 \subset \mathbb{Q}_p$ é um atlas que torna G uma variedade p-ádica. Além disso, os mapas $g \mapsto g$ e $g \mapsto g^{-1}$ de G em G são analíticos.

Exemplo 2.2.2. Mostraremos na Seção 3 deste capítulo que $\mathbb{Q}_p$ é um grupo p-ádico analítico.

Duas afirmações [4, capítulo 8] facilmente verificáveis e úteis para nós são:

1. A composição de funções analíticas é analítica.
2. Uma função ser analítica depende do seu comportamento local, isto é, dada $f : X \to Y$ onde $X \subset \bigcup_i X_i$ com X_i aberto em X, então $f|_{X_i}$ ser analítica, para cada i, implica f analítica em X.

Proposição 2.2.1. *Seja G um grupo topológico contendo um subgrupo aberto H que tem a estrutura de um grupo p-ádico analítico. Suponha que, para cada $g \in G$, existe uma vizinhança aberta V_g da identidade em H tal que $gV_gg^{-1} \subset H$ e o mapa τ dada por $x \mapsto gxg^{-1}$ de V_g em H é analítico. Então existe uma única estrutura de variedade analítica em G estendendo a estrutura de variedade de H que torna G um grupo p-ádico analítico.*

Demonstração. Sejam T um transverso à esquerda de H em G, $\mathcal{A}$ um atlas em H e $p_g : G \to G$,$c_g : H \to G$ funções dadas por $p_g(x) = gx$ e $c_g(x) = gxg^{-1}$. Para cada $t \in T$, definamos

$$\mathcal{A}_t = \{(tU, \varphi_t, n) : (U, \varphi, n) \in \mathcal{A}\}$$

onde $\varphi_t : tU \to \mathbb{Z}_p^n$ é dado por $\varphi_t(x) = \varphi(t^{-1}x)$. Dado $t \in T$ considere a restrição p_g à tH. Sabemos que $gt = sh$ para algum $s \in T$ e $h \in H$. Note que, para cada $(U, \varphi, n), (V, \psi, m) \in \mathcal{A}$, a função $\psi_s \circ p_g \circ \varphi_t^{-1}$ é a função $\psi \circ p_h \circ \varphi^{-1}$ (considerando-se os domínios apropriados) que é analítica pois H é um grupo analítico, logo, a restrição p_g é analítica em tH para todo t. Portanto, p_g é analítica em G. Por hipótese, existe uma vizinhança aberta da identidade V_g tal que $V_g \subset H \cap g^{-1}Hg$ e τ é analítico. Note que, para $h \in H$, hV_g é uma vizinhança aberta de h e assim, a restrição $c_g : hV_g \to ghg^{-1}H$ é a composição $f_{h^{-1}} \circ \tau \circ f_{ghg^{-1}}$, logo, c_g é analítica em uma vizinhança aberta de h, para todo $h \in H$. Portanto, c_g é analítica em H. O mapa $(g, h) \mapsto gh^{-1}$ de $G \times G$ em G é analítico, pois este mapa restrito à $sH \times tH$ é analítico para todo $s, t \in T$, uma vez que, para quaisquer $h_1, h_2 \in H$,

$$(sh_1)(th_2)^{-1} = st^{-1}t(h_1h_2^{-1})t^{-1},$$

ou seja, é composição de funções analíticas. Com isso, tomando $\tilde{\mathcal{A}} = \bigcup_t \mathcal{A}_t$ é um atlas em G e isso estende a estrutura analítica de H à G.

Agora, seja $\mathcal{B}$ outro atlas de G que torna G um grupo p-ádico analítico estendendo a estrutura analítica de H, ou seja, $\mathcal{A} \subset \mathcal{B}$. Sendo G um grupo p-ádico analítico, para cada $g \in G$, a função p_g (agora considerando o atlas $\mathcal{B}$) é analítica. Com isso, se $(U, \varphi, n) \in A$ $(V, \psi, n) \in B$, então $\phi \circ p_{g^{-1}} \circ \psi^{-1}$ e $\psi \circ p_g \circ \varphi^{-1}$ são analíticas, mas essas funções são $\varphi_g \circ \psi^{-1}$ e $\psi \circ \varphi_g^{-1}$, respectivamente (considerando-se os domínios apropriados). Assim, os atlas $\tilde{\mathcal{A}}$ e $\mathcal{B}$ são compatíveis. Isso mostra a unicidade da extensão. □

Essa proposição nos fornece um critério verificar se um grupo G tem a estrutura de uma variedade p-ádica analítica, o que será útil para demonstrarmos uma forte relação entre grupos analíticos e grupos uniformes. Antes disso, precisamos de alguns lemas técnicos.

Nos próximos lemas, consideraremos G um grupo topológico.

Lema 2.2.1. *Sejam $u_1, ..., u_r \in G$ e ponha $v_i = u_i - 1$ para cada i. Se $\lambda_1, ..., \lambda_r \in \mathbb{Z}_p$, então*

$$u_1^{\lambda_1} \cdots u_r^{\lambda_r} = \sum_{a \in \mathbb{N}^r} \binom{\lambda_1}{a_1} \cdots \binom{\lambda_r}{a_r} v_1^{a_1} \cdots v_r^{a_r}$$

onde $a = (a_1, ..., a_r)$.

Lema 2.2.2. *Sejam $u_1, ..., u_r \in G$ se $p > 2$ e $u_1, ..., u_r \in \Phi(G)$ se $p = 2$. Defina $g = (g_1, ..., g_n) : \mathbb{Z}_p^r \to \mathbb{Z}_p^n$ por $g_i(\lambda_1, ..., \lambda_r) = \tilde{u_i}$ onde $u_1^{\lambda_1} \cdots u_r^{\lambda_r} = a_1^{\tilde{u_1}} \cdots a_r^{\tilde{u_n}}$. Então g é analítica em $\mathbb{Z}_p^r$.*

As demonstrações desses lemas podem ser lidas em [4, capítulo 8].

Teorema 2.2.1. *Seja G um grupo topológico contendo um subgrupo aberto N que é pro-p e uniforme. Então G é um grupo p-ádico analítico.*

Demonstração. Como N é pro-p uniforme, então existem $g_1, ..., g_n$ geradores topológicos de N. Se $p > 2$, defina $H = N$ e $u_i = g_i$; senão, defina $H = P_2(N)$ e $u_i = g_i^2$, para cada $i = 1, ..., n$. De acordo com essas definições, $H = \langle u_1, ..., u_n \rangle$. Defina $\varphi : H \to \mathbb{Z}_p^n$ por $\varphi(x) = (\lambda_1, ..., \lambda_n)$ onde $x = u_1^{\lambda_1} \cdots u_n^{\lambda_n}$. Então o atlas $\mathcal{A} = \{(H, \varphi, n)\}$ torna H um grupo p-ádico analítico.

Seja $\epsilon = 1$ se $p > 2$ e $\epsilon = 2$ caso contrário. Defina $f : \mathbb{Z}_p^n \times \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ por $f(r, s) = t$ onde

$$\left(\prod_1^n u_i^{r_i}\right)\left(\prod_1^n u_i^{s_i}\right)^{-1} = \prod_1^n u_i^{t_i}.$$

Defina $\tilde{f} : \mathbb{Z}_p^{2n} \to \mathbb{Z}_p^n$ por $\tilde{f}(\lambda_1, ..., \lambda_{2n}) = u$ onde

$$\prod_1^{2n} u_i^{\lambda_i} = \prod_1^n g_i^{\tilde{u_i}}$$

com $u_{n+1} = u_{n-i+1}^{-1}$. Se $\epsilon = 1$, então

$$u_1^{\lambda_1} \cdots u_{2n}^{\lambda_{2n}} = g_1^{\tilde{u_1}} \cdots g_n^{\tilde{u_n}}$$

se torna

$$(u_1^{\lambda_1} \cdots u_n^{\lambda_n})(u_n^{-\lambda_{n+1}} \cdots u_1^{-\lambda_{2n}}) = g_1^{\tilde{u_1}} \cdots g_n^{\tilde{u_n}},$$

ou seja, $f = \tilde{f}$. Se $\epsilon = 2$, então o mesmo argumento auxiliado pela igualdade $u_i = a_i^2$ conclui que $f = \dfrac{\tilde{f}}{2}$. Uma vez que $\tilde{f}$ é analítica pelo Lema 2.2.2, então f é analítica. Isso mostra que o mapa $(x, y) \mapsto xy^{-1}$ de $H \times H$ em H é analítico com respeito à estrutura de variedade de H. Dado $g \in G$, temos que $H \cap g^{-1}Hg$ é um subgrupo aberto de H e, portanto, existe $m \in \mathbb{N}$ tal que $V_g = P_{m+1}(H) \subset H \cap g^{-1}Hg$. Sendo V_g um subgrupo aberto de H, V_g possui uma estrutura de variedade induzida por H dada pelo atlas $\{(V_g, \varphi|_{V_g}, n)\}$ onde $\varphi|_{V_g} : V_g \to p^m\mathbb{Z}_p^n$ é sobrejetor. Defina $w_i = gu_i^{p^m}g^{-1}$ e as funções $\tilde{h} : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ por $\tilde{h}(\lambda_1, ...\lambda_n) = u$ onde

$$\prod_1^n w_i^{\lambda_i} = \prod_1^n g_i^{\tilde{u_i}},$$

e $h : p^m\mathbb{Z}_p^n \to \mathbb{Z}_p^n$ por $h(r) = s$ onde

$$g\left(\prod_1^n u_i^{r_i}\right)g^{-1} = \prod_1^n u_i^{s_i}.$$

Pelo lema 2.2.2, a função $\tilde{h}$ é analítica e uma ideia similar a que foi usada anteriormente mostra que $h(p^m\lambda) = \epsilon^{-1}\tilde{h}(\lambda)$ para $\lambda \in \mathbb{Z}_p^n$, logo, h é analítica em $p^m\mathbb{Z}_p^n$. Isso mostra que para cada $g \in G$ existe uma vizinhança V_g da identidade em H tal que $gV_gg^1 \subset H$ e que o mapa $x \mapsto gxg^{-1}$ de V_g em H é analítico. Pela Proposição 2.2.1, segue que G é p-ádico analítico. □

Podemos obter uma recíproca do teorema acima. Estudaremos uma categoria particular de grupos analíticos que nos permitirá atingir esse objetivo.

Definição 2.2.2. Um *grupo padrão* G de dimensão n sobre $\mathbb{Q}_p$ é um grupo p-ádico analítico tal que sua estrutura analítica é definida por um atlas global $\{(G, \varphi, n)\}$ onde φ é um homomorfismo sobrejetor de G em $p\mathbb{Z}_p^n$ se $p > 2$ ou de G em $4\mathbb{Z}_p^n$ se $p = 2$, satisfazendo $\varphi(1) = 0$ e, para cada $j = 1, ..., n$, existem $P_j(X, Y) \in \mathbb{Z}_p[[X, Y]]$ tais que

$$\varphi_j(xy^{-1}) = P_j(\varphi(x), \varphi(y))$$

para todo $x, y \in G$ onde $\varphi = (\varphi_1, ..., \varphi_n)$.

Na definição acima estamos considerando as uplas X e Y formadas por variáveis comutativas.

Podemos reformular a última exigência da definição da seguinte maneira: para cada $j = 1, ..., n$ existem $M(X, Y) \in \mathbb{Z}_p[[X, Y]]$ e $I_j(X) \in \mathbb{Z}_p[[X]]$ tais que, para todo $x, y \in G$,

$$\varphi_j(xy) = M_j(\varphi(x), \varphi(y))$$

e

$$\varphi_j(x^{-1}) = I_j(\varphi(x))$$

O teorema abaixo é um resultado chave para obter uma recíproca do teorema 2.2.1.

Teorema 2.2.2. *Seja G um grupo padrão de dimensão n sobre $\mathbb{Q}_p$. Então G é um pro-p grupo uniforme de dimensão n sobre $\mathbb{Q}_p$.*

Para demonstrar esse teorema precisamos de alguns lemas técnicos (suas demonstrações podem ser lidas em [4, capítulo 8]).

Lema 2.2.3. *Seja G um grupo padrão sobre $\mathbb{Q}_p$ e, para $a = (a_1, ..., a_r) \in \mathbb{N}^r$, denotemos*

$$\langle a \rangle = a_1 + \cdots + a_r.$$

Se $P_j(X, Y)$, para $j = 1, ..., n$ são as séries da definição de grupo padrão, então

$$P_j(X, Y) = X_j - Y_j + \sum_{(a,b)\in I} \alpha_{j,ab} X^a Y^b,$$

onde $I = \{(a, b) \in \mathbb{N}^r \times \mathbb{N}^r : \langle a \rangle + \langle b \rangle \geq 2, b \neq 0\}$, para cada j. Se $M_j(X, Y)$, para $j = 1, ..., n$ são as séries da reformulação da definição de grupo padrão, então

$$M_j(X, Y) = X_j + Y_j + \sum_{(a,b)\in J} \beta_{j,ab} X^a Y^b,$$

onde $I = \{(a, b) \in \mathbb{N}^r \times \mathbb{N}^r : \langle a \rangle \geq 1, \langle b \rangle \geq 1\}$, para cada j.

Lema 2.2.4. *Seja G um grupo padrão sobre $\mathbb{Q}_p$ com atlas global $\{(G, \varphi, n)\}$. Então existem $F_1(X), ..., F_n(X) \in \mathbb{Z}_p[[X]]$ tais que*

$$\varphi(x^p) = F(\varphi(x))$$

onde $F = (F_1, ..., F_n)$, para todo $x \in G$ e

$$F_i(X) = pX_i + \sum_{\langle a \rangle > 1} c_{i,a} X^a$$

para cada i onde $c_{i,a} \in \mathbb{Z}_p$ para cada (i, a). Além disso, se $p \neq 2$, então $c_{i,a} \equiv 0 \pmod{p}$ sempre que $\langle a \rangle = 2$.

Além disso, iremos usar o fato de que um grupo p-ádico analítico possui um subgrupo aberto que é um grupo padrão com respeito a estrutura analítica induzida [4, Teorema 8.9].

Demonstração do Teorema 2.2.2. Seja $\{(G, \varphi, n)\}$ um atlas global satisfazendo as condições da definição de grupo padrão. Definamos $G(i) = \varphi^{-1}(p^i \mathbb{Z}_p^n)$ onde $i \geq 1$ se $p > 2$ e $i \leq 2$ caso contrário. Pela definição de φ, $\{G(i)\}_i$ é uma base de vizinhanças da identidade em G. Por definição

$$\varphi_j(xy^{-1}) = P_j(\varphi(x), \varphi(y))$$

onde $P_j(X, Y) \in \mathbb{Z}_p[X, Y]$ e $\varphi = (\varphi_1, ..., \varphi_n)$. Então, pelo Lema 2.2.3,

$$\varphi_k(xy^{-1}) \equiv \varphi_k(x) - \varphi_k(y) \pmod{p^{j+\min\{i,j\}}}$$

para cada $x \in G(i)$, $y \in G(j)$ e $k = 1, ..., n$. Se $i = j$, então temos

$$\varphi_k(xy^{-1}) \equiv \varphi_k(x) - \varphi_k(y) \pmod{p^{2i}}$$

para cada $x, y \in G(i)$, o que implica $\varphi(xy^{-1}) \in p^i\mathbb{Z}_p^n$ e assim, $xy^{-1} \in G(i)$, isto é, $G(i)$ é um subgrupo de G. Além disso, φ induz um homomorfismo sobrejetor de $G(i)$ em $p^i\mathbb{Z}_p^n/p^{i+1}\mathbb{Z}_p^n$ com núcleo $\varphi^{-1}(p^{i+1}\mathbb{Z}_p^n) = G(i+1)$. Com isso,

$$G(i)/G(i+1) \simeq p^i\mathbb{Z}_p^n/p^{i+1}\mathbb{Z}_p^n = (\mathbb{Z}/p\mathbb{Z})^n.$$

De acordo com isso, $G(i)$ é um subgrupo subnormal de índice p^r em G. Mais que isso, pelo Lema 2.2.4, se $x \in G(i)$ então

$$\varphi_k(x^p) \equiv p\varphi_k(x) \pmod{p^{i+2}}$$

para cada j e note que $\lambda \mapsto p\lambda$ induz um isomorfismo entre $p^i\mathbb{Z}_p^n/p^{i+1}\mathbb{Z}_p^n$ e $p^{i+1}\mathbb{Z}_p^n/p^{i+2}\mathbb{Z}_p^n$, logo, $x \mapsto x^p$ induz um isomorfismo entre $G(i)/G(i+1)$ e $G(i+1)/G(i+1)$ com $G(i+1) = G(i)^pG(i+1)$. Indutivamente é fácil ver que $G(i+1) = G(i)^pG(i+m)$ para todo $m \geq 1$. Tomando a interseção, então $G(i+1) = \overline{G(i)^p}$. Agora, $G(2) = G$, $G(3) = \overline{G^p} \triangleleft G$ e, indutivamente, $G(i) \triangleleft G$ para cada $i \geq 2$.

Agora, se $p > 2$ temos

$$G/\overline{G^p} = G(1)/G(2) \simeq (\mathbb{Z}/p\mathbb{Z})^n,$$

ou seja, $G/\overline{G^p}$ é abeliano. Se $p = 2$, tomando $y \in G(4)$ e "passando" por $G(3)$, vemos que existe $x \in G(2) = G$ tal que $y \equiv x^4 \pmod{G(n)}$ para todo $n \geq 4$. Assim,

$$G(4) \subset \overline{G^4}.$$

Temos também o isomorfismo entre $G(2)/G(4)$ e $2^2\mathbb{Z}_2^n/2^4\mathbb{Z}_2^n$ decorrente da definição de $G(i)$ e da igualdade dada pelo Lema 2.2.3. Então, $G/\overline{G^4}$ é abeliano. Portanto, G é powerful e em qualquer caso $\mathrm{d}(G) = n$.

Uma vez que $G(i+1) = \overline{G(i)^p}$ e $P_2(G) = \Phi(G) = G^p$, por [4, Teorema 3.6], vemos que $G_i = G(i)$ se $p > 2$ e $G_i = G(i+1)$ caso contrário. Concluímos então que G é uniforme. □

O último resultado essencial para conseguirmos a recíproca desejada é:

Teorema 2.2.3. *Se G é um grupo p-ádico analítico, então G tem um subgrupo aberto H que é um grupo padrão com respeito a estrutura de variedade induzida de G.*

A demonstração desse teorema [4, Teorema 8.29] utiliza técnicas muito semelhantes as que usamos para provar o teorema anterior, por isso será omitida.

Juntando todas as partes podemos enunciar o seguinte resultado:

Teorema 2.2.4. *Seja G um grupo topológico. Então G possui a estrutura de um grupo p-ádico analítico se, e somente se, G contém um subgrupo aberto pro-p uniforme.*

O Teorema 2.2.4 traz várias consequências relevantes para os grupos p-ádicos analíticos. Por exemplo:

Corolário 2.2.1. *Seja G um grupo p-ádico analítico. Então G é compacto se, e somente se, G é profinito.*

Demonstração. Suponha que G seja um grupo p-ádico analítico compacto. Então G tem um subgrupo H que é aberto pro-p uniforme. Note que

$$G \subset \bigcup_g gH.$$

Como H é Hausdorff, então G também é. Se V é uma vizinhança aberta de 1 em G, então $V \cap H$ é uma vizinhança aberta de 1 em H e, além disso, podemos escolher $\tilde{V} \leq_o H$ com $\tilde{V} \subset V$. Uma vez que $\tilde{V} \leq_o G$, então os subgrupos abertos de G constituem uma base de vizinhanças para a identidade em G. Logo, G é um grupo profinito. A recíproca é trivial. □

Uma curiosidade é que os exercícios 9 e 10 de [4, capítulo 1] nos permitem concluir que $\mathrm{SL}_n(\mathbb{Z}_p)$ possui um subgrupo aberto pro-p uniforme, logo, é p-ádico analítico.

2.3 Números p-ádicos

Os números p-ádicos surgem em diversas áreas diferentes da Matemática. Desde a solução de equações usando o princípio de Hasse até aplicações em criptografia, e assuntos mais avançados como dinâmica. Isso é claro, além de toda importância na teoria dos números e, em geral, na Álgebra. Nesta seção iremos apresentar uma construção dos inteiros p-ádicos como um exemplo de grupo profinito e os racionais p-ádicos como uma variedade analítica.

Existem algumas formas distintas (que geram resultados equivalentes) de construir o conjunto dos inteiros p-ádicos.

Definição 2.3.1. Definimos o conjunto $\mathbb{Z}_p$ dos *inteiros p-ádicos* para ser

$$\mathbb{Z}_p = \left\{ \sum_{j=0}^{\infty} a_j p^j : 0 \leq a_j < p \right\}.$$

Mostraremos agora que podemos construir $\mathbb{Z}_p$ como um grupo profinito.

Considere $G_i = \mathbb{Z}/p^i\mathbb{Z}$ e defina $\pi_{ij} : G_j \to G_i$ para $j \geq i$ por

$$\pi_{ij}(n + p^j\mathbb{Z}) = n + p^i\mathbb{Z}$$

para $n \in \mathbb{Z}$. Então existe

$$L = \varprojlim_i G_i.$$

Agora, defina $f_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$ por

$$f_i\left(\sum_{j=0}^{\infty} a_j p^j\right) = \sum_{j=0}^{i-1} a_j p^j + p^i\mathbb{Z}$$

e $g : \mathbb{Z}_p \to L$ por

$$g(\alpha) = (f_i(\alpha))_i.$$

Aqui $(f(\alpha))_i$ pode ser visto como um vetor e $1 \leq i$ são as coordenadas. Uma vez que f_i é um homomorfismo, então g também é. Além disso, $g(x) = 0$ se, e só se, $f_i(\alpha) = 0$ o que ocorre somente quando $\alpha = 0$. Assim, $\ker g = \{0\}$. Se $\beta \in L$, então $\beta = (b_i + p^i\mathbb{Z})_i$ com $0 \leq i$. Tome b_i com $0 \leq b_i < p^i$ e defina $a_0 = b_1$. Para $1 \leq i$, p^i divide $x_{i+1} - x_i$ e assim, $x_{i+1} - x_i = a_i p^i$. Uma vez que

$$x_{i+1} = \sum_{0}^{i} a_j p^j$$

com $0 \leq a_i < p^i$, então

$$\beta = g\left(\sum_{j=0}^{\infty} a_j p^j\right),$$

logo, g é um isomorfismo. Definamos $U \subset \mathbb{Z}_p$ aberto se $g(U)$ é aberto em L (com isso tornamos g contínua). Além disso, definamos

$$\alpha \oplus \beta = g^{-1}(g(\alpha) + g(\beta)),$$

$$\alpha \otimes \beta = g^{-1}(g(\alpha)g(\beta)).$$

Então nós tornamos g um isomorfismo de anéis topológicos. Logo,

$$\mathbb{Z}_p \simeq L,$$

Assim, podemos ver $\mathbb{Z}_p$ como um anel (em particular, um grupo) pro-p.

Uma observação talvez imediata é que podemos pensar em $\mathbb{Z}$ como o subconjunto de $\mathbb{Z}_p$ formado pelos elementos $\sum_{j=0}^{\infty} a_j p^j$ onde $a_j \neq 0$ apenas para um quantidade finita de j.

Note que

$$g\left(p\left(\sum_{j=0}^{\infty} a_j p^j\right)\right) = g\left(\sum_{j=1}^{\infty} a_{j-1} p^j\right),$$

logo repetindo esse processo,

$$p^i\left(\sum_{j=0}^{\infty} a_j p^j\right) = \sum_{j=i}^{\infty} a_{j-i} p^j$$

o que implica $p^i\mathbb{Z}_p$ aberto em $\mathbb{Z}_p$ de índice de p^i. Como $p^i\mathbb{Z}_p = \ker f_i$, então $p^i\mathbb{Z}_p$ é um subgrupo normal de $\mathbb{Z}_p$. Qualquer outro subgrupo normal N de índice p^i deve satisfazer $p^i(\mathbb{Z}_p/N) = 0$. Mas $\mathbb{Z}_p/p^i\mathbb{Z}_p \simeq \mathrm{Im}(f_i)$ é cíclico de ordem p^i de modo que $H = p^i\mathbb{Z}_p$, isto é, os subgrupos abertos de $\mathbb{Z}_p$ são os subgrupos $p^i\mathbb{Z}_p$ com $i \in \mathbb{N}$. Além disso, $p^i\mathbb{Z}_p$ são os ideais de $\mathbb{Z}_p$. Sabemos que se H é um subgrupo fechado de um grupo profinito G, então H é a interseção de todos os subgrupos abertos de G que contém H. Com isso, já sabemos como são os subgrupos fechados de $\mathbb{Z}_p$, uma vez que sabemos quem são os abertos. Como interseção de ideais é um ideal, então os subgrupos fechados de $\mathbb{Z}_p$ também são ideais. Agora, considere $x \in \mathbb{Z}_p$ diferente de 0 e o mapa ψ dado por $y \mapsto xy$. Então $\{y \in \mathbb{Z}_p : xy = 0\} = \ker\psi$ é um subgrupo fechado, mas $\ker\psi$ não contém nenhum $p^i\mathbb{Z}_p$, logo, devemos ter $\ker\psi = \{0\}$ e isso mostra que $\mathbb{Z}_p$ é um domínio.

Uma definição simples do que são os racionais p-ádicos é tomar o corpo de frações de $\mathbb{Z}_p$, mas neste ponto nosso interesse é estudar os racionais p-ádicos como uma variedade. Por isso faremos uma construção analítica.

Não definiremos valores absolutos e sequências de Cauchy em $\mathbb{Q}$, mas o leitor interessado pode consultar [5, capítulo 3].

Seja $|\cdot|_p$ um valor absoluto não-arquimediano em $\mathbb{Q}$ e definamos $\mathcal{C}$ para ser o conjunto das sequências de Cauchy com respeito $|\cdot|_p$. Definindo

$$(x_n) \oplus (y_n) = (x_n + y_n),$$

$$(x_n) \otimes (y_n) = (x_n y_n),$$

tornamos $\mathcal{C}$ um anel comutativo com identidade. Apesar disso, $\mathcal{C}$ não é um corpo já que possui divisores de 0, podemos tomar as sequências

$$1, 0, 0, ...$$

e

$$0, 1, 0, ...$$

para ver isso.

Existe um problema com $\mathcal{C}$: mesmo que duas sequências de Cauchy diferentes possam ter o mesmo limite, elas ainda são objetos diferentes. A ideia que usaremos para resolver esse problema é identificar a condição que faz com que duas sequências tenham o mesmo limite e após isso, colocar tais sequências numa mesma classe.

Considere o conjunto

$$\mathcal{N} = \left\{ (x_n) \in \mathcal{C} : \lim_{n\to\infty} |x_n|_p = 0 \right\}.$$

É fácil ver que $\mathcal{N}$ é um ideal de $\mathcal{C}$, mais que isso, $\mathcal{N}$ é um ideal maximal [5, Lema 3.2.8].

Definição 2.3.2. Definimos o corpo dos *racionais p-ádicos* por

$$\mathbb{Q}_p = \mathcal{C}/\mathcal{N}.$$

O mapa $x \mapsto (x)$ nos permite olhar $\mathbb{Q}$ como um subconjunto de $\mathbb{Q}_p$. Essa construção é conhecida como "completamento" de $\mathbb{Q}$, pois $\mathbb{Q}_p$ é completo. Para ser mais preciso, considerando a norma p-ádica em $\mathbb{Q}_p$, podemos torná-lo um espaço métrico completo. Considerando a sequência (p^{-i}), vemos que $\mathbb{Q}_p$ não pode ser compacto, visto que essa sequência não possui subsequência convergente. Uma vez que $\mathbb{Q}_p$ não é compacto, não é profinito e assim, não é possível construir $\mathbb{Q}_p$ do mesmo modo que construímos $\mathbb{Z}_p$.

Agora, para cada $i \in \mathbb{N}$, $p^{-i}\mathbb{Z}_p$ é um aberto em $\mathbb{Q}_p$, além disso,

$$\mathbb{Q}_p \subset \bigcup_i p^{-i}\mathbb{Z}_p.$$

Defina $\varphi_i : p^{-i}\mathbb{Z}_p \to \mathbb{Q}_p$ por $\varphi_i(x) = p^i x$. Então $c_i = (p^{-i}\mathbb{Z}, \varphi_i, 1)$ é uma carta local e $\mathcal{A} = \{c_i : i \in \mathbb{N}\}$ é um atlas. Logo, $\mathbb{Q}_p$ é uma variedade p-ádica analítica. Em geral, $\mathbb{Q}_p^n$ é uma variedade p-ádica analítica e a construção disso é similar a que fizemos aqui (com as devidas adaptações). Agora note que o mapa $(x, y) \mapsto x - y$ de $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$ é analítico, o que torna $\mathbb{Q}_p$ um grupo p-ádico analítico.

Capítulo 3

Correspondência entre certas categorias de Grupos e Álgebras

As estruturas de Grupos e Álgebras de Lie têm algumas similaridades, no sentido de ter comportamentos parecidos. Veremos agora como certos tipos de Grupos e Álgebras de Lie têm mais do que algumas similaridades; eles se correspondem perfeitamente. Vale ressaltar que é esperado que o leitor tenha familiaridade com as definições e resultados básicos sobre uma álgebra.

Os principais teoremas deste capítulo foram baseados em [18] e [4].

3.1 Álgebras de Lie

Nesta seção e nas próximas consideraremos A um anel comutativo com unidade, salvo menção contrária. Aqui introduziremos os conceitos e propriedades básicas de álgebras de Lie que serão suficientes para dar sentido ao que faremos na próxima seção.

Definição 3.1.1. Uma *álgebra de Lie* L sobre A é uma A-álgebra L, isto é, L é um A-módulo munido de uma operação binária $[\cdot,\cdot]_L : L \times L \to L$ bilinear, que satisfaz

$$[[x, y, z]] + [y, [z, x]] + [z, [x, y]] = 0$$

e, além disso, $[a, a]_L = 0$ para todo $a \in A$. A operação $[\cdot,\cdot]_L$ é chamada *colchete de Lie*.

Exemplo 3.1.1. Sabemos que $\mathbb{R}^3$ é um $\mathbb{R}$-módulo. Defina $[x, y]_{\mathbb{R}} : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ por $[x, y]_{\mathbb{R}} = x \times y$ onde $x \times y$ é o produto vetorial entre $x = (x_1, x_2, x_3)$ e $y = (y_1, y_2, y_3)$ gerado pelo determinante da matriz

$$x \times y = \begin{pmatrix} e_1 & e_2 & e_3 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix}$$

onde $\{e_1, e_2, e_3\}$ é a base canônica de $\mathbb{R}^3$. A fórmula de Lagrange para o produto vetorial diz que

$$x \times (y \times z) = (x \cdot z)y - (x \cdot y)z$$

onde $x \cdot z$ e $x \cdot y$ representam o produto interno. Com isso, temos que

$$y \times (z \times x) = (y \cdot x)z - (y \cdot z)x$$

e

$$z \times (x \times y) = (z \cdot y)x - (z \cdot x)y.$$

Uma vez que o produto interno é comutativo, então

$$x \times (y \times z) + y \times (z \times x) + z \times (x \times y) = 0.$$

Além disso, é claro que $[x, x]_{\mathbb{R}} = 0$. Assim, $[x, x]_{\mathbb{R}}$ torna $\mathbb{R}^3$ uma álgebra de Lie.

Definição 3.1.2. Um *anel de Lie* é um grupo abeliano L equipado com uma operação $[\cdot, \cdot]_L : L \times L \to L$ bilinear, que satisfaz a identidade de Jacobi e, além disso, $[a, a]_L = 0$ para todo $a \in A$.

Exemplo 3.1.2. O espaço vetorial $\mathbb{R}^3$ é um grupo aditivo abeliano, então tomando $[x, y]_{\mathbb{R}}$ definida no exemplo anterior, $\mathbb{R}^3$ se torna um anel de Lie.

Esse exemplo ilustra o fato de qualquer Álgebra de Lie ser também um anel de Lie.

Note que se um anel de Lie L possui a estrutura de um A-módulo, então L é também uma álgebra de Lie.

Definição 3.1.3. Seja L uma álgebra de Lie. Um *ideal* de L é um submódulo $I \neq \emptyset$ satisfazendo $[a, x]_L \in I$ para todo $a \in L$ e $x \in I$.

Sendo percebida a semelhança entre um ideal de uma álgebra de Lie e de um anel, é de se imaginar que eles satisfazem as mesmas propriedades básicas como: soma de dois ideais é um ideal, interseção de dois ideias é um ideal etc. Essas propriedades são facilmente demonstráveis. Os ideais, assim como na teoria de anéis, desempenham um papel importante na teoria das álgebras de Lie. Uma boa referência para estudar com mais detalhes é [2].

Definição 3.1.4. Um conjunto M junto com um mapa $m : M \times M \to M$ dado por $m(x, y) = xy$ é um *magma*.

Dado um conjunto finito X defina indutivamente $X_1 = X$ e

$$X_n = \bigsqcup_{p+q=n} X_p \times X_q.$$

Defina

$$M_X = \bigsqcup_{n=1}^{\infty} X_n$$

e considere o mapa $m_X : M_X \times M_X \to M_X$ por meio de $i : X_p \times X_q \to X_{p+q} \subset M_X$ onde i é inclusão canônica induzida pela definição de X_n. Note que, por definição, M_X é uma magma, chamado de *magma livre* em X. Um elemento $\omega \in M_X$ é chamado de *palavra não-associativa* em X. Se $\omega \in M_X$, então $\omega \in X_p \times X_q$ onde $p + q = n$, assim existe um único n tal que $\omega \in X_n$. O *comprimento* $\ell(\omega)$ de ω é o único n tal que $\omega \in X_n$.

Se N é um magma e $f : X \to N$ é um mapa, defina indutivamente $F(x, y) = F(x)F(y)$ para $x, y \in X_p \times X_q$. Então F pode ser definida em M_X e, além disso, tomando $n = 1$ na união disjunta M_X, vemos que F é uma extensão de f. Também é fácil ver que F é um homomorfismo. Por fim, qualquer extensão de X que é um homomorfismo de magma vai ter que "concordar" com F em M_X. Com isso podemos enunciar a seguinte afirmação:

Proposição 3.1.1. *Sejam N um magma e $f : X \to N$ um mapa. Então existe um único homomorfismo de magma $F : M_X \to N$ que estende f.*

Agora, defina por A_X uma A-álgebra do magma livre M_X. Então $\alpha \in A_X$ é dado por

$$\alpha = \sum_{1}^{m} c_m m$$

onde $c_m \in A$. Como aplicação direta da proposição anterior, temos o seguinte resultado:

Proposição 3.1.2. *Sejam B uma A-álgebra e $f : X \to B$ um mapa. Então existe um único homomorfismo de A-álgebras $F : A_X \to B$ que estende f.*

Essa proposição nos permite enunciar uma outra definição.

Definição 3.1.5. O conjunto A_X é uma *álgebra livre* em X.

Note que, por definição, A_X satisfaz os requisitos para ser uma álgebra graduada. Obviamente os elementos homogêneos de grau n são as combinações lineares das palavras de M_X de comprimento n.

Seja I o ideal de A_X gerado por elementos da forma aa e $(ab)c + (bc)a + (ca)b$, onde $a, b, c \in A_X$. Usaremos a notação

$$J(a, b, c) = (ab)c + (bc)a + (ca)b.$$

Defina por $\tilde{I}$ o conjunto dos elementos $a \in A_X$ tais que toda componente homogênea de a pertence a I. Note que $\tilde{I} \subset I$ e $\tilde{I}$ é um ideal de A_X. Um elemento $x \in A_X$ pode ser escrito como soma das suas componentes homogêneas, isto é,

$$x = \sum x_n.$$

Então

$$xx = \sum x_n^2 + \sum_{n<m} (x_n x_m + x_m x_n) = \sum x_n^2 + \sum_{n<m} (x_n + x_m)^2 - x_n^2 - x_m^2,$$

logo, $xx \in \tilde{I}$. Além disso, uma vez que

$$x = \sum x_n, y = \sum y_n, z = \sum z_n,$$

pela definição de $J(x, y, z)$ temos

$$J(x, y, z) = \sum_{i,j,k} J(x_i, y_j, z_k),$$

logo, $J(x, y, z) \in \tilde{I}$. Portanto, $\tilde{I} = I$ e assim I é um ideal graduado de A_X. Com isso, A_X/I tem herda uma estrutura de álgebra graduada. Note também que, por construção, A_X/I satisfaz a identidade de Jacobi e $(aa) = 0$ para todo $a \in A_X/I$, ou seja, A_X/I é uma álgebra de Lie.

Definição 3.1.6. O quociente A_X/I é uma *álgebra de Lie livre* sobre X.

É comum denotar A_X/I por L_X.

Por fim, se $|X| = d$ é finito e $L_X^{(n)}$ é a componente homogênea de grau n de posto $\ell_d(n)$, então $L_X^{(n)}$ será livre e

$$\ell_d(n) = \frac{1}{n} \sum_{k|n} \mu(k) d^{n|k}$$

onde μ é a função de Möbius. A justificativa dessas afirmações exigem algumas definições e cálculos de álgebra tensorial que fogem ao nosso propósito, mas podem ser encontradas em [18, Parte I, Capítulo 4, Seção 4].

3.2 A série de Campbell-Hausdorff

Nesta seção consideraremos A uma $\mathbb{Q}_p$-álgebra normada completa com respeito à norma $|\cdot|$. Além disso, usaremos várias propriedades de uma série de potências formal que não apresentaremos aqui para evitar um prolongamento que não acrescenta ao nosso objetivo.

A nossa ideia principal é apresentar alguns pontos chave para que possamos desenvolver este capítulo evitando lidar desnecessariamente com muitos lemas técnicos. Contudo, o leitor que tiver interesse em tais pontos pode consultar [4] ou, para uma leitura mais simplificada, [6].

Nosso objetivo neste ponto é apenas apresentar a série de Campbell-Hausdorff que será extremamente relevante para que possamos obter uma conexão entre grupos pro-p uniformes e álgebras de Lie sobre $\mathbb{Z}_p$.

Se X é uma n-upla de variáveis não necessariamente comutativas, denotaremos apenas nesta seção

$$W = W(X) = \{w(X) = X_{i_1} \cdots X_{i_m}\}$$

o monóide livre gerado por $X_1, ..., X_n$. A palavra vazia é denotada por 1 e o *grau* de $w(X)$ é m. O produto em $W(X)$ é feito por justaposição de palavras.

Definição 3.2.1. Seja $f : A \to D$ uma função onde D é um subconjunto aberto de A^n. Dizemos que f é *estritamente analítica* em D se existe

$$F(X) = \sum_{w \in W} a_w w \in \mathbb{Q}_p \langle\langle X \rangle\rangle$$

tal que para cada $x \in D$

$$\lim_{w \in W} |a_w|_p \, w(|x|) = 0$$

e

$$f(x) = F(x).$$

Note que $|a_w|_p$ representa a norma p-ádica de a_w em $\mathbb{Q}_p$, que é definida por $|0|_p = 0$ e $|a|_p = p^{-k}$ se $a \in p^k\mathbb{Z}_p - p^{k+1}\mathbb{Z}_p$, e $w(|x|)$ é induzido pela norma da $\mathbb{Q}_p$-álgebra A da seguinte maneira:

$$w(|x|) = \omega(|x_1|, ..., |x_n|)$$

considerando a topologia produto em A^n.

Outra observação é que para que a série $F(X)$ possa ser calculada em x, precisamos garantir a convergência e, em $\mathbb{Q}_p$, a convergência de uma série ocorre exatamente quando o termo geral tem limite 0, por isso a primeira exigência da definição 3.2.1 serve para garantir a existência de $F(x)$, já que $|a_w w(x)| \leq |a_w|_p \, |w(|x|)|$.

Considere as seguintes séries de uma variável

$$\mathcal{E}(X) = \sum_{n=0}^{\infty} \frac{1}{n!} X^n$$

e

$$\mathcal{L}(X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} X^n.$$

Definamos o conjunto

$$A_0 = \begin{cases} \{x \in A : |x| \leq p^{-1}\} & \text{se } p \neq 2, \\ \{x \in A : |x| \leq 2^{-2}\} & \text{se } p = 2. \end{cases}$$

Usando algumas propriedades simples de convergências de séries de potências e valoração p-ádica, podemos concluir que existem funções estritamente analíticas $\exp : A_0 \to 1 + A_0$ e $\log : 1 + A_0 \to A_0$ tais que $\exp(x) = \mathcal{E}(x)$ e $\log(1 + x) = \mathcal{L}(x)$ para todo $x \in A_0$. Além disso, as funções exp e log satisfazem as seguintes propriedades:

(i) $(\log \circ \exp)(x) = x$,

(ii) $(\exp \circ \log)(1 + x) = 1 + x$,

(iii) $\log(1 + x)^n = n \log(1 + x)$ para cada $n \in \mathbb{Z}$,

(iv) $\exp(nx) = \exp(x)^n$ para cada $n \in \mathbb{Z}$.

Por fim, as funções exp e log também são contínuas.

Definamos agora

$$P(X, Y) = \mathcal{E}(X)\mathcal{E}(Y) - 1 \in \mathbb{Q}_p \langle\langle X, Y \rangle\rangle$$

e

$$C(X, Y) = \mathcal{E}(-X)\mathcal{E}(-Y)\mathcal{E}(X)\mathcal{E}(Y) \in \mathbb{Q}_p \langle\langle X, Y \rangle\rangle .$$

Definição 3.2.2. A *série de Campbell-Hausdorff* $\Phi(X, Y)$ é definida por

$$\Phi(X, Y) = (\mathcal{L} \circ P)(X, Y)$$

e o *comutador de Campbell-Hausdorff* é definido por

$$\Psi(X, Y) = (\mathcal{L} \circ C)(X, Y).$$

Escolhendo $x, y \in A_0$, temos

$$\Phi(x, y) = \log(\exp(x)\exp(y))$$

e

$$\Psi(x, y) = \log(\exp(-x)\exp(-y)\exp(x)\exp(y)).$$

Se $H_i(X_1, X_2, X_3) = X_i$ e $H_{ij}(X_1, X_2, X_3) = (X_i, X_j)$, então a série de Campbell-Hausdorff satisfaz a identidade

$$\Phi \circ (H_1, \Phi \circ H_{23}) = \Phi \circ (\Phi \circ H_{12}, H_3).$$

O caso em que a n-upla $X = (X_1, ..., X_n)$ é formada por variáveis comutativas (que será o caso de nosso maior interesse) produz resultados análogos a esses; são os mesmos resultados com as devidas adaptações.

3.3 Correspondência entre Grupos Uniformes e Álgebras de Lie

Neste ponto já temos as ferramentas suficientes para apresentar uma ideia da correspondência entre certos tipos de grupos uniformes e álgebras de Lie. Não faremos uma construção totalmente detalhada, daremos apenas uma ideia de como tal correspondência é construída. Isso é um caso particular da correspondência de Lazard. O leitor que estiver interessado em uma construção com a apresentação de todos os detalhes pode encontrá-la em [4].

Relembre o enunciado do Teorema 1.3.1 do primeiro capítulo: "*Sejam G um grupo pro-p uniforme de dimensão d e $\{g_1, ..., g_n\}$ um conjunto minimal que gera G topologicamente. Então $(G, +)$ é um $\mathbb{Z}_p$-módulo livre sobre $\{g_1, ..., g_n\}$*".

Considere G um grupo pro-p uniforme. Dados $g, h \in G$ e um inteiro positivo n, temos que $g^{p^n}, h^{p^n} \in G_{n+1}$, logo,

$$\left[g^{p^n}, h^{p^n}\right] \in [G_{n+1}, G_{n+1}]$$

e por [4, Proposição 1.16] temos que $[G_{n+1}, G_{n+1}] \leq G_{2n+2}$, ou seja,

$$\left[g^{p^n}, h^{p^n}\right] \in G_{2n+2},$$

$$[g, h]_n := \left[g^{p^n}, h^{p^n}\right]^{p^{-2n}}$$

onde o lado direito da igualdade é um comutador de elementos do grupo G.

Por [4, Lema 4.28], $([g,h]_n)_m$ será uma sequência de Cauchy e então possui um limite. Definamos então

$$[g,h] := \lim_{n\to\infty} [g,h]_n.$$

Um trabalho que se resume a calcular equivalências em G_i mostra que $[\cdot,\cdot]$ torna $(G,+)$ uma álgebra de Lie sobre $\mathbb{Z}_p$

Existe uma maneira alternativa de construir uma álgebra de Lie associada à G através do mapa $\log : G \to \widehat{A}$ onde $\widehat{A}$ é uma álgebra associativa sobre $\mathbb{Q}_p$. Tal caminho alternativo faz uso de álgebras de grupo e da série de Campbell-Hausdorff.

Construímos um conjunto $H = \log G \subset \widehat{A}$ com colchete de Lie $[h,k]_L = hk - kh$ e um isomorfismo, dado pela função log, entre as álgebras de Lie $(G,+,[\cdot,\cdot]_L)$ e $(H,+,[\cdot,\cdot]_L)$ (com o cuidado de considerar as operações em cada conjunto), onde $\widehat{A}$ é precisamente o completamento de uma álgebra normada A sobre $\mathbb{Q}_p$.

Uma vez que o segundo caminho nos dá uma álgebra de Lie isomorfa à que pudemos construir anteriormente com mais facilidade, não será necessário abordá-lo. Essa construção pode ser lida em [4, Capítulo 7].

Denotando por $\Phi(X,Y)$ a série de Campbell-Hausdorff apresentada no capítulo anterior, existe um reformulação importante desta série que nos será útil nesta seção.

Sabemos que $\mathbb{Q}_p \langle\langle X,Y \rangle\rangle$ é uma álgebra associativa. Definindo

$$[U_1,U_2] = U_1U_2 - U_2U_1$$

fazemos com que $\mathbb{Q}_p \langle\langle X,Y \rangle\rangle$ tenha a estrutura de uma álgebra de Lie. Definimos indutivamente

$$[U_1,...,U_r] = [[U_1,...,U_{r-1}],U_r]$$

e para uma n-upla de inteiros positivos $e = (e_1,...,e_n)$, sejam

$$\langle e \rangle = \sum_1^n e_i$$

e

$$[X,Y]_e = [X, \underbrace{Y,...,Y}_{e_1 \text{ vezes}}, \underbrace{X,...,X}_{e_2 \text{ vezes}}, ...].$$

Além disso, defina q_e para ser um racional constante que satisfaz $p^{n-1}q_e \in p\mathbb{Z}_p$ se $p > 2$ ou $2^{2n-2}q_e \in 4\mathbb{Z}_p$ se $p = 2$. Denotaremos também $\epsilon = 1$ se $p > 2$ ou $\epsilon = 2$ se $p = 2$. Essas notações serão consideradas ao longo desta seção. Agora podemos enunciar a proposição (veja [4, Teorema 6.28]):

Proposição 3.3.1. *Seja*

$$\Phi(X, Y) = \sum_{n\in\mathbb{N}} s_n(X, Y)$$

a série de Campbell-Hausdorff onde $s_n(X, Y)$ é a soma dos termos de grau n. Então,

$$s_0(X, Y) = 0, \quad s_1(X, Y) = X + Y, \quad s_2(X, Y) = \frac{1}{2}(XY - YX);$$

e

$$s_n(X, Y) = \sum_{\langle e\rangle=n-1} q_e[X, Y]_e, \quad \forall n \geq 3.$$

Além disso,

$$\lim_{\langle e\rangle\to\infty} \left|p^{\epsilon\langle e\rangle}q_e\right| = 0.$$

Definição 3.3.1. Uma álgebra de Lie L é *powerful* se é um $\mathbb{Z}_p$-módulo livre finitamente gerado tal que $[L, L]_L \leq p^\epsilon L$.

Uma vez que um A-módulo M é finitamente gerado se, e só se, M é isomorfo à um quociente de A^d para algum inteiro positivo d, essa definição é equivalente a: Uma álgebra de Lie L sobre $\mathbb{Z}_p$ é *powerful* se $L \simeq \mathbb{Z}_p^d$ para algum inteiro positivo d e $[L, L]_L \leq p^\epsilon L$. Lembre que um reticulado de Lie L é um anel de Lie que é um A-módulo livre de posto finito onde A é um domínio de ideais principais e, por isso, é comum também nomear L por $\mathbb{Z}_p$*-reticulado de Lie uniforme*

Uma vez que cada termo $s_n(X, Y)$ de

$$\Phi(X, Y) = \sum_{n} s_n(X, Y)$$

é uma soma finita, logo pode ser calculado, então a série

$$\tilde{\Phi}(x, y) = \sum_{n=0}^{\infty} s_n(x, y),$$

para $x, y \in L$, converge em L, o que é rigorosamente provado mostrando que a sequência das somas parciais é de Cauchy. Isso nos permite definir uma operação binária $* : L\times L \to L$ dada por

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

Teorema 3.3.1. *Seja L uma álgebra de Lie powerful. A operação $*$ torna L um grupo pro-p uniforme. Se $\{g_1, ..., g_n\}$ é uma base para L sobre $\mathbb{Z}_p$, então $\{g_1, ..., g_n\}$ é um conjunto de geradores (topológicos) para o grupo $(L, *)$.*

Demonstração. Mostrar que $(L, *)$ é um grupo é simples, exceto pela demonstração da associatividade que usa muitos cálculos e propriedades de séries, o que torna bastante trabalhoso apesar de não ser difícil (mostrar que $(x * y) * z \equiv x * (y * z) \pmod{p^n L}$ para todo inteiro $\mathbb{N}$) e assim, será omitido por brevidade (veja [4, Lema 9.9]).

Se $[x, y]_L = 0$, então $u_n(x, y) = 0$ para todo $n \geq 2$, então $x * y = x + y$, pois $u_0(x, y) = 0$. Além disso, $x^{-1} = -x$, logo, tomando a notação multiplicativa para a operação " $*$ ", podemos escrever $x^m = mx$ para todo $m \in \mathbb{Z}$. Com isso,

$$p^t L = \{x^{p^t} : x \in L\}$$

é um subgrupo de $(L, *)$ para todo t. Sendo L uma álgebra de Lie powerful, então $p^t L$ também é, por isso

$$L^{p^t} = \overline{L^{p^t}} = p^t L$$

para todo t. Suponha agora que $x - y \in p^t L$. Então $x - y = p^t z$ para algum $z \in L$. Usando a Proposição 3.3.1, podemos concluir que

$$xy^{-1} = x - y + \sum_{n \geq 2} u_n(x, -y) \in p^t L$$

e

$$xy^{-1} = v \in p^t L,$$

o que implica

$$x - y = v * y - y \in p^t L.$$

Note que para cada t, $|L : L^{p^t}| = |L : p^t L| = p^{tn}$. Além disso, a família $\{x + p^t L\}_t$ é uma base para os abertos de L e as classes aditivas $x + p^t L$ são equivalentes às classes multiplicativas xL^{p^t}, daí podemos concluir que $(L, *)$ é um grupo topológico tal que os seus conjuntos abertos têm índice potência de p, ou seja, $(L, *)$ é um grupo pro-p. Note que

$$x * y - (x + y) \in pL$$

para cada $x, y \in L$ [4, Corolário 6.38]. Como as classes multiplicativas e aditivas são equivalentes, então L/L^p é abeliano. Além disso por [4, Corolário 6.38], temos que

$$x * y - (x + y) - \frac{1}{2}[x, y]_L \in 4L$$

para cada $x, y \in L$. Com isso, tomando a congruência módulo $4L$, podemos ver que

$$x * y - y * x = [x, y]_L \in 4L.$$

Assim, L/L^p é abeliano se $p > 2$ e L/L^4 é abeliano se $p = 2$, isto é, L é um grupo pro-p powerful. Além disso, como $|L : L^{p^t}| = p^{tn}$ para todo t, concluímos que $(L, *)$ é uniforme de dimensão n. Recorrendo novamente ao fato de

$$x * y - (x + y) \in pL,$$

obtemos um isomorfismo entre as estruturas aditiva e multiplicativa. O subgrupo de Frattini de $(L, *)$ é exatamente L^p o que implica ser $\{g_1, ..., g_n\}$ um gerador topológico para $(L, *)$. □

A ideia desta prova é feita com mais detalhes em [4, Teorema 9.8].

Esta seção mostra que existe uma correspondência entre álgebras de Lie powerful e grupos pro-p uniforme. De fato, com mais alguns argumentos (veja [4, Teorema 9.10]) podemos resumir está seção no seguinte teorema:

Teorema 3.3.2. *Existe um isomorfismo entre as categorias dos grupos pro-p uniforme e das álgebras de Lie powerful.*

A prova de tal fato usa a construção alternativa da álgebra de Lie de um grupo pro-p uniforme que foi mencionada anteriormente. A princípio, não precisaremos necessariamente de um isomorfismo entre essas categorias, será suficiente apenas saber que podemos obter uma álgebra de Lie powerful partindo de um grupo pro-p uniforme e também o contrário usando as operações dadas pela fórmula de Campbell-Hausdorff.

Exemplo 3.3.1. Sejam G o grupo não-abeliano de ordem 27 definido por

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_3 \right\}$$

e L o anel de Lie definido por

$$L = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} : a, b, c \in \mathbb{F}_3 \right\}.$$

Sabemos, pela fórmula de Campbell-Hausdorff, que os mapas exp e log geram uma correspondência entre G e L; definindo as aproximações $x \mapsto 1 + x + \dfrac{x^2}{2}$ e $1 + x \mapsto x - \dfrac{x^2}{2}$,

conseguimos uma bijeção entre G e L. Lembrando que as operações de grupo são dadas por $xy = \log(\exp(x)\exp(y))$, podemos verificar, expandindo exp e depois usando o fato de o comutador de dois elementos é central em um anel de Lie com classe de nilpotência 2, que além de $1 = \exp(0)$,

$$\exp(x)\exp(y) = \exp\left(x + y + \frac{1}{2}[x, y]\right)$$

e

$$\exp(x)\exp(x^{-1}) = \exp(x + x^{-1}),$$

logo,

$$xy = \log(\exp(x)\exp(y)) = x + y + \frac{1}{2}[x, y]$$

e

$$0 = \log(\exp(x)\exp(x^{-1})) = x + x^{-1},$$

de modo que,

$$x^{-1} = -x.$$

Assim, podemos construir a operação no grupo partindo das operações da álgebra de Lie. De modo semelhante podemos construir as operações do anel de Lie a partir das operações de grupo.

O exemplo acima é um caso particular do que é formulado como Correspondência de Lazard para p-grupos finitos e pode ser enunciado como:

Teorema 3.3.3. *A fórmula de Campbell-Hausdorff gera uma correspondência entre os p-grupos finitos com classe de nilpotência menor que p e os anéis de Lie com classe de nilpotência menor que p cujo grupo aditivo é um p-grupo finito.*

Capítulo 4

Largura de palavras em Subgrupos Verbais

Neste capítulo iremos começar a olhar diretamente para o assunto principal desta dissertação. Aqui veremos o que é a largura de uma palavra em um grupo e trataremos dos pontos fundamentais para que possamos desenvolver esta definição, bem como suas consequências, até o final do último capítulo. Enunciaremos e provaremos também alguns resultados que terão consequências diretas e claras no que faremos posteriormente.

4.1 Comutadores e Subgrupos Verbais

Nossa ideia aqui é introduzir de maneira direta os subgrupos verbais além de revisitar brevemente as definições dos comutadores.

Definição 4.1.1. Uma *palavra* é uma expressão da forma

$$w(x_1, ..., x_n) = \prod_{j=1}^{s} x_{i_j}^{\epsilon_j}$$

onde $i_1, ..., i_s \in \{1, ..., n\}$ e $\epsilon_j = \pm 1$. Dizemos que s é a *largura* de w, fazendo a convenção de $s = 0$ para a palavra vazia.

Além disso, sabemos que uma palavra pode ser vista com um elemento do grupo livre F_n sobre $\{x_1, ..., x_n\}$.

Seja $w = w(x_1, ..., x_n)$ uma palavra e considere G um grupo. Defina $w : G^{(n)} \to G$ por

$$w(g_1, ..., g_n) = \prod_{j=1}^{s} g_{i_j}^{\epsilon_j}$$

onde $G^{(n)} = \underbrace{G \times \cdots \times G}_{n \text{ times}}$. Isso é conhecido como *mapa verbal*

A forma de operar duas palavras é por justaposição, isto é,

$$\left(\prod_{j=1}^{s} x_{i_j}^{\epsilon_j}\right)\left(\prod_{k=1}^{t} y_{i_k}^{\sigma_k}\right) = \prod_{l=1}^{s+t} z_{i_l}^{\lambda_l}$$

onde $z_{i_l} = x_{i_j}$ se $l \leq s$ e $z_{i_l} = y_{i_k}$ se $l \geq s+1$. Duas palavras w e v serão equivalentes se

$$w(g_1, ..., g_n) = v(g_1, ..., g_n)$$

para todo $(g_1, ..., g_n) \in G^{(n)}$. Pela definição do mapa verbal, então w e v são equivalentes se pudermos transformar w em v com um número finito de inserções ou remoções de xx^{-1} ou $x^{-1}x$ onde x representa uma variável.

Seja $\pi_g : F_n \to G$ o único homomorfismo tal que π_g manda x_i em g_i para cada i, então

$$w(g_1, ..., g_n) = w \circ \pi_g,$$

ou seja, um elemento de F_n induz o mesmo mapa verbal independente do representante escolhido.

Se G é um grupo e w o mapa verbal, definamos

$$G_w = \{w(g_1, ..., g_n)^{\pm 1} : (g_1, ..., g_n) \in G^{(n)}\}.$$

O conjunto G_w é conhecido como *conjunto dos w-valores*.

Definição 4.1.2. Sejam G um grupo e $w : G^{(n)} \to G$ um mapa verbal. O *subgrupo verbal* correspondente à w é

$$w(G) = \langle G_w \rangle .$$

Se $S \subset G$, definamos

$$S^{*m} = \{s_1^{\pm 1} \cdots s_m^{\pm 1} : s_i \in S \quad \forall i \in \{1, ..., m\}\}$$

onde $m \in \mathbb{N}$.

Definição 4.1.3. Sejam G um grupo e w o mapa verbal. Dizemos que w tem *largura finita* se existe $m \in \mathbb{N}$ tal que

$$w(G) = G_w^{*m}.$$

O menor m satisfazendo tal condição será chamado de *largura* de w em G. Se não existe m com tal propriedade, diremos que w tem *largura infinita*.

Exemplo 4.1.1. Se G é um grupo abeliano, então

$$w(g_1, ..., g_n)^{-1} = w(g_1^{-1}, ..., g_n^{-1})$$

para qualquer palavra w. Assim, cada w deve ter largura 1 em G.

Definição 4.1.4. Sejam G um grupo e $S \subset G$. Dizemos que S tem *largura finita* em G se existe $m \in \mathbb{N}$ tal que

$$\langle S \rangle = S^{*m}.$$

O menor m satisfazendo tal condição será chamado de *largura* de S em G. Se não existe m com tal propriedade, diremos que S tem *largura infinita*.

Suponha que G seja um grupo e H um subgrupo finito normal de G tal que w tem largura finita em G/H. Temos que

$$w(G)/(H \cap w(G)) = w(G)H/H = G_w^{*m}H/H = G_w^{*m}/(H \cap G_w^{*m}),$$

logo,

$$w(G) = G_w^{*m}(H \cap w(G)).$$

Uma vez que $|H \cap w(G)| < \infty$, segue que $H \cap w(G) \subset G_w^r$ para algum $r \in \mathbb{N}$. Logo, $w(G) = G_w^{*(m+r)}$. Isso nos permite enunciar a seguinte proposição

Proposição 4.1.1. *Sejam G um grupo e $K \leq H$ subgrupos normais de G com H/K finito e $K \subset G_w^{*r}$ para algum r. Se w tem largura finita em G/H, então w tem largura finita em G.*

Relembre que, dados um grupo G e $g, h \in G$, o comutador de g, h é definido por

$$[g, h] = ghg^{-1}h^{-1},$$

e se H, K são grupos, então

$$[H, K] = \langle [h, k] : h \in H, k \in K \rangle .$$

Indutivamente, se $H_1, ..., H_n$ são subgrupos de G, então

$$[H_1, ..., H_n] = [[H_1, ..., H_{n-1}], H_n].$$

Denotaremos

$$\gamma_2(G) = [G, G] = G'$$

e

$$\gamma_n(G) = [\gamma_{n-1}(G), G].$$

Definição 4.1.5. A família $\{\gamma_i(G)\}_{i\in\mathbb{N}}$ é conhecida como *série central inferior*.

Proposição 4.1.2. *Seja G um grupo nilpotente tal que $G = G'\langle x_1, ..., x_m\rangle$. Então*

$$\gamma_{n+m}(G) = \prod_{(i_1,...,i_n\in\{1,...,m\}^{(n)})} [\gamma_m(G), x_{i_1}, ..., x_{i_n}].$$

Uma simples demonstração pode ser vista em [17, Proposição 1.2.7].

Por indução se mostra que $[\gamma_m(G), \gamma_n(G)] \leq \gamma_{m+n}(G)$.

Também por indução, é fácil mostrar que se $\varphi : G \to K$ é um homomorfismo sobrejetivo, então $\varphi(\gamma_n(G)) = \gamma_n(K)$. Assim, dado qualquer automorfismo ϕ de G, vemos que ϕ fixa $\gamma_n(G)$. Podemos então enunciar uma conhecida proposição:

Proposição 4.1.3. *O grupo $\gamma_n(G)$ é um subgrupo característico de G, para todo $n \in \mathbb{N}$.*

Uma vez que todo subgrupo característico é normal, temos que $\gamma_n(G)$ é um subgrupo normal de G, o que nos permite trabalhar com quocientes.

4.2 Subgrupos Verbais e Grupos Profinitos

Para finalizar, iremos ver como os subgrupos verbais se relacionam com os grupos profinitos, mais especificamente com os grupos pro-p, e apresentaremos alguns resultados que serão usados no futuro, além de olhar algumas propriedades básicas.

Sejam G um grupo e W um conjunto de palavras. Definamos

$$G_W = \bigcup_{w\in W} G_w.$$

O subgrupo $W(G) = \langle G_W\rangle$ é o *subgrupo verbal* de W em G. Convenientemente chamamos G_W de *vocabulário* de W em G. Dadas duas palavras $w, \nu \in W$ de comprimento n e m, respectivamente, definamos

$$(w \cdot \nu)(g_1, ..., g_n, h_1, ..., h_m) = w(g_1, ..., g_n)\nu(h_1, ..., h_n).$$

Se $W = \{w, \nu\}$, então

$$G_W \subset G_{w\cdot\nu} \subset w(G)\nu(G),$$

logo,

$$W(G) \leq w(G)v(G).$$

Uma vez que $w(G), v(G) \subset W(G)$, então

$$W(G) = (w \cdot v)(G) = w(G)v(G),$$

o que implica a largura de $w \cdot v$ ser menor ou igual à largura de w mais a largura de v. Indutivamente esse resultado pode ser estendido a $W = \{w_1, ..., w_k\}$. Com esse resultado podemos mostrar a seguinte proposição:

Proposição 4.2.1. *Se G é um grupo pro-p de posto finito d e W uma coleção de palavras tal que toda palavra de W tem largura finita em G, então $W(G)$ tem largura finita em G. Mais que isso, se a largura de cada palavra de W é limitada por L, então a largura de $W(G)$ é limitada por dL.*

Antes da demonstração, é importante observar o seguinte fato: "*se todo subgrupo fechado de um grupo pro-p G é topologicamente finitamente gerado, então toda cadeia de subgrupos fechados possui um elemento maximal após uma quantidade finita de etapas.*". Da fato, seja

$$H_1 \leq \cdots \leq H_n \leq \cdots$$

uma cadeia de subgrupos fechados. Tomando $H = \overline{\bigcup_i H_i}$, então H é fechado e finitamente gerado, de onde segue que $\Phi(H)$ é aberto em H o que implica $H/\Phi(H)$ finito. Se considerarmos a cadeia

$$H_1\Phi(H)/\Phi(H) \leq \cdots \leq H_n\Phi(H)/\Phi(H) \leq \cdots$$

veremos que ela deve possuir um elemento maximal e, consequentemente, deve existir algum H_k maximal para a primeira cadeia. Note que se o grupo pro-p G tiver posto finito, então automaticamente toda cadeia de subgrupos fechados possui um elemento maximal após uma quantidade finita de etapas.

Demonstração da Proposição 4.2.1. Seja $g_1 \in G_W$. Se $\overline{\langle g_1 \rangle} \neq \overline{W(G)}$, então existe $g_2 \in W(G) - \overline{\langle g_1 \rangle}$. Indutivamente, obtemos uma cadeia

$$\overline{\langle g_1 \rangle} \leq \overline{\langle g_1, g_2 \rangle} \leq \cdots \leq \overline{\langle g_1, g_2, ..., g_n \rangle} \leq \cdots$$

onde $g_i \in G_W$ para todo i. Sendo G um grupo pro-p de posto finito, então essa cadeia possui um elemento maximal, ou seja, existem $g_1, ..., g_m \in G_W$ tais que $\overline{\langle g_1, ..., g_m \rangle} = \overline{W(G)}$. Um conjunto gerador com m elementos em um grupo pro-p de posto d contém um subconjunto gerador com d elementos, logo, devemos ter $m = d$ e

$$\overline{\langle g_1, ..., g_d \rangle} = \overline{W(G)}.$$

Sejam $w_1, ..., w_d \in W$ tais que g_i um w_i-valor para cada i. Se $w = w_1 \cdot w_2 \cdots w_d$, então

$$\langle g_1, ..., g_d \rangle \leq w(G) \leq W(G). \qquad (*)$$

Seja ℓ_i a largura de g_i para cada i. Pelo argumento anterior, a largura de $w(G)$ é menor ou igual a $\ell_1 + \cdots + \ell_d$. Uma vez que a largura é finita, então $w(G)$ é fechado (mostraremos essa afirmação abaixo). Então segue de $(*)$ que $w(G) = W(G)$ e a largura de $W(G)$ é menor ou igual a $\ell_1 + \cdots + \ell_d$, mas se cada $\ell_i \leq L$ então a largura de $W(G)$ é menor ou igual a dL. □

Quando consideramos uma palavra w sobre um grupo profinito, podemos obter consequências interessantes. Por exemplo:

Proposição 4.2.2. *Sejam G um grupo profinito e w uma palavra. Então w tem largura finita se, e somente se, $w(G)$ é fechado em G.*

Demonstração. Seja $m \in \mathbb{N}$ a largura de w em G. Temos que G_w é a imagem de $G^{(n)}$ sobre o mapa verbal w que é claramente contínuo, logo G_w é fechado em G (pois G é, em particular, compacto). Por definição

$$w(G) = G_w^{*m},$$

o que implica $w(G)$ fechado em G. Suponha agora $w(G)$ fechado em G. Temos que

$$w(G) = \bigcup_{i=1}^{\infty} G_w^{*i}$$

com G_w^{*i} fechado em G. Pelo Teorema da Categoria de Baire, ao menos um dos conjuntos fechados desta união tem interior não vazio, isto é, existe $m \geq 1$ tal que G_w^{*m} contém um subconjunto aberto não vazio U de $w(G)$. Note que podemos escrever

$$w(G) = \bigcup_{g \in w(G)} gU$$

com cada gU aberto. Mas $w(G)$ é compacto, então

$$w(G) \subset \bigcup_{i=1}^{n} g_i U$$

com $g_i \in w(G)$. Escolhendo k tal que $g_1, ..., g_n \in G_w^{*k}$, temos

$$w(G) \subset G_w^{*(m+k)},$$

logo, w tem largura finita. □

A partir deste ponto iremos começar a construir alguns resultados chave para a conclusão de alguns dos teoremas principais.

Definição 4.2.1. Sejam F um grupo livre e w uma palavra de F. Dizemos que w é uma $\mathcal{N}_p$-palavra se para todo grupo pro-p finitamente gerado H, o grupo $H/\overline{w(H)}$ é virtualmente nilpotente.

Lembre que um grupo é dito ser virtualmente nilpotente se possui um subgrupo normal de índice finito que é nilpotente.

Existe uma maneira de caracterizar as $\mathcal{N}_p$-palavras por meio de um teorema. Uma demonstração desse teorema pode ser vista em [17, seções 4.3 - 4.4]. Não a apresentaremos com o objetivo de não tornar este trabalho excessivamente longo, visto que essa demonstração exige o conhecimento de alguns outros conceitos e teoremas que excedem o propósito desta dissertação.

Teorema 4.2.1. *Sejam F um grupo livre e w uma palavra de F. Então as seguintes afirmações são equivalentes:*

(i) *w é uma $\mathcal{N}_p$-palavra.*

(ii) *se H é um grupo pro-p livre sobre um conjunto de dois elementos, então $H/w(H)$ é virtualmente nilpotente.*

(iii) $w(C_p \wr \mathbb{Z}) \neq \{1\}$.

(iv) $w \notin (F')^p F''$.

Para encerrar esta seção, provaremos um resultado que, por mais que pareça desconexo com que fizemos neste capítulo, será essencial para o que iremos fazer no próximo.

Proposição 4.2.3. *Sejam G um grupo pro-p finitamente gerado e H um subgrupo pro-p livre gerado por $x_1, ..., x_d, z$ com $d = \mathrm{d}(G)$. Sejam $y_1, ..., y_s$ geradores de $\overline{\langle x_1, ..., x_d \rangle^{p^t}}$ e suponha que, para quaisquer $i_1, ..., i_n \in \{1, 2, ..., s\}$, existe $v_{i_1,...,i_n}$ sendo um produto de, no máximo, k w-valores em H satisfazendo*

$$v_{i_1,...,i_n}(x_1, ..., x_d, z) = [z, y_{i_1}, ..., y_{i_n}] r_{i_1,...,i_n}(x_1, ..., x_d, z),$$

$r_{i_1,...,i_n}(x_1, ..., x_d, z) \in \gamma_{n+2}(H^{p^t})$. *Então se $m \geq n + 1$,*

$$\gamma_{n+1}(G^{p^t}) = \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1, ..., h_d, H^{p^t}) \gamma_m(G^{p^t}),$$

onde $h_1, ..., h_d$ são geradores de G.

Demonstração. Sejam $h_1, ..., h_d$ geradores de G. Se $a \in \gamma_m(G^{p^t})$, $g \in G$ e $r \in \gamma(H^{p^t})$ então é claro que

$$r(h_1, ..., h_d, g) \equiv r(h_1, ..., h_d, ga) \pmod{\gamma_m(G^{p^t})},$$

já que $\gamma_m(G^{p^t})$ é um subgrupo normal. Usando a definição 4.1.5 para γ_{m-l+1}, segue por indução em l que

$$r(h_1, ..., h_d, g) \equiv r(h_1, ..., h_d, ga) \pmod{\gamma_{m+l-1}(G^{p^t})},$$

onde $r \in \gamma_l(H^{p^t})$.

Note que

$$\gamma_{n+1}(G^{p^t}) = \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1, ..., h_d, H^{p^t})\gamma_{n+1}(G^{p^t}).$$

Considere $m \geq n+1$ e suponha que a igualdade

$$\gamma_{n+1}(G^{p^t}) = \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1, ..., h_d, H^{p^t})\gamma_m(G^{p^t})$$

seja verdadeira, ou seja, para algum $h \in \gamma_{n+1}(G^{p^t})$ existem $\mathfrak{g} = g_{i_1,...,i_n} \in H^{p^t}$ e $u \in \gamma_m(G^{p^t})$ tais que

$$h = \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1, ..., h_d, \mathfrak{g})u.$$

Como

$$u \equiv \prod_{i_1,...,i_n} [t_{i_1,...,i_n}, \tilde{y}_{i_1}, ..., \tilde{y}_{i_n}] \pmod{\gamma_{m+1}(G^{p^t})}$$

com $\tilde{y}_{i_j} = y_j(h_1, ..., h_d)$ e $t_{i_1,...,i_n} \in \gamma_{m-n}(G^{p^t})$, temos

$$h \equiv \prod_{i_1,...,i_n} [\mathfrak{g}t_{i_1,...,i_n}, \tilde{y}_{i_1}, ..., \tilde{y}_{i_n}] r_{i_1,...,i_n}(h_1, ..., h_d, \mathfrak{g}t_{i_1,...,i_n}) \pmod{\gamma_{m+1}(G^{p^t})}.$$

Aplicando o parágrafo anterior à $r_{i_1,...,i_n}(h_1, ..., h_d, \mathfrak{g}t_{i_1,...,i_n})$, temos

$$h \equiv \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1, ..., h_d, \mathfrak{g}t_{i_1,...,i_n}) \pmod{\gamma_{m+1}(G^{p^t})},$$

e, portanto,

$$\gamma_{n+1}(G^{p^t}) = \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1, ..., h_d, H^{p^t})\gamma_m(G^{p^t})$$

para todo $m \geq n+1$. □

O conjunto

$$\prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1,...,h_d)$$

é fechado. Tomando então a interseção de $\gamma_{n+1}(G^{p^t})$ para todo $m \geq n+1$, temos que

$$\gamma_{n+1}(G^{p^t}) = \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1,...,h_d, H^{p^t}),$$

pois

$$\bigcap_m \gamma_m(G^{p^t}) = \{1\}.$$

Assim, podemos enunciar o seguinte corolário:

Corolário 4.2.1. *Sejam G um grupo pro-p finitamente gerado e H um subgrupo pro-p livre gerado por $x_1,...,x_d,z$ com $d = \mathrm{d}(G)$. Sejam $y_1,...,y_s$ geradores de $\overline{\langle x_1,...,x_d\rangle}^{p^t}$ e suponha que, para quaisquer $i_1,...,i_n \in \{1,2,...,s\}$, existe $v_{i_1,...,i_n}$ sendo um produto de, no máximo, k w-valores em H satisfazendo*

$$v_{i_1,...,i_n}(x_1,...,x_d,z) = [z, y_{i_1},...,y_{i_n}]r_{i_1,...,i_n}(x_1,...,x_d,z),$$

$r_{i_1,...,i_n}(x_1,...,x_d,z) \in \gamma_{n+2}(H^{p^t})$. *Então*

$$\gamma_{n+1}(G^{p^t}) = \prod_{i_1,...,i_n} v_{i_1,...,i_n}(h_1,...,h_d, H^{p^t}).$$

onde $h_1,...,h_d$ são geradores de G.

O leitor que tiver interesse numa leitura aprofundada sobre palavras de comprimento infinito em grupos pro-p pode consultar [17, Seção 4.5]

Capítulo 5

A demonstração do teorema principal

Neste capítulo iremos demonstrar alguns resultados que nos permitirão obter como consequência o teorema principal. Não provaremos todos os resultados, apenas aqueles que fazem uso das ferramentas que construímos. Um ponto a se destacar também é o teorema que garante que palavras em grupos p-ádicos analíticos compactos tem largura finita, apesar disso ele não apresenta uma possível cota superior para as larguras. Na última seção apresentaremos uma extensão do resultado para grupos pro-p aos grupos pronilpotentes.

5.1 Largura de palavras em grupos p-ádicos analíticos compactos

Consideraremos $X = (X_1, ..., X_m)$ uma m-upla de variáveis comutativas. Também definiremos

$$\mathbb{Q}_p\{X\} = \left\{ \sum_i a_i X^i \in \mathbb{Q}_p[[X]] : |a_i|_p \to 0 \text{ se } |i| \to \infty \right\}$$

onde $|\cdot|_p$ é a norma p-ádica em $\mathbb{Q}_p$ e $\langle i \rangle = i_1 + \cdots + i_m$ para $i = (i_1, ..., i_m)$ com $i_j \in \mathbb{N}$ e $X^i = X^{i_1} \cdots X^{i_m}$. O conjunto $\mathbb{Q}_p\{X\}$ é chamado de *anel das séries de potências restritas* em X. O anel $\mathbb{Z}_p\{X\}$ é um subanel de $\mathbb{Q}_p\{X\}$ consistindo dos elementos de $\mathbb{Q}_p\{X\}$ com coeficientes em $\mathbb{Z}_p$. Além disso, $L = (\mathbb{Z}_p^{(m)}, +)$ será considerada uma variedade p-ádica.

O objetivo desta seção é mostrar que uma palavra w de um grupo livre F sempre terá largura finita em um grupo p-ádico analítico compacto. Para provar isso precisaremos de alguns lemas auxiliares.

O entendimento da demonstração dos próximos lemas é importante pois conectam as ideias que estudamos até aqui.

Lema 5.1.1. *Sejam* $Y = (Y_1, ..., Y_n)$ *e* $f = (f_1, ..., f_m)$ *uma m-upla consistindo de m séries de potências formais de* $\mathbb{Z}_p\{Y\}$ *tais que* $f(e) = e$ *onde* $e = (0, ..., 0)$. *Ponha*

$$S = f(\mathbb{Z}_p^{(n)}) = \{(f_1(x), ..., f_m(x)) : x \in \mathbb{Z}_p^{(n)}\} \subset \mathbb{Z}_p^{(m)}.$$

Então a largura de S *em* $(\mathbb{Z}_p^{(m)})$ *é finita.*

Demonstração. Sejam $K = \mathbb{Z}_p^{(n)}$, $L = (\mathbb{Z}_p^{(m)}, +)$ e $A = \langle S \rangle$. Se

$$L_1 = \{l \in L : p^k l \in A \text{ para algum } k\}$$

então podemos reorganizar os geradores de L para encontrar um subgrupo L_2 de L tal que $L = L_1 \oplus L_2$. Além disso, podemos mudar as coordenadas de L para que L_1 seja dado pelas equações $\{x_{s+1} = \cdots = x_m = 0\}$. Nessas coordenadas, um elemento de L se escreve como

$$(x_1, ..., x_s, 0, ..., 0).$$

Com isso, a imagem do mapa f tem a forma

$$(h_1, ..., h_s, 0, ..., 0).$$

Assim, podemos supor sem perda de generalidade, que S gera um subgrupo aberto em L.

Dado $a \in K$ definamos $g_a(Y) = f(Y) - f(a)$. Uma vez que as séries de potências $(f_1(x), ..., f_m(x))$ são convergentes para $x \in \mathbb{Z}_p$, claramente g_a é um mapa analítico de K em L satisfazendo $g(e) = e$. Note que g_a induz um mapa analítico $T_a g_a : T_a K \to T_e L$. Os mapas $e_i : T_a^* K \to \mathbb{Q}_p$ definidos por $e_i(q) = (\partial_i q)(a)$ formam uma base para $T_a K$. Similarmente, os mapas $h_i : T_e^* L \to \mathbb{Q}_p$ definidos por $h_i(q) = (\partial_i q)(e)$ formam uma base para $T_e L$. Note que, na coordenada x_j,

$$(T_a g_a)(e_i)(x_j) = e_i(f_j - f_j(a)) = \partial_i f_j(a).$$

Assim,

$$(T_a g_a)(e_i) = \sum_{j=1}^{m} \partial_i f_j(a) h_j.$$

Considere o subespaço V de T_eL gerado por todas as imagens de T_ag_a para todo a, isto é, $V = \mathrm{Span}\{T_ag_a(T_aK) : a \in K\}$. Uma vez que $\dim V < m$ existem constantes α_1,...,α_m com algum $\alpha_i \neq 0$ tais que

$$0 = \sum_{j=1}^{m}(T_ag_a)(e_i)(x_j)\alpha_j = \sum_{j=1}^{m}\alpha_j\partial_i f_j(a) = \partial_i\left(\sum_{j=1}^{m}\alpha_j f_j\right)(a)$$

para todo $a \in K$ e $1 \leq i \leq n$. Com isso, tomando $g = \sum_{j=1}^{m} a_j f_j$ segue de $\partial_i g = 0$ que g é constante, mas $f(e) = e$ implica $g(e) = e$, ou seja, g é a função nula. Note que isso contradiz o fato de que S gera um subgrupo aberto em L, logo, $V = T_eL$. Assim, existem a_1,...,$a_m \in K$ tais que

$$T_{a_1}g_{a_1}(T_{a_1}K) + \cdots + T_{a_m}g_{a_m}(T_{a_m}K) = T_eL.$$

Defina $h : K^{(m)} \to L$ por $h(b_1, ..., b_m) = g_{a_1}(b_1) + \cdots g_{a_m}(b_m)$ e tome $b = (a_1, ..., a_m)$. Pela linearidade do mapa tangente, temos

$$T_bh(T_bK^{(m)}) = T_eL.$$

Então pelo Teorema 2.1.2, h é uma submersão em b e existe $U \subset h(K^{(m)})$ aberto em L. A interseção de um aberto em L com A é um aberto em A, ou seja, S^{*m} contém um aberto em A. Agora, uma vez que A é um grupo profinito, existe um subgrupo aberto B de A e um $a \in A$ tal que $a + B \subset S^{*m}$. Note que $A = S^{*l}$ para algum l, logo, $A = S^{*(m+l)}$. Portanto, S tem largura finita. □

De acordo com a Seção 3.3, para um grupo pro-p uniforme H, existe uma correspondente álgebra de Lie powerful H e para uma álgebra de Lie powerful H, a fórmula de Campbell-Hausdorff nos permite construir um grupo pro-p uniforme H. Sendo H uma álgebra de Lie powerful sobre $\mathbb{Z}_p$ iremos fixar um sistema de geradores livre sobre $\mathbb{Z}_p$ de H, o que significa que se $x \in \mathsf{H}$, então x corresponde a $(x_1, ..., x_n) \in \mathbb{Z}_p^{(m)}$. A m-upla $(x_1, ..., x_m)$ será chamado de *coordenadas* de x e também iremos considerar H como $\mathbb{Z}_p^{(m)}$. Fazendo essas identificações, o produto de dois elementos de H é dado por uma m-upla $(F_1, ..., F_m) \in \mathbb{Z}_p\{X\}^{(m)}$ (veja [2, Seção 8,Capítulo 2]). Nos próximos lemas, H será um grupo pro-p uniforme e H sua correspondente álgebra de Lie powerful.

Agora, note que uma vez que $\langle S\rangle$ é abeliano, a largura de S em $(\mathsf{H}, +)$ é o mesmo de S em H (H e H estão identificados de acordo com o parágrafo anterior). Assim, como consequência imediata do lema anterior temos o seguinte corolário:

Corolário 5.1.1. *Sejam $Y = (Y_1, ..., Y_n)$ e $f = (f_1, ..., f_m)$ m-uplas consistindo de m séries de potências formais de $\mathbb{Z}_p\{Y\}$ tal que $f(e) = e$. Ponha*

$$S = f(\mathbb{Z}_p^{(n)}) = \{(f_1(x), ..., f_m(x)) : x \in \mathbb{Z}_p^{(n)}\} \subset H.$$

Se o grupo gerado por S é abeliano, então a largura de S em H é finito.

Podemos ainda estender o Corolário 5.1.1 ao caso em que S é normal em H. A demonstração segue uma linha diferente do Lema 5.1.1; nela definimos um ideal R de H, faremos uma mudança de coordenadas em R para que um elemento de H/R seja unicamente determinado com respeito a $\mathbb{Z}_p$. Isso nos permitirá concluir que $\overline{\langle S \rangle}$ tem largura finita. Vejamos em detalhes:

Lema 5.1.2. *Sejam $Y = (Y_1, ..., Y_n)$ e $f = (f_1, ..., f_m)$ m-uplas consistindo de m séries de potências formais de $\mathbb{Z}_p\{Y\}$. Ponha*

$$S = f(\mathbb{Z}_p^{(n)}) = \{(f_1(x), ..., f_m(x)) : x \in \mathbb{Z}_p^{(n)}\} \subset H.$$

Suponha que $f(e) = e$ e que S é normal em H. Então o comprimento de S em H é finito.

Demonstração. Se $T = \langle S \rangle$, então T é normal em H, pois S é. Defina o conjunto

$$R = \{x \in H : x^{p^k} \in [T, T] \text{ para algum } k\}.$$

Uma vez que cada elemento de $[T, T]$ é um produto de elementos de S, que é normal em H, é fácil ver que R é normal em H. Segue também que R é um ideal de H. Além disso, como H é pro-p e livre de torção, o grupo $\overline{H} = H/R$ é pro-p e livre de torção. Note que

$$[\overline{H}, \overline{H}] \leq [H, H]R/R \leq H^p R/R = \overline{H}^p,$$

ou seja, $\overline{H}$ é powerful e, portanto, $\overline{H}$ é um grupo pro-p uniforme. De modo similar ao que foi feito no lema anterior, podemos escolher as coordenadas $\{x_1, ..., x_m\}$ de H de forma que R seja definido pelas equações $\{x_0, ..., x_s = 0\}$. Nessas coordenadas a imagem de f é $(g_1, ..., g_m)$. Uma vez que $\{x_1, ..., x_s\}$ definem R e um elemento de $\overline{\mathsf{H}}$ é uma classe de H/R, as primeiras s coordenadas de $(x_1, ..., x_m)$ em H definem unicamente um elemento $\overline{x}$ de $\overline{\mathsf{H}}$. Assim, a composição de f com o epimorfismo natural $\mathsf{H} \to \mathsf{H}/R$ é da forma $(g_1, ..., g_s)$.

Temos que

$$S/R \cap R/R = R/R$$

e S/R e R/R são ambos subgrupos normais de $\overline{H}$, logo, $\overline{S} = SR/R$ gera um subgrupo abeliano em $\overline{H}$ e assim, pelo corolário anterior, existe l_1 tal que $T = S^{*l_1}R$. O grupo

$R/[T,T]$ é finito então existe k tal que $R = S^{*k}[T,T]$ o que implica $T = S^{*l_2}[T,T]$ para algum l_2. Já que H é uniforme, T é finitamente gerado. Sejam $t_1, ..., t_l \in S$ geradores de T como um grupo pro-p. Então por [4, prova da Proposição 1.19],

$$[T,T] = [t_1,T]\cdots[t_l,T].$$

Como S é normal $t_i t t_i^{-1} t^{-1} = \tilde{t}t^{-1}$ para qualquer $t \in T$ e $i = 1, ..., l$, logo, $[T,T] \subset S^{*2l}$. Portanto, $T = S^{*(2l+l_2)}$. □

Agora estamos em condições de provar o teorema mencionado no início da seção.

Teorema 5.1.1 (Zapirain)**.** *Seja G um grupo analítico p-ádico compacto. Então qualquer palavra w de um grupo livre F tem largura finita em G.*

Demonstração. O grupo G é p-ádico analítico e então, por consequência do Teorema 2.2.4, G tem um subgrupo aberto pro-p normal uniforme H. Seja $\{a_i : 1 \leq i \leq |G:H|\}$ um transverso de G por H. Para cada $i = (i_1, ..., i_k)$ defina a função $g_i : H^{(2k)} \to H$ por

$$g_i(h_{1,i}, ..., h_{2k,i}) = w(a_{i_1}h_{1,i}, ..., a_{i_k}h_{k,i})w(a_{i_1}h_{k+1,i}, ..., a_{i_k}h_{2k,i})^{-1}.$$

Escolha qualquer ordem de k-uplas e defina $f = \prod_i g_i$. Note que como i varia entre 1 e $|G:H|$ e cada i é uma k-upla, a função f está definida em $H^{2k|G:H|^k}$. Se nós considerarmos H como $\mathbb{Z}_p^{(m)}$, então f é uma m-upla de funções de $\mathbb{Z}_p\{Y\}$ com $Y = (Y_1, ..., Y_n)$ onde $n = 2mk|G:H|^k$. Seja $S = f(\mathbb{Z}_p^{(n)})$ e $T = \langle S \rangle$. Se $h, h_1, ..., h_k \in H$ e $1 \leq i_1, ..., i_k \leq |G:H|$, então um cálculo direto mostra que

$$w(a_{i_1}h_1, ..., a_{i_k}h_k)^h = w(a_{i_1}[a_{i_1},h]h_1^h, ..., a_{i_k}[a_{i_k},h]h_k^h).$$

Assim, para $h \in H$ tem-se $S^h \subset S$, isto é, S é normal em H o que implica T normal em G. Pelo lema anterior, existe l tal que $T = S^{*l}$. Pela definição de S^{*l} é fácil ver que $S^{*l} \subset (G_w)^{*2lmk|G:H|^k}$, logo, $T \subset (G_w)^{*m_1}$ para algum m_1.

Considere o grupo $\overline{G} = G/T$. Uma vez que o transverso de G por H tem finitos elementos, a palavra w tem uma quantidade finita de valores distintos em $\overline{G}$. Uma vez que $\overline{G}$ é grupo p-ádico analítico, então $\overline{G}$ é linear. Pela solução de Merzljakov para o problema de Hall para grupos lineares (veja [11]), a palavra w é concisa na classe dos grupos lineares, isto é, se w assume uma quantidade finita de valores distintos em $\overline{G}$ então $w(\overline{G})$ é finito, logo, $w(\overline{G}) = w(G)/T$ é finito, isto é,

$$w(G) = (G_w)^{*m_2}T = (G_w)^{*(m_1+m_2)}$$

para algum m_2. □

Está claro que esta demonstração depende fundamentalmente de diferentes áreas da matemática; ela se baseia dentre outras coisas, no teorema da função inversa. Na história da matemática é comum encontrar exemplos de diferentes demonstrações para um mesmo teorema na tentativa de seguir apenas uma área, como é o caso do teorema de Burnside para solubilidade de grupos. O aluno de doutorado de Dan Segal, Nicholas Simons, provou o teorema acima de maneira alternativa, com uma prova baseada exclusivamente em ideias de teoria de grupos (veja [19]).

Um resultado recente (veja [1]) mostra que para $n \geq 3$, existe uma constante c_n tal que a largura de w em $\mathrm{SL}_n(\mathbb{Z})$ é, no máximo, c_n para cada palavra w. Apesar do Teorema 5.1.1 garantir que a largura de uma palavra é finita em qualquer grupo p-ádico analítico compacto, isso não nos dá informações sobre o valor da largura ou, ao menos, uma possível cota superior para as palavras w. É fácil ver que se G é não trivial e abeliano, então existe uma cota superior: o número 1. No caso geral, ainda não se tem uma solução para este problema.

5.2 Largura de palavras em grupos pro-p finitamente gerados

Nesta seção iremos ver algumas ferramentas que serão úteis na obtenção da recíproca do teorema principal deste trabalho.

Relembre que, de acordo com a Definição 4.2.1, w é uma $\mathcal{N}_p$-palavra se para todo grupo pro-p finitamente gerado H, o grupo $H/\overline{w(H)}$ é virtualmente nilpotente.

Além disso, no capítulo 4, provamos um teorema que caracteriza as $\mathcal{N}_p$-palavras que, junto ao teorema que provaremos a seguir, irá fornecer a caracterização dos subgrupos verbais fechados.

Teorema 5.2.1. *Sejam w uma $\mathcal{N}_p$-palavra e G um grupo pro-p finitamente gerado. Então $w(G)$ é fechado em G.*

Demonstração. Denote $\mathrm{d}(G)$ por d. Seja H um grupo pro-p livre de posto finito e sejam $x_1, ..., x_d, z$ os geradores de H. Uma vez que w é uma $\mathcal{N}_p$-palavra, existe $N \triangleleft H$ com $\overline{w(H)} \subset N$, $N/\overline{w(H)} \triangleleft H/\overline{w(H)}$ tem índice finito, logo, $(H/\overline{w(H)})/(N/\overline{w(H)}) = \Gamma$ é um p-grupo finito. Podemos então encontrar t tal que $\Gamma^{p^t} = \{1\}$ o que implica $K = H^{p^t}\overline{w(H)}/\overline{w(H)} \leq N/\overline{w(H)}$. Além disso, como K é nilpotente, existe n tal que $\gamma_n(K) = \{1\}$ e com isso, $\gamma_n(H^{p^t}) \leq \overline{w(H)}$.

Sejam agora $y_1, ..., y_n$ geradores de $\overline{\langle x_1, ..., x_d \rangle^{p^t}}$ (observe que cada y_i é uma palavra pro-p em x_i). Note que $\gamma_{n+2}(H^{p^t}) \leq \gamma_{n+1}(H^{p^t}) \leq \gamma_n(H^{p^t}) \leq \overline{\omega(H)}$. Além disso, H/H^{p^t} e $H^{p^t}/\gamma_n(H^{p^t})$ os grupos pro-p p-ádicos analíticos e, consequentemente, $H/\gamma_n(H^{p^t})$ é um grupo pro-p p-ádico analítico. Pelo Teorema 5.1.1, existe k tal que, para quaisquer $i_1, ..., i_n \in \{1, ..., s\}$, temos

$$[z, y_{i_1}, ..., y_{i_n}] \equiv v_{i_1,...,i_n} \pmod{\gamma_{n+2}(H^{p^t})}$$

onde $v_{i_1,...,i_n}$ é um produto de no máximo k w-valores em H. Portanto,

$$v_{i_1,...,i_n}(x_1, ..., x_d, z) = [z, y_{i_1}, ..., y_{i_n}] r_{i_1,...,i_n}(x_1, ...x_d, z)$$

onde $r_{i_1,...,i_n}(x_1, ...x_d, z) \in \gamma_{n+2}(H^{p^t})$.

Se $h_1, ..., h_d$ são os geradores de G, usando o Corolário 4.2.1, podemos ver que que $\gamma_{n+1}(G^{p^t})$ é um subgrupo fechado de $w(G)$. Aplicando então o Teorema 5.1.1 ao grupo $G/\gamma_{n+1}(G^{p^t})$ pelas mesmas razões apresentadas no segundo parágrafo e então

$$w(G)/\gamma_{n+1}(G^{p^t}) = w(G/\gamma_{n+1}(G^{p^t}))$$

é fechado. Novamente, tomando a interseção sobre n, concluímos que $w(G)$ é fechado. □

Iremos precisar de mais um lema, que requer algumas definições.

Definição 5.2.1. Seja G um grupo (não necessariamente pro-p). Definamos

$$D_1(G) = G$$

e

$$D_{i+1}(G) = D^p_{\lceil n/p \rceil} \prod_{i+j=n} [D_i, D_j].$$

O subgrupo $D_i(G)$ é chamado de *i-ésimo subgrupo de dimensão* de G.

É fácil ver que $\gamma_i(G) \leq D_i(G)$. Existe um resultado muito mais forte que esse:

$$D_n(G) = \prod_{ip^j \geq n} \gamma_i(G)^{p^j}.$$

Esse resultado foi provado por Lazard e pode ser visto em ([4, Teorema 11.2]).

Agora, considere G um grupo pro-p, $D_i(G)$ o i-ésimo subgrupo de dimensão de G, K um grupo pro-p livre de posto d e $N \neq \{1\}$ um subgrupo normal fechado de K. Definamos $N_i = N \cap D_i(G)$ e, a partir disso,

- $a_i = \log_p |D_i(K) : D_{i+1}(K)|$,
- $b_i = \log_p |K : D_{i+1}(K)|$,
- $c_i = \log_p |N_i : N_{i+1}|$,
- $d_i = \log_p |N : N_{i+1}| = \log_p |ND_{i+1}(K) : D_{i+1}(K)|$.

Observe que a_i e c_i são "muito parecidos". Cada N_i considera apenas uma parte do subgrupo $D_i(G)$. Conforme se aumenta o índice i, é razoável imaginar que a diferença entre a_i e c_i fica cada vez menor. O mesmo ocorre com b_i e d_i.

Lema 5.2.1. *De acordo com o que definimos anteriormente, tem-se*

(i) $a_n = \dfrac{d^n}{n}(1 + o(1))$,

(ii) $b_n = \dfrac{d^{n+1}}{(d-1)n}(1 + o(1))$,

(iii) $c_n = \dfrac{d^n}{n}(1 + o(1))$,

(iv) $d_n = \dfrac{d^{n+1}}{(d-1)n}(1 + o(1))$,

sempre que $n \to \infty$.

A demonstração utiliza essencialmente algumas ferramentas de álgebras de Lie que não foram apresentadas aqui. Apesar disso, para o nosso interesse é suficiente usar este resultado já provado, uma vez que não faz uso de nenhuma técnica específica usando o que desenvolvemos (veja [9, Lema 4.3]).

Proposição 5.2.1. *Sejam K um grupo pro-p livre e N um subgrupo normal fechado não trivial de K. Se K tem posto d, então existe $g \in N$ tal que g não pode ser escrito como produto de menos do que $\dfrac{d}{3}$ valores da palavra $x^p[y, z]$ em K. Se K tem posto infinito, então para qualquer $l \in \mathbb{N}$ existe $g \in N$ tal que g não pode ser escrito como produto de menos do que l valores da palavra $x^p[y, z]$ em K.*

Demonstração. Inicialmente note que, pelo Lema 5.2.1,

$$|K : D_n(K)| = p^{b_{n-1}} = p^{\frac{d^n}{(d-1)(n-1)}(1+o(1))}$$

e

$$|ND_{n+1}(K) : D_{n+1}(K)| = p^{\frac{d^{n+1}}{(d-1)n}(1+o(1))}.$$

Para cada subconjunto fechado V de K a *dimensão de Hausdorff* de V em K é definida para ser

$$\dim_K V = \lim_{n\to\infty} \inf \frac{\log_p |VD_n(K) : D_n(K)|}{\log_p |K : D_n(K)|}.$$

Temos então que

$$\dim_K N = \lim_{n\to\infty} \inf \frac{\log_p |ND_n(K) : D_n(K)|}{\log_p |K : D_n(K)|} = 1.$$

Como $[D_n(K), K] \leq D_{n+1}(K)$ e $D_n(K)^p \leq D_{pn}(K) \leq\leq D_{n+1}(K)$, segue que a palavra $w = x^p[y, z]$ tem, no máximo, $|K : D_n(K)|^3 = p^{3b_{n-1}}$ valores em $K/D_{n+1}(K)$. Assim, temos

$$\begin{aligned}\dim_K K_w &= \lim_{n\to\infty} \inf \frac{\log_p |K_w D_{n+1}(K) : D_{n+1}(K)|}{\log_p |K : D_{n+1}(K)|} \\ &\leq \lim_{n\to\infty} \inf \frac{\log_p |K : D_n(K)|}{\log_p |K : D_{n+1}(K)|} \\ &= \frac{3}{d}.\end{aligned}$$

Além disso, dado $S \subset K$ e $t \geq 1$, como

$$|S^{*t} D_n(K) : D_n(K)| \leq |SD_n(K) : D_n(K)|^t$$

para cada n, podemos ver que

$$\dim_K S^{*t} \leq t \dim_K S.$$

Se cada elemento de N pode ser escrito como produto de menos que $\frac{d}{3}$ valores da palavra $x^p[y, z]$ em K, então

$$N \subset (K_w)^{*t}$$

onde t é algum natural menor que $\frac{d}{3}$. Logo, temos

$$\dim_K N \leq \dim_K (K_w)^{*t} \leq t \dim_K K_w < \frac{d}{3} \cdot \frac{3}{d} = 1,$$

uma contradição.

Agora, para qualquer $d > 1$ um grupo pro-p livre de posto infinito é residualmente livre pro-p de posto d. Para ver isso, basta tomar um grupo livre F_d gerado por um conjunto de d elementos e, nesse grupo livre, escolher algum subgrupo que não seja finitamente gerado. Uma vez que esse subgrupo tem posto infinito, então é isomorfo ao nosso subgrupo inicial. Com isso, existe um homomorfismo sobrejetor $\varphi : K \to H$ onde H é um grupo pro-p livre de posto d tal que $\varphi(N) \neq \{1\}$. Então a primeira parte da proposição implica a segunda. □

Teorema 5.2.2. *Sejam F um grupo livre não abeliano, p um número primo e G um grupo pro-p livre finitamente gerado não abeliano. Se existe uma palavra não trivial $w \in (F')^p F''$, então $w(G)$ não é fechado.*

Demonstração. Suponha que $w(G)$ seja fechado. Então existe k tal que qualquer elemento de $w(G)$ é um produto de, no máximo, k w-valores. Por hipótese, $w \in (F')^p F''$ o que significa que existe l tal que qualquer elemento de $w(G)$ é um produto de, no máximo, l valores da palavra $x^p[y,z]$ em G'. Mas G' não pode ser gerado por uma quantidade finita de elementos, ou seja, é um grupo pro-p livre de posto infinito e $w(G)$ é seu subgrupo normal não trivial. Assim, estamos em contradição com a Proposição 5.2.1, logo, $w(G)$ deve ser fechado. □

Se o grupo livre F for abeliano, então não há nada a fazer, uma vez que

$$F' = [F, F] = \{1\}.$$

Então, podemos concluir que $w(G)$ fechado para todo grupo pro-p finitamente gerado G (com $w \neq 1$) implica $w \notin (F')^p F''$.

Como curiosidade, uma tese não publicada de Peter Stroud mostra que se w é uma palavra em um grupo abeliano, então $w(G)$ tem largura finita (veja [15]). Mais que isso, a Proposição 2.1.2 de [17] nos garante que se w é uma palavra e G um grupo virtualmente abeliano (grupos abelianos são virtualmente abelianos), então $w(G)$ tem largura finita consequentemente, pela proposição 4.2.2, $w(G)$ é fechado.

Pelos Teoremas 4.2.1 e 5.2.1, vemos que $w \notin (F')^p F''$ implica $w(G)$ fechado para todo grupo pro-p finitamente gerado G. Assim, podemos finalmente enunciar o resultado principal:

Teorema 5.2.3 (Zapirain)**.** *Seja $w \neq 1$ uma palavra de um grupo livre F. Então as seguintes afirmações são equivalentes:*

(i) $w(G)$ é fechado para todo grupo pro-p finitamente gerado G,

(ii) $w \notin (F')^p F''$.

5.3 Uma generalização para os grupos pronilpotentes

O objetivo desta seção é estender o teorema principal aos grupos pronilpotentes (definiremos abaixo o que são). As ideias usadas na demonstração desta generalização são similares as que usamos no caso já provado, a diferença se dá pela necessidade de estender

o conceito de $\mathcal{N}_p$-palavra, visto que não pode ser aplicado a grupos pronilpotentes em geral.

Definição 5.3.1. Um grupo pronilpotente é um grupo isomorfo ao limite inverso de um sistema inverso de grupos nilpotentes finitos.

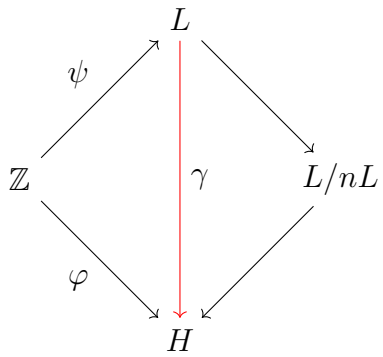
Exemplo 5.3.1. Os mapas $\varphi_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ definidos por $\varphi_{nm}(x \pmod m) = x \pmod n$ são morfismos sobrejetivos que tornam $(\mathbb{Z}/n\mathbb{Z}, \varphi_{nm})$ um sistema inverso de grupos finitos. Além disso, é fácil ver que existe o limite

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

Afirmamos que

$$\widehat{\mathbb{Z}} = \prod_{p\in\pi} \mathbb{Z}_p = L$$

onde π é o conjunto dos números primos. Existem diversas maneiras de provar essa afirmação. Definindo o mapa $\psi : \mathbb{Z} \to L$ por $\psi(x) = (x, ..., x, ...)$, Wilson mostra a igualdade garantindo a existência de um único morfismo contínuo $\gamma : L \to H$ onde H é um grupo finito, tal que $\varphi = \gamma \circ \psi$



ideia que está representada no diagrama comutativo acima. De maneira mais sofisticada, podemos usar teoria das categorias para mostrar que

$$\mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$$

e

$$\mathrm{Hom}\left(\prod_{p\in\pi} \mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p\right) = \bigoplus_{p\in\pi} \mathbb{Q}_p/\mathbb{Z}_p$$

implicam um isomorfismo entre $\widehat{\mathbb{Z}}$ e $\prod_{p\in\pi} \mathbb{Z}_p$ através de um isomorfismo canônico entre $\mathbb{Q}/\mathbb{Z}$ e $\bigoplus_{p\in\pi} \mathbb{Q}_p/\mathbb{Z}_p$.

Contudo, nosso interesse neste exemplo não é descobrir qual o limite inverso, mas notar que uma vez que cada $\mathbb{Z}/n\mathbb{Z}$ é nilpotente e não é um p-grupo para cada n não primo, temos um grupo pronilpotente que não é pro-p;

Definição 5.3.2. Sejam F um grupo livre e w uma palavra de F. Dizemos que w é uma $\mathcal{N}$-palavra se para todo grupo pronilpotente finitamente gerado H, o grupo $H/\overline{w(H)}$ é virtualmente nilpotente.

Lema 5.3.1. *Seja w uma palavra do grupo livre F. Então w é uma $\mathcal{N}$-palavra se, e somente se, w é uma $\mathcal{N}_p$-palavra para todo primo p.*

Demonstração. Se w é uma $\mathcal{N}$-palavra, então claramente w é uma $\mathcal{N}_p$-palavra para todo primo p. Reciprocamente, suponha que w seja uma $\mathcal{N}_p$-palavra para todo primo p. Sejam U um grupo livre gerado por d elementos e T o quociente residualmente nilpotente maximal de $U/w(U)$. Seja $\mathcal{C}_{Nil}$ a classe dos grupos finitos nilpotentes e defina

$$K = \bigcap_{N \in \mathfrak{n}} N$$

onde

$$\mathfrak{n} = \{N \lhd U : w(U) \leq N, U/N \in \mathcal{C}_{Nil}\}.$$

Note que o quociente residualmente nilpotente maximal é dado por

$$T \simeq (U/w(U))/(K/w(U)),$$

e daí podemos concluir que, se $\widehat{T}_p$ é o completamento pro-p de T, então $w(\widehat{T}_p) = 1$. Sendo $\widehat{T}_p$ um grupo pro-p finitamente gerado e w uma $\mathcal{N}_p$-palavra, então $\widehat{T}_p$ deve ser virtualmente nilpotente e de posto finito. Por [10, p. 175], T está imerso em $\prod_{p \in \pi} \widehat{T}_p$ para algum conjunto finito de primos π. Uma vez que w é, em particular, uma $\mathcal{N}_p$-palavras para todo $p \in \pi$, então T é virtualmente nilpotente. Se H é um grupo pronilpotente finitamente gerado, $\tilde{H} = H/\overline{w(H)}$ e $d = d(H)$, para qualquer subgrupo T_1 de H que é denso e gerado por d elementos, pela maximalidade de T, T_1 deve ser um quociente de T. Assim, T_1 é virtualmente nilpotente e, pela densidade, $\tilde{H}$ tem que ser virtualmente nilpotente. Portanto, w é uma $\mathcal{N}$-palavra. □

A importância deste lema é justificada pela seguinte observação: seja G um grupo pronilpotente. Se $U <_o G$ o subgrupo

$$N = \bigcap_{g} gUg^{-1}$$

é normal em G com G/N nilpotente o que implica $N_G(U) \neq U$. Se S é um subgrupo de Sylow de G, então $N_G(S) \subset U$ para algum $U \leq_o G$. É fácil ver que devemos ter

$U = N_G(U)$ e assim, $U = G$. Disso segue que devemos ter $N_G(S) = G$ e, portanto, S é normal em G. Sejam agora π o conjunto dos divisores primos de $|G|$, $\{S_p\}_{p\in\pi}$ o conjunto dos subgrupos de Sylow e

$$K_p = \overline{\bigcup_{q\neq p} S_q}.$$

Note que $|K_p|$ e p são coprimos, logo, $K_p \cap S_p = \{1\}$ para cada p e $\bigcap_p K_p = 1$. Se $H = \overline{\langle S_p \rangle}$, então $|G : H| = 1$, isto é, $G = H$. Por [20, Lema 2.4.2], podemos concluir que G é isomorfo ao produto cartesiano de todos os S_p. Reciprocamente, se G é isomorfo ao produto cartesiano dos seus subgrupos de Sylow, uma vez que qualquer grupo pro-p é pronilpotente e o produto cartesiano de grupos pronilpotentes deve ser pronilpotente, então G é pronilpotente. Essa observação nos permite enunciar a seguinte proposição

Proposição 5.3.1. *Um grupo G é pronilpotente se, e somente se, é isomorfo ao produto cartesiano dos seus pro-p subgrupos de Sylow.*

Note que essa proposição resolve imediatamente a igualdade do exemplo 5.3.1.

Essa proposição induz a ideia de aplicar a equivalência obtida no Lema 5.3.1 nos pro-p subgrupos de Sylow de um grupo pronilpotente. De fato, essa é essencialmente a ideia da demonstração que veremos abaixo.

Teorema 5.3.1 (Zapirain)**.** *Seja $1 \neq w$ uma palavra do grupo livre F. Então as seguintes afirmações são equivalentes:*

(i) $w(G)$ é fechado para todo grupo pronilpotente finitamente gerado G,

(ii) $w \notin \bigcup_{p\ primo} (F')^p F''$.

Demonstração. Uma vez que um grupo pronilpotente é, em particular, um grupo pro-p, a afirmação (i) implica (ii) pelo Teorema 5.2.3. Se $w \notin \bigcup_p (F')^p F''$, então w é uma $\mathcal{N}_p$-palavra para todo primo p, logo, o Lema 5.3.1 diz que w é uma $\mathcal{N}$-palavra.

Sejam G um grupo pronilpotente finitamente gerado, $d = \mathrm{d}(G)$ e H um grupo livre pronilpotente gerado por $x_1, ..., x_d, z$. Usando a mesma ideia do Teorema 5.2.1, obtemos t, n tais que $\gamma_n(H^t) \leq \overline{w(H)}$. Como G é pronilpotente, G pode ser escrito como produto dos seus pro-p subgrupos de Sylow. Seja $G = G_1 \times G_2$ onde G_2 é o produto dos pro-p subgrupos de Sylow tais que $p \in \pi(t)$ onde $\pi(t)$ é o conjunto dos divisores primos de t e G_2 o produto dos pro-p subgrupos de Sylow restantes.

Note que pelo Teorema 5.2.3, $w(G_1)$ é fechado. Escreva $H = H_1 \times H_2$ da mesma maneira que G. Pela construção de H_2, temos que $\gamma_n(H_2) \leq \overline{w(H_2)}$ por razões similares

as que foram observadas no primeiro parágrafo da demonstração do Teorema 5.2.1. Novamente, usando as mesmas ideias do segundo parágrafo da demonstração do Teorema 5.2.1, podemos concluir que qualquer elemento de $\gamma_n(G_2)$ é um produto de, no máximo, k w-valores em H_2 para algum $k > 0$. Por [17, Teorema 2.1.1], sendo G_2 nilpotente finitamente gerado, w deve ter largura finita em G. Uma vez que $w(G_2)$ tem largura finita e G_2 é um grupo nilpotente finitamente gerado de classe $n-1$, então, em particular, $w(G_2/\gamma_n(G_2))$ tem largura finita, logo, $w(G_2/\gamma_n(G_2))$ é fechado e, como

$$w(G_2/\gamma_n(G_2)) = w(G_2)/\gamma_n(G_2),$$

então $w(G_2)$ é fechado.

Concluímos então que $w(G_1)$ e $w(G_2)$ são ambos fechados e, consequentemente, $w(G)$ é fechado. □

5.4 Uma alternativa ao uso do Problema Restrito de Burnside

A ideia desta seção é mostrar como o Teorema 5.2.1 depende da solução para o Problema Restrito de Burnside. Introduziremos o problema contextualizando brevemente e veremos como é possível evitar a utilização desse resultado com as ferramentas que estudamos aqui.

No artigo intitulado "On an unsettled question in the theory of discontinuous groups" William Burnside ([13, p. 923, tradução nossa]) escreve: "Um ponto ainda não decidido na teoria dos grupos descontínuos é quando a ordem de um grupo pode não ser finita, enquanto a ordem de cada elemento que ele contém é finita."

Suponha que G seja um grupo e que, para cada elemento $g \in G$, existe um $n \in \mathbb{N}$ (que, possivelmente, depende de g) tal que $g^n = 1$. Tais grupos são chamados de *periódicos*. Burnside queria determinar em quais casos esses grupos têm ordem finita. Neste ponto surge a seguinte questão:

Problema 1 (Problema Geral de Burnside)**.** Se G é um grupo periódico finitamente gerado, G deve necessariamente ser finito?

Um potencial problema é que, uma vez que n depende do elemento escolhido, pode não existir uma cota superior. O caminho para evitar esse caso é pedir que exista um $n \in \mathbb{N}$ tal que $g^n = 1$ para qualquer $g \in G$; nesse caso dizemos que G tem *expoente limitado* e o menor n satisfazendo tal condição é chamado de *expoente* de G. Isso reduz o problema inicial no seguinte:

Problema 2 (Problema de Burnside)**.** Se G é um grupo periódico finitamente gerado de expoente limitado, G deve necessariamente ser finito?

Pouco tempo depois, Burnside e Issai Schur obtiveram dois resultados relevantes que dão uma resposta parcialmente positiva ao problema. Eles conseguiram concluir que qualquer subgrupo de $\mathrm{GL}(n, \mathbb{C})$ de expoente limitado e qualquer subgrupo periódico finitamente gerado de $\mathrm{GL}(n, \mathbb{C})$ são ambos finitos (veja [3] e [16]). Além de uma resposta parcialmente positiva, esses resultados também mostraram que se o problema possuir contraexemplos, os contraexemplos não serão por meio de grupos lineares, o que deixa a tarefa de encontrá-los consideravelmente mais difícil. Alguns anos mais tarde, uma variação desse problema trouxe atenção novamente à essa questão.

Definição 5.4.1. Sejam F_m o grupo livre de posto m e $F_m^n \subset F_m$ o subgrupo gerado pelos elementos da forma g^n para todo $g \in G$. Uma vez que o $F_m^n \triangleleft F_m$, o quociente F_m/F_m^n é um grupo. Esse grupo é chamado de *grupo de Burnside* e é denotado por $B(m, n)$.

A essa altura, Burnside já havia mostrado alguns casos em que $B(m, n)$ tem ordem finita.

Problema 3 (Problema Restrito de Burnside)**.** Existem, a menos de isomorfismo, apenas uma quantidade finita de grupos com m geradores e expoente n?

Em 1958, Philip Hall e Graham Higman fizeram um grande avanço na direção de resolver esse problema (veja [7]).

Teorema 5.4.1. *Seja $n = p_1^{r_1} \cdots p_k^{r_k}$ a decomposição do natural n em primos distintos. Suponha que sejam válidas as seguintes afirmações:*

(i) O Problema Restrito de Burnside é verdadeiro para grupos de expoente $p_i^{r_i}$,

(ii) Existe uma quantidade finita de grupos simples de expoente n,

(iii) O grupo de automorfismos externos $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ é solúvel para qualquer grupo finito simples de expoente n.

Então o Problema Restrito de Burnside é verdadeiro para qualquer grupo de expoente n.

Na década de 80 a classificação dos grupos simples finitos, apesar de não estar totalmente completa, deixou apenas a veracidade do item (i) em aberto. Em 1989, Efim Zel'manov anunciou ter provado o item restante (veja [21]); a demonstração usa essencialmente ferramentas de álgebras de Lie. A prova de Zel'manov cobre todos os casos onde p é um primo diferente de 2, mas Burnside já havia mostrado que $B(m, 2)$ é um produto de uma quantidade finita de cópias de $\mathbb{Z}/2\mathbb{Z}$. A demonstração de Zel'manov deu a ele uma Medalha Fields, obtida em 1994.

A solução para o Problema Restrito de Burnside (veja [21]) permite concluir que, para $w = x^{p^n}$, $w(H)$ é fechado para qualquer grupo pro-p finitamente gerado H. Se assumirmos que, ao invés de ser virtualmente nilpotente, o grupo $H/\overline{w(H)}$ é nilpotente para todo grupo pro-p H finitamente gerado, então conseguimos mostrar que $H^{p^n} = w(H)$ é fechado sem usar a solução de Zel'manov.

Teorema 5.4.2 (Zapirain)**.** *Sejam F um grupo livre e $w \in F$. Se $t = w^p$, $t(H)$ fechado implica $w(H)$ aberto para qualquer grupo pro-p finitamente gerado H.*

Demonstração. Seja H um grupo pro-p livre não abeliano finitamente gerado. Suponha que $w(H)$ não é aberto. Sendo H não abeliano, $\overline{w(H)}$ é um grupo pro-p livre de posto infinito. Usando as mesmas ideias do Teorema 5.2.2, concluímos que $t(H)$ não é fechado, uma contradição. Assim, $\overline{w(H)}$ deve ser aberto, de modo que $H/\overline{w(H)}$ é nilpotente. Logo w é de largura finita e então $w(H)$ é fechado, o que implica $w(H)$ aberto. □

Referências Bibliográficas

[1] AVNI, N., CHEN, M., 2019, "Words have bounded width in $\mathrm{SL}_n(\mathbb{Z})$", *Compositio Mathematica*, v. 155, n. 7, pp. 1245 – 1258.

[2] BOURBAKI, N., 1975, *Lie Algebras and Lie Groups: chapters 1 - 3.* 1 ed. Grã-Bretanha, Herman.

[3] BURNSIDE, W., 1905, "On criteria for the finiteness of the order of a group of linear substitutions", *Proceedings of the London Mathematical Society*, v. s2-3, n. 1, pp. 435 – 440.

[4] DIXON, J., ET AL, 2003, *Analytic pro-p groups. No. 61.* 2 ed. Cambridge, Cambridge University Press.

[5] GOUVÊA, F. Q., 1993, *p-adic Numbers: An Introduction.* 1 ed. Berlim, Springer-Verlag.

[6] HALL, B., 2015, *Lie groups, Lie algebras, and representations: an elementary introduction*, v. 222. 2 ed. Nova Iorque, Springer.

[7] HALL, P., HIGMAN, G., 1956, "On the p-length of p-soluble groups and reduction theorems for Burnside's Problem", *Proceedings of the London Mathematical Society*, v. s3-6, n. 1, pp. 1 – 42.

[8] HUPPERT, B., 1979, "Subgroups of finite index in profinite groups", *Math. Z*, v. 168, pp. 71 – 76.

[9] JAIKIN-ZAPIRAIN, A., 2008, "On the verbal width of finitely generated pro-p groups", *Revista Matemática Iberoamericana*, v. 24, n. 2, pp. 617 – 630.

[10] LUBOTZKY, A., SEGAL, D., 2003, *Subgroup Growth*, v. 212. 1 ed. Basel, Birkhäuser.

[11] MERZLJAKOV, Y., 1996, "Verbal and marginal subgroups of linear groups", *Dokl. Akad. Nauk SSSR*, v. 177, n. 5, pp. 1008 – 1011.

[12] MORANDI, P., 1996, *Field and Galois Theory.* 1 ed. Nova Iorque, Springer-Verlag.

[13] NEUMANN, P. M., MANN, A. J. S., TOMPSON, J. C., 2004, *The Collected Papers of William Burnside*, v. 1. 1 ed. Nova Iorque, Oxford University Press.

[14] RIBES, L., ZALESSKII, P., 2000, *Profinite Groups*. 2 ed. Berlim, Springer.

[15] ROMAN'KOV, V. A., 1982, "Width of verbal subgroups in solvable groups", *Algebra i Logika*, v. 21, n. 1, pp. 60 – 72.

[16] SCHUR, I., 1911, "Über Gruppen periodischer substitutionen", *Sitzungsber. Preuss. Akad. Wiss*, pp. 619 – 627.

[17] SEGAL, D., 2009, *Words: notes on verbal width in groups*, v. 361. 1 ed. Nova Iorque, Cambridge University Press.

[18] SERRE, J. P., 2009, *Lie algebras and Lie groups: 1964 lectures given at Harvard University*. 2 ed. Berlim, Springer-Verlag.

[19] SIMONS, N., 2009, *The Width of Verbal Subgroups in Profinite Groups*. Tese de doutorado, Universidade de Oxford.

[20] WILSON, J., 1998, *Profinite Groups*, v. 19. 1 ed. Nova Iorque, Oxford University Press.

[21] ZEL'MANOV, E. I., 1990, "Solution of the restricted Burnside problem for groups of odd exponent", *Izv. Akad. Nauk SSSR Ser. Mat.*, v. 54, n. 1, pp. 42 – 59.