Yuri Santos Rêgo

A Desigualdade de Golod-Šafarevič para Grupos Pro-p e Grupos Abstratos

CAMPINAS
2014

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

YURI SANTOS RÊGO

A DESIGUALDADE DE GOLOD-ŠAFAREVIČ PARA GRUPOS PRO-p E GRUPOS ABSTRATOS

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em matemática.

Orientadora: Dessislava Hristova Kochloukova

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO YURI SANTOS RÊGO, E ORIENTADA PELA PROFA. DRA. DESSISLAVA HRISTOVA KOCHLOUKOVA.

Assinatura da Orientadora

CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

R265d

Rêgo, Yuri Santos, 1989-
A desigualdade de Golod-Šafarevič para grupos pro-p e grupos abstratos / Yuri Santos Rêgo. – Campinas, SP : [s.n.], 2014.

Orientador: Dessislava Hristova Kochloukova.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos grupos. 2. Grupos profinitos. 3. Grupos finitos. I. Kochloukova, Dessislava Hristova,1970-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: The Golod-Shafarevich inequality for pro-p groups and abstract groups
Palavras-chave em inglês:
Group theory
Profinite groups
Finite groups
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Dessislava Hristova Kochloukova [Orientador]
Ilir Snopche
Aline Gomes da Silva Pinto
Data de defesa: 08-08-2014
Programa de Pós-Graduação: Matemática

Dissertação de Mestrado defendida em 08 de agosto de 2014 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof.(a). Dr(a). DESSISLAVA HRISTOVA KOCHLOUKOVA

Prof.(a). Dr(a). ILIR SNOPCHE

Prof.(a). Dr(a). ALINE GOMES DA SILVA PINTO

Abstract

In this work we study the main results presented by J. Wilson in [20] which extend the Golod-Šafarevič Inequality [7] to a large class of infinite pro-p and abstract groups. In the first chapter we present the basic theory of abstract free groups, focusing on finite presentations. Next we study profinite groups, with focus on pro-p groups. This study ranges from definitions to basic algebraic and topological properties, as well as the case of finitely generated groups and the Frattini subgroup, and notions of completion, free pro-p groups, presentations in the pro-p scenario and completed group algebras. In the last chapter we study the main results regarding finite presentations of pro-p and abstract groups, following [20] and [21], which include soluble groups and implications on the structure of certain groups for which the Inequality holds. In the appendixes we briefly relate the presented theory to pro-p groups of finite rank and homology and cohomology in the pro-p case.

Keywords: Group Theory, Pro-p Groups, Finitely Presented Groups, Golod-Shafarevich.

Resumo

Neste trabalho estuda-se os principais resultados dados por J. Wilson em [20], relacionados à Desigualdade de Golod-Šafarevič [7] para uma ampla classe de grupos pro-p e abstratos infinitos. Apresentamos a teoria básica de grupos livres abstratos, levando à noção de apresentação de grupos, com foco em apresentações finitas. É feito um estudo sobre grupos profinitos, particularmente no caso pro-p. Abrange-se definições, propriedades algébricas e topológicas básicas, bem como o caso de finitos geradores e o subgrupo de Frattini, e conceitos de completamentos, de grupos pro-p livres, de apresentações no caso pro-p e de álgebras de grupo completas. No capítulo final estudamos os resultados principais para grupos pro-p e abstratos finitamente apresentáveis, seguindo [20] e [21], que incluem grupos solúveis e implicações na estrutura de certos grupos satisfazendo a Desigualdade. Os anexos relacionam a teoria aqui apresentada a grupos pro-p de posto finito e homologia e cohomologia no caso pro-p.

Palavras-chave: Teoria de Grupos, Grupos Pro-p, Grupos Finitamente Apresentáveis, Golod-Shafarevich.

Sumário

À minha família
e à Paula.

Agradecimentos

Aqui me concedo uma certa “licença poética” para (quem sabe) melhor expressar o sentimento de gratidão a todos que me permitiram chegar nesse ponto da minha jovem trajetória. O leitor que estiver familiarizado com o tema pode pular esta seção sem prejuízo ao entendimento do texto.

Primeiramente, agradeço ao CNPq, pelo apoio financeiro, que possibilitou a execução deste trabalho.

Em segundo lugar, o agradecimento canônico à minha família, que de canônica não tem nada. Destaque para minhas avós Maria Emília e Jacira, por serem os alicerces do meu mundo. Agradeço à doutora e madrinha tia Ana, pelas grandes motivações acadêmicas, incentivos e tantos cuidados – fossem médicos, pseudo-maternais, ou só de tia mesmo. Agradeço a tia Remédios e tio Ricardo, pelo apoio de pseudo-pais e o eterno incentivo. A Bia, Arthur e Marina, pela irmandade de nascença. Também agradeço, claro, aos Santos como conjunto, por serem motivo de alegria e inspiração – em particular, como profissionais. E agradeço, obviamente, à minha mãe Zequinha e à minha mana Marina. Porque a vida começa com as risadas sem motivo olhando um para a cara do outro, com os “minha filho...”, com o modo lagarta, e com o empenho em sermos pessoas melhores.

Agradeço aos grandes amigos que tive a sorte de achar ao longo desses anos. Tribeca, Concorrência, Burmo, Desossado, Arturo, AlienKanibal, a “parcerage” de vocês – acadêmica ou não – ao longo dessas 1.1 a 2 décadas foi essencial.

Aos novos companheiros e amigos que fiz graças à Matemática. À Paula e ao Jatobá, pelo tripé desbravador da graduação. A todos os companheiros de estudo (e muitas vezes de descontração), pela força e ferrenha briga com exercícios, provas, trabalhos, seminários... Muito obrigado a todos por enriquecerem minha formação.

Aproveitando a convergência aos agradecimentos acadêmicos, sou imensamente grato a todos os professores que contribuíram para minha formação, tanto profissional quanto pessoal.

Ao professor Francivaldo Melo, pelos ensinamentos e aulas inspiradoras – nas mais diversas matérias, diga-se.

Aos professores Maurício Ayala-Rincón, Mauro Luiz Rabelo e Celius Antônio Magalhães, pelos exemplos de pessoas fantásticas e grandes profissionais que são, pelos ensinamentos matemáticos, pela paciência, pelas dicas, pelas enormes ajudas quanto à carreira, pelos incentivos e, também, pelas risadas. Minha carreira de aspirante a matemático deve muito aos três.

Ao professor Nigel Pitt, pelas lições e conselhos – vulgo “broncas” – nas tomadas de decisões. Aos professores Leandro Cioletti e Luís Henrique de Miranda, pelas conversas e conselhos sobre a carreira matemática.

À professora Aline Pinto, pelos excepcionais cursos de álgebra lecionados e influência direta na minha carreira e escolha de área. Agradeço-a também pelos ensinamentos, conversas, ajuda e incentivos, e até por algumas piadas. Não somente, agradeço-a por todo o cuidado, comentários, sugestões e críticas em relação ao presente trabalho, fazendo-o enriquecer.

Ao professor Ilir Snopche, pelo interesse, disposição e atenção na avaliação deste trabalho, bem como pelas sugestões, correções, críticas e comentários que implicaram em valorosos aprimoramentos nesta dissertação.

Agradeço a todos os professores e funcionários do IMECC/Unicamp que contribuíram com minha formação e me auxiliaram. Ao professor Adriano Moura, pelo "baque" – positivo – logo na chegada, no seu curso de Álgebra Linear. Ao professor Plamen Kochloukov, pelas conversas e conselhos antes e depois da minha chegada à Unicamp, e pela paciência e disposição em ajudar.

Agradeço também aos bons amigos e colegas de estudo que fiz nesses longos curtos 2 anos de IMECC. A toda a turma, do reclamão ranzinza ao importante professor do centro-oeste. Em especial, ao Matheus e à Rafa, que apesar de virem de antes, tornaram-se aqui valiosos e queridíssimos amigos.

Sou grato aos membros da Banca Examinadora, os professores Ilir Snopche e Aline Pinto, Adriano Moura e Lucio Centrone, por aceitarem o convite e se disponibilizarem a avaliar e contribuir com este trabalho.

Expresso, também, meu profundo agradecimento à professora Dessislava Hristova Kochloukova. Não só por ter me aceitado como orientando de mestrado, mas também pela enorme paciência, pelas críticas construtivas, pelas conversas e conselhos, pelas dicas, pelo incentivo e pela ajuda nesta e em outras etapas da minha carreira acadêmica. E, principalmente, pelo exemplo de profissional e pessoa excepcional que é.

E, claro, agradeço à Paula. Pelo enorme companheirismo, pela "boniteza", pela inspiração – na matemática e fora dela, pelas pequenas (grandes) coisas bobas, pelas risadas, pela convivência engrandecedora, pela paciência, pelo grande apoio sempre e por ser, acima de tudo, a maravilhosa pessoa que é. Obrigado pais da Paula, pela Paula.

Introdução

Na Teoria de Grupos, os problemas de descrever concretamente um dado grupo G e extrair propriedades do mesmo podem ser abordados de diversas formas. Uma das maneiras mais compactas de se descrever G completamente é através de geradores e relações – mais especificamente, através de uma apresentação de G. Dados um conjunto de geradores X e um conjunto de relações R, o grupo G com apresentação $\langle X \mid R\rangle$ é o "grupo mais livre possível" sobre X sujeito às condições definidas por R. Diversos grupos podem ser descritos intuitivamente via geradores e relações, como por exemplo o grupo diedral, grupos cíclicos, grupos abelianos finitamente gerados, produtos diretos e produtos livres de grupos. Formalmente, uma apresentação de G consiste em um epimorfismo $\pi : F \twoheadrightarrow G$, no qual F é um grupo livre sobre X e $\ker(\pi) = \langle R^F\rangle$ (vide Seção 1.2).

A noção de apresentação de grupos não se restringe à classe dos grupos abstratos, mas pode ser também traduzida a certas classes de grupos topológicos – em particular, à dos grupos pro-p. Dado $p \in \mathbb{N}$ um número primo, um grupo topológico G é dito pro-p quando G é o limite inverso de um sistema inverso de p-grupos finitos. Equivalentemente, G é compacto, totalmente desconexo, e todos os seus subgrupos normais abertos têm índices potências de p. Todo p-grupo finito munido da topologia discreta é, em particular, pro-p. O exemplo clássico – e talvez mais importante, historicamente – de grupo pro-p infinito é o grupo aditivo dos inteiros p-ádicos, $\mathbb{Z}_p$, que se comporta no cenário pro-p como o análogo aos inteiros $\mathbb{Z}$ no cenário abstrato. Desde a descoberta dos inteiros p-ádicos por K. Hensel no final do século XIX, grupos pro-p emergiram como ricos objetos de estudo em diversas áreas da matemática (vide [12], [4], [8], [21], [16]).

Assim como a relação entre $\mathbb{Z}$ e $\mathbb{Z}_p$, alguns conceitos e propriedades podem ser traduzidos do caso abstrato para o caso pro-p, como a noção de grupos pro-p livres. No contexto acima descrito, uma apresentação $\overline{\langle X \mid R\rangle}_{\hat{p}}$ do grupo pro-p G consiste em um epimorfismo contínuo $\pi : \widehat{F}_p \twoheadrightarrow G$, no qual $\widehat{F}_p$ é um grupo pro-p livre com base X e $\ker(\pi) = \overline{\langle R^{\widehat{F}_p}\rangle}$ (vide Seção 2.4). Em ambos os cenários (abstrato e pro-p), um grupo é dito finitamente apresentável quando admite apresentação com finitos geradores e finitas relações.

Apresentações de grupos são um tema central das teorias combinatória e geométrica de grupos (vide [13], [3] e [9] para o caso abstrato, e [21] e [16] para geradores e relações no caso pro-p). O problema de se construir uma apresentação de um grupo pode ser complicado, especialmente no que tange ao número de geradores e de relações. Para que G seja finitamente apresentável, é necessário que o mesmo seja finitamente gerado. Fixado então o número de geradores, quantas relações devem ocorrer numa dada apresentação finita de um grupo (pro-p ou abstrato) G?

Um dos trabalhos de meados do século XX, com grande influência em diversas áreas da álgebra, foi publicado pelos matemáticos russos Evgeny Golod e Igor' Šafarevič. Em 1964, os mesmos

provaram, via técnicas de álgebra não-comutativa para aneis locais, a célebre Desigualdade de Golod-Šafarevič [7]. As técnicas então apresentadas tiveram impacto direto na solução de 3 importantes problemas em aberto: o problema da finitude das torres de corpos de classes de Hilbert, na Teoria dos Números; o problema de Kuroš, na Álgebra Não-Comutativa; e o problema geral de Burnside, na Teoria de Grupos (vide Capítulo 3). Não somente, as técnicas de Golod e Šafarevič permitiram também estabelecer uma cota inferior para o número de relações na apresentação de um p-grupo finito, a partir do número mínimo de geradores de um tal grupo, respondendo parcialmente à pergunta proposta acima para grupos pro-p *finitos*.

Desde o Teorema de Golod-Šafarevič, grupos e álgebras com propriedades relacionadas à Desigualdade vêm sendo ativamente estudados (vide, por exemplo, [5], para um apanhado geral). Neste trabalho, estudamos os resultados principais dados por John S. Wilson em seu artigo *"Finite presentations of pro-p groups and discrete groups"* [20], no qual o resultado de Golod e Šafarevič é estendido a uma ampla classe de grupos pro-p *infinitos*, incluindo grupos solúveis e aqueles que satisfazem a condição maximal para subgrupos normais. Dentre as consequências, estabelece-se uma versão da Desigualdade para apresentações de grupos *abstratos*, bem como implicações no número de geradores de certos subgrupos dos grupos para os quais vale a Desigualdade.

A estrutura deste trabalho é dada como segue.

No Capítulo 1 desenvolvemos a teoria básica de grupos livres abstratos visando o estudo de grupos finitamente apresentáveis, seguindo os livros de Rotman [19], Johnson [9] e Cohen [3].

No Capítulo 2 apresentamos os conceitos e algumas propriedades básicas de espaços e grupos profinitos, focando então no caso dos grupos pro-p, seguindo os livros de L. Ribes e P. Zalesskii [16] e J. Wilson [21]. Primeiramente, introduzimos os conceitos de grupos profinitos e pro-p através de limites inversos, com alguns exemplos e propriedades, incluindo completamentos e o caso dos inteiros p-ádicos. Em seguida, focamos em grupos pro-p finitamente gerados, relacionando algumas propriedades ao subgrupo de Frattini. Por fim, é feito o estudo de grupos pro-p livres e apresentações de grupos pro-p, com algumas propriedades de apresentações finitas e uma caracterização do grupo pro-p livre finitamente gerado relacionada à álgebra das séries formais de potências sobre o corpo de ordem prima p.

A parte principal desta Dissertação, dada no Capítulo 3, consiste no estudo do artigo [20] de J. Wilson. A forma da Desigualdade de Golod-Šafarevič como dada por Wilson é fundamentada na caracterização do grupo pro-p livre com base finita como subgrupo multiplicativo da álgebra das séries formais de potências sobre o corpo $\mathbb{F}_p$ (ver Teorema 2.4.45). Os resultados principais do caso pro-p (ver Teoremas 3.2.4 e 3.1.8 e Corolários 3.2.6, 3.2.7 e 3.2.9) são aqui apresentados seguindo a exposição dada no livro *"Profinite Groups"* [21] de J. Wilson. As aplicações para grupos abstratos (ver Teorema 3.2.11 e Corolário 3.2.12) são apresentadas seguindo o artigo [20].

Acrescentamos ainda 2 anexos. O primeiro trata de grupos pro-p de posto finito, visto que os mesmos satisfazem as condições do Teorema 3.2.4 (ver Corolário 3.2.6). Foram incluídas algumas propriedades e comentários sobre tais grupos, com poucas demonstrações. A exposição aqui dada segue os textos de Dixon-du Sautoy-Mann-Segal [4] e Wilson [21]. O segundo anexo é sobre Homologia e Cohomologia de grupos pro-p. A exposição aqui dada é bastante resumida, sem demonstrações, com referências a importantes resultados que indicam uma outra abordagem para o estudo de propriedades de finitude de grupos pro-p – nesse caso, geradores e relações. Os teoremas citados em tal anexo podem ser vistos nos textos de Ribes e Zalesskii [16] e Wilson [21].

Capítulo 1

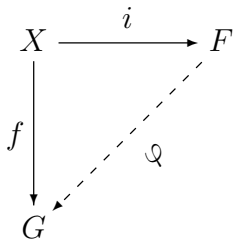
Grupos Abstratos

Neste capítulo será feita uma introdução ao estudo de grupos abstratos[1] livres, a fim de estabelecer a definição abstrata de apresentação de um grupo. Tal conceito é muitas vezes visto intuitivamente em cursos de álgebra, e é uma ferramenta bastante útil na construção de grupos a partir de certas propriedades definidoras simples - a saber, geradores e relações.

1.1 Grupos Livres

Os conceitos básicos e a construção do grupo livre, apresentados a seguir, seguem as linhas vistas em Cohen [3] e Rotman [19]. Suas propriedades básicas, bem como um maior aprofundamento no assunto, podem ser vistas em Cohen [3] e Johnson [9].

Definição 1.1.1. Dados X um conjunto arbitrário, F um grupo e $i : X \to F$ função, dizemos que (F, i) é livre sobre X quando,



dados quaisquer G grupo e $f : X \to G$ função, existir um único homomorfismo de grupos $\varphi : F \to G$ tal que $\varphi \circ i = f$. Nesse caso, dizemos que φ é o homomorfismo que estende a função f.

Exemplo 1.1.2. O grupo trivial, denotado $\{1\}$ (ou $\{0\}$), é livre sobre o conjunto vazio $\varnothing$.

Exemplo 1.1.3. O grupo aditivo dos inteiros $\mathbb{Z}$ é livre sobre qualquer conjunto unitário $\{x\}$ por meio da (única) aplicação $i(x) = 1 \in \mathbb{Z}$. De fato, sejam $(G, \cdot)$ grupo e $f : \{x\} \to G$ qualquer.

[1] Alguns autores tratam de grupos abstratos (arbitrários) como grupos discretos. Evitaremos tal terminologia para evitar confusão com os grupos topológicos a serem estudados nos capítulos seguintes, que relacionam-se a grupos que de fato carregam a topologia discreta.

Defina $\varphi : \mathbb{Z} \to G$ a ser $\varphi(n) = f(x)^n$. Tem-se $\varphi \circ i(x) = \varphi(1) = f(x)^1 = f(x)$, isto é, $\varphi \circ i = f$. Além disso, $\forall m, n \in \mathbb{Z},\ \varphi(m+n) = f(x)^{m+n} = f(x)^m \cdot f(x)^n = \varphi(m) \cdot \varphi(n)$. Portanto, φ é homomorfismo de grupos. A unicidade de φ é consequência da sua definição.

Nosso próximo objetivo é provar a existência de um grupo livre sobre um conjunto arbitrário dado. Para isso, estabeleceremos primeiro algumas noções e propriedades a serem utilizadas na demonstração.

Faremos a construção clássica do grupo livre via *palavras reduzidas* sobre um conjunto X e utilizaremos o *método de van der Waerden* na prova do teorema seguinte para garantir que o conjunto F a ser construído é de fato grupo com a operação que definiremos. A aplicação i será então facilmente determinada, e checar que (F, i) é livre sobre X nada mais será do que um processo rotineiro.

Seja X um conjunto. Tome agora um conjunto diferente de X, mas para o qual existe uma bijeção do mesmo com X. Denotaremos tal conjunto por X^{-1}, com a bijeção $x \mapsto x^{-1}$. Quando conveniente, denotaremos os elementos $x \in X$ por $x^1 = x \in X$, para diferenciá-los dos elementos de X^{-1}. Fixe ainda um conjunto unitário disjunto de X e X^{-1}, denotado por $\{\lambda\}$. Defina $\mathcal{A} = X \cup X^{-1} \cup \{\lambda\}$. Com isso, dado $a \in \mathcal{A}$ com $a \neq \lambda$, podemos escrever $a = x^\varepsilon$, no qual $\varepsilon = \pm 1$. Definamos então

$$W_0 = \{(a_1, a_2, \ldots, a_n, \ldots) \mid n \in \mathbb{N},\ a_i = \lambda\ \forall i \geq n \text{ e } a_j \in \mathcal{A}\backslash\{\lambda\}\ \forall j < n\}.$$

Tal conjunto é chamado o conjunto das palavras sobre o alfabeto X, e os elementos $a_i \neq \lambda$ que aparecem como as coordenadas numa palavra $w \in W_0$ são chamados as *letras* de w. Note que, no caso $n = 1$, tem-se a (única) palavra $(\lambda, \lambda, \ldots, \lambda, \ldots) \in W_0$, chamada a *palavra vazia*, a qual denotaremos simbolicamente por 1. Dito de outra forma, $1 \in W_0$ é a única palavra sobre X que não possui letras. Evidentemente, tem-se a identificação natural $X \hookrightarrow W_0$ dada por $x \mapsto (x, \lambda, \ldots, \lambda, \ldots)$.

Dada $w = (a_1, a_2, \ldots, a_n, \ldots) \in W_0$ como acima, definimos o *comprimento* da palavra w a ser o inteiro $l(w) = n - 1$. Ou seja, $l(w)$ é o número de letras de w. Em particular, $l(w) = 0$ se, e só se, $w = 1$. Dizemos ainda que as letras $a \mapsto (a, \lambda, \ldots, \lambda, \ldots) \in W_0,\ a \neq \lambda$, são as (únicas) palavras de comprimento 1.

Veja que toda palavra sobre X possui apenas um número finito de letras, podendo este ser nulo. Dada $w \in W_0$, podemos utilizar uma notação muito mais prática. Caso $l(w) = 0$, já denotamos $w = 1$. Caso $l(w) = k \geq 1$, podemos escrever

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k},$$

com $x_j \in X$ e $\varepsilon_j = \pm 1$, para denotar a palavra $w = (a_1, a_2, \ldots, a_k, \lambda, \lambda, \ldots) \in W_0$ tal que $a_j = x_j^{\varepsilon_j}$ e $j = 1, \ldots, k$. Note que tal escrita é única, pois duas sequências $(a_i)_{i \in \mathbb{N}}$ e $(b_i)_{i \in \mathbb{N}}$ são iguais se, e só se, $a_i = b_i$ para todo i.

O conjunto W_0 possui uma operação binária, chamada *concatenação* de palavras. Dadas $v, w \in W_0$ arbitrárias, definimos a concatenação de v e w a ser a palavra vw, construída da seguinte forma: se $v = 1$, então $vw = w$; analogamente, se $w = 1$, então $vw = v$; caso sejam $v \neq 1 \neq w$, escrevendo

$v = y_1^{\delta_1} y_2^{\delta_2} \cdots y_l^{\delta_l}$ e $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$ como acima, define-se $vw = y_1^{\delta_1} y_2^{\delta_2} \cdots y_l^{\delta_l} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$. Segue-se que toda palavra não-vazia é a concatenação de suas letras.

Dada uma palavra $w \in W_0$, dizemos que $v \in W_0$ é uma *subpalavra* de w quando $v = 1$ ou $v = x_i^{\varepsilon_i} \cdots x_j^{\varepsilon_j}$, caso sejam $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \neq 1$ e $1 \leq i \leq j \leq k$. Um *prefixo* de $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \neq 1$ é qualquer subpalavra v da forma $v = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_j^{\varepsilon_j}$ ou $v = 1$, no qual $j \leq k$. Analogamente, um *sufixo* de $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \neq 1$ é qualquer subpalavra u da forma $u = x_i^{\varepsilon_i} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$ ou $u = 1$, no qual $i \geq 1$. Como a única subpalavra da palavra vazia é ela própria, convencionamos que seu único sufixo (e seu único prefixo) é a própria palavra vazia 1.

Seja $w \in W_0$. Definimos sua *inversa* $w^{-1} \in W_0$ da seguinte maneira: se $w = 1$, pomos $w^{-1} = 1$; se $w = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \neq 1$ pomos $w^{-1} = x_k^{-\varepsilon_k} \cdots x_1^{-\varepsilon_1}$. Tem-se então que $1^{-1} = 1$ e $(w^{-1})^{-1} = w,\ \forall w \in W_0$.

Dizemos que uma palavra $w \in W_0$ é *reduzida* quando w não contem subpalavras não-vazias da forma vv^{-1}. Convenciona-se, em particular, que a palavra vazia $1 \in W_0$ é reduzida. Note que a concatenação de palavras reduzidas não é necessariamente reduzida, já que $l(w) \neq 0$ implica que ww^{-1} é não-reduzida. Vê-se ainda que toda subpalavra de uma palavra reduzida é também reduzida.

Façamos uma observação importante. Para quaisquer duas palavras *reduzidas* $w, w' \in W_0$, podemos escrever $w = uv$ e $w' = v^{-1}u'$, para uma única subpalavra maximal $v \in W_0$ e subpalavras u de w e u' de w'. Com isso queremos dizer que v é o *único sufixo de w de maior comprimento* tal que v^{-1} é prefixo (de comprimento maximal) da palavra w'. Para garantir isso, basta ver que as subpalavras $v,\ u$ ou u' podem ser vazias. Mais precisamente, o caso $v = 1$ ocorre quando a (possível) última letra de w não for o inverso da (possível) primeira letra de w', e os outros dois casos ocorrem quando w^{-1} é prefixo de w' e vice-versa. Tem-se que a unicidade da escrita de palavras e a exigência de comprimento máximo de v garantem que v é única, e também que a (possível) última letra de u *não* pode ser inversa da (possível) primeira letra de u'.

Para ilustrar o fato acima, considere $w = xx_1^{\varepsilon_1} x_2^{\varepsilon_2} x_3^{\varepsilon_3}$ e $w' = x_3^{-\varepsilon_3} x_2^{-\varepsilon_2} x_1^{-\varepsilon_1} y$ reduzidas, no qual $x \neq y$. Tem-se que $\widetilde{v} = x_2^{\varepsilon_2} x_3^{\varepsilon_3}$ é um sufixo de w tal que $w = u\widetilde{v}$ e $w' = \widetilde{v}^{-1}u'$, no qual $u = xx_1^{\varepsilon_1}$ e $u' = x_1^{-\varepsilon_1} y$. Porém, $l(\widetilde{v})$ *não* é a subpalavra de comprimento maximal com tal propriedade, e portanto $\widetilde{v}$ não pode ser o sufixo maximal como acima. Nesse exemplo, o sufixo procurado é $v = x_1^{\varepsilon_1} x_2^{\varepsilon_2} x_3^{\varepsilon_3}$, e tem-se $w = xv,\ w = v^{-1}y$.

Feitas tais considerações, prosseguiremos com a existência e unicidade do grupo livre.

Teorema 1.1.4. Seja X um conjunto. Então:

i. Existem F grupo e $i : X \to F$ função injetiva tais que (F, i) é livre sobre X;

ii. Se (F_1, i_1) e (F_2, i_2) são livres sobre X, então existe um único $\varphi : F_1 \to F_2$ isomorfismo de grupos tal que $\varphi \circ i_1 = i_2$.

Demonstração. **i**. **(Existência)** Manteremos a notação estabelecida anteriormente. Dado então X conjunto arbitrário, considere W_0 o conjunto das palavras sobre X e a operação de *concatenação*, como acima.

Defina $F = \{w \in W_0 \mid w \text{ é reduzida}\}$. Definamos um produto $\cdot$ em F a ser a seguinte operação: dadas $w, w' \in F$, podemos escrever, de maneira única, $w = uv$ e $w' = v^{-1}u'$ como

nos parágrafos acima (v de comprimento maximal); ponha então $w \cdot w' = uu'$. Veja que uu' de fato pertence a F, pois como observado anteriormente, a (possível) última letra de u *não* é inversa da (possível) primeira letra de u', ou seja, uu' não contem subpalavras da forma tt^{-1}, sendo portanto reduzida. Tal operação é chamada *justaposição*.

Nossa primeira observação é que, para qualquer $w \in F$, tem-se $1 \cdot w = 1w = w = w1 = w \cdot 1$ e $w \cdot w^{-1} = 1 = w^{-1} \cdot w$. Assim, a palavra vazia é elemento neutro para $\cdot$, e todo elemento de F admite inverso para tal operação. Mostrando associatividade, garantiremos que F é grupo com a justaposição.

Para cada $x \in X$ e $\varepsilon = \pm 1$, considere as aplicações $\sigma_{x^\varepsilon} : F \to F$ definidas por:

$$\sigma_{x^\varepsilon}(w) = \begin{cases} x^\varepsilon, \text{ se } w = 1; \\ x^\varepsilon x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}, \text{ se } w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \neq 1 \text{ e } x^\varepsilon \neq (x_1^{\varepsilon_1})^{-1}; \\ x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}, \text{ se } w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \neq 1 \text{ e } x^\varepsilon = (x_1^{\varepsilon_1})^{-1}. \end{cases}$$

Veja que $\sigma_{x^\varepsilon} \circ \sigma_{x^{-\varepsilon}} = \sigma_{x^{-\varepsilon}} \circ \sigma_{x^\varepsilon} = id_F$. Logo, vale a relação $(\sigma_{x^\varepsilon})^{-1} = \sigma_{x^{-\varepsilon}}$, e tem-se $\sigma_{x^\varepsilon} \in S_F$, no qual S_F denota o grupo das permutações (bijeções) de F. Considere agora H o subgrupo de S_F gerado por $\Sigma_X := \{\sigma_x \mid x \in X\}$.

Sendo $H = \langle \Sigma_X \rangle$, tem-se que para todo $\alpha \in H \backslash \{id_F\}$ podemos escrever $\alpha = \sigma_{x_1}^{n_1} \circ \sigma_{x_2}^{n_2} \circ \cdots \circ \sigma_{x_k}^{n_k}$, no qual $x_i \in X$, $n_i \in \{-1, 1\}$, e ainda $\sigma_{x_i}^{n_i} \neq (\sigma_{x_{i+1}}^{n_{i+1}})^{-1}$, pois caso contrário poderíamos cancelar tais termos inversos da fatoração da permutação α. Além disso, tal fatoração é única, pois $\alpha(1) = x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \in F \subset W_0$ e já observamos que a escrita de uma palavra é única. Dessa forma, para cada $\alpha \in H$, existe uma única $w \in F$ tal que $\alpha(1) = w$ (no caso $\alpha = id_F$, tem-se $w = 1 \in F$). Afirmamos que, para $\alpha, \beta \in H$ com $\alpha(1) = w \in F$ e $\beta(1) = w' \in F$, vale $\alpha \circ \beta(1) = w \cdot w'$. De fato, escreva $w = uv$ e $w' = v^{-1}u'$ como na definição de *justaposição*. Denotando $\delta, \gamma, \delta' \in H$ as (únicas) permutações tais que $\delta(1) = u$, $\gamma(1) = v$ e $\delta'(1) = u'$, a fatoração de $\alpha, \beta \in H = \langle \Sigma_X \rangle$ nos dá $\alpha = \delta \circ \gamma$ e $\beta = \gamma^{-1} \circ \delta'$. Além disso, tem-se $\delta \circ \gamma(1) = uv$ e $\gamma^{-1} \circ \delta'(1) = v^{-1}u'$. Logo,

$$\alpha \circ \beta(1) = (\delta \circ \gamma) \circ (\gamma^{-1} \circ \delta')(1) = \delta \circ \delta'(1) = uu' = w \cdot w'.$$

A associatividade de $\cdot$ em F torna-se imediata. Sejam $w_1, w_2, w_3 \in F$ quaisquer, e tome $\alpha_1, \alpha_2, \alpha_3 \in H$ as (únicas) permutações tais que $\alpha_1(1) = w_1$, $\alpha_2(1) = w_2$, $\alpha_3(1) = w_3$. Como H é grupo com a composição de permutações $\circ$, tem-se

$$w_1 \cdot (w_2 \cdot w_3) = \alpha_1 \circ (\alpha_2 \circ \alpha_3)(1) = (\alpha_1 \circ \alpha_2) \circ \alpha_3(1) = (w_1 \cdot w_2) \cdot w_3.$$

Portanto, F é um grupo, com a operação de justaposição de palavras.

Como toda palavra unitária é reduzida, tome $i : X \to F$ como sendo a identificação natural $x \mapsto x = (x, \lambda, \ldots, \lambda, \ldots) \in F \subset W_0$. Evidentemente, i é injetiva. Afirmamos que (F, i) é livre sobre X.

Sejam G grupo e $f : X \to G$ função. Defina $\varphi : F \to G$ a ser $\varphi(1) = 1_G$ e $\varphi(w) = f(x_1)^{\varepsilon_1} f(x_2)^{\varepsilon_2} \cdots f(x_k)^{\varepsilon_k}$ se $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \in F \backslash \{1\}$. Por construção $\varphi \circ i = f$. Dadas

$w, w' \in F$ quaisquer, escreva $w = uv$ e $w = v^{-1}u'$ como na definição de justaposição. Tem-se $\varphi(w \cdot w') = \varphi((uv) \cdot (v^{-1}u')) = \varphi(uu')$. Como a (possível) última letra de u *não* é inversa da (possível) primeira letra de u', segue-se da definição de φ que $\varphi(uu') = \varphi(u)\varphi(u')$. Novamente da definição, $\varphi(\widehat{w}^{-1}) = \varphi(\widehat{w})^{-1},\ \forall \widehat{w} \in F$, o que implica $\varphi(u)\varphi(u') = \varphi(u)\varphi(v)\varphi(v)^{-1}\varphi(u') = \varphi(u)\varphi(v)\varphi(v^{-1})\varphi(u')$. Mais uma vez, como a (possível) última letra de u *não* é inversa da (possível) primeira letra de v, vale $\varphi(u)\varphi(v) = \varphi(uv)$. Analogamente, $\varphi(v^{-1})\varphi(u') = \varphi(v^{-1}u')$. Logo,

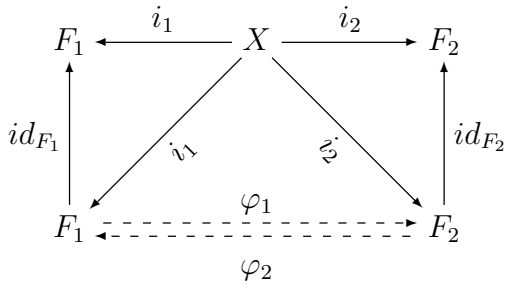
$$\varphi(w \cdot w') = \varphi(uu') = \varphi(uv)\varphi(v^{-1}u') = \varphi(w)\varphi(w'),$$

ou seja, $\varphi : F \to G$ é homomorfismo de grupos. Para a unicidade, suponha que $\psi : F \to G$ seja também homomorfismo tal que $\psi \circ i = f$. Sendo ψ homomorfismo, tem-se $\psi(1) = 1_G = \varphi(1)$. Para $w = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_k^{\varepsilon_k} \in F\backslash\{1\}$ qualquer, tem-se

$$\begin{aligned}\psi(w) &= \psi(x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}) = \psi(x_1^{\varepsilon_1})\psi(x_2^{\varepsilon_2}) \cdots \psi(x_k^{\varepsilon_k}) = \psi(x_1)^{\varepsilon_1}\psi(x_2)^{\varepsilon_2} \cdots \psi(x_k)^{\varepsilon_k} \\ &= (\psi \circ i(x_1))^{\varepsilon_1}(\psi \circ i(x_2))^{\varepsilon_2} \cdots (\psi \circ i(x_k))^{\varepsilon_k} = f(x_1)^{\varepsilon_1}f(x_2)^{\varepsilon_2} \cdots f(x_k)^{\varepsilon_k} \\ &= \varphi(w).\end{aligned}$$

Logo, φ é única. Portanto, (F, i) é livre sobre X.

ii. **(Unicidade)** Observe primeiro que, da propriedade universal do grupo livre, id_{F_1} e id_{F_2} são os únicos homomorfismos tais que $id_{F_1} \circ i_1 = i_1$ e $id_{F_2} \circ i_2 = i_2$. Novamente da propriedade universal, existem únicos homomorfismos $\varphi_1 : F_1 \to F_2$ e $\varphi_2 : F_2 \to F_1$ tais que $\varphi_1 \circ i_1 = i_2$ e $\varphi_2 \circ i_2 = i_1$. Logo, $(\varphi_1 \circ \varphi_2) \circ i_2 = i_2$ e $(\varphi_2 \circ \varphi_1) \circ i_1 = i_1$, e assim a unicidade inicialmente apontada implica $\varphi_1 \circ \varphi_2 = id_{F_2}$ e $\varphi_2 \circ \varphi_1 = id_{F_1}$. Portanto $\varphi := \varphi_1 : F_1 \to F_2$ é isomorfismo, com $\varphi \circ i_1 = i_2$.



□

Devido ao Teorema 1.1.4, passaremos a tratar *do* Grupo Livre F sobre um conjunto X e, quando conveniente, consideraremos F como o conjunto das palavras reduzidas sobre X com a operação de justaposição.

A escolha da notação $i : X \to F$ também é sugestiva: como vimos na demonstração de existência, i é injetiva, e assim passamos a identificar X como subconjunto de F via $i : X \hookrightarrow F$. Com isso, é usual dizermos simplesmente que F é *o* Grupo Livre sobre X, omitindo a inclusão i. Ainda em tais considerações, dizemos que X é uma *base* do grupo F (ao invés da imagem $i(X)$). Passamos então a adotar a notação $F = F_X$ quando quisermos especificar o conjunto base.

Como sugerem a notação e a prova do Teorema 1.1.4, tem-se o seguinte:

Proposição 1.1.5. Se F é livre sobre X, então $\langle X \rangle = F$.

Demonstração. Segue direto da construção do grupo livre como o grupo das palavras reduzidas sobre X, e da sua unicidade a menos de isomorfismo.

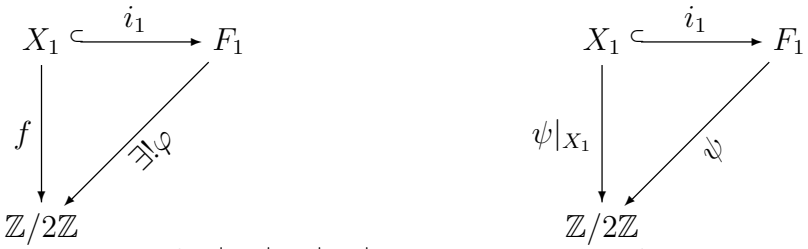
□

Note que a base de um grupo livre F nunca é única se $F \neq \{1\}$. De fato, se F é livre sobre X, então X^{-1} é também uma base de F, pois tanto X^{-1} gera F como grupo, quanto poderíamos ter tomado $j : X^{-1} \to F,\ x^{-1} \mapsto x^{-1} = (x^{-1}, \lambda, \ldots, \lambda, \ldots)$ na construção dada no Teorema 1.1.4 e feito a demonstração dali em diante substituindo X por X^{-1}. Assim, faz sentido indagarmos se ao menos o número de elementos das bases de F é invariante.

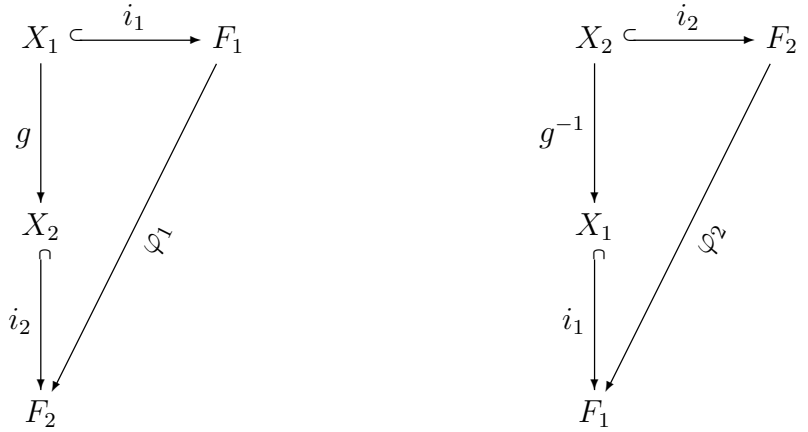
Proposição 1.1.6. Sejam X_1 e X_2 conjuntos finitos, (F_1, i_1) e (F_2, i_2) grupos livres sobre X_1 e X_2, respectivamente. Então $F_1 \cong F_2 \iff |X_1| = |X_2|$.

Demonstração. Denote $\mathrm{Hom}(A, B)$ o conjunto dos homomorfismos entre os grupos A e B.

Suponha F_1 e F_2 isomorfos. Da propriedade universal, para cada função $f : X \to \mathbb{Z}/2\mathbb{Z}$ existe um único homomorfismo $\varphi : F \to \mathbb{Z}/2\mathbb{Z}$ (que estende $X_1 \xhookrightarrow{i_1} F_1$). Por outro lado, todo homomorfismo $\psi : F_1 \to \mathbb{Z}/2\mathbb{Z}$ estende a restrição $\psi|_{X_1} : X_1 \to \mathbb{Z}/2\mathbb{Z}$, e pela propriedade universal, ψ é o único homomorfismo com tal propriedade. Logo, existe uma bijeção entre o conjunto de funções de X a $\mathbb{Z}/2\mathbb{Z}$ e o conjunto de homomorfismos de F_1 a $\mathbb{Z}/2\mathbb{Z}$, donde $|\operatorname{Hom}(F_1, \mathbb{Z}/2\mathbb{Z})| = |\{f : X_1 \to \mathbb{Z}/2\mathbb{Z} \mid f \text{ é função}\}| = 2^{|X_1|}$. Analogamente, $|\operatorname{Hom}(F_2, \mathbb{Z}/2\mathbb{Z})| = 2^{|X_2|}$. Como $F_1 \cong F_2$, tem-se $2^{|X_1|} = |\operatorname{Hom}(F_1, \mathbb{Z}/2\mathbb{Z})| = |\operatorname{Hom}(F_2, \mathbb{Z}/2\mathbb{Z})| = 2^{|X_2|}$. Portanto, $|X_1| = |X_2|$.



Reciprocamente, suponha $|X_1| = |X_2|$. Então existe uma bijeção $g : X_1 \to X_2$. Da propriedade universal, existe um único homomorfismo $\varphi_1 : F_1 \to F_2$ tal que $\varphi_1 \circ i_1 = i_2 \circ g$. Da mesma forma, existe um único homomorfismo $\varphi_2 : F_2 \to F_1$ tal que $\varphi_2 \circ i_2 = i_1 \circ g^{-1}$. Logo, $i_1 = \varphi_2 \circ (i_2 \circ g) = (\varphi_2 \circ \varphi_1) \circ i_1$, donde $\varphi_2 \circ \varphi_1 = id_{F_1}$, já que a identidade é o único homomorfismo que estende i_1. Analogamente, obtem-se $\varphi_1 \circ \varphi_2 = id_{F_2}$. Portanto, $F_1 \cong F_2$.



□

Tal resultado é válido também para bases infinitas [3, Proposição 6, p.12], cuja prova depende

do axioma da escolha, e a qual não abordaremos aqui. A invariância da cardinalidade da base nos permite estabelecer:

Definição 1.1.7. Dado F_X o grupo livre com base X, definimos $\text{posto}(F_X) = |X|$.

Dado qualquer conjunto, já garantimos a existência de um grupo livre sobre tal conjunto. Ampliamos agora nossa noção de grupo livre para grupos arbitrários.

Definição 1.1.8. Um grupo G é dito livre se existe um conjunto X tal que G é isomorfo ao grupo livre F_X.

As noções anteriormente estabelecidas apresentam-se de modo análogo. Se $\theta : F_X \to G$ é isomorfismo, dizemos que $\theta(X)$ é uma *base* para G, e que G é livre sobre $\theta(X)$. Novamente, G não possui uma única base se $G \neq \{1\}$ (basta considerar, por exemplo, automorfismos de G e as respectivas imagens da base). Porém, da Proposição 1.1.6, a cardinalidade das bases de G é invariante, e a bijeção nos dá $|\theta(X)| = |X|$. Dizemos então que $|X|$ é o *posto* de G. Assim como no caso do grupo livre, em que identificamos naturalmente a base $X \xhookrightarrow{i} F_X$, podemos, quando conveniente, identificar a base X como subconjunto de G por meio da aplicação injetiva $\theta \circ i : X \hookrightarrow G$.

Evidentemente, se G é um grupo livre, então G se comporta como o grupo das palavras *reduzidas* sobre sua base, no seguinte sentido: se F_X é livre sobre X com $\theta : F_X \to G$ isomorfismo, então todo elemento de G da forma $g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}$ é não-trivial, se $g_1, \ldots, g_k \in \theta(X)$ e $g_i^{\varepsilon_i} \neq (g_{i+1}^{\varepsilon_i+1})^{-1}$. Tal fato segue da construção dada no Teorema 1.1.4. Como consequência, subgrupos gerados por subconjuntos de uma base são também livres.

Proposição 1.1.9. Seja F_X grupo livre com base $X \subset F_X$. Se $Y \subseteq X$, então $\langle Y \rangle \leq F_X$ é livre com base Y.

Demonstração. Da observação acima, o único elemento trivial do conjunto de palavras reduzidas sobre X é a própria palavra vazia, e o mesmo vale para Y, já que $Y \subseteq X$. A construção do grupo livre sobre Y e a Proposição 1.1.5 garantem o resultado. □

A propriedade acima não se restringe somente a subgrupos gerados por elementos de uma base. Um resultado muito mais forte das teorias combinatória e geométrica de grupos, devido a J. Nielsen e O. Schreier, é valido. Citamo-lo a seguir. Referimos ao leitor [9, p. 22], para uma demonstração combinatória via o método do transversal de Schreier, ou [19, pp. 383-384] para uma demonstração geométrica utilizando ações de grupos sobre complexos e seus grupos fundamentais.

Teorema 1.1.10. Sejam F um grupo livre e $H \leq F$. Então H é livre e, se $[F : H]$ e $\text{posto}(F)$ são finitos, então

$$\text{posto}(H) = [F : H](\text{posto}(F) - 1) + 1.$$

Veremos em seguida mais algumas propriedades de grupos livres.

Definição 1.1.11. Uma palavra reduzida não-trivial $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \in F_X \backslash \{1\}$ é dita *ciclicamente reduzida* se $x_1^{\varepsilon_1} \neq (x_k^{\varepsilon_k})^{-1}$, isto é, a primeira letra de w não é inversa da última letra de w.

Observe que, se $w \in F_X \backslash \{1\}$ é ciclicamente reduzida então, para cada inteiro positivo n,

$$w^n = \underbrace{w \cdot w \cdot w \cdots w}_{\text{n termos}} = \underbrace{www \cdots w}_{\text{n termos}},$$

donde $l(w^n) = n \cdot l(w)$.

Proposição 1.1.12. Para cada palavra não trivial w em um grupo livre F_X, existem palavras $u, v \in F_X$ tais que v é ciclicamente reduzida e $w = uvu^{-1}$.

Demonstração. Seja $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k} \in F_X \backslash \{1\}$. Tem-se que

$$w^2 = w \cdot w = (x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}) \cdot (x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}).$$

Da definição de justaposição, existem $w_1, w_2, w_3 \in F_X$ subpalavras de w tais que simultaneamente $w = w_1 w_2$ e $w = w_2^{-1} w_3$, e ainda $w \cdot w = w_1 w_3$. Na notação $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}$, queremos dizer que existe $m \geq 0$ tal que

$$w^2 = w \cdot w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_{k-m}^{\varepsilon_{k-m}} x_{1+m}^{\varepsilon_{1+m}} \cdots x_{k-1}^{\varepsilon_{k-1}} x_k^{\varepsilon_k}.$$

Observe que $m = 0 \iff w$ é ciclicamente reduzida, e nesse caso basta tomar $u = 1$ e $v = w$. Caso contrário, como a subpalavra w_2 acima tem comprimento maximal, segue-se que $x_{k-m}^{\varepsilon_{k-m}} \neq (x_{1+m}^{\varepsilon_{1+m}})^{-1}$. Ponha então $u = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m}$ e $v = x_{1+m}^{\varepsilon_{1+m}} \cdots x_{k-m}^{\varepsilon_{k-m}}$. Por construção, v é ciclicamente reduzida, e deduz-se da equação acima que $w = uvu^{-1}$. □

Corolário 1.1.13. Todo grupo livre é *livre de torção*, isto é, o único elemento de ordem finita num grupo livre é o elemento neutro.

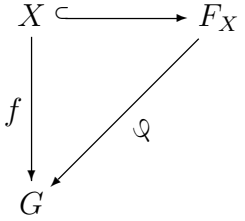
Demonstração. Seja F_X grupo livre com base X. Lembremos que, para qualquer $w \in F_X$, vale $l(w) = 0 \iff w = 1$. Com isso, dada $w \in F_X \backslash \{1\}$ arbitrária, basta provar que $l(w^n) > 0$, para todo inteiro positivo n. Pela Proposição 1.1.12, podemos escrever $w = uvu^{-1}$, no qual $v \in F_X \backslash \{1\}$ é ciclicamente reduzida e, em particular, $l(v) \geq 1$. Dessa forma,

$$w^n = \underbrace{(uvu^{-1}) \cdot (uvu^{-1}) \cdot (uvu^{-1}) \cdots (uvu^{-1})}_{\text{n termos}} = uv^n u^{-1}.$$

Logo, $l(w^n) \geq l(v^n) = n \cdot l(v) > n > 0$, ou seja, $w^n \neq 1$. □

Proposição 1.1.14. Todo grupo é quociente de um grupo livre.

Demonstração.



Seja G um grupo arbitrário e fixe X um conjunto qualquer para o qual existe uma bijeção $f : X \to G,\ x_g \mapsto g \in G$. Considere então F_X o grupo livre com base X. Pela propriedade universal, existe um homomorfismo $\varphi : F_X \to G$ que estende f. Como f é bijeção, φ é sobrejetiva. Logo, pelo Teorema do Isomorfismo, $F_X / \ker(\varphi) \cong \mathrm{Im}(\varphi) = G$.

□

1.2 Geradores e Relações

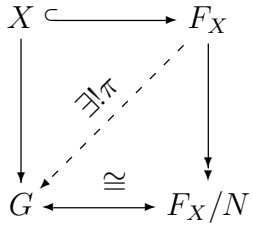
Estabeleceremos nesta seção as propriedades definidoras de um grupo, previamente mencionadas, que conduzem a uma noção geral de apresentações de grupos. Uma definição simples de geradores e relações, aqui adotada, é dada em Rotman [19]. Propriedades e exemplos adicionais podem ser encontrados em Cohen [3], Johnson [9] e Magnus-Karrass-Solitar [13].

A Proposição 1.1.14 nos permite estabelecer a definição formal de geradores e relações em um grupo arbitrário, que determinam completamente tal grupo como o "mais livre possível" restrito às condições (relações) dadas.

Recordamos o leitor que, dados H um grupo e $S \subset H$, o subgrupo $K = \langle S^H \rangle$ gerado pelos conjugados de elementos[2] de S é o menor subgrupo normal de H que contem o conjunto S.

Definição 1.2.1. Dados G um grupo, X um conjunto e $R \subset F_X$ um subconjunto do grupo livre com base X, dizemos que o par (X, R) é uma *apresentação* do grupo G quando $G \cong F_X/N$, no qual $N = \langle R^{F_X} \rangle$. Nesse caso, os elementos de X são ditos os *geradores*, e os elementos de R são ditas as *relações* na apresentação dada.
Equivalentemente, dados G um grupo, X um conjunto e $\pi : F_X \twoheadrightarrow G$ um epimorfismo do grupo livre com base X sobre G, dizemos que π é uma *apresentação* de G. Nesse caso, tomando-se um subconjunto $R \subset F_X$ tal que $\ker \pi = \langle R^{F_X} \rangle$, retorna-se à notação acima e diz-se que o par (X, R) é uma apresentação de G.

É comum denotar-se $G = \langle X \mid R \rangle$ para dizer que (X, R) é uma apresentação de G. Outra notação comum é identificar os elementos $r \in R$ por equações $r = 1$ na apresentação $G = \langle X \mid R = 1 \rangle$. Tal notação é conveniente em certos contextos devido ao epimorfismo $\pi : F_X \to G$ com $\ker(\pi) = N = \langle R^{F_X} \rangle$ pois, no grupo quociente $F_X/N \cong G$, os elementos $r \in R$ são todos triviais, isto é, $rN = N = 1_{F_X/N} = 1_G$.



Ainda em tais considerações, podemos identificar uma relação da forma $uv^{-1} \in R$ tanto por uma equação $uv^{-1} = 1$ quanto por uma equação $u = v$. Quando nenhuma relação é dada, isto é, caso $R = \varnothing$, costuma-se denotar $G = \langle X \mid \rangle$. Em diferentes contextos pode ser também conveniente utilizar a definição via epimorfismo, isto é, dizer que $\pi : F_X \twoheadrightarrow G$ é uma apresentação de G, para explicitar possíveis contas ou resultados.

Sem maiores comentários, utilizaremos qualquer uma das notações dadas, quando for conveniente.

Exemplo 1.2.2. $(X, \varnothing)$ é uma apresentação do grupo livre F_X. Tais grupos são os únicos a admitirem apresentações sem relações.

[2] Alguns autores denotam $K = \langle S \rangle^H$.

Exemplo 1.2.3. $\langle x \mid x = 1\rangle$ é uma apresentação do grupo trivial.

Exemplo 1.2.4. $\mathbb{Z}/\mathbb{Z}_n = \langle x \mid x^n\rangle$ é uma apresentação do grupo cíclico de ordem n.

Exemplo 1.2.5. $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, (xy)^2 = 1\rangle$ é uma apresentação do grupo diedral de ordem $2n$.

Exemplo 1.2.6. Se $G = \langle X \mid R\rangle$ e $H = \langle Y \mid S\rangle$, então o produto direto é dado por $G \times H = \langle X \cup Y \mid R \cup S \cup \{[x, y] \ : \ x \in X, y \in Y\}\rangle$ e o produto livre é dado por $G * H = \langle X \cup Y \mid R \cup S\rangle$.

Trabalhemos um pouco mais na Definição 1.2.1. Seria tentador identificar o conjunto de geradores X como subconjunto do grupo $G = \langle X \mid R\rangle$. Porém, sendo $\pi : F_X \twoheadrightarrow G$ uma apresentação de G, não necessariamente a aplicação $f = \pi|_X : X \subset F_X \to G$ é injetiva. Assim, contextualmente, pode ser mais seguro tratar da *família de geradores* $\{\pi(x)\}_{x\in X}$ de G. Não somente isso, mas o fato de ser $R \subset F_X$ nos dá a possibilidade de acrescentar relações *redundantes* na apresentação dada, no seguinte sentido: sendo $G = \langle X \mid R\rangle$, é possível que exista $S \subset F_X$ tal que $G = \langle X \mid R \cup S\rangle$ também.

Exemplo 1.2.7. Considere $G = \langle x, y \mid x^n y^{-n-1},\ xyxy^{-1}x^{-1}y^{-1}\rangle = \langle x, y \mid x^n = y^{n+1},\ xyx = yxy\rangle$. A segunda relação nos dá $(xy)x(xy)^{-1} = y$, e assim $y^n = ((xy)x(xy)^{-1})^n = (xy)x^n(xy)^{-1}$. Substituindo duas vezes a primeira relação, obtem-se $y^n = xyy^{n+1}y^{-1}x^{-1} = xy^{n+1}x^{-1} = xx^nx^{-1} = x^n$. De volta na primeira relação, conclui-se que $y = 1$, e assim a segunda relação implica $x = 1$. Portanto G é o grupo trivial.

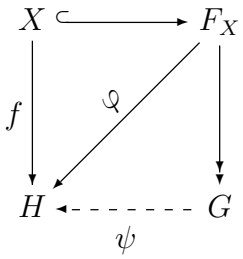
Exemplo 1.2.8. Sejam $n \in \mathbb{N}$ e $R = \bigcup_{k\in\mathbb{N}}\{x^{kn}\} \subset F_{\{x\}}$, e considere $G = \langle x \mid R\rangle$. Note que G é um grupo cíclico. Agora, a primeira relação de R é dada por $x^n = 1$, e assim $x^{kn} = 1$ para todo $k \in \mathbb{N}$. Dessa forma, os elementos não-triviais de G são aqueles de ordem menor ou igual a $n - 1$. Portanto $G \cong \mathbb{Z}/n\mathbb{Z}$.

Exemplo 1.2.9. Seja $G = \langle x, y \mid x^3,\ y^2,\ x^{-1}y^{-1}xy\rangle$. A última relação nos mostra que G é um grupo abeliano, e assim todo elemento $g \in G$ é da forma $g = x^n y^m$, para $n, m \in \mathbb{Z}$. Deduz-se então das duas primeiras relações que os elementos não-triviais de G são $x,\ x^2,\ y,\ xy$ e x^2y, de modo que $|G| = 6$. Verifica-se que G é o grupo cíclico gerado pelo elemento xy, cuja ordem é 6. Portanto, $G \cong \mathbb{Z}/6\mathbb{Z}$.

A propriedade intuitiva de ser $G = \langle X \mid R\rangle$ o "grupo mais livre possível" gerado por X e sujeito às condições (relações definidoras) determinadas por R pode ser formalizada no seguinte teorema, devido a W. von Dyck.

Teorema 1.2.10. (von Dyck) Seja $G = \langle X \mid R\rangle = F_X/N$, no qual $N = \langle R^{F_X}\rangle$. Sejam ainda H um grupo, $f : X \to H$ função e $\varphi : F_X \to H$ o homomorfismo que estende f. Se $R \subset \ker(\varphi)$, então existe um homomorfismo $\psi : G \to H$ tal que $\psi(xN) = f(x),\ \forall x \in X$. Mais ainda, ψ é sobrejetiva se $H = \langle f(X)\rangle$.

Demonstração. O teorema é consequência do seguinte resultado algébrico clássico: Se $\delta : A \to B$ é homomorfismo e $\pi : A \to C$ é epimorfismo, então ($\ker\pi \subseteq \ker\delta \implies \exists!\theta : C \to B$ homomorfismo tal que $\theta \circ \pi = \delta$).



Pelo comentário acima basta mostrar que $N \subset \ker(\varphi)$. Tem-se $N = \langle R \rangle^{F_X} = \{grg^{-1} \mid g \in F_X,\ r \in R\}$. Dado então $n = grg^{-1} \in N$, tem-se que $\varphi(n) = \varphi(grg^{-1}) = \varphi(g)\varphi(r)\varphi(g)^{-1}$. Como $R \subset \ker(\varphi)$, por hipótese, segue-se que $\varphi(n) = \varphi(g)\varphi(g)^{-1} = 1_H$. Logo, $N \subset \ker(\varphi)$. Agora, se $H = \langle f(X) \rangle$, é imediato que ψ é sobrejetora, já que o conjunto $\{xN \mid x \in X\}$ gera o grupo G e $\psi(xN) = f(x)$, $\forall x \in X$.

□

Corolário 1.2.11. Sejam $G = \langle X \mid R \rangle$, Y conjunto arbitrário e $S \subset F_{X \cup Y}$ qualquer. Denote $N = \langle R^{F_X} \rangle$ e $\widehat{N} = \langle (R \cup S)^{F_{X \cup Y}} \rangle$. Então existe um homomorfismo $\psi : G \to H = \langle X \cup Y \mid R \cup S \rangle$ que "fixa" X, isto é, $\psi(xN) = x\widehat{N}$, $\forall x \in X$.

Demonstração. Basta tomar f a composição $X \hookrightarrow X \cup Y \hookrightarrow F_{X \cup Y} \twoheadrightarrow H$, $\varphi : F_X \to H$ o homomorfismo que estende f e aplicar o Teorema de von Dyck. □

1.3 Grupos Finitamente Apresentáveis

Encerraremos este capítulo com o caso particular de nosso interesse, o de apresentações finitas.

Definição 1.3.1. Um grupo G é dito *finitamente apresentável* quando admite alguma apresentação $G = \langle X \mid R \rangle$ tal que X e R são ambos finitos.

Evidentemente, todo grupo finito é finitamente apresentável, pois basta tomar o conjunto das relações como o conjunto induzido pela tabela de multiplicação do grupo, e os geradores como todos os elementos do grupo. Porém, à medida que a ordem do grupo aumenta, a apresentação dada pela tabela de multiplicação torna-se muito carregada, o que dificulta inferir propriedades do grupo. Mesmo apresentações finitas de grupos de ordem pequena, como no Exemplo 1.2.7, podem não fornecer tão trivialmente informações sobre o grupo.

Em todo caso, é natural considerar conveniente trabalhar com a menor quantidade possível de relações. Evidência disso é a própria definição de apresentação como um epimorfismo $\pi : F_X \twoheadrightarrow G$, pois quanto menos relações tivermos, mais "próximo" o quociente G será do grupo livre F_X, que por sua vez é um objeto bastante conhecido. Veremos mais adiante condições que estimam a quantidade de relações numa apresentação, a partir do número de geradores. Tal estimativa relaciona-se à desigualdade de Golod-Šafarevič [7]. Uma das implicações do Teorema a ser provado é que, caso seja "pequeno" o número de relações (no sentido a ser apresentado), o grupo será "grande" (no sentido de admitir certos quocientes infinitos).

Em geral, o problema de se determinar se um dado grupo é finitamente apresentável é difícil. Por outro lado, há algumas situações favoráveis – como as dadas abaixo, de subgrupos e extensões – nas quais há condições simples para resolver tal problema.

Proposição 1.3.2. Sejam $G = \langle X \mid R \rangle$ um grupo finitamente apresentável com $|X| = d$ e $|R| = r$, e $H \leq G$ um subgrupo com índice finito n. Então H admite apresentação finita com $d_1 = n(d-1)+1$ geradores e $r_1 = nr$ relações.

Demonstração. Denote $F = F_X$, $\pi : F \twoheadrightarrow G$ o epimorfismo proveniente da apresentação $G = \langle X \mid R\rangle \cong F/N$, $\ker\pi = N = \langle R^F\rangle$. Defina $F_1 = \pi^{-1}(H) \leq F$. Tem-se posto$(F_1) = d_1$ e $[F : F_1] = [G : H] = n$. Pelo Teorema 1.1.10, F_1 é grupo livre e vale $d_1 = n(d-1)+1$.

Como o índice de F_1 em F é $n < \infty$, podemos tomar $T = \{t_1, \ldots, t_n\}$ conjunto finito de F tal que $F = \cup_{i=1}^n t_i F_1$. Denote $R = \{u_1, \ldots, u_r\}$. Para cada $f \in F$, existe (único) j tal que $f \in t_j F_1$, digamos $f = t_j\tilde{f}$. Com isso, $f^{-1}u_i f = \tilde{f}^{-1}t_j^{-1}u_i t_j\tilde{f} \in \{t_j^{-1}u_i t_j\}^{F_1}$. Logo, $R \subseteq \ker\pi = \pi^{-1}(\{1\}) \subset \pi^{-1}(H) = F_1$. Mais ainda, $\langle R^F\rangle = \langle(\cup_{j=1}^n R^{t_j})^{F_1}\rangle$, de modo que o conjunto $R_0 = \cup_{j=1}^n R^{t_j}$ gera o núcleo da restrição $\pi_1 = \pi|_{F_1} : F_1 \twoheadrightarrow H$. Logo, $r_1 = |R_0| = \sum_{j=1}^n |R^{t_j}| = n \cdot |R| = nr$. □

Proposição 1.3.3. Sejam G um grupo e $K \triangleleft G$. Se K e G/K são finitamente apresentáveis, então G é finitamente apresentável.

Demonstração. Sejam $\alpha : F_X \twoheadrightarrow K$ e $\beta : F_Y \twoheadrightarrow G/K$ apresentações finitas de K e G/K com $\ker\alpha = \langle R^{F_X}\rangle$ e $\ker\beta = \langle S^{F_Y}\rangle$. Sem perda de generalidade, suponha $X \cap Y = \varnothing$. Considere então $F = F_{X\cup Y}$ o grupo livre com base $X \cup Y$. Identificaremos aqui $F_X \hookrightarrow F$ e $F_Y \hookrightarrow F$, e portanto $R, S \subset F$.

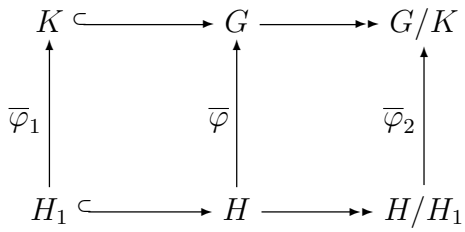
Para cada $y_j \in Y$, fixe $g_j \in G$ tal que $g_j K = \beta(y_j)$. Defina $f : X \cup Y \to G$ a função tal que $f(x_i) = \alpha(x_i)$ e $f(y_j) = g_j$, $\forall x_i \in X$, $y_j \in Y$. Da propriedade universal do grupo livre, existe um único homomorfismo $\varphi : F \to G$ tal que $\varphi|_{X\cup Y} = f$ e, por construção, φ é sobrejetiva. Afirmamos que existe $T \subset F$ finito tal que $\ker\varphi = \langle T^F\rangle$, o que implicará o resultado.

Dado $s_l \in S$ arbitrário, existe $t_l \in F_X \leq F$ tal que $\varphi(s_l) = \varphi(t_l)$, pois $\varphi(s_l)K = \beta(s_l) = 1_{G/K}$, isto é, $\varphi(s_l) \in K = \operatorname{Im}\alpha$. Analogamente, para quaisquer $y_j \in Y$, $x_i \in X$, existe $u_{ij} \in F_X \leq F$ tal que $\varphi(y_j^{-1}x_i y_j) = \varphi(u_{ij})$, pois $\varphi(y_j^{-1}x_i y_j)K = (\beta(y_j)^{-1}\alpha(x_i)\beta(y_j))K = 1_{G/K} = K$, já que $\alpha(x_i) \in K$ e K é normal em G. Definamos então $\widetilde{S} = \{t_l^{-1}s_l \mid s_l \in S\}$, $\widetilde{T} = \{u_{ij}^{-1}y_j^{-1}x_i y_j \mid x_i \in X,\ y_j \in Y\}$ e $T = R \cup \widetilde{S} \cup \widetilde{T}$, e denote $N = \langle T^F\rangle$.

Seja $H = \langle X \cup Y \mid T\rangle = F/N$. Por simplicidade, identifiquemos X e Y com suas imagens em $F/N = H$. Por construção, $N \subseteq \ker\varphi$, e assim podemos considerar $\overline{\varphi}$ o epimorfismo induzido por φ em $\overline{\varphi} : H \to G$, notando que $\overline{\varphi}$ satisfaz $\overline{\varphi}(x_i) = \alpha(x_i)$ e $\overline{\varphi}(y_j) = g_j$, $\forall x_i \in X$, $y_j \in Y$. Considere agora $H_1 = \langle X\rangle \leq H$ o subgrupo de H gerado pela imagem de X em H. Como $T \supset R$, as relações R que definem a apresentação $K = \langle X \mid R\rangle$ são todas válidas em $H = \langle X \cup Y \mid T\rangle$, o que implica que $\overline{\varphi}_1 := \overline{\varphi}|_{H_1} : H_1 \to K$ é isomorfismo. Mais ainda, vale que $\overline{\varphi}_1(h) = \alpha(x_1^{\varepsilon_1}\cdots x_m^{\varepsilon_m})$, para todo $h \in H_1 = \langle X\rangle$ escrito como palavra reduzida $h = x_1^{\varepsilon_1}\cdots x_m^{\varepsilon_m}$ sobre $X \subset F_X \leq F$.

Agora, como as relações na apresentação $H = \langle X \cup Y \mid T\rangle$ incluem $\widetilde{T} = \{u_{ij}^{-1}y_j^{-1}x_i y_j \mid x_i \in X,\ y_j \in Y\} \subset T$, segue-se que $H_1 = \langle X\rangle \leq H$ é normal, pois os elementos $u_{ij} \in \widetilde{T}$ foram escolhidos em $F_X \leq F$, i.e., são palavras reduzidas sobre X. Podemos considerar então o quociente H/H_1. Como, por construção, vale que $\overline{\varphi}(H_1) \subseteq L$, induz-se um epimorfismo $\overline{\varphi}_2 : H/H_1 \to G/K$ tal que $\overline{\varphi}_2(hH_1) = \overline{\varphi}(h)K$. Mas, nesse caso, as relações S que definem a apresentação $G/K = \langle Y \mid S\rangle$ são todas válidas em $H/H_1 = \frac{\langle X\cup Y \mid T\rangle}{\langle X\rangle}$, pois $\overline{\varphi}(x_i) = \alpha(x_i)$ e $\overline{\varphi}(y_j) = g_j$ $\forall x_i \in X$, $y_j \in Y$. Isso significa que $\overline{\varphi}_2 : H/H_1 \to G/K$ é isomorfismo.

Em outras palavras, construímos o diagrama comutativo



no qual os homomorfismos nas linhas são as inclusões e projeções naturais, respectivamente, e os dois homomorfismos nos extremos são isomorfismos. Logo, o homomorfismo $\overline{\varphi}$ é bijetivo, ou seja, $G \cong H = \langle X \cup Y \mid T \rangle$. □

Como vimos na seção anterior, mesmo grupos finitos podem ter apresentações infinitas, com elementos redundantes no conjunto de geradores ou no conjunto de relações. Convém também questionar se a noção de finitamente apresentável está bem-definida, no sentido de que toda apresentação de um grupo finitamente apresentável deveria poder ser "transformada" numa apresentação finita. Veremos mais adiante que sim.

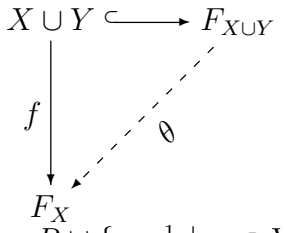
O Corolário 1.2.11 do Teorema de von Dyck fornece uma formalização do que ocorre ao adicionarmos relações à apresentação de um grupo: se não adicionarmos geradores, obtemos um quociente da apresentação original; por outro lado, podemos construir subgrupos da apresentação se pudermos (no quociente do grupo livre) "fixar injetivamente" subconjuntos dos geradores, restritos às relações dadas. Como vimos no Exemplo 1.2.8, tal processo pode resultar num isomorfismo. Isso significa que podemos tanto adicionar relações *redundantes* a uma apresentação (Exemplo 1.2.8), quanto remover geradores (Exemplo 1.2.7), ou ainda modificar o conjunto gerador (Exemplo 1.2.9). Vejamos agora maneiras de passar de uma apresentação a outra.

Notemos que se $G = \langle X \mid R \rangle$ e $S \subset N = \langle R^{F_X} \rangle$ é qualquer, então vale ainda $G = \langle X \mid R \cup S \rangle$, já que relações acrescidas por S em nada influenciam no quociente $F_X/N \cong G$. Estabelece-se a

Definição 1.3.4. Dizemos que uma apresentação $\langle X \mid R \cup S \rangle$ vem da apresentação $\langle X \mid R \rangle$ via uma *transformação geral de Tietze do tipo I* quando $S \subset N = \langle R^{F_X} \rangle$. Nas mesmas condições, dizemos que $\langle X \mid R \rangle$ vem de $\langle X \mid R \cup S \rangle$ via uma *transformação geral de Tietze do tipo I'*. Nesse caso, ambas apresentam o mesmo grupo, isto é, $\langle X \mid R \rangle = \langle X \mid R \cup S \rangle$.

Trabalhemos agora no caso de apresentações às quais são adicionados novos geradores. Considere novamente uma apresentação $G = \langle X \mid R \rangle$ e seja Y conjunto tal que $X \cap Y = \varnothing$. Com isso, para cada elemento de Y podemos fixar um único elemento de F_X, definindo-se uma aplicação injetiva $\iota : Y \to F_X,\ y \mapsto g_y$. Nessa notação, defina $S = \{y g_y^{-1} \mid y \in Y\} \subset F_{X \cup Y}$ (aqui, estamos identificando $F_X \hookrightarrow F_{X \cup Y}$, e assim $R \subset R \cup S \subset F_{X \cup Y}$). Afirmamos que $H = \langle X \cup Y \mid R \cup S \rangle$ é também uma apresentação de G. Para ver isso, construiremos um epimorfismo $\beta : H \twoheadrightarrow G$ e um homomorfismo $\alpha : G \to H$ tais que $\alpha \circ \beta = id_H$, o que implicará que β é injetiva e, portanto, isomorfismo.

Denote $N = \langle R^{F_X} \rangle$ e $\widehat{N} = \langle (R \cup S)^{F_{X \cup Y}} \rangle$, $\varphi : F_X \to F_X/N \cong G$ e $\psi : F_{X \cup Y} \to F_{X \cup Y}/\widehat{N} \cong H$

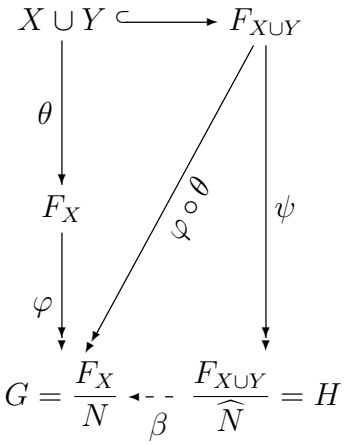


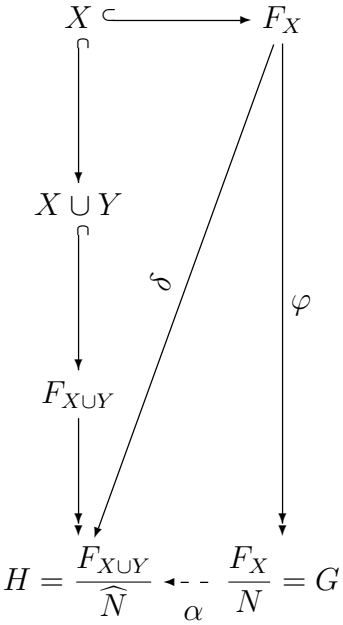
as projeções canônicas. Defina uma função $f : X \cup Y \to F_X$ de modo que $f(x) = x$ e $f(y) = g_y$, $\forall x \in X, y \in Y$. Pela propriedade universal do grupo livre, existe um único homomorfismo $\theta : F_{X\cup Y} \to F_X$ que estende f, e assim $\theta(x) = x$, $\theta(y) = g_y$, $\forall x \in X$, $y \in Y$. Tem-se portanto um epimorfismo $\varphi \circ \theta : F_{X\cup Y} \to F_X/N$, já que $F_X/N = \langle \{xN\}_{x\in X} \rangle = \langle \{\varphi \circ \theta(x)\}_{x\in X} \rangle$. Veja agora que $R \cup S = R \cup \{yg_y^{-1} \mid y \in Y\} \subset \ker(\varphi \circ \theta)$, pois para quaisquer $r \in R \subset F_X \subset F_{X\cup Y}$, $y \in Y$ e $g_y \in F_X \subset F_{X\cup Y}$ tem-se

$$\varphi \circ \theta(r) = \varphi(r) = rN = N = 1 \in F_X/N,$$

$$\varphi \circ \theta(yg_y^{-1}) = \varphi(\theta(y)\theta(g_y)^{-1}) = \varphi(g_y)\varphi(g_y)^{-1} = 1 \in F_X/N,$$

já que θ fixa X e leva y em g_y. Logo, pelo Teorema 1.2.10, existe um epimorfismo $\beta : F_{X\cup Y}/\widehat{N} \twoheadrightarrow F_X/N$ tal que $\beta(x\widehat{N}) = xN$, $\forall x \in X$.





Por outro lado, pela propriedade universal do grupo livre, a inclusão de X em $X \cup Y \subset F_{X\cup Y}$ e a projeção $F_{X\cup Y} \xrightarrow{\psi} F_{X\cup Y}/\widehat{N}$ induzem um (único) homomorfismo $\delta : F_X \to F_{X\cup Y}/\widehat{N}$ tal que $\delta(x) = x\widehat{N}$, $\forall x \in X$. Tem-se que $R \subset \ker(\delta) \subset F_X$, pois como δ fixa X e $R \subset \langle (R \cup S)^{F_{X\cup Y}} \rangle = \widehat{N}$, vale $\delta(r) = r\widehat{N} = \widehat{N} = 1 \in F_{X\cup Y}/\widehat{N}$. Mais uma vez, o Teorema 1.2.10 nos garante que existe $\alpha : F_X/N \to F_{X\cup Y}/\widehat{N}$ tal que $\alpha(xN) = x\widehat{N}$, $\forall x \in X$. Mostremos que $\alpha \circ \beta = id : F_{X\cup Y}/\widehat{N} \to F_{X\cup Y}/\widehat{N}$. Já vimos que para qualquer $x \in X$, $\alpha \circ \beta(x\widehat{N}) = \alpha(xN) = x\widehat{N}$. Agora, para todo $y \in Y$ tem-se $y\widehat{N} = g_y\widehat{N}$, pois $yg_y^{-1} \in S \subset \langle (R \cup S)^{F_{X\cup Y}} \rangle = \widehat{N}$. Logo, para todo $y \in Y$, tem-se $\alpha \circ \beta(y\widehat{N}) = \alpha \circ \beta(g_y\widehat{N}) = \alpha(g_yN) = g_y\widehat{N}$. Ou seja, $\alpha \circ \beta$ fixa todos os elementos geradores de $F_{X\cup Y}/\widehat{N}$, donde $\alpha \circ \beta = id$, como queríamos. Com isso, podemos estabelecer a seguinte:

Definição 1.3.5. Dizemos que uma apresentação $\langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y\in Y}\rangle$ vem da apresentação $\langle X \mid R\rangle$ via uma *transformação geral de Tietze do tipo II* quando $X \cap Y = \varnothing$. Nas mesmas condições, dizemos que $\langle X \mid R\rangle$ vem de $\langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y\in Y}\rangle$ via uma *transformação geral de Tietze do tipo II'*. Nesse caso, ambas apresentam o mesmo grupo, isto é, $\langle X \mid R\rangle \cong \langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y\in Y}\rangle$.

Estamos finalmente em condições de relacionar apresentações distintas de um mesmo grupo.

Teorema 1.3.6. Dada uma apresentação de um grupo, qualquer outra apresentação do mesmo grupo pode ser obtida da primeira via uma sequência de transformações gerais de Tietze.

Demonstração. Sejam $\langle X \mid R\rangle$ e $\langle Y \mid S\rangle$ apresentações de um mesmo grupo G. Suponhamos inicialmente que $X \cap Y = \varnothing$. Denote $N_R = \langle R^{F_X}\rangle$ e $N_S = \langle S^{F_Y}\rangle$, e considere as projeções canônicas $\varphi : F_X \twoheadrightarrow F_X/N_R = G$, $\psi : F_Y \twoheadrightarrow F_Y/N_S = G$. Para cada $y \in Y$, escolha $g_y \in F_X$ tal que $\psi(y) = \varphi(g_y)$, e para cada $x \in X$, escolha $h_x \in F_Y$ tal que $\varphi(x) = \psi(h_x)$. Note que, pela construção dada anteriormente, $\langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y\in Y}\rangle$ também é uma apresentação de G, obtida de $\langle X \mid R\rangle$ via uma transformação geral de Tietze do tipo II. Denote $\widehat{N}_R = \langle (R \cup \{yg_y^{-1}\}_{y\in Y})^{F_{X\cup Y}}\rangle$ e $\theta : F_{X\cup Y} \twoheadrightarrow F_{X\cup Y}/\widehat{N}_R = G$. Agora, para quaisquer $x \in X,\ y \in Y$, tem-se $\theta(x) = \varphi(x)$ e $1 = \theta(yg_y^{-1})$, donde $\theta(y) = \theta(g_y) = \varphi(g_y)$, já que $g_y \in R \subset F_X \subset F_{X\cup Y}$. Mas, por construção, $\psi(y) = \varphi(g_y) = \theta(y)$, de modo que $\theta(h) = \psi(h),\ \forall h \in F_Y$. Assim, $\theta(s) = \psi(s) = 1,\ \forall s \in S \subset N_S \subset F_Y$, pois $F_Y/N_S = G = F_{X\cup Y}/\widehat{N}_R$. Mais ainda, para qualquer $x \in X$ e o correspondente $h_x \in F_Y$, vale $\theta(h_x) = \psi(h_x) = \varphi(x) = \theta(x)$, ou seja, $\theta(xh_x^{-1}) = 1$. Com isso conclui-se que os conjuntos S e $\{xh_x^{-1}\}_{x\in X}$ estão contidos em $\widehat{N}_R$. Logo,

$$\langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y\in Y} \cup S \cup \{xh_x^{-1}\}_{x\in X}\rangle$$

é ainda uma apresentação de G, obtida da apresentação $G = \langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y\in Y}\rangle$ via uma transformação geral de Tietze do tipo I. Por raciocínio análogo, $\langle X \cup Y \mid S \cup \{xh_x^{-1}\}_{x\in X}\rangle$ é uma apresentação de G obtida de $G = \langle Y \mid S\rangle$ via uma transformação geral de Tietze do tipo II, e

$$\langle X \cup Y \mid S \cup \{xh_x^{-1}\}_{x\in X} \cup R \cup \{yg_y^{-1}\}_{y\in Y}\rangle$$

é uma apresentação de G obtida de $G = \langle X \cup Y \mid S \cup \{xh_x^{-1}\}_{x\in X}\rangle$ via uma transformação geral de Tietze do tipo I.

Portanto, $\langle Y \mid S\rangle$ é obtida de $\langle X \mid R\rangle$ via uma sequência de transformações gerais de Tietze do tipo II, tipo I, tipo I' e tipo II', respectivamente.

Suponhamos agora que $X \cap Y \neq \varnothing$. Tome $\widetilde{X}$ um conjunto tal que $|\widetilde{X}| = |X|$, com uma bijeção $x \mapsto \tilde{x}$, e com $\widetilde{X} \cap Y = \varnothing = \widetilde{X} \cap X$. Induz-se assim uma bijeção $R \to \widetilde{R}$, $r \mapsto \tilde{r}$ e um grupo $\widetilde{G} = \langle \widetilde{X} \mid \widetilde{R}\rangle$. Tem-se $\widetilde{G} \cong G$, de modo que $\langle \widetilde{X} \mid \widetilde{R}\rangle$ também é uma apresentação de G. Como $\widetilde{X} \cap Y = \varnothing = \widetilde{X} \cap X$, aplicando-se o raciocínio usado no caso anterior, segue-se que $\langle \widetilde{X} \mid \widetilde{R}\rangle$ vem de ambas $\langle X \mid R\rangle$, $\langle Y \mid S\rangle$ via sequências de transformações gerais de Tietze, e portanto $\langle Y \mid S\rangle$ vem de $\langle X \mid R\rangle$ via uma sequência de transformações gerais de Tietze. □

Proposição 1.3.7. Sejam G um grupo finitamente gerado e $X \subset G$ conjunto gerador qualquer de G. Então existe subconjunto finito $Y \subset X$ tal que G é gerado por Y.

Demonstração. Sendo G finitamente gerado, existe $Z \subset G$ finito tal que $G = \langle Z \rangle$. Mas cada $z \in Z$ pode ser escrito da forma $z = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$, no qual $\varepsilon_i \in \{-1, 0, 1\},\ \forall i$. Como Z é finito, existe um subconjunto finito $Y \subset X$ tal que $Z \subset \langle Y \rangle$, e assim $G = \langle Y \rangle$. □

Proposição 1.3.8. Sejam G um grupo finitamente apresentável e $\langle X \mid R \rangle,\ \langle Y \mid S \rangle$ apresentações de G. Se $X,\ R$ e Y são todos conjuntos finitos, então existe $T \subseteq S$ tal que $G = \langle Y \mid T \rangle$.

Demonstração. Lembremos que $S \subset \langle R^{F_X} \rangle$ implica que $G = \langle X \mid R \cup S \rangle = \langle X \mid R \rangle$, e que $X \cap Y = \varnothing$ implica que $G = \langle X \mid R \rangle = \langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y \in Y} \rangle = \langle X \cup Y \mid S \cup \{xh_x^{-1}\}_{x \in X} \rangle = \langle Y \mid S \rangle$.

Sem perda de generalidade, suponha que $X \cap Y = \varnothing$. Aplicando transformações de Tietze do tipo II, obtem-se $G = \langle X \mid R \rangle = \langle X \cup Y \mid R \cup \{yg_y^{-1}\}_{y \in Y} \rangle = \langle X \cup Y \mid S \cup \{xh_x^{-1}\}_{x \in X} \rangle = \langle Y \mid S \rangle$. Isso significa que $s = 1_G$ e $xh_x^{-1} = 1_G$ para quaisquer $s \in S$ e $x \in X$, de modo que $\{xh_x^{-1}\}_{x \in X} \subset \langle (R \cup \{yg_y^{-1}\}_{y \in Y})^{F_{X \cup Y}} \rangle$. Logo, via transformações de Tietze do tipo I, vem $G = \langle X \cup Y \mid R_1 \cup \{xh_x^{-1}\}_{x \in X} \rangle$, no qual $R_1 = \{yg_y^{-1}\}_{y \in Y} \cup R$. Note que $|\{xh_x^{-1}\}_{x \in X}|$ e $|\{yg_y^{-1}\}_{y \in Y}|$ são finitos, pois X e Y são finitos.

Agora, $R \subset F_X \subset F_{X \cup Y}$ e $\{yg_y^{-1}\}_{y \in Y} \subset F_X \subset F_{X \cup Y}$, de modo que para cada $r \in R$ e g_y podemos escrever $r = a_1^{\varepsilon_1} \cdots a_k^{\varepsilon_k}$ e $g_y = b_1^{\delta_1} \cdots b_l^{\delta_l}$, no qual $a_i, b_j \in X$. Defina $R_2 \subset F_{X \cup Y}$ um conjunto com a mesma cardinalidade de R_1, obtido por substituir-se em cada palavra $w \in R_1$ as (possíveis) letras $x \in X$ pelos seus elementos $h_x \in F_Y \subset F_{X \cup Y}$ correspondentes. Com isso queremos dizer que, se $w_1 \in R_1$ é da forma $w_1 = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$ ou $w_1 = yg_y^{-1} = y \cdot b_l^{-\delta_l} \cdots b_1^{-\delta_1},\ x_i, b_j \in X$, então o correspondente $w_2 \in R_2$ é da forma $w_2 = (h_{x_1})^{\varepsilon_1} \cdots (h_{x_k})^{\varepsilon_k}$ ou $w_2 = y \cdot (h_{b_l})^{-\delta_l} \cdots (h_{b_1})^{-\delta_1}$, respectivamente.

Como $xh_x^{-1} = 1_G$ para todo $x \in X$, vale que $w_1 w_2^{-1} = 1_G$ para qualquer $w_1 \in R_1$ e seu correspondente $w_2 \in R_2$. Isso signinfica que os conjuntos R_1 e R_2 representam as mesmas relações em G, donde $G = \langle X \cup Y \mid R_2 \cup \{xh_x^{-1}\}_{x \in X} \rangle$. Mas $h_x \in F_Y \subset F_{X \cup Y}$ para todo $x \in X$, donde $R_2 \subset F_Y$. Logo, via transformações de Tietze do tipo II', $G = \langle Y \mid R_2 \rangle$.

Por serem R e $\{yg_y^{-1}\}_{y \in Y}$ finitos, segue-se que R_1 é finito e portanto R_2 também é finito. Sendo $\langle Y \mid S \rangle = G = \langle Y \mid R_2 \rangle$, valem $R_2 \subset \langle S^{F_Y} \rangle = \langle \{hsh^{-1} \mid s \in S,\ h \in F_Y\} \rangle$ e $S \subset \langle R_2^{F_Y} \rangle$. Com isso podemos, para cada $w_2 \in R_2$, escolher (finitos) elementos de S que aparecem na fatoração de w_2 como elemento de $\langle \{hsh^{-1} \mid s \in S,\ h \in F_Y\} \rangle$. Defina então $T \subset S$ o conjunto de tais elementos, que é finito pois R_2 é finito, digamos $T = \{s_1, \ldots, s_m\}$. Logo,

$$\langle S^{F_Y} \rangle = \langle R_2^{F_Y} \rangle \subset \langle T^{F_Y} \rangle \subset \langle S^{F_Y} \rangle = \langle R_2^{F_Y} \rangle.$$

Portanto $\langle Y \mid T \rangle$ é uma apresentação (finita) de G. □

Corolário 1.3.9. Se G é um grupo finitamente apresentável, então toda apresentação $G = \langle Y \mid S \rangle$ admite subconjuntos *finitos* $Z \subset Y,\ T \subset S$ tais que $\langle Z \mid T \rangle$ é uma apresentação (finita) de G.

Demonstração. Seja $G = \langle X \mid R \rangle$ uma apresentação finita de G, e seja $\langle Y \mid S \rangle$ uma apresentação qualquer de G. Como X é finito, G é finitamente gerado, e assim a Proposição 1.3.7 implica que existe $Z \subset Y$ finito tal que Z gera G. Em particular, os elementos de S podem ser vistos como produtos de elementos de Z e seus inversos. Considere então a apresentação $G = \langle Z \mid S \rangle$. Como $X,\ R$ e Z são finitos, segue-se da Proposição 1.3.8 que existe $T \subset S$ finito tal que $G = \langle Z \mid T \rangle$, como queríamos. □

Capítulo 2

Grupos Pro-p

Este capítulo dedica-se ao estudo de uma certa classe de grupos topológicos, a saber, os grupos pro-p. A abordagem aqui utilizada passa pelo conceito de sistemas e limites inversos e grupos profinitos. Propriedades, exemplos e caracterizações aqui apresentados seguem as linhas dadas em Wilson [21] e Ribes e Zalesskii [16]. Ao fim do capítulo, introduz-se os conceitos de grupo pro-p livre e apresentações de grupos pro-p, traduzidos do caso abstrato, dado no capítulo anterior, para o contexto pro-p. São também expostos conceitos relacionados às álgebras de grupo completas. Os resultados finais deste trabalho dizem respeito a apresentações finitas de grupos abstratos e pro-p, e a caracterização do grupo pro-p livre de base finita dada na última seção deste capítulo será essencial em tais resultados.

Recordamos o leitor que um grupo $(G, \cdot)$ é dito um grupo topológico quando G é um espaço topológico para o qual a aplicação $G \times G \to G,\ (x, y) \mapsto xy^{-1}$, é contínua (no qual $G \times G$ é munido da topologia do produto). Referimos ao leitor os livros [14] e [1] para propriedades básicas de espaços e grupos topológicos, com destaque para espaços (grupos) compactos, Hausdorff e totalmente desconexos.

Daqui em diante, dado G um grupo topológico, utilizaremos as notações $H_1 \leq_c G,\ H_2 \leq_o G,\ N_1 \lhd_c G,\ N_2 \lhd_o G$ para dizer que H_1 é um subgrupo fechado, H_2 é um subgrupo aberto, N_1 é um subgrupo normal fechado e N_2 é um subgrupo normal aberto de G, respectivamente.

2.1 Limites Inversos

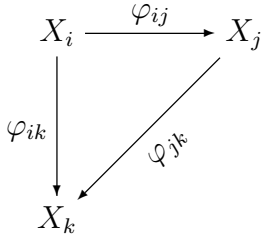
Definição 2.1.1. Seja $(I, \preceq)$ um conjunto parcialmente ordenado. Dizemos que I é *direcionado* quando, para quaisquer $i, j \in I$, existir $k \in I$ tal que $i \preceq k$ e $j \preceq k$.

Exemplo 2.1.2. $I = \mathbb{N}$ o conjunto dos números naturais, com a ordem usual, é direcionado.

Exemplo 2.1.3. Seja X um conjunto. Tome $I = \mathcal{P}(X)$ o conjunto das partes de X com a ordem induzida pela relação de continência de conjuntos: dados $A,\ B \in I$, pomos $A \succeq' B \iff A \supseteq B$. Então $(I, \preceq')$ é direcionado, pois dados $A,\ B \in \mathcal{P}(X)$, vale $A \cup B \supseteq A, B \in \mathcal{P}(X)$.

Exemplo 2.1.4. Analogamente, dados X conjunto e $I = \mathcal{P}(X)$, considere em I a ordem induzida pela inclusão de conjuntos: dados $A,\ B \in I$, pomos $A \succeq B \iff A \subseteq B$. Então $(I, \preceq)$ é direcionado, pois dados $A, B \in \mathcal{P}(X)$, vale $A \cap B \subseteq A, B \in \mathcal{P}(X)$.

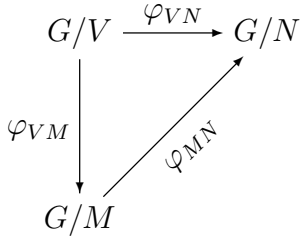
Definição 2.1.5. Sejam $\{X_i\}_{i\in I}$ uma família de espaços topológicos (ou grupos, aneis, módulos, grupos topológicos, aneis topológicos, etc.), indexados por um conjunto direcionado I, e $\{\varphi_{ij} : X_i \to X_j \mid i,j \in I, i \succeq j\}$ uma família de aplicações contínuas (respectivamente, homomorfismos, homomorfismos contínuos). Dizemos que $(X_i, \varphi_{ij})_I$ é um *Sistema Inverso* (ou *Sistema Projetivo*) de espaços topológicos (respectivamente, grupos, aneis, módulos, grupos topológicos, aneis topológicos, etc.) indexado[1] por I quando $\varphi_{ii} = id_{X_i}$ e $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ sempre que tais funções estiverem definidas, sendo $i,j,k \in I$ e $i \succeq j \succeq k$. Em outras palavras, todos os diagramas como abaixo, quando definidos, são comutativos.



Exemplo 2.1.6. Dados I um conjunto direcionado qualquer e X um espaço topológico (grupo, anel, módulo, grupo topológico, anel topológico, etc.), defina $X_i = X,\ \forall i \in I$, e $\varphi_{ij} = id_X,\ \forall i,j \in I$. Então $(X_i, \varphi_{ij})_I = (X, id_X)_I$ é sistema inverso, chamado de *sistema inverso constante*.

Exemplo 2.1.7. Sejam $I = \mathbb{N}$ com a ordem usual, $p \in \mathbb{N}$ primo, e $G_i = \mathbb{Z}/p^i\mathbb{Z}$, para cada $i \in I$. Para $i,j \in I$ com $i \geq j$, ponhamos $\varphi_{ij} : G_i \to G_j$ a ser $\varphi_{ij}(n + p^i\mathbb{Z}) = n + p^j\mathbb{Z},\ \forall n \in \mathbb{Z}$. Então $(G_i, \varphi_{ij})_I$ pode ser visto como sistema inverso de grupos (abelianos finitos), de espaços topológicos (na topologia discreta), de aneis, de $\mathbb{Z}$-módulos, ou ainda de grupos (aneis, $\mathbb{Z}$-módulos) topológicos (na topologia discreta).

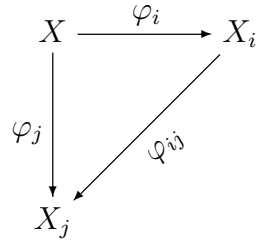
Exemplo 2.1.8. Construções semelhantes à anterior podem ser feitas de maneira mais geral. Sejam G um grupo (ou grupo topológico) e $I \subset \mathcal{P}(G)$ um conjunto de *subgrupos normais* de G tal que $N_1, N_2 \in I \implies \exists N_3 \in I$ com $N_3 \leq N_1 \cap N_2$. Defina agora uma relação de ordem em I, semelhante à dada no Exemplo 2.1.4: dados $M, N \in I$, ponha $M \succeq N \iff M \leq N$. Então $(I, \preceq)$ é direcionado. Vê-se que os homomorfismos (respectivamente, homomorfismos contínuos) naturais $\varphi_{MN} : G/M \to G/N,\ gM \mapsto gN$ são tais que os diagramas



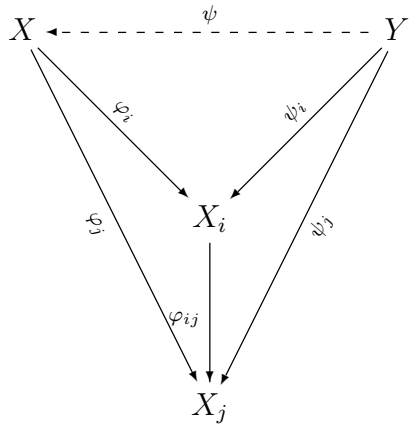
comutam, quaisquer que sejam $M, N \in I$ com $M \leq N$ e $V \leq M \cap N$. Logo, $(G/M, \varphi_{MN})_I$ define um sistema inverso de grupos (respectivamente, grupos topológicos).

[1] Alguns autores definem sistemas inversos sobre conjuntos (parcialmente ordenados) não necessariamente direcionados.

Definição 2.1.9. Seja $(X_i, \varphi_{ij})_I$ um sistema inverso de espaços topológicos (grupos, aneis, módulos, grupos topológicos, etc.). Dado X espaço topológico (grupo, anel, módulo, grupo topológico, etc.) e uma família de aplicações $\{\varphi_i : X \to X_i \mid i \in I\}$, dizemos que tal família é *compatível* quando φ_i é contínua (respectivamente, homomorfismo, homomorfismo contínuo) para todo $i \in I$, e ainda $\varphi_{ij} \circ \varphi_i = \varphi_j$, sempre que $i, j \in I$ e $i \succeq j$. Em outras palavras, todos os diagramas como abaixo, quando definidos, são comutativos.



Definição 2.1.10. Um *Limite Inverso* de um sistema inverso $(X_i, \varphi_{ij})_I$ de espaços topológicos (grupos, aneis, módulos, grupos topológicos, etc.) consiste em um espaço topológico X (grupo, anel, módulo, grupo topológico, etc.) e uma família de aplicações compatíveis $\varphi_i : X \to X_i$ com a seguinte propriedade universal: para quaisquer Y espaço topológico (grupo, anel, módulo, grupo topológico, etc.) e $\psi_i : Y \to X_i$ família de aplicações compatíveis, existe uma única aplicação contínua (respectivamente, homomorfismo, homomorfismo contínuo) $\psi : Y \to X$ tal que $\varphi_i \circ \psi = \psi_i$, $\forall i \in I$, ou seja, todos os diagramas como abaixo, quando definidos, são comutativos.



As aplicações φ_i do limite inverso são chamadas *projeções*, porém não são necessariamente sobrejetivas. Alguns autores chamam limites inversos de *limites projetivos*.

Como de praxe na definição de objetos universais, veremos que os limites inversos são únicos, em um certo sentido. Convém também nos perguntarmos sobre a existência dos limites inversos. Ambos os resultados são dados a seguir.

Teorema 2.1.11. Seja $(X_i, \varphi_{ij})_I$ sistema inverso de espaços topológicos (grupos, aneis, módulos, grupos topológicos, aneis topológicos, etc.). Então:

i. Existe (X, φ_i) Limite Inverso de $(X_i, \varphi_{ij})_I$;

ii. Se (X, φ_i) e (Y, ψ_i) são limites inversos de $(X_i, \varphi_{ij})_I$, então existe um único $\bar{\varphi} : X \to Y$ homeomorfismo (respectivamente, isomorfismo, isomorfismo topológico) tal que $\psi_i \circ \bar{\varphi} = \varphi_i,\ \forall i \in I$.

Demonstração. **i. Existência.**

Para fins didáticos, provaremos dois casos: o de sistema inverso de espaços topológicos, e o de sistema inverso de grupos. A primeira razão é que, na construção do limite, ficará explicitada a estrutura inerente ao conjunto e às aplicações compatíveis que o compõem. O segundo motivo é que os casos em classes como módulos e grupos topológicos são provados de maneira análoga, bastando substituir pelos conjuntos e aplicações respectivas, de maneira apropriada.

Caso 1) Sistema Inverso de Espaços Topológicos.

Considere $\prod_{i\in I} X_i$ o Produto Cartesiano dos espaços X_i, munido da topologia do produto, isto é, a topologia gerada pela base $\mathcal{B} = \{\prod_{j\in I} U_j \mid U_j \subset X_j \text{ é aberto } \forall j \in I, \text{ e } U_j \neq X_j \text{ apenas para finitos índices } j\}$. Considere ainda as projeções canônicas $\pi_j : \prod_{i\in I} X_i \to X_j,\ x = (x_i)_{i\in I} \mapsto \pi_j(x) = x_j$, que são contínuas na topologia do produto.

Definamos $X = \{x \in \prod_{i\in I} X_i \mid \varphi_{ij} \circ \pi_i(x) = \pi_j(x),\ \forall i, j \in I \text{ tais que } i \succeq j\}$, e $\varphi_i = \pi_i|_X : X \to X_i$ as restrições das projeções canônicas a X. Afirmamos que (X, φ_i) é limite inverso de $(X_i, \varphi_{ij})_I$.

De fato, observe primeiro que as aplicações φ_i são compatíveis, pois dados $i, j \in I$ com $i \succeq j$, tem-se que $\forall x \in X,\ \varphi_{ij} \circ \varphi_i(x) = \varphi_{ij} \circ \pi_i(x) = \pi_j(x) = \varphi_j(x)$. Suponha agora que Y seja espaço topológico e $\psi_i : Y \to X_i$ sejam aplicações compatíveis. Definamos $\psi : Y \to \prod_{i\in I} X_i,\ y \mapsto (\psi_i(y))_{i\in I}$. Com isso, ψ é contínua e $\mathrm{Im}(\psi) \subset X$, pois dados $y \in Y$ arbitrário e $j, k \in I$ com $j \succeq k$,

$$\begin{aligned}\varphi_{jk} \circ \pi_j(\psi(y)) &= \varphi_{jk} \circ \pi_j((\psi_i(y))_{i\in I}) = \varphi_{jk}(\psi_j(y)) \\ &= \psi_k(y) = \pi_k((\psi_i(y))_{i\in I}) = \pi_k(\psi(y)).\end{aligned}$$

Logo, $\psi(y) \in X$. Obtem-se ainda que, para quaisquer $y \in Y,\ j \in I$,

$$\varphi_j \circ \psi(y) = \varphi_j((\psi_i(y))_{i\in I}) = \pi_j|_X((\psi_i(y))_{i\in I}) = \psi_j(y).$$

Por fim, a unicidade de ψ é consequência de sua definição. Portanto, (X, φ_i) é limite inverso de $(X_i, \varphi_{ij})_I$.

Caso 2) Sistema Inverso de Grupos.

Considere $\prod_{i\in I} X_i$ o produto direto dos grupos X_i, com a operação usual coordenada-a-coordenada, isto é, dados $x = (x_i)_{i\in I}, y = (y_i)_{i\in I} \in \prod_{i\in I} X_i$, o produto $x \cdot y = (x_i \cdot y_i)_{i\in I}$. Considere ainda as projeções canônicas $\pi_j : \prod_{i\in I} X_i \to X_j,\ x = (x_i)_{i\in I} \mapsto \pi_j(x) = x_j$, que são homomorfismos de grupos quando consideramos a operação coordenada-a-coordenada.

Definamos $X = \{x \in \prod_{i\in I} X_i \mid \varphi_{ij} \circ \pi_i(x) = \pi_j(x),\ \forall i, j \in I \text{ tais que } i \succeq j\}$, e $\varphi_i = \pi_i|_X : X \to X_i$ as restrições das projeções canônicas a X. Afirmamos que (X, φ_i) é limite inverso de $(X_i, \varphi_{ij})_I$.

Para verificar tal afirmação, devemos mostrar primeiro que X é subgrupo de $\prod_{i\in I} X_i$, para que as aplicações φ_i sejam homomorfismos. Dados $x = (x_i)_{i\in I}, y = (y_i)_{i\in I} \in X$ arbitrários e $j, k \in I$ tais que $j \succeq k$, tem-se que $\varphi_{jk} \circ \pi_j(xy^{-1}) = \varphi_{jk} \circ \pi_j((x_i y_i^{-1})_{i\in I}) = \varphi_{jk}(x_j y_j^{-1}) = \varphi_{jk}(x_j) \cdot \varphi_{jk}(y_j)^{-1}$, pois φ_{jk} é homomorfismo. Mas $\varphi_{jk}(x_j)\cdot\varphi_{jk}(y_j)^{-1} = (\varphi_{jk}\circ\pi_j(x))\cdot(\varphi_{jk}\circ\pi_j(y))^{-1} = (\pi_k(x)) \cdot (\pi_k(y))^{-1}$, pois $x, y \in X$. Como as projeções canônicas são homomorfismos, tem-se $(\pi_k(x)) \cdot (\pi_k(y))^{-1} = \pi_k(xy^{-1})$. Ou seja, $x, y \in X$ implica $\varphi_{jk} \circ \pi_j(xy^{-1}) = \pi_k(xy^{-1})$, donde $xy^{-1} \in X$. Logo, X é subgrupo de $\prod_{i\in I} X_i$.

Observe que as aplicações φ_i são compatíveis, pois dados $i, j \in I$ com $i \succeq j$, tem-se que $\forall x \in X$, $\varphi_{ij} \circ \varphi_i(x) = \varphi_{ij} \circ \pi_i(x) = \pi_j(x) = \varphi_j(x)$. Sejam agora Y grupo e $\psi_i : Y \to X_i$ família de aplicações compatíveis. Definamos $\psi : Y \to \prod_{i\in I} X_i,\ y \mapsto (\psi_i(y))_{i\in I}$. Como cada ψ_i é homomorfismo, tem-se que ψ é homomorfismo, e vale ainda $\mathrm{Im}(\psi) \subset X$, pois dados $y \in Y$ arbitrário e $j, k \in I$ com $j \succeq k$,

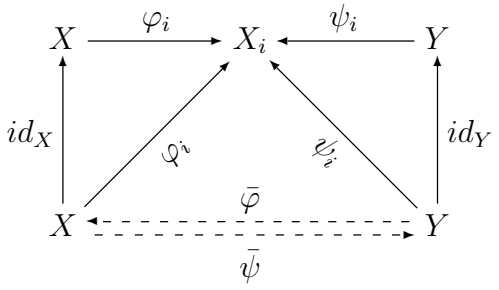
$$\begin{aligned}\varphi_{jk} \circ \pi_j(\psi(y)) &= \varphi_{jk} \circ \pi_j((\psi_i(y))_{i\in I}) = \varphi_{jk}(\psi_j(y)) \\ &= \psi_k(y) = \pi_k((\psi_i(y))_{i\in I}) = \pi_k(\psi(y)).\end{aligned}$$

Logo, $\psi(y) \in X$. Tem-se ainda que, para quaisquer $y \in Y,\ j \in I$,

$$\varphi_j \circ \psi(y) = \varphi_j((\psi_i(y))_{i\in I}) = \pi_j|_X((\psi_i(y))_{i\in I}) = \psi_j(y).$$

Por fim, a unicidade de ψ é consequência de sua definição. Portanto, (X, φ_i) é limite inverso de $(X_i, \varphi_{ij})_I$.

ii. **(Unicidade)** Sejam (X, φ_i) e (Y, ψ_i) limites inversos de $(X_i, \varphi_{ij})_I$. Então existem



$\bar\varphi : Y \to X,\ \bar\psi : X \to Y$ tais que $\varphi_i \circ \bar\varphi = \psi_i$ e $\psi_i \circ \bar\psi = \varphi_i,\ \forall i \in I$. Assim, $\psi_i \circ (\bar\psi \circ \bar\varphi) = \psi_i$ e $\varphi_i \circ (\bar\varphi \circ \bar\psi) = \varphi_i,\ \forall i \in I$. Por outro lado, pela unicidade da aplicação proveniente da propriedade universal do limite inverso, tem-se que id_Y e id_X são os únicos morfismos tais que $\psi_i \circ id_Y = \psi_i$ e $\varphi_i \circ id_X = \varphi_i,\ \forall i \in I$. Logo, $\bar\psi \circ \bar\varphi = id_Y$ e $\bar\varphi \circ \bar\psi = id_X$, o que conclui a demonstração.

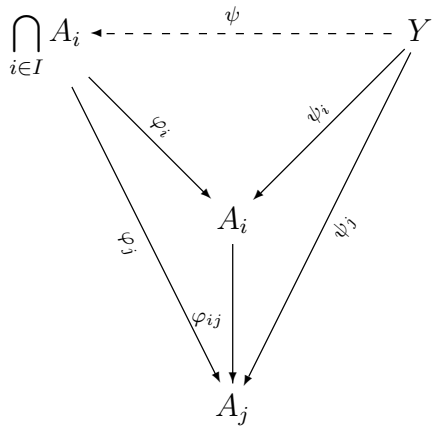
□

Devido ao Teorema 2.1.11, passaremos a tratar *do* limite inverso de um sistema dado, e utilizaremos a notação $X = \varprojlim X_i$, comumente omitindo as projeções φ_i, quando não houver risco de confusão. Além disso, quando necessário, trataremos do limite inverso como o espaço (grupo, anel, módulo, grupo topológico, anel topológico, etc.) X construído na demonstração acima, sem menção explícita.

Exemplo 2.1.12. O limite inverso do sistema inverso constante $(X, id_X)_I$ nada mais é que o próprio X, com a aplicação identidade, pois nesse caso o conjunto X como construído no Teorema 2.1.11 é a diagonal de $\prod_{i\in I} X$.

Exemplo 2.1.13. Sejam $I = \mathbb{N}$, A um espaço (grupo, anel, módulo, grupo topológico, etc.), e $\cdots A_3 \subset A_2 \subset A_1 \subset A$ uma cadeia de subespaços fechados (subgrupos, subaneis, submódulos, subgrupos fechados, etc.) de A. Para cada $i, j \in I$ com $i \geq j$, ponha $\varphi_{ij} : A_i \to A_j$ as inclusões canônicas. Afirmamos que $\varprojlim A_i = \bigcap_{i\in I} A_i$, com as inclusões, denotadas $\varphi_i : \bigcap_{j\in I} A_j \to A_i$.

De fato, veja primeiro que as aplicações φ_i são compatíveis, pois $\forall a \in \bigcap_{i\in I} A_i,\ \forall i, j \in I,\ i \geq j,\ \varphi_{ij}(\varphi_i(a)) = \varphi_{ij}(a) = a = \varphi_j(a)$. Além disso, tais aplicações são também morfismos (i.e., são contínuas, são homomorfismos, são homomorfismos contínuos, etc.) pois as mesmas são as inclusões e $A_i \subset A_j$ sempre que $i \geq j$. Verifiquemos agora a Propriedade Universal do limite inverso. Sejam Y um espaço (grupo, anel, módulo, grupo topológico, etc.) e $\psi_i : Y \to A_i$ família de morfismos compatíveis. Defina $\psi : Y \to \bigcap_{i\in I} A_i$ tal que $\psi(y) = \psi_i(y)$, no qual $i \in I$ é um índice qualquer. Precisamos mostrar que ψ está bem-definida, isto é, que a imagem de $y \in Y$ por ψ independe da escolha do índice i. Pois, sejam $i, j \in I$ quaisquer, e $y \in Y$ arbitrário. Na ordem usual de $I = \mathbb{N}$ podemos supor, sem perda de generalidade, que $i \geq j$. Nesse caso, $\psi_i(y) \in A_i$ e $\psi_j(y) \in A_j$. Por outro lado, $A_i \subset A_j$, e $\varphi_{ij} : A_i \to A_j$ é a inclusão. Logo, $\varphi_{ij}(\psi_i(y)) = \psi_i(y)$. Como ψ_i e ψ_j são compatíveis, obtem-se $\psi_i(y) = \varphi_{ij}(\psi_i(y)) = \psi_j(y)$, portanto ψ está bem-definida. Mais ainda, é claro que ψ é morfismo e $\varphi_i \circ \psi = \psi_i,\ \forall i \in I$. Sendo o Limite Inverso único a menos de isomorfismo, tem-se $\varprojlim A_i = \bigcap_{i\in I} A_i$.



Vejamos algumas propriedades topológicas básicas de limites inversos.

Proposição 2.1.14. Sejam $(X_i, \varphi_{ij})_I$ sistema inverso de espaços (grupos, aneis, módulos) topológicos e $X = \varprojlim X_i$. Então:

i. X_i Hausdorff, $\forall i \in I \implies X$ Hausdorff;

ii. X_i Totalmente Desconexo, $\forall i \in I \implies X$ Totalmente Desconexo;

iii. X_i Hausdorff, $\forall i \in I \implies X$ é subespaço fechado (respectivamente, subgrupo fechado, subanel fechado, submódulo fechado) de $\prod_{i\in I} X_i$;

iv. X_i compacto e Hausdorff, $\forall i \in I \implies X$ compacto e Hausdorff;

v. $X_i \neq \varnothing$, compacto e Hausdorff, $\forall i \in I \implies X \neq \varnothing$.

Demonstração. **i**. Todo subespaço de um espaço Hausdorff é Hausdorff, e o produto de espaços Hausdorff é Hausdorff, na topologia do produto, donde o resultado.

ii. Suponha, por absurdo, que X não seja totalmente desconexo. Nesse caso, existe $A \subset X$ subespaço conexo, com pelo menos dois elementos distintos, digamos $x = (x_i)_{i\in I}$ e $y = (y_i)_{i\in I}$. Sendo tais elementos distintos, existe $j \in I$ tal que $x_j \neq y_j$. Como $\varphi_j : X \to X_j$ é contínua, tem-se que $\varphi_j(A) \subset X_j$ é um subespaço conexo de X_j. Porém, $\varphi_j = \pi_j|_X$, donde $\varphi_j(x) = x_j \neq y_j = \varphi_j(y)$, o que implica que $\varphi_j(A)$ tem, pelo menos, dois elementos distintos. Mas, sendo X_j totalmente desconexo, a cardinalidade de $\varphi_j(A)$ é obrigatoriamente igual a 1. Uma contradição. Portanto, X é totalmente desconexo.

iii. Para quaisquer $j, k \in I$ com $j \succeq k$, denotemos $X_{jk} = \{x \in \prod_{i\in I} X_i \mid \varphi_{jk} \circ \pi_j(x) = \pi_k(x)\}$. Pelo teorema anterior, $X = \{x \in \prod_{i\in I} X_i \mid \varphi_{ij} \circ \pi_i(x) = \pi_j(x),\ \forall i, j \in I \text{ tais que } i \succeq j\}$. Visto de outra forma, $X = \bigcap_{j\succeq k} X_{jk}$. Como X_i é Hausdorff, $\forall i \in I$, e as aplicações $\varphi_{jk} \circ \pi_j : \prod_{i\in I} X_i \to X_k$ e $\pi_k : \prod_{i\in I} X_i \to X_k$ são contínuas, $\forall j, k \in I$ com $j \succeq k$, segue-se que os conjuntos X_{jk} são fechados em $\prod_{i\in I} X_i$, por serem conjuntos de elementos cujas imagens por funções contínuas, num contradomínio Hausdorff, coincidem. Assim, como a interseção arbitrária de conjuntos fechados é fechada, segue-se que X é fechado.

iv. Se cada X_i é compacto, então $\prod_{i\in I} X_i$ é compacto, pelo Teorema de Tychonoff. Como X é subconjunto fechado de um espaço compacto, segue-se que X é também compacto.

v. Pelo item anterior, X é compacto. Na notação do item **(iii)**, os conjuntos X_{jk} são fechados, e $X = \bigcap_{j\succeq k} X_{jk}$. Suponha, por absurdo, que $X = \varnothing$. Sendo $X = \bigcap_{j\succeq k} X_{jk}$ compacto, existem um inteiro n e índices $j_1, ..., j_n, k_1, ..., k_n \in I$ tais que $\bigcap_{r=1}^{n} X_{j_r k_r} = \varnothing$. Agora, como I é direcionado, podemos tomar $l \in I$ tal que $l \succeq j_r \succeq k_r,\ \forall r \in \{1, ..., n\}$. Sendo $X_l \neq \varnothing$, fixemos $x_l \in X_l$ qualquer. Construamos um elemento $x = (x_i)_{i\in I} \in \prod_{i\in I} X_i$ definindo

$$\begin{cases} x_i = \varphi_{li}(x_l), \text{ se } i \preceq l \\ x_i \in X_i \text{ qualquer, se } i \succ l. \end{cases}$$

Agora, veja que $x \in \bigcap_{r=1}^{n} X_{j_r k_r}$, pois para qualquer $r \in \{1, ..., n\}$,

$$\varphi_{j_r k_r} \circ \pi_{j_r}(x) = \varphi_{j_r k_r}(x_{j_r}) = \varphi_{j_r k_r}(\varphi_{l k_r}(x_l)) = \varphi_{l k_r}(x_l) = x_{k_r} = \pi_{k_r}(x),$$

contradizendo o fato de ser $\bigcap_{r=1}^{n} X_{j_r k_r} = \varnothing$. Portanto, $X \neq \varnothing$.

□

Proposição 2.1.15. Sejam $(X_i, \varphi_{ij})_I$ sistema inverso de espaços (grupos, aneis, módulos) topológicos e $(X, \varphi_i)_I = \varprojlim X_i$. Se cada X_i é compacto, Hausdorff e não-vazio, então:

i. A coleção $\mathcal{B} = \{\varphi_i^{-1}(U) \mid i \in I \text{ e } U \subset X_i \text{ é aberto}\}$ é uma base para a topologia de X;

ii. Se $V \subset X$ é tal que $\varphi_i(V) = X_i,\ \forall i \in I$, então V é denso em X;

iii. Dados Y espaço topológico e $f : Y \to X$, tem-se que f é contínua se, e somente se, as compostas $\varphi_i \circ f$ são contínuas $\forall i \in I$;

Demonstração. Novamente, consideremos $X = \varprojlim X_i$ como na construção dada no Teorema 2.1.11, isto é,

$$X = \{x \in \prod_{i \in I} X_i \mid \varphi_{ij} \circ \pi_i(x) = \pi_j(x),\ \forall i, j \in I \text{ tais que } i \succeq j\}$$

e $\varphi_i = \pi_i|_X$, no qual $\pi_j : \prod_{i \in I} X_i \to X_j$ são as projeções canônicas.

i. Lembremos que $\prod_{i \in I} X_i$ é munido da topologia produto, e assim qualquer aberto $A \subset X$ é da forma $A = X \bigcap \pi_{j_1}^{-1}(U_1) \bigcap \cdots \bigcap \pi_{j_n}^{-1}(U_n)$, no qual cada U_r é aberto em X_{j_r}. Queremos provar então que para todo $a \in A$, existem $i \in I$ e $U \subseteq X_i$ aberto tais que $\varphi_i^{-1}(U) \subseteq A$. Seja $a = (a_k)_{k \in I} \in A$. Como I é direcionado, existe $i \in I$ tal que $i \succeq j_1, \ldots, j_n$. Como cada aplicação $\varphi_{mn} : X_m \to X_n$ é contínua, cada $\varphi_{ij_r}^{-1}(U_r)$ é aberto em $X_i,\ 1 \leq r \leq n$. Além disso, $a_i \in \varphi_{ij_r}^{-1}(U_r)$, já que $\varphi_{ij}(a_i) = a_j$ para qualquer j com $i \succeq j$, pois $a = (a_k)_{k \in I} \in X = \varprojlim X_i$. Tome então $U = \bigcap_{r=1}^{n} \varphi_{ij_r}^{-1}(U_r)$, que é aberto em X_i por ser interseção finita de abertos, notando que $a_i \in U$. Como $\varphi_i : X \to X_i$ é contínua, $\varphi_i^{-1}(U)$ é aberto em X, e $a \in \varphi_i^{-1}(U)$ pois $\varphi_i(a) = \pi_i(a) = a_i$. Afirmamos que $\varphi_i^{-1}(U) \subseteq A$. Dado $b = (b_k)_{k \in I} \in \varphi_i^{-1}(U)$, tem-se $b_i \in U$ e $\varphi_{ij_r}(b_i) = \varphi_{ij_r}(\pi_i(b)) = \pi_{j_r}(b) = b_{j_r} \in U_r$ para $1 \leq r \leq n$, de modo que $b \in X \bigcap \pi_{j_1}^{-1}(U_1) \bigcap \cdots \bigcap \pi_{j_n}^{-1}(U_n) = A$, como queríamos.

ii. Para mostrar que V é denso em X, basta mostrar que $V \bigcap \varphi_i^{-1}(U) \neq \varnothing$ para quaisquer $i \in I$ e $U \subset X_i$ aberto, pelo item anterior. Dados então tais i e U, como $X_i \neq \varnothing$ e $\varphi_i(V) = X_i$ vale que $\varphi_i(V) \bigcap U \neq \varnothing$, donde $V \bigcap \varphi_i^{-1}(U) \neq \varnothing$.

iii. Se f é contínua, então $\varphi_i \circ f$ é contínua pois φ_i é contínua. Reciprocamente, se $\varphi_i \circ f : Y \to X_i$ é contínua então, para qualquer $U \subseteq X_i$ aberto vale que $f^{-1}(\varphi_i^{-1}(U)) = (\varphi_i \circ f)^{-1}(U) \subseteq Y$ é aberto. Como $\mathcal{B} = \{\varphi_i^{-1}(U) \mid i \in I \text{ e } U \subset X_i \text{ é aberto}\}$ é uma base para a topologia de X pelo item **(i)**, o resultado segue-se.

□

Nas seções seguintes estaremos interessados em alguns espaços (particularmente, grupos) que aparecem como limites inversos de certos sistemas cujos conjuntos subjacentes são finitos.

Definição 2.1.16. Dizemos que um espaço topológico X é *profinito* quando $X = \varprojlim X_i$, no qual cada X_i é espaço topológico *finito e discreto*.

O prefixo "pro" nesta teoria refere-se usualmente a espaços (grupos, aneis, módulos, etc.) que são limites inversos (limites *pro*jetivos). As duas proposições anteriores já nos fornecem boas propriedades de espaços profinitos, herdadas da finitude dos espaços do sistema inverso associado.

Lema 2.1.17. Sejam X um espaço compacto Hausdorff e $C \subset X$ a componente conexa de um ponto $x \in X$. Então $C = \bigcap_{Y \in \mathcal{C}_x} Y$, no qual $\mathcal{C}_x = \{Y \subseteq X \mid x \in Y,\ Y \text{ é aberto e fechado}\}$.

Demonstração. Denote $W = \bigcap_{Y \in \mathcal{C}_x} Y$. Como cada tal Y é aberto e fechado em X e $C \subset X$ é conexo, segue-se que $C \subset Y$, $\forall Y \in \mathcal{C}_x$, ou seja, $C \subseteq W$.

Para mostrar que $W \subseteq C$, é suficiente mostrar que W é conexo, já que $x \in W \cap C$. Sejam então $A, B \subset X$ abertos tais que $W = (A \cap W) \cup (B \cap W) = (A \cup B) \cap W$ e $A \cap B = \varnothing$. Sem perda de generalidade, suponha $x \in A$ (e portanto $A \neq \varnothing$). Tem-se $\varnothing = (X \setminus (A \cup B)) \cap W = (X \setminus (A \cup B)) \cap (\bigcap_{Y \in \mathcal{C}_x} Y)$. Tem-se que $X \setminus (A \cup B)$ e W são fechados.

Agora, por ser um espaço compacto e Hausdorff, X é em particular um espaço normal. Logo, para cada $w \in W$, existem $Y_w \in \mathcal{C}_x$ e $Z_w \subset X$ abertos tais que $w \in Y_w \subseteq Z_w$, $W \subset Z_w$ e $(X \setminus (A \cup B)) \cap Z_w = \varnothing$. Desse modo, $(X \setminus (A \cup B)) \cap (\bigcup_{w \in W} Z_w) = \varnothing$. Como W é compacto, existem $w_1, \ldots, w_n \in W$ tais que $W \subset \bigcup_{i=1}^n Z_{w_i}$ e $(X \setminus (A \cup B)) \cap (\bigcup_{i=1}^n Z_{w_i}) = \varnothing$. Mas $W \subset Y_{w_i} \subset Z_{w_i}$ para todo i, donde $(X \setminus (A \cup B)) \cap (\bigcap_{i=1}^n Y_{w_i}) = \varnothing$. Tem-se que $\widetilde{W} := \bigcap_{i=1}^n Y_{w_i}$ é uma vizinhança aberta e fechada de x, o que implica que $\widetilde{W} \supset W$, e de $(X \setminus (A \cup B)) \cap \widetilde{W} = \varnothing$ segue-se que $\widetilde{W} \subset A \cup B$, e assim $\widetilde{W} = (A \cap \widetilde{W}) \cup (B \cap \widetilde{W})$

Tem-se que $A \cap \widetilde{W}$ e $B \cap \widetilde{W}$ são abertos, porém $(X \setminus (B \cap \widetilde{W})) \cap \widetilde{W} = ((X \setminus B) \cup (X \setminus \widetilde{W})) \cap \widetilde{W} = (X \setminus B) \cap \widetilde{W} = A \cap \widetilde{W}$, o que implica que $A \cap \widetilde{W}$ é fechado, por ser interseção de fechados. Logo, $W \subset A \cap \widetilde{W} \subset A$, e portanto $B = \varnothing$. □

Vimos na Proposição 2.1.14 que todo espaço profinito é compacto, Hausdorff e totalmente desconexo. A recíproca de fato é válida. Mais especificamente, a Proposição 2.1.15 e o lema anterior são necessários na prova do seguinte:

Teorema 2.1.18. Seja X um espaço topológico. São equivalentes:

i. X é profinito;

ii. X é compacto, Hausdorff e totalmente desconexo;

iii. X é compacto, Hausdorff e sua topologia admite uma base formada por subespaços simultaneamente abertos e fechados.

As primeiras implicações do teorema acima são claras. Na implicação **(iii)** $\implies$ **(ii)**, constroi-se o homeomorfismo $X \cong \varprojlim_{R \in \mathcal{R}} X/R$, no qual $\mathcal{R}$ é a coleção das relações de equivalência R de X tais que toda classe de equivalência xR de R é um subconjunto simultaneamente fechado e aberto de X. Referimos ao leitor [16, p. 11] para uma demonstração completa.

Como veremos adiante, valem caracterizações análogas à do Teorema 2.1.18 para outras estruturas advindas de limites inversos, como grupos profinitos, grupos pro-p, aneis, módulos e álgebras profinitas, dentre outros.

2.2 Grupos Profinitos e Pro-p

Estudaremos agora dois casos particulares de espaços profinitos.

Definição 2.2.1. Dizemos que um *grupo* G é *profinito* quando G é o limite inverso de um sistema inverso de grupos *finitos*, vistos como grupos topológicos através da topologia discreta.

Note então que todo grupo profinito é um grupo topológico, como consequência da construção dada no Teorema 2.1.11.

Exemplo 2.2.2. Todo grupo finito G é um grupo profinito (com a topologia discreta), por ser o limite inverso do sistema constante (G, id_G).

Nosso caso de maior interesse é uma particularização dos grupos profinitos, dada a seguir.

Definição 2.2.3. Seja p um número primo. Dizemos que G é um *grupo pro-p* se G é o limite inverso de um sistema inverso de p-grupos *finitos*, vistos como grupos topológicos através da topologia discreta.

Ao tratarmos de grupos pro-p, subentende-se que p é um número primo arbitrário, porém fixado.

Exemplo 2.2.4. Todo p-grupo finito, munido da topologia discreta, é um grupo pro-p.

Exemplo 2.2.5. O limite inverso $G = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ do sistema inverso dado no Exemplo 2.1.7 é um grupo pro-p.

Daremos abaixo caracterizações úteis de grupos profinitos e pro-p, análogas ao Teorema 2.1.18, relacionando sua topologia à estrutura de seus subgrupos normais. Para isso, utilizaremos o resultado seguinte.

Proposição 2.2.6. Seja G grupo topológico compacto.

i. Toda vizinhança aberta e fechada da identidade $1 \in G$ contem um subgrupo normal aberto de G;

ii. Se G é totalmente desconexo, então $F = \bigcap_{N \lhd_o G} FN$, para todo $F \subset G$ fechado.

Demonstração. **i**. Seja $U \subset G$ vizinhança aberta e fechada de 1. Para cada $g \in U$, tem-se que $V_g = g^{-1}U$ é vizinhança aberta e fechada de 1, e vale $gV_g = U$. Da continuidade do produto existem L_g e R_g vizinhanças abertas e fechadas contendo 1 tais que $L_gR_g \subseteq V_g$. Pondo $S_g = L_g \cap R_g$, obtem-se que S_g é aberto e fechado, $1 \in S_g$ e $S_gS_g \subseteq V_g$. Assim, $\bigcup_{g\in U} gS_g$ é uma cobertura de U por abertos. Por compacidade, existem $g_1, \ldots, g_n \in U$ tais que $U \subseteq \bigcup_{i=1}^n g_iS_{g_i}$. Pondo $S = \bigcap_{i=1}^n S_{g_i}$ vem $1 \in S$ e $US \subseteq \bigcup_{i=1}^n g_iS_{g_i}S \subseteq \bigcup_{i=1}^n g_iV_{g_i} \subseteq U$, e assim $S \subseteq U$. Defina então $T = S \cap S^{-1}$. Tem-se que T é uma vizinhança simétrica de 1,

aberta e fechada, contida em U. Considere agora $H = \langle T \rangle \leq G$ o subgrupo (abstrato) de G gerado por T. Como T é simétrico, vale que

$$H = \{1\} \cup \left(\bigcup_{n \geq 1} \underbrace{T \cdot T \cdots T}_{n \text{ termos}} \right).$$

Logo, H é aberto, e por ser G compacto, H tem índice finito em G. Mais, como $T \subseteq S \subseteq U$, vale que $T \cdot T \subseteq US \subseteq U$, e indutivamente todo produto $T \cdot T \cdots T$ está contido em U. Daí que $H \subseteq U$. Finalmente, defina $N = \bigcap_{g \in G} g^{-1} H g$ o *cerne* de H, seu maior subgrupo o qual é normal em G. Note que N é fechado. Como o índice de H em G é finito, obtem-se que o índice de N em G é também finito, e portanto N é um subgrupo normal aberto de G tal que $N \subseteq H \subseteq U$.

ii. Tem-se $F \subseteq \bigcap_{N \lhd_o G} FN$ pois $F = F \cdot 1 \subseteq FN, \ \forall N \leq G$.

Por outro lado, $\bigcap_{N \lhd_o G} FN \subseteq F \iff G \setminus F \subseteq G \setminus (\bigcap_{N \lhd_o G} FN) = \bigcup_{N \lhd_o G} (G \setminus FN)$. Dado $g \in G \setminus F$, existe $\widetilde{U} \subset G$ aberto tal que $g \in \widetilde{U} \subseteq G \setminus F$, pois F é fechado. Assim, $U = g^{-1}\widetilde{U}$ é vizinhança aberta de $1 \in G$. Agora, como G é totalmente desconexo, seus subconjuntos unitários são fechados, pois tais conjuntos são as componentes conexas de G. Em particular, $\{1\}$ é fechado e portanto o grupo topológico G é Hausdorff. Logo, pelo Lema 2.1.17, $\{1\} = \bigcap_{Y \in \mathcal{C}_1} Y$, no qual $\mathcal{C}_1 = \{Y \subseteq G \mid 1 \in Y, \ Y \text{ é aberto e fechado}\}$. Em particular, $(G \setminus U) \cap (\bigcap_{Y \in \mathcal{C}_1} Y) = \varnothing$, e assim para cada $x \in G \setminus U$ existe $Y_x \in \mathcal{C}_1$ tal que $x \notin Y_x$. A compacidade de G nos dá então que existem $Y_1, \ldots, Y_n \in \mathcal{C}_1$ tais que $(G \setminus U) \cap (\bigcap_{i=1}^n Y_i) = \varnothing$. Dessa forma, $V = \bigcap_{i=1}^n Y_i$ é uma vizinhança aberta e fechada de 1. Pelo item anterior, existe um subgrupo normal aberto $N \lhd_o G$ tal que $N \subseteq V \subseteq U = g^{-1}\widetilde{U}$. Com isso, $gN \subseteq \widetilde{U} \subseteq G \setminus F$, donde $gN \cap F = \varnothing$. Portanto, $G \setminus F \subseteq \bigcup_{N \lhd_o G} (G \setminus FN)$.

□

Teorema 2.2.7. Seja G um grupo topológico. São equivalentes:

i. G é um grupo profinito;

ii. G é compacto e totalmente desconexo;

iii. G é compacto, Hausdorff, e seus subgrupos normais abertos formam um sistema fundamental de vizinhanças $\mathcal{N}$ da identidade $1 \in G$.

Demonstração. **(i)** $\implies$ **(ii)** Suponha que G seja profinito. Por definição, $G = \varprojlim G_i$, no qual cada G_i é grupo finito com a topologia discreta. Então G é compacto, Hausdorff e totalmente desconexo, pela Proposição 2.1.14.

(ii) $\implies$ **(i)** Notemos primeiro que G é também Hausdorff, pois o mesmo é totalmente desconexo, o que implica que suas componentes conexas são seus subconjuntos unitários. Em particular, $\{1\} \leq G$ é fechado, e portanto o grupo topológico G é Hausdorff. Além disso, todo subgrupo aberto H de G tem índice finito, pois $\bigcup_{g \in G} gH = G$ é uma cobertura de G por abertos e G é compacto. Em particular, para cada $N \lhd_o G$ vale que G/N é um grupo finito.

Seja $\mathcal{N} = \{N \lhd G \mid N \text{ é aberto}\}$. Para $M, N \in \mathcal{N}$, ponha $N \preceq M$ se M é subgrupo de N. Com isso, $(\mathcal{N}, \preceq)$ é direcionado. Pondo $\varphi_{MN} : G/M \twoheadrightarrow G/N$ os homomorfismos (contínuos) canônicos, $(G/M, \varphi_{MN})_{\mathcal{N}}$ torna-se sistema inverso de grupos finitos. Denote $\widehat{G} = \varprojlim G/N$, e considere $\theta : G \to \prod_{N\in\mathcal{N}} G/N$ o homomorfismo (contínuo) dado por $\theta(g) = (gN)_{N\in\mathcal{N}}$.

Afirmamos que θ é injetiva. Tem-se $\ker\theta = \bigcap_{N\in\mathcal{N}} N$. Como G é totalmente desconexo, $\{1\}$ é fechado, e por ser também G compacto, segue-se da Proposição 2.2.6 que $\{1\} = \bigcap_{N\lhd_o G} 1 \cdot N = \bigcap_{N\in\mathcal{N}} N = \ker\theta$.

Note ainda que $\operatorname{Im}\theta \subseteq \widehat{G}$. Pelo Teorema 2.1.11,

$$\begin{aligned}\widehat{G} &= \varprojlim G/N \\ &= \{x \in \prod_{N\in\mathcal{N}} G/N \mid \varphi_{LM} \circ \pi_L(x) = \pi_M(x),\ \forall L, M \in \mathcal{N} \text{ tais que } L \leq M\} \\ &= \{(g_N N)_{N\in\mathcal{N}} \in \prod_{N\in\mathcal{N}} G/N \mid g_L M = g_M M,\ \forall L, M \in \mathcal{N} \text{ tais que } L \leq M\},\end{aligned}$$

no qual as aplicações π_M denotam as projeções canônicas. Em particular, como $\theta(g) = (gN)_{N\in\mathcal{N}}$, tem-se $\varphi_{KL} \circ \pi_K \circ \theta(g) = \varphi_{KL}(gK) = gL = \pi_L \circ \theta(g)$, qualquer que seja $g \in G$. Ou seja, $\theta(G) \subseteq \widehat{G}$.

Com isso, tem-se $\theta : G \to \widehat{G}$, sendo θ monomorfismo contínuo. Agora, θ é também sobrejetiva. De fato, $\pi_M(\theta(G)) = G/M,\ \forall M \lhd_o G$, o que implica que $\theta(G)$ é denso em $\widehat{G}$ pela Proposição 2.1.15. Por serem θ contínua, G compacto e $\widehat{G}$ Hausdorff, vale que $\theta(G)$ é fechado em $\widehat{G}$. Logo, $\theta(G) = \overline{\theta(G)} = \widehat{G}$.

Assim, $\theta : G \to \widehat{G}$ é isomorfismo de grupos. Sendo θ contínua e bijetiva, G compacto e $\widehat{G}$ Hausdorff, segue-se que θ é homeomorfismo de espaços topológicos, e portanto θ é isomorfismo de grupos topológicos.

(i) $\iff$ **(iii)** Esta equivalência é semelhante à provada anteriormente. A primeira implicação segue novamente da Proposição 2.1.14, em conjunto com o primeiro item Proposição 2.1.15 – que implica que os subgrupos normais abertos de G formam um sistema fundamental de vizinhanças da identidade. A implicação contrária é análoga ao caso **(ii)** $\Rightarrow$ **(i)**. Basta construir o mesmo sistema inverso indexado por $\mathcal{N} = \{N \lhd G \mid N \text{ é aberto}\}$, e considerar seu limite inverso $\widehat{G}$ e o mesmo homomorfismo contínuo $\theta : G \to \widehat{G}$. Tem-se que θ é injetiva pois, caso contrário, existira $g \in \ker\theta \setminus \{1\} = (\bigcap_{N\in\mathcal{N}} N) \setminus \{1\}$, e como $\mathcal{N}$ é um sistema fundamental de vizinhanças abertas da identidade não existiriam abertos de G separando g de 1, isto é, não existiriam $U, V \subset G$ abertos disjuntos com $1 \in U,\ g \in V$, contradizendo o fato de G ser Hausdorff. A prova da sobrejetividade de θ é análoga, assim como a verificação de que θ é homeomorfismo. □

De modo análogo, prova-se o seguinte:

Teorema 2.2.8. Seja G um grupo topológico. São equivalentes:

i. G é um grupo pro-p;

ii. G é compacto, totalmente desconexo, e todo subgrupo normal aberto $N \lhd_o G$ é tal que G/N é p-grupo finito;

iii. G é compacto, Hausdorff, e seus subgrupos normais abertos têm índice potência de p e formam um sistema fundamental de vizinhanças $\mathcal{N}$ da identidade $1 \in G$.

Demonstração. Basta mimetizar a demonstração do Teorema 2.2.7, observando que se G é pro-p com $(G, \varphi_i)_I = \varprojlim (G_i, \varphi_{ij})_I$, então $\ker \varphi_i$ tem índice potência de p para todo $i \in I$, pois $G/\ker \varphi_i \cong \operatorname{Im} \varphi_i \leq G_i$ sendo cada G_i um p-grupo finito. □

Pelas construções dadas nas demonstrações acima, todo grupo profinito ou pro-p pode ser escrito como o limite inverso dos seus quocientes por subgrupos normais abertos $G = \varprojlim_{N \lhd_o G} G/N$, no qual as aplicações do limite inverso são as projeções canônicas.

Dos teoremas anteriores podemos extrair de imediato propriedades muito úteis de grupos profinitos e pro-p, a saber, que tais classes de grupos topológicos são "bem comportadas" em relação a subgrupos, quocientes e produtos diretos. Isso nos permite construir alguns grupos pro-p a partir de grupos pro-p já conhecidos.

Proposição 2.2.9. Seja G um grupo profinito. São válidas:

i. $H \leq_c G \implies H$ é profinito, com a topologia do subespaço;

ii. $N \lhd_c G \implies G/N$ é profinito, com a topologia quociente;

iii. $\{G_\lambda\}_{\lambda \in \Lambda}$ família de grupos profinitos $\implies \prod_{\lambda \in \Lambda} G_\lambda$ é grupo profinito, com a topologia do produto. Em particular, o limite inverso de um sistema inverso de grupos profinitos é ainda um grupo profinito;

iv. G pro-p e $H \leq_c G \implies H$ é pro-p, com a topologia do subespaço;

v. G pro-p e $N \lhd_c G \implies G/N$ é pro-p, com a topologia quociente;

vi. $\{G_\lambda\}_{\lambda \in \Lambda}$ família de grupos pro-p $\implies \prod_{\lambda \in \Lambda} G_\lambda$ é grupo pro-p, com a topologia do produto. Em particular, o limite inverso de um sistema inverso de grupos pro-p é ainda um grupo pro-p.

Demonstração. **i**. H é compacto por ser subespaço fechado de um compacto, e H é totalmente desconexo pois G é totalmente desconexo.

ii. Sendo N fechado em G obtem-se que G/N é Hausdorff. Da continuidade da aplicação quociente $\pi(g) = gN \in G/N$, segue-se que G/N é compacto. Pela construção da topologia quociente e pelo Teorema da Correspondência de (sub)grupos, segue-se que os subgrupos normais abertos de G/N formam uma base de vizinhanças abertas da identidade $1 \in G/N$.

iii. Na topologia do produto, o produto de espaços totalmente desconexos é totalmente desconexo e, do Teorema de Tychonoff, o produto de compactos é compacto. A segunda afirmação segue da construção dada no Teorema 2.1.11, pois o limite inverso de um sistema inverso de grupos (pro)finitos é um subgrupo fechado do produto direto de tais grupos (análogo ao item **(iii)** da Proposição 2.1.14).

iv. Já vimos que H é profinito. Basta provar que seus subgrupos normais abertos têm índice potência de p. Seja então $M \lhd_o H$. Como H é fechado em G, sua topologia é induzida pela topologia de G, de modo que $\{H \cap N \mid N \lhd_o G\}$ é um sistema fundamental de vizinhanças abertas de $1 \in H$. Em particular, existe $N \lhd_o G$ tal que $H \cap N \subseteq M$, e assim $[H : M]$ divide $[H : H \cap N]$. Do Teorema do Isomorfismo, $H/(N \cap H) \cong (HN)/N = \pi(H)$, no qual $\pi : G \to G/N$ denota a projeção canônica. Como G/N é p-grupo finito e $\pi(H) \leq G/N$, o resultado segue-se.

v. Análogo ao item **(ii)**.

vi. Analogamente ao item **(iii)**, já temos que $\widehat{G} := \prod_{\lambda \in \Lambda} G_\lambda$ é compacto e Hausdorff. Seja $N \lhd_o \widehat{G}$. Basta provar que o índice $[\widehat{G} : N]$ é potência de p. Pela definição da topologia do produto e pelo terceiro item do Teorema 2.2.8, existem finitos índices $\lambda_1, \ldots, \lambda_n \in \Lambda$ e $N_{\lambda_i} \lhd_o G_{\lambda_i}$ tais que $\widetilde{N} := \bigcap_{i=1}^n \pi_{\lambda_i}^{-1}(N_{\lambda_i}) \lhd_o N$, donde existe um epimorfismo natural $\widehat{G}/\widetilde{N} \twoheadrightarrow \widehat{G}/N$. Mas $\widehat{G}/\widetilde{N} = \widehat{G}/(\bigcap_{i=1}^n \pi_{\lambda_i}^{-1}(N_{\lambda_i})) \cong \prod_{i=1}^n G_{\lambda_i}/N_{\lambda_i}$, de modo que $\widehat{G}/\widetilde{N}$ é produto direto finito de p-grupos finitos, sendo portanto p-grupo finito.

□

2.2.1 Inteiros p-ádicos e Completamentos

A demonstração dada para os teoremas 2.2.7 e 2.2.8 aponta uma maneira construtiva de obter grupos profinitos e pro-p a partir de grupos conhecidos: se G é um grupo abstrato, podemos visualizar G como grupo topológico com uma topologia "adequada", e assim o grupo $\widehat{G} = \varprojlim_{N \lhd_o G} G/N$ será profinito ou pro-p. Mais ainda, G possui imagem homomórfica (contínua) $\iota(G)$ *densa* em $\widehat{G}$, pela aplicação natural $\iota(g) = (gN)_{N \lhd_o G}$. Melhor, se ι é injetiva, podemos identificar naturalmente $G \hookrightarrow \widehat{G}$ e assim $\overline{G} = \widehat{G}$. Daremos um exemplo de tal construção no caso em que o grupo dado é o anel dos inteiros $\mathbb{Z}$.

Definição 2.2.10. Sejam G um grupo abstrato e $\mathcal{N}(G) = \{N \lhd G \mid [G : N] < \infty\}$ a família de seus subgrupos normais de índice finito. Podemos tornar G um grupo topológico pondo $\mathcal{N}(G)$ a ser um sistema fundamental de vizinhanças abertas[2] do elemento neutro $1 \in G$. Nesse caso, chamamos tal topologia de *topologia profinita* do grupo abstrato G. Analogamente, dado $p \in \mathbb{N}$ primo e considerando $\mathcal{N}_p(G) = \{N \lhd G \mid [G : N] < \infty \text{ e } G/N \text{ é } p\text{-grupo}\}$, dizemos que a topologia induzida[3] por $\mathcal{N}_p(G)$ é a *topologia pro-p* do grupo abstrato G.

Fixe $p \in \mathbb{N}$ um número primo. Ao invés da topologia usual (discreta) de $\mathbb{Z}$, considere a topologia induzida pela família de seus p-subgrupos, isto é, sua topologia pro-p. Denote $\widehat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$. Por construção, $\widehat{\mathbb{Z}}_p$ é grupo (de fato, anel) pro-p, e a aplicação $\iota : \mathbb{Z} \to \widehat{\mathbb{Z}}_p$ dada por $\iota(n) = (n + p^i\mathbb{Z})_{i \in \mathbb{N}}$ é contínua, nas topologias acima consideradas. Tem-se que ι é injetiva, pois $\ker \iota = \bigcap_{i \in \mathbb{N}} p^i\mathbb{Z} = \{0\}$, donde identificamos naturalmente $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}_p$ e, como vimos, $\overline{\mathbb{Z}} = \widehat{\mathbb{Z}}_p$.

[2]Note que $N_1, N_2 \lhd G$ com $[G : N_1], [G : N_2] < \infty \implies [G : N_1 \cap N_2] < \infty$.

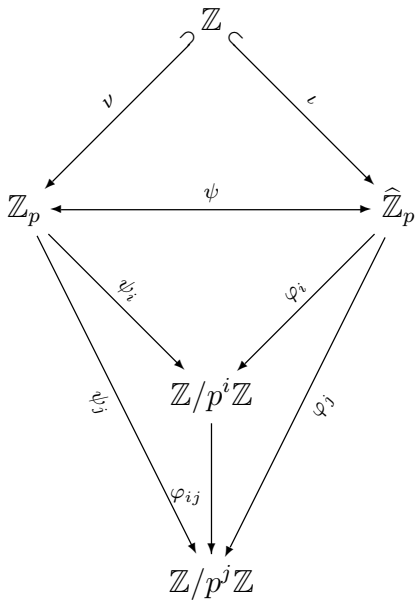
[3]Similarmente, $N_1 \cap N_2$ tem índice potência de p caso N_1 e N_2 tenham tal propriedade.

Obteremos agora uma bijeção que permite uma útil identificação para o anel pro-p $\widehat{\mathbb{Z}}_p$. Seguindo uma tradição da teoria dos números, denote

$$\mathbb{Z}_p = \left\{ \sum_{i\geq 0} a_i p^i \mid a_i \in \mathbb{Z},\ 0 \leq a_i < p \right\}$$

o conjunto da somas (inteiras) infinitas formais sobre potências do número primo fixado p.

Proposição 2.2.11. Denote $\varphi_i,\ \varphi_{ij}$ as projeções canônicas no limite inverso $(\widehat{\mathbb{Z}}_p, \varphi_i)_{\mathbb{N}} = \varprojlim(\mathbb{Z}/p^i\mathbb{Z}, \varphi_{ij})_{\mathbb{N}}$. Existem funções $\psi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$, função injetiva $\nu : \mathbb{Z} \to \mathbb{Z}_p$, e uma *bijeção* $\psi : \mathbb{Z}_p \to \widehat{\mathbb{Z}}_p$ tais que, para quaisquer $i, j \in \mathbb{N}$ com $i \geq j$, o diagrama abaixo comuta:



Demonstração. A existência de $\nu : \mathbb{Z} \to \mathbb{Z}_p$ é consequência do fato de que todo número inteiro z pode ser descrito "em base p", isto é, de maneira única como uma soma $z = \sum_{i\geq 0} a_i p^i$ com $0 \leq a_i < p$, no qual tal soma é *finita* se $z \geq 0$, notando que a expansão de $-1 \in \mathbb{Z}$ é dada pela soma formal $\sum_{i\geq 0}(p-1)p^i$. Nesse sentido, identificamos $\nu(z) = \sum_{i\geq 0} a_i p^i$ como a inclusão natural de $\mathbb{Z}$ em $\mathbb{Z}_p$.

Definamos agora $\psi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$ por

$$\psi_i \left(\sum_{k\geq 0} a_k p^k \right) = \sum_{k=0}^{i-1} a_k p^k + p^i\mathbb{Z}.$$

Com tal definição, as aplicações ψ_i são compatíveis com as aplicações φ_{ij} do sistema inverso, isto é, $\varphi_{ij} \circ \psi_i = \psi_j$.

Seja então $\psi : \mathbb{Z}_p \to \widehat{\mathbb{Z}}_p$ dada por

$$z = \sum_{k\geq 0} a_k p^k \mapsto (\psi_n(z))_{n\geq 1} = \left(\sum_{k=0}^{n-1} a_k p^k + p^n\mathbb{Z} \right)_{n\geq 1}.$$

Congruências módulo p^i para um inteiro $z \in \mathbb{Z}$ garantem que $\psi \circ \nu(z) = \iota(z)$. Além disso, é também imediato da definição de ψ que $\varphi_i \circ \psi = \psi_i$. Resta mostrar que ψ é uma bijeção.

Suponha que $\psi(z_1) = \psi(z_2)$, com $z_1 = \sum_{i\geq 0} a_i p^i$, $z_2 = \sum_{i\geq 0} \widetilde{a}_i p^i$. Então, para todo $n \in \mathbb{N}$, $\sum_{i=0}^{n-1} a_i p^i + p^n\mathbb{Z} = \sum_{i=0}^{n-1} \widetilde{a}_i p^i + p^n\mathbb{Z}$. Assim, $a_0 - \widetilde{a}_0 = m_0 p$ para algum $m_0 \in \mathbb{Z}$. Como $0 \leq a_0, \widetilde{a}_0 < p$, vem $a_0 = \widetilde{a}_0$, de modo que $a_1 - \widetilde{a}_1$ também é múltiplo de p e, de modo análogo, $a_1 = \widetilde{a}_1$. Indutivamente, $a_i = \widetilde{a}_i$, $\forall i \geq 0$, ou seja, $z_1 = z_2$. Logo, ψ é injetiva.

Seja $x = (x_n + p^n\mathbb{Z})_{n\in\mathbb{N}} \in \widehat{\mathbb{Z}}_p$. Ponha $a_0 = x_1$. Sendo $(\widehat{\mathbb{Z}}_p, \varphi_i)_{\mathbb{N}} = \varprojlim(\mathbb{Z}/p^i\mathbb{Z}, \varphi_{ij})_{\mathbb{N}}$, tem-se $x_2 + p\mathbb{Z} = \varphi_2 \circ \varphi_{2,1}(x) = \varphi_1(x) = x_1 + p\mathbb{Z}$, e assim existe $a_1 \in \mathbb{Z}$ com $x_2 - x_1 = a_1 p$ e $0 \leq a_1 < p$. Logo, $x_2 = x_1 + a_1 p = a_0 + a_1 p = \sum_{i=0}^{1} a_i p^i$. Repetindo-se tal processo iteradamente, obtem-se por indução que para cada $n \in \mathbb{N}$, existem $a_0, \ldots, a_n$ tais que $x_n = \sum_{i=0}^{n-1} a_i p^i$ e $0 \leq a_i < p$. Ponha $z = \sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p$, no qual os índices a_i são como acima. Segue-se que

$$\psi(z) = (\psi_n(z))_{n\in\mathbb{N}} = \left(\sum_{i=0}^{n-1} a_i p^i + p^n\mathbb{Z}\right)_{n\in\mathbb{N}} = x.$$

Portanto, ψ é sobrejetiva. □

Devido à proposição anterior, podemos tornar $\mathbb{Z}_p = \{\sum_{i\geq 0} a_i p^i \mid a_i \in \mathbb{Z},\ 0 \leq a_i < p\}$ um anel topológico, comutativo e com elemento unidade, através da bijeção $\psi : \mathbb{Z}_p \to \widehat{\mathbb{Z}}_p$. Basta definir em $\mathbb{Z}_p$ a topologia

$$\tau = \{U \subseteq \mathbb{Z}_p \mid \psi(U) \subseteq \widehat{\mathbb{Z}}_p \text{ é aberto}\},$$

com as operações de soma $z_1 + z_2 = \psi^{-1}(\psi(z_1) + \psi(z_2))$ e produto $z_1 z_2 = \psi^{-1}(\psi(z_1)\psi(z_2))$. Com isso, $\mathbb{Z}_p$ é isomorfo, como anel topológico, a $\widehat{\mathbb{Z}}_p$. Mais ainda, devido à comutatividade do diagrama dado na Proposição 2.2.11, passamos a identificar livremente $\mathbb{Z}_p = \widehat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ com as aplicações $\psi_i : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^i\mathbb{Z}$ definidas em 2.2.11, e assim $\mathbb{Z}_p$ é um anel pro-p. $\mathbb{Z}_p$ é chamado o *anel dos inteiros p-ádicos*.

Observamos ainda que, novamente devido à comutatividade do diagrama dado em 2.2.11, as operações de soma e produto em $\mathbb{Z}_p$, como definidas acima, estendem a soma e produto usuais de $\mathbb{Z}$ e, da maneira como construímos, $\mathbb{Z} \overset{\nu}{\hookrightarrow} \mathbb{Z}_p$ é um mergulho de aneis topológicos (ainda considerando em $\mathbb{Z}$ a topologia pro-p). Passamos a identificar $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, e como vimos $\overline{\mathbb{Z}} = \mathbb{Z}_p$. Dessa forma, as operações em $\mathbb{Z}_p$ coincidem com as operações de somas formais[4] (nesse caso, comutativas), isto é,

$$\left(\sum_{i\geq 0} a_i p^i\right) + \left(\sum_{i\geq 0} b_i p^i\right) = \sum_{i\geq 0}(a_i + b_i)p^i \quad \text{e} \quad \left(\sum_{i\geq 0} a_i p^i\right) \cdot \left(\sum_{j\geq 0} b_j p^j\right) = \sum_{i\geq 0}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) p^i.$$

A identificação de $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ como o anel das somas infinitas sobre potências de p nos permite extrair propriedades úteis de tal anel, algumas listadas a seguir.

Proposição 2.2.12. Seja $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ o anel dos inteiros p-ádicos, com os homomorfismos contínuos $\psi_i(\sum_{j\geq 0} a_j p^j) = \sum_{j=0}^{i-1} a_j p^j + p^i\mathbb{Z}$. São válidos:

[4]Note que aqui as operações $a_i + b_i$ e $a_i b_j$ são feitas da maneira usual, podendo-se depois reescrever a soma e o produto em novas expansões p-ádicas com a exigência de que os coeficientes não sejam múltiplos de p.

i. $\ker \psi_i = p^i\mathbb{Z}_p$, $\{p^i\mathbb{Z}_p\}_{i\geq 0}$ é um sistema fundamental de vizinhanças abertas do 0, e $\mathbb{Z}_p/p^i\mathbb{Z}_p \cong \mathbb{Z}/p^i\mathbb{Z},\ \forall i \geq 0$;

ii. $\mathbb{Z}_p$ é um domínio de integridade;

iii. $\mathbb{Z}_p$ admite uma cadeia descendente de ideais fechados

$$\mathbb{Z}_p \supseteq p\mathbb{Z}_p \supseteq p^2\mathbb{Z}_p \supseteq p^3\mathbb{Z}_p \supseteq \cdots,$$

no qual $\bigcap_{i\geq 0} p^i\mathbb{Z}_p = \{0\}$. Além disso, $p\mathbb{Z}_p$ é o único ideal maximal de $\mathbb{Z}_p$, e tem-se $\mathcal{U}(\mathbb{Z}_p) = \mathbb{Z}_p \setminus p\mathbb{Z}_p$, no qual $\mathcal{U}(\mathbb{Z}_p)$ é o grupo das unidades de $\mathbb{Z}_p$;

iv. $\mathbb{Z}_p$ é não-enumerável;

v. Para quaisquer G grupo pro-p e $f : \mathbb{Z} \to G$ homomorfismo contínuo (sendo $\mathbb{Z}$ munido da topologia pro-p), existe um único homomorfismo contínuo $\theta : \mathbb{Z}_p \to G$ tal que $\theta|_{\mathbb{Z}} = f$;

vi. Dado G grupo pro-p, existe um único homomorfismo contínuo $\mathbb{Z}_p \times G \to G$, denotado $(z, g) \mapsto g^z$, tal que: $g^n = \underbrace{g \cdot g \cdots g}_{n \text{ termos}},\ \forall n \in \mathbb{Z}$; $g^{z_1+z_2} = g^{z_1}g^{z_2}$ e $(g^{z_1})^{z_2} = g^{z_1z_2},\ \forall z_1, z_2 \in \mathbb{Z}_p$.

Mais ainda, se $g_1, g_2 \in G$ comutam, então $(g_1g_2)^z = g_1^z g_2^z$.

Demonstração. **i**. Tem-se que $p^i\mathbb{Z}_p = \{\sum_{j=i}^{\infty} a_{j-i}p^j \mid a_j \in \mathbb{Z},\ 0 \leq a_j < p\}$ e $\ker \psi_i = \{\sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p \mid \sum_{j=0}^{i-1} a_j p^j$ é múltiplo de $p^i\}$, ou seja, $p^i\mathbb{Z}_p = \ker \psi_i$. As outras afirmações então seguem da identificação $(\mathbb{Z}_p, \psi_i)_{\mathbb{N}} = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$, notando que cada ψ_i é sobrejetiva.

ii. Sejam $z_1 = \sum_{i\geq 0} a_i p^i,\ z_2 = \sum_{j\geq 0} b_j p^j$ ambos não-nulos, isto é, existem i e j menores possíveis tais que $a_i \neq 0 \neq b_j$. Denote $z_1z_2 = \sum_{k\geq 0} c_k p^k$, pondo $0 \leq c_k < p$ para todo k. Nesse caso, tem-se que $c_{i+j} \equiv a_ib_j \mod p$. Como $0 < a_i, b_j < p$, segue-se que $c_{i+j} \neq 0$, e assim $z_1z_2 \neq 0$.

iii. Como $p^i\mathbb{Z}_p = \ker \psi_i = \psi_i^{-1}(\{0\})$, cada $p^i\mathbb{Z}_p$ é um ideal fechado de $\mathbb{Z}_p$, e as inclusões são evidentes. Sendo $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ o corpo de ordem p, tem-se que $p\mathbb{Z}_p$ é um ideal maximal. E $p\mathbb{Z}_p$ é único pois se $z \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, então z é uma unidade, o que implica que cada ideal não contido em $p\mathbb{Z}_p$ é o próprio $\mathbb{Z}_p$. Verifiquemos então que $\mathbb{Z}_p = \mathcal{U}(\mathbb{Z}_p) \cup p\mathbb{Z}_p$.

Dado $z \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, tem-se $z = \sum_{i\geq 0} a_i p^i$ com $0 < a_0 < p$. Com isso, existe $b_0 \in \mathbb{Z}$ tal que $0 < b_0 < p$ e $a_0b_0 \equiv 1 \mod p$, digamos $a_0b_0 = 1 + c_0p$ com $0 < c_0 < p$. Assim,

$$zb_0 = \left(a_0 + \sum_{i\geq 1} a_i p^i\right) b_0 = 1 + w,$$

no qual $w = c_0p + b_0 \sum_{i\geq 1} a_i p^i \in p\mathbb{Z}_p$. Mostrando que $1 + w \in \mathcal{U}(\mathbb{Z}_p)$, obter-se-á $z(b_0(1 + w)^{-1}) = 1$, i.e., $z \in \mathcal{U}(\mathbb{Z}_p)$. Definindo-se $s_n = \sum_{i=1}^{n-1}(-w)^i$ para cada $n \in \mathbb{N}$, obtem-se que $(1 + w)(1 + s_n) = 1 - w^n \in 1 + p^n\mathbb{Z}_p$. Como $\{p^n\mathbb{Z}_p\}_{n\in\mathbb{N}}$ é um sistema fundamental de vizinhanças abertas do 0 e $\bigcap_{n\in\mathbb{N}} p^n\mathbb{Z}_p = \{0\}$, segue-se que $w^n \to 0$ e $\lim_{n\to\infty} s_n$ converge, digamos a s. Assim, a continuidade da soma e do produto garantem que $(1 + w)(1 + s) = (1 + w)(1 + \lim s_n) = \lim(1 - w^n) = 1$, ou seja, $1 + w$ admite inverso multiplicativo $1 + s$, como queríamos.

iv. Como $\mathbb{Z}_p = \{\sum_{i\geq 0} a_i p^i \mid a_i \in \mathbb{Z},\ 0 \leq a_i < p\}$ está em bijeção com o conjunto das sequências infinitas cujos termos estão em $\{0, 1, \ldots, p-1\}$, basta aplicar o Método da Diagonal de Cantor para obter o resultado.

v. Sejam G grupo pro-p e $f : \mathbb{Z} \to G$ homomorfismo contínuo. Identifiquemos novamente $(\mathbb{Z}_p, \psi_i)_{\mathbb{N}} = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$. Pela construção dada no Teorema 2.2.8, podemos escrever $G = \varprojlim_{M \lhd_o G} G/M$, com as projeções canônicas $\varphi_M : G \twoheadrightarrow G/M$ e $\varphi_{MN} G/M \twoheadrightarrow G/N$ se $M \leq N$. Para cada $M \lhd_o G$, como f é contínua, existe i minimal tal que $p^i\mathbb{Z} \subseteq f^{-1}(M)$. Logo, existe único homomorfismo contínuo $\widetilde{f}_M : \mathbb{Z}/p^i\mathbb{Z} \to G/M$ tal que $\widetilde{f}_M(z + p^i\mathbb{Z}) = f(z)M$. Defina então a família de homomorfismos contínuos

$$\theta_M : \mathbb{Z}_p \xrightarrow{\psi_i} \mathbb{Z}/p^i\mathbb{Z} \xrightarrow{\widetilde{f}_M} G/M,\ M \lhd_o G.$$

Tem-se que $\varphi_{MN} \circ \theta_M = \theta_N$ sempre que $M \leq N$. Pela propriedade universal do limite inverso, existe único homomorfismo contínuo $\theta : \mathbb{Z}_p \to G$ tal que $\varphi_M \circ \theta = \theta_M$, ou seja, $\varphi_M \circ \theta|_{\mathbb{Z}} = \varphi_M \circ f$, para qualquer $M \lhd_o G$. Afirmamos que $\theta|_{\mathbb{Z}} = f$. Para cada $z \in \mathbb{Z}$, tem-se $\theta(z)(f(z))^{-1} \in \ker \varphi_M = M$, para todo $M \lhd_o G$. Assim,

$$\theta(z)(f(z))^{-1} \in \bigcap_{M \lhd_o G} M = \{1\},$$

ou seja, $\theta(z) = f(z)$, como queríamos. Por fim, se $\tau : \mathbb{Z}_p \to G$ é outro homomorfismo contínuo tal que $\tau|_{\mathbb{Z}} = f$, tem-se $\tau|_{\mathbb{Z}} = f = \theta|_{\mathbb{Z}}$ e, sendo $\mathbb{Z}$ denso em $\mathbb{Z}_p$, segue-se que $\tau = \theta$.

vi. Para cada $g \in G$, a aplicação potenciação $f_g : \mathbb{Z} \to G,\ f_g(n) = g^n$ é homomorfismo contínuo, nas topologias consideradas, e possui as propriedades de soma e produto do enunciado. Logo, pelo item anterior, cada tal função estende-se a um único homomorfismo contínuo $\theta_g : \mathbb{Z}_p \to G,\ g^z := \theta_g(z)$, com as propriedades do enunciado. Definindo-se a ação contínua $\mathbb{Z}_p \times G \to G$ por $(z, g) \mapsto \theta_g(z)$, o resultado segue-se.

□

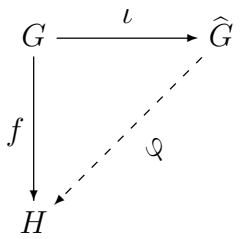
Observe que, como $\mathbb{Z}_p$ é um domínio de integridade, podemos construir $\mathbb{Q}_p$ o seu corpo de frações, chamado o *corpo dos números p-ádicos*.

O método aqui apresentado, via limite inverso, não é a única maneira de se construir o anel dos inteiros p-ádicos $\mathbb{Z}_p$. De fato, as propriedades topológicas de $\mathbb{Z}_p$ vistas acima garantem que tal anel é exatamente o mesmo que pode ser construído através da métrica induzida pela *valoração p-ádica*, chamada a *métrica p-ádica*, $|\cdot|_p$. Define-se tal métrica no corpo dos números racionais $\mathbb{Q}$, e o corpo dos números p-ádicos $\mathbb{Q}_p$ é tomado como o quociente do *espaço métrico completo* com relação a $|\cdot|_p$ (que é um anel) pelo ideal maximal das sequências que tendem a zero na métrica dada. $\mathbb{Z}_p$ é então obtido como o anel de valoração $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. Referimos ao leitor o texto de Gouvêa [8] para a abordagem acima descrita dos números p-ádicos. Na Seção 3.3 de [8] (em particular, [8, Corolário 3.3.5]) tem-se a verificação de algumas das propriedades aqui descritas, que garantem que ambas as construções produzem o mesmo anel topológico.

Como visto no item **(v)** da Proposição 2.2.12, $\mathbb{Z}_p$ possui uma propriedade universal. Mais ainda, se inspecionarmos a demonstração de tal resultado, vemos que as únicas propriedades utilizadas foram as advindas do limite inverso $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$. Alternativamente, dizemos que $\mathbb{Z}_p$ é o *completamento pro-p* de $\mathbb{Z}$, e a propriedade universal supracitada nos leva à:

Definição 2.2.13. Seja G um grupo abstrato.

i. Munindo G da topologia profinita, dizemos que um par $(\widehat{G}, \iota)$ é um *completamento profinito* de G, no qual $\widehat{G}$ é um grupo profinito e $\iota : G \to \widehat{G}$ é homomorfismo contínuo, quando $\overline{\iota(G)} = \widehat{G}$ e,



para quaisquer H grupo profinito e $f : G \to H$ homomorfismo contínuo, existir um único $\varphi : \widehat{G} \to H$ homomorfismo contínuo tal que $\varphi \circ \iota = f$;

ii. Analogamente, munindo G da topologia pro-p, dizemos que um par $(\widehat{G}_p, \nu)$ é um *completamento pro-p* de G, no qual $\widehat{G}_p$ é um grupo pro-p e $\nu : G \to \widehat{G}_p$ é um homomorfismo contínuo, quando $\overline{\nu(G)} = \widehat{G}_p$ e, para quaisquer H grupo pro-p e $f : G \to H$ homomorfismo contínuo, existir um único $\varphi : \widehat{G}_p \to H$ homomorfismo contínuo tal que $\varphi \circ \nu = f$.

Antecipadamente, já fixamos acima a notação para completamentos pois, como de praxe com objetos universais, mostra-se a unicidade dos completamentos, a menos de isomorfismo topológico.

Teorema 2.2.14. Seja G um grupo arbitrário. Então:

i. Existem $(\widehat{G}, \iota)$ e $(\widehat{G}_p, \nu)$ completamentos profinito e pro-p de G, respectivamente;

ii. Se $\widehat{G}_1$ e $\widehat{G}_2$ são completamentos profinitos (ou pro-p) de G com respectivas funções $\iota_1 : G \to \widehat{G}_1$ e $\iota_2 : G \to \widehat{G}_2$, então existe um único isomorfismo de grupos topológicos $\varphi : \widehat{G}_1 \to \widehat{G}_2$ tal que $\varphi \circ \iota_1 = \iota_2$.

Demonstração. A existência de completamentos de um grupo qualquer já foi essencialmente verificada, e por isso apenas a esboçaremos aqui. Primeiramente, deve-se notar que ambos $\mathcal{N} := \mathcal{N}(G) = \{N \triangleleft G \mid [G : N] < \infty\}$ e $\mathcal{N}_p := \mathcal{N}_p(G) = \{N \triangleleft G \mid [G : N] < \infty \text{ e } G/N \text{ é } p\text{-grupo}\}$ são direcionados, similarmente ao Exemplo 2.1.8. Define-se então $\widehat{G} = \varprojlim_{N \in \mathcal{N}} G/N$ e $\widehat{G}_p = \varprojlim_{N \in \mathcal{N}_p} G/N$, com as aplicações naturais $\iota(g) = (gN)_{N \in \mathcal{N}}$ e $\nu(g) = (gN)_{N \in \mathcal{N}_p}$. Ambas são homomorfismos contínuos, pelas definições das topologias profinitas e pro-p. De maneira análoga ao feito nas demonstrações dos teoremas 2.2.7 e 2.2.8, $\iota(G) \subset \widehat{G}$ e $\nu(G) \subset \widehat{G}_p$ são densos. E, de modo inteiramente análogo ao feito na prova do item **(v)** da Proposição 2.2.12, $\widehat{G}$ e $\widehat{G}_p$ possuem as respectivas propriedades universais dos completamentos profinito e pro-p.

Verifiquemos a unicidade no caso profinito (o caso pro-p é inteiramente análogo). Da propriedade universal dos completamentos, existem únicos $\varphi := \varphi_1 : \widehat{G}_1 \to \widehat{G}_2$ e $\varphi_2 : \widehat{G}_2 \to \widehat{G}_1$ homomorfismos contínuos tais que $(\varphi \circ \varphi_2) \circ \iota_2 = \iota_2$ e $(\varphi_2 \circ \varphi) \circ \iota_1 = \iota_1$. Mais uma vez da universalidade, $id_{\widehat{G}_1}$ e $id_{\widehat{G}_2}$ são os únicos homomorfismos contínuos tais que $id_{\widehat{G}_2} \circ \iota_2 = \iota_2$ e $id_{\widehat{G}_1} \circ \iota_1 = \iota_1$. O resultado segue-se. □

Como consequência da construção dos completamentos, as aplicações $\iota : G \to \widehat{G}$ e $\nu : G \to \widehat{G}_p$ são injetivas se, e somente, G é um grupo, respectivamente, *residualmente finito* ou *residualmente* p, isto é, a interseção de seus subgrupos normais de índice finito é trivial (respectivamente, a interseção de seus subgrupos normais cujos índices são potências de p é trivial).

2.3 Grupos Pro-p Finitamente Gerados

Definição 2.3.1. Sejam G um grupo profinito e $X \subset G$. Dizemos que X gera G como grupo topológico quando o subgrupo abstrato $\langle X \rangle$ é denso em G, isto é, $G = \overline{\langle X \rangle}$. Quando X é finito, dizemos que G é finitamente gerado (como grupo topológico). Nesse caso, denotamos $d(G)$ como sendo a menor cardinalidade dentre os conjuntos geradores de G. Caso G não seja finitamente gerado, denotamos $d(G) = \infty$.

Quando não houver risco de confusão, diremos simplesmente que o conjunto X gera o grupo profinito G, ao invés de dizer que X gera G topologicamente.

Exemplo 2.3.2. O grupo abeliano aditivo $\mathbb{Z}_p$ é gerado, como grupo topológico, por $\{1\}$, pois $\langle 1 \rangle = \mathbb{Z}$ e $\overline{\mathbb{Z}} = \mathbb{Z}_p$. Assim como $\mathbb{Z}$ é o único grupo cíclico infinito, seu análogo pro-p $\mathbb{Z}_p$ é o único grupo pro-p *procíclico* (i.e., um grupo topológico que é o limite inverso de p-grupos cíclicos finitos).

Exemplo 2.3.3. De maneira geral, devido ao item **(vi)** da Proposição 2.2.12, todo grupo pro-p procíclico G (ou seja, tal que $d(G) = 1$) pode ser caracterizado por $G = \overline{\langle g \rangle} = \{g^z \mid z \in \mathbb{Z}_p\}$, para algum $g \in G \setminus \{1\}$.

Exemplo 2.3.4. Analogamente a $\mathbb{Z}_p$, o completamento profinito $\widehat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ de $\mathbb{Z}$ é tal que $d(\widehat{\mathbb{Z}}) = 1$, pois $\langle 1 \rangle = \mathbb{Z}$ e $\overline{\mathbb{Z}} = \widehat{\mathbb{Z}}$.

Assim como subgrupos de índice finito em grupos abstratos finitamente gerados são também finitamente gerados, tem-se um resultado semelhante no caso profinito:

Proposição 2.3.5. Se G é um grupo profinito com $d(G) < \infty$ e $H \leq_o G$, então H também é finitamente gerado.

Demonstração. Tome um subconjunto finito $\widetilde{X} \subset G$ tal que $G = \overline{\langle \widetilde{X} \rangle}$. Defina $X = \widetilde{X} \cup \widetilde{X}^{-1}$. Tem-se que X é finito, $X^{-1} = X$, e vale ainda $G = \overline{\langle X \rangle}$. Como H é aberto e G é compacto, o índice $n = [G : H]$ é finito. Logo, podemos tomar $T = \{t_1, \ldots, t_n\} \subset G$ tal que $G = \cup_{i=1}^{n} H t_i$, e podemos supor que $1 \in T$, digamos $t_1 = 1$. Para cada $g \in G$, denote s_g o elemento de T tal que $Hg = Hs_g$. Com isso, defina $Y = \{tx(s_{tx})^{-1} \mid x \in X,\ t \in T\}$. Como X e T são finitos, Y é também finito. Denote $K = \overline{\langle Y \rangle}$. Por construção, K é (topologicamente) finitamente gerado

e $K \leq_c H$. Mostremos que de fato vale $K = H$. Dados $k \in K$, $x \in X$ e $t \in T$, tem-se que $ktx = ktx(s_{tx})^{-1}s_{tx} \in KT$. Em particular, como $1 \in KT$, obtem-se que $X \subseteq KTX \subseteq KT$, e indutivamente qualquer produto finito $X \cdot X \cdots X$ está contido em KT. Por ser $X = X^{-1}$, segue-se que $\langle X \rangle \leq KT$. Mas $K \leq_c G$ e T é finito, donde $G = \overline{\langle X \rangle} \subseteq KT \subseteq G$. Ou seja, $\cup_{i=1}^{n} Ht_i = G = \cup_{i=1}^{n} Kt_i$, e conclui-se que $H \subseteq K$. □

Definição 2.3.6. Dado um grupo profinito G, a interseção de todos os seus *subgrupos maximais abertos* (próprios) é dita o *subgrupo de Frattini* de G, denotado $\Phi(G)$.

Note que o subgrupo de Frattini $\Phi(G)$ é um subgrupo normal fechado. Isso segue do fato de que $\Phi(G)$ é um *subgrupo característico* do grupo profinito G, isto é, para cada automorfismo contínuo $f : G \to G$ vale $f(\Phi(G)) \subseteq \Phi(G)$. Tal afirmação é consequência da propriedade de que isomorfismos (no caso, contínuos) preservam subgrupos maximais. Fica definido então o grupo profinito $G/\Phi(G)$, chamado o *quociente de Frattini* de G.

No caso de grupos pro-p, o subgrupo de Frattini possui propriedades interessantes. Começaremos com alguns resultados básicos, do caso geral.

Definição 2.3.7. Um elemento g de um grupo profinito G é dito um *não-gerador* quando a implicação $(G = \overline{\langle X, g \rangle} \implies G = \overline{\langle X \rangle})$ for verdadeira, para qualquer conjunto de geradores $X \subset G$. Em outras palavras, g pode ser omitido de qualquer conjunto de geradores de G.

Proposição 2.3.8. Para qualquer G grupo profinito, $\Phi(G) = \{g \in G \mid g \text{ é não-gerador }\}$.

Demonstração. Denote $\widetilde{N} = \{g \in G \mid g \text{ é não gerador}\}$.

Lembremos que todo subgrupo aberto de um grupo topológico é também fechado. Seja H subgrupo aberto maximal (próprio) de G. Dado $g \in G$ um não-gerador, suponha, por absurdo, que $g \notin H$. Considere o subgrupo $\overline{\langle H, g \rangle}$. Tem-se $\overline{\langle H \rangle} = \overline{H} = H \subsetneq G$, de modo que $\overline{\langle H, g \rangle} = G$ já que H é maximal (próprio). Como g é não-gerador, $\overline{\langle H, g \rangle} = H \neq G$, uma contradição. Logo, $g \in H$ e assim $\widetilde{N} \subseteq \Phi(G)$.

Reciprocamente, seja $g \in \Phi(G)$ e suponha, por absurdo, que $g \notin \widetilde{N}$. Isso significa que existe $X \subsetneq G$ tal que $\overline{\langle X, g \rangle} = G$ mas $\overline{\langle X \rangle} \neq G$. Como $\overline{\langle X \rangle}$ é fechado, tem-se $\overline{\langle X \rangle} = \bigcap_{N \in \mathcal{N}} N\overline{\langle X \rangle}$, no qual $\mathcal{N} = \{N \subset G \mid N \text{ é subgrupo normal aberto}\}$. Podemos tomar então $M \leq_o G$ maximal com respeito às propriedades de *conter* $\overline{\langle X \rangle}$ e *não* conter g. Nesse caso, M é de fato subgrupo maximal de G, pois se $M \subsetneq H \leq_o G$, então $H \geq \overline{\langle X, g \rangle} = G$. Com isso, $g \notin M \supset \Phi(G)$, uma contradição. Portanto $g \in \widetilde{N}$, isto é, $\Phi(G) \subseteq \widetilde{N}$, como queríamos. □

Proposição 2.3.9. Sejam G grupo profinito, H subgrupo fechado de G, e $X \subset \Phi(G)$ qualquer. Se $G = \overline{\langle H, X \rangle}$, então $G = H$. Em particular, se $H\Phi(G) = G$, então $G = H$.

Demonstração. Como $\Phi(G)$ é o conjunto dos não-geradores de G, tem-se que $G = \overline{\langle H, X \rangle} = \overline{\langle H \rangle} = \overline{H} = H$. □

Lema 2.3.10. Seja G grupo profinito finitamente gerado. Então $d(G) = d(G/\Phi(G))$.

Demonstração. Denote $\pi : G \twoheadrightarrow \frac{G}{\Phi(G)}$ a projeção canônica. Evidentemente, $d(G) \geq d(G/\Phi(G))$. Seja $X \subset G$ tal que $\pi(X)$ gera $G/\Phi(G)$ e $d(G/\Phi(G)) = |X|$. Então $G = \overline{\pi^{-1}(\langle \pi(X) \rangle)} = \overline{\langle X \rangle}\Phi(G) = \overline{\langle X, \Phi(G) \rangle} = \overline{\langle X \rangle}$, pela Proposição 2.3.9. Logo, $d(G/\Phi(G)) \geq d(G)$. □

Daremos agora a caracterização mais forte do subgrupo de Frattini no caso pro-p.

Teorema 2.3.11. Seja G um grupo pro-p. Então:

i. Todo subgrupo maximal aberto (próprio) de G tem índice p;

ii. O quociente de Frattini $G/\Phi(G)$ é um espaço vetorial sobre o corpo $\mathbb{F}_p$ de ordem p. Em particular, se G é finitamente gerado, então $G/\Phi(G) = \bigoplus_{i=1}^{d(G)} \mathbb{F}_p$;

iii. $\Phi(G) = \overline{G'G^p}$, no qual $G^p = \{g^p \mid g \in G\}$ é o subgrupo das p-potências de G, e $G' = [G, G]$ é o subgrupo dos comutadores.

Demonstração. **i**. Seja M subgrupo maximal aberto de G. Então M é fechado, e M tem índice finito em G por ser G compacto. Considere $M_G = \bigcap_{g\in G} g^{-1}Mg$ o *cerne* de M em G, seu maior subgrupo o qual é normal em G. Como $[G : M] < \infty$, o índice de M_G em G é também finito. Tem-se que M_G é subgrupo (normal) fechado de G. Logo, $\widetilde{G} = G/M_G$ é um p-grupo finito, e $\widetilde{M} = M/M_G$ é um subgrupo maximal de $\widetilde{G}$. Considere $N_{\widetilde{G}}(\widetilde{M}) = \{\bar{g} \in \widetilde{G} \mid \bar{g}^{-1}\widetilde{M}\bar{g} = \widetilde{M}\}$ o *normalizador* de $\widetilde{M}$ em $\widetilde{G}$, e

$$\gamma_1(\widetilde{G}) = \widetilde{G} \geq \gamma_2(\widetilde{G}) = [\widetilde{G}, \widetilde{G}] = \widetilde{G}' \geq \gamma_3(\widetilde{G}) = [\gamma_2(\widetilde{G}), \widetilde{G}] \geq \dots$$

a *série central descendente* de $\widetilde{G}$. Como todo p-grupo finito é nilpotente, a série central descendente de $\widetilde{G}$ estabiliza no subgrupo trivial, e portanto existe índice i tal que $\gamma_{i+1}(\widetilde{G}) \leq \widetilde{M}$ mas $\gamma_i(\widetilde{G}) \subsetneq \widetilde{M}$. Como $[\gamma_i(\widetilde{G}), \widetilde{M}] \leq [\gamma_i(\widetilde{G}), \widetilde{G}] = \gamma_{i+1}(\widetilde{G}) \leq \widetilde{M}$, segue-se que $\gamma_i(\widetilde{G}) \leq N_{\widetilde{G}}(\widetilde{M})$ e, em particular, $\widetilde{M} \subsetneq N_{\widetilde{G}}(\widetilde{M})$. Como $\widetilde{M}$ é subgrupo maximal de $\widetilde{G}$, segue-se que $N_{\widetilde{G}}(\widetilde{M}) = \widetilde{G}$, isto é, $\widetilde{M}$ é normal em $\widetilde{G}$. Agora, a maximalidade de $\widetilde{M}$ implica que o p-grupo finito $\widetilde{G}/\widetilde{M}$ não possui subgrupos não-triviais. Logo, $\widetilde{M}$ tem índice p em $\widetilde{G}$, e portanto

$$[G : M] = \left|\frac{G/M_G}{M/M_G}\right| = [\widetilde{G} : \widetilde{M}] = p.$$

ii. Escreva $\Phi(G) = \bigcap\limits_{\lambda\in L} M_\lambda$, sendo $\{M_\lambda\}_{\lambda\in L}$ a família de todos os subgrupos maximais abertos de G. Considere o homomorfismo

$$\begin{aligned} f : G &\longrightarrow\!\!\!\!\!\rightarrow \prod_{\lambda\in L} \frac{G}{M_\lambda} \\ g &\longmapsto (gM_\lambda)_{\lambda\in L}. \end{aligned}$$

Tem-se que $\ker(f) = \bigcap_{\lambda\in L} M_\lambda = \Phi(G)$. Pelo item anterior, $G/M_\lambda \cong \mathbb{F}_p$, e assim $\mathrm{Im}(f)$ é um subespaço do espaço vetorial $\prod\limits_{\lambda\in L} \mathbb{F}_p$. O resultado segue-se do Teorema do Isomorfismo.

iii. Como $G/\Phi(G)$ é espaço vetorial sobre o corpo $\mathbb{F}_p$, vale que $G/\Phi(G)$ é abeliano e cada elemento $\overline{g} \in G/\Phi(G)$ é tal que $(\overline{g})^{p+1} = \overline{g}$. Logo, $\overline{G'G^p} \subset \Phi(G)$.

Seja agora $a \in G \backslash \overline{G'G^p}$ arbitrário. Mostremos que $a \notin \Phi(G)$. Como G é Hausdorff e compacto, existem $U_1, U_2 \subset G$ abertos disjuntos tais que $a \in U_1$ e $\overline{G'G^p} \subset U_2$. Note que $1 \in U_2$, já que $\overline{G'G^p}$ é subgrupo. Pelo Teorema 2.2.8, existe N subgrupo normal aberto de G tal que $N \subset a^{-1}U_1$ e $N \subset U_2$, de modo que $aN \cap \overline{G'G^p} = \varnothing$. Considere os p-grupos finitos

$$H = G/N \text{ e } K = \frac{\overline{G'G^p}N}{N} \lhd H,$$

e denote $\overline{a} = aN \in H$. O quociente H/K é um grupo abeliano finito com a propriedade de que para todo $h \in H$ tem-se $h^p \in K$. Segue-se da Classificação de Grupos Abelianos Finitos que H/K é isomorfo a uma soma direta finita $\bigoplus_{i=1}^n \mathbb{F}_p$. Como $aN \cap \overline{G'G^p} = \varnothing$, tem-se que $\overline{a}K$ é um elemento não-trivial de $H/K \cong \bigoplus_{i=1}^n \mathbb{F}_p$. Sendo $\mathbb{F}_p$ cíclico de ordem prima p, podemos construir $\widetilde{M}$ subgrupo maximal do p-grupo finito $H = G/N$ tal que sua projeção em H/K é um subgrupo maximal que *não* contem $\overline{a}K$, no qual $\overline{a} = aN$. Isso significa que podemos obter M subgrupo maximal aberto de G tal que $a \notin M \supset \Phi(G)$. Portanto, $\Phi(G) \subset \overline{G'G^p}$.

□

Em outras palavras, o teorema acima nos diz que o quociente de Frattini $G/\Phi(G)$ de um grupo pro-p G é seu quociente maximal abeliano de expoente p.

Encerramos esta seção com uma equivalência que relaciona a quantidade de geradores de um grupo pro-p à estrutura topológica de seu subgrupo de Frattini.

Proposição 2.3.12. Seja G um grupo profinito finitamente gerado. Para cada $n \in \mathbb{N}$, G admite apenas um número *finito* de subgrupos normais abertos cujos índices são iguais a n.

Demonstração. Se $N \lhd_o G$, então $N = \ker \varphi_N$, para algum epimorfismo $\varphi_N : G \twoheadrightarrow X$, no qual X é um grupo finito com $|X| = n = [G : N]$. Agora, como G é finitamente gerado, cada tal epimorfismo φ_N fica unicamente determinado pelas imagens por φ_N dos geradores de G no grupo finito X. Logo, o conjunto $\{\varphi_N \mid \varphi_N : G \twoheadrightarrow X \text{ é epimorfismo}\}$ é finito. Como existe apenas uma quantidade finita de grupos X cuja cardinalidade é n, o resultado segue-se. □

Teorema 2.3.13. Seja G um grupo pro-p. G é finitamente gerado se, e somente se, seu subgrupo de Frattini $\Phi(G)$ é aberto.

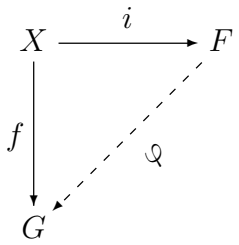
Demonstração. Suponha G finitamente gerado. Pelo Teorema 2.3.11, cada subgrupo maximal aberto M de G tem índice índice p. Pela Proposição 2.3.12, existe apenas uma quantidade finita de tais subgrupos maximais abertos, digamos $M_1, \ldots, M_n$. Ou seja, $\Phi(G) = \bigcap_{i=1}^n M_i$. Logo, $\Phi(G)$ é aberto, por ser a interseção finita de abertos.

Reciprocamente, suponha $\Phi(G)$ aberto. Sendo então $\Phi(G) \lhd_o G$, vale que o quociente de Frattini $G/\Phi(G)$ é um p-grupo finito, donde existe $X \subseteq G$ conjunto finito tal que $\pi(X)$ gera $G/\Phi(G)$, no qual $\pi : G \twoheadrightarrow G/\Phi(G)$ denota a projeção canônica. Com isso, $G = \overline{\langle X \rangle}\Phi(G) = \overline{\langle X \rangle}$, pela Proposição 2.3.9. □

2.4 Grupos Pro-p Livres e Apresentações de Grupos Pro-p

Nesta seção fazemos um paralelo ao estudo feito no Capítulo 1 sobre grupos livres abstratos. Novamente via uma propriedade universal define-se, agora no cenário pro-p, um objeto análogo ao grupo livre abstrato (1.1.1). Nosso objetivo é traduzir para o contexto pro-p a noção de apresentações (1.2.1) e apresentações finitas (1.3.1), e estudar algumas propriedades de grupos pro-p finitamente apresentáveis. As noções de grupo pro-p livre aqui usadas seguem as linhas de [16].

Definição 2.4.1. Sejam X um espaço topológico profinito, F um grupo pro-p e $i : X \to F$ uma aplicação contínua tal que a imagem de X por i gera F como grupo topológico, isto é, $F = \overline{\langle i(X)\rangle}$. Dizemos que F (com a aplicação i) é um *grupo pro-p livre* sobre o espaço profinito X quando,



dados quaisquer G grupo pro-p e $f : X \to G$ função contínua com $\overline{\langle f(X)\rangle} = G$, existir um único homomorfismo contínuo $\varphi : F \to G$ tal que $\varphi \circ i = f$. Nesse caso, dizemos que φ é o homomorfismo (contínuo) que estende a função contínua f, e dizemos ainda que X é uma *base* de F.

Semelhante ao que ocorre no caso abstrato, tem-se os seguintes resultados básicos.

Proposição 2.4.2. Se F é um grupo pro-p livre sobre um espaço profinito X com a aplicação $i : X \to F$, então i é injetiva e $1 \notin i(X)$.

Demonstração. Se $X = \{x\}$, segue-se da propriedade universal do grupo pro-p livre que existe um único homomorfismo contínuo $\varphi : F \to \mathbb{F}_p$ tal que $\varphi \circ i(x) = 1 \in \mathbb{F}_p$, donde $i(X) \cap \ker \varphi = \varnothing$.

Suponha agora que X tenha pelo menos dois elementos, e sejam $x, y \in X$ distintos. Consideremos a coleção $\mathcal{R}$ de todas as relações de equivalência R de X tais que suas respectivas classes laterais $zR \subset X$ são subespaços simultaneamente abertos e fechados em X. Pelo item **(iii)** do Teorema 2.1.18, existe $R \in \mathcal{R}$ tal que as classes laterais xR e yR são distintas. Considere o espaço X/R com a topologia quociente, G o p-grupo finito $G = \mathbb{F}_p \oplus \mathbb{F}_p$, e $\widetilde{f} : X/R \to G$ uma aplicação contínua qualquer tal que $\widetilde{f}(xR) = (1, 0)$ e $\widetilde{f}(yR) = (0, 1)$. Ponha $f : X \to G$ a composição $f = \widetilde{f} \circ \pi$, no qual $\pi : X \twoheadrightarrow X/R$ denota a projeção canônica. Tem-se então que f é contínua e, da universalidade do grupo pro-p livre, existe único homomorfismo contínuo $\varphi : F \to G$ tal que $\varphi \circ i = f$. Como $f(x) \neq f(y)$, vem $i(x) \neq i(y)$, e assim i é injetiva. Além disso, por construção, $\{i(x), i(y)\} \cap \ker \varphi = \varnothing$, de modo que a arbitrariedade de $x, y \in X$ implica que $1 \notin i(X)$. □

Teorema 2.4.3. Seja X um espaço profinito. Então:

i. Existem F grupo pro-p e $i : X \to F$ função contínua tais que F (com a função i) é grupo pro-p livre sobre X;

ii. Se F_1 e F_2 são grupos pro-p livres sobre X, com respectivas funções $i_1 : X \to F_1$ e $i_2 : X \to F_2$, então existe um único isomorfismo de grupos topológicos $\varphi : F_1 \to F_2$ tal que $\varphi \circ i_1 = i_2$.

Demonstração. **i**. Seja F_X o grupo livre *abstrato* (1.1.1) com base X, identificando o espaço $X \hookrightarrow F_X$, e considere

$$\mathcal{N} = \{N \lhd F_X \mid [F_X : N] \text{ é potência de } p \text{ e, } \forall g \in F_X,\ gN \cap X \text{ é aberto em } X\}.$$

Tem-se então que $\mathcal{N}$ é conjunto direcionado, pela ordem induzida pela inclusão de conjuntos (analogamente ao Exemplo 2.1.8). Ponha $(F, \varphi_N)_{\mathcal{N}} = \varprojlim_{N\in\mathcal{N}}(F_X/N, \varphi_{MN})_{\mathcal{N}}$, e $i : X \to F$ a restrição a X do homomorfismo natural $\iota : F_X \to \varprojlim F_X/N$ dado por $\iota(g) = (gN)_{N\in\mathcal{N}}$. Como para cada $M \in \mathcal{N}$ as composições $\varphi_M \circ i(x) = xM$ são contínuas, segue-se da Proposição 2.1.15 que i é contínua. Sejam agora G um grupo pro-p e $f : X \to G$ contínua tal que $\overline{\langle f(X)\rangle} = G$. Verifiquemos para F a propriedade universal de grupo pro-p livre. Como G é o limite inverso de p-grupos finitos, digamos $(G, \psi_j) = \varprojlim(G_j, \psi_{jk})$, basta verificar a propriedade para cada p-grupo G_j e as aplicações contínuas $f_j := \psi_j \circ f : X \to G_j$ assumindo $G_j = \langle f_j(X)\rangle$. Ou seja, queremos mostrar que existe um único homomorfismo contínuo $\varphi_j : F \to G_j$ tal que $\varphi_j \circ i = f_j$. Por ser F_X o grupo livre (abstrato) com base X, existe (único) epimorfismo (de grupos abstratos) $\widetilde{\varphi}_j : F_X \twoheadrightarrow G_j$ tal que $\widetilde{\varphi}_j|_X = f_j$. Como G_j é p-grupo finito, tem-se $H := \ker\widetilde{\varphi}_j \in \mathcal{N}$, e a composição $\varphi_j : F \xrightarrow{\varphi_H} F_X/H \xrightarrow{\cong} G_j$ é o único homomorfismo contínuo tal que $\varphi_j \circ i = f_j$.

ii. Da universalidade do grupo pro-p livre, id_{F_1} e id_{F_2} são os únicos homomorfismos contínuos tais que $id_{F_1} \circ i_1 = i_1$ e $id_{F_2} \circ i_2 = i_2$. Novamente da universalidade, existem únicos homomorfismos contínuos $\varphi_1 : F_1 \to F_2$ e $\varphi_2 : F_2 \to F_1$ tais que $\varphi_1 \circ i_1 = i_2$ e $\varphi_2 \circ i_2 = i_1$. Logo, $(\varphi_1 \circ \varphi_2) \circ i_2 = i_2$ e $(\varphi_2 \circ \varphi_1) \circ i_1 = i_1$, e assim a unicidade inicialmente apontada implica $\varphi_1 \circ \varphi_2 = id_{F_2}$ e $\varphi_2 \circ \varphi_1 = id_{F_1}$. Portanto $\varphi := \varphi_1 : F_1 \to F_2$ é isomorfismo de grupos topológicos.

□

Mais uma vez, temos unicidade do objeto universal em questão, e passamos a tratar *do* grupo pro-p livre sobre um espaço profinito X, denotado $\widehat{F(X)}_p$. Dado então um grupo pro-p G, dizemos que G é livre com base X quando G é isomorfo (como grupo topológico) ao grupo pro-p livre $\widehat{F(X)}_p$ sobre o espaço profinito X.

Uma observação. Alguns autores consideram o grupo pro-p livre $\widehat{F(X)}_p$ com uma restrição a mais: a aplicação $i : X \to \widehat{F(X)}_p$ deve *convergir a* 1, isto é, todo aberto de $\widehat{F(X)}_p$ contem todos os pontos de $i(X)$, à exceção de um número finito de tais pontos. Um tal grupo às vezes é denotado $F^r_{\hat{p}}(X)$, o grupo pro-p livre *restrito*. A razão para não considerarmos tal restrição neste trabalho se deve ao nosso interesse em grupos finitamente apresentáveis: se a base X do grupo pro-p livre $\widehat{F(X)}_p$ é finita (espaço topológico discreto compacto), então $\widehat{F(X)}_p$ coincide com o grupo pro-p livre restrito $F^r_{\hat{p}}(X)$.

Daqui em diante particularizaremos nosso estudo de grupos pro-p livres àqueles que possuem base *finita*. Em particular, resultados obtidos na Seção 2.3 valem para tais grupos.

Não à toa escolhemos a notação $\widehat{F(X)}_p$ para representar o grupo pro-p livre com base X. De fato, a demonstração dada no Teorema 2.4.3 evidencia a ligação entre o grupo livre abstrato e o grupo livre pro-p, a saber, via o completamento pro-p, visto na Seção 2.2.1. A seguir enunciamos resultados estabelecendo tal ligação.

Proposição 2.4.4. Seja $F = \widehat{F(X)}_p$ o grupo pro-p livre sobre um conjunto finito X com n elementos. Então qualquer conjunto de geradores de F com n elementos é uma base de F. Além disso, se $\widetilde{X}$ é uma outra base de F, vale $|\widetilde{X}| = n$.

Demonstração. Denote $X = \{x_1, \dots, x_n\}$ e seja $Y = \{y_1, \dots, y_n\} \subset F$ um outro conjunto gerador de F. Da universalidade, considere $\varphi : F \to F$ o (único) homomorfismo contínuo tal que $\varphi(x_i) = y_i$. Tem-se então que φ é epimorfismo. Queremos garantir que φ é isomorfismo de grupos topológicos. Se φ for injetiva então φ será também homeomorfismo, já que F é compacto. Basta mostrar então a injetividade de φ. Para cada $n \in \mathbb{N}$, considere $\mathcal{N}_n = \{N \lhd F \mid N \text{ é aberto e } [F : N] = n\}$ e a função $\Psi_n : \mathcal{N}_n \to \mathcal{N}_n$ dada por $\Psi_n(N) = \varphi^{-1}(N)$. Tem-se que Ψ_n é injetiva e, como $\mathcal{N}_n$ é finito pela Proposição 2.3.12, segue-se que Ψ_n é uma bijeção. Mas, se M é um qualquer subgrupo normal aberto de F, então M é um p-grupo finito, e assim existem $n \in \mathbb{N}$ e $N \in \mathcal{N}_n$ tais que $M = \Psi_n(N) = \varphi^{-1}(N)$. Em particular, $M \supseteq \varphi^{-1}(\{1\}) = \ker\varphi$, donde $\ker\varphi \subseteq \bigcap_{N \lhd_o F} N = \{1\}$.

Agora, seja $\widetilde{X} = \{z_1, \dots, z_m\}$ outra base de F e suponha, por absurdo, que $m \neq n$. Sem perda de generalidade, suponha $m > n$. Considere $f : \widetilde{X} \to F$ dada por $f(z_i) = x_i$, se $1 \leq i \leq n$, e $f(z_i) = 1$, caso contrário. Da universalidade, existe homomorfismo contínuo $\varphi : \widehat{F(\widetilde{X})}_p \to F$ que estende f, e φ é evidentemente sobrejetivo. Por argumento inteiramente análogo ao acima, obtem-se que $\ker\varphi \subseteq \bigcap_{N \lhd_o F(\widetilde{X})_{\hat{p}}} N = \{1\}$, donde $\widehat{F(\widetilde{X})}_p$ é isomorfo a F, uma contradição. Portanto, $|\widetilde{X}| = n$. □

Em decorrência da proposição acima, estabelecemos a:

Definição 2.4.5. Dado um grupo pro-p livre $F = \widehat{F(X)}_p$ com base X, definimos $\text{posto}(F) = |X|$, a cardinalidade de uma (qualquer) base de F.

Note que $\text{posto}(\widehat{F(X)}_p) = d(\widehat{F(X)}_p)$, i.e., a cardinalidade da base de $\widehat{F(X)}_p$ é obrigatoriamente seu número minimal de geradores.

Teorema 2.4.6. Seja F_X o grupo livre abstrato sobre um conjunto finito X. Então o completamento pro-p $\widehat{F}_p$ de F_X é o grupo pro-p livre com base X. Em particular, $\text{posto}(F_X) = \text{posto}(\widehat{F(X)}_p)$.

Demonstração. Segue imediatamente da construção do grupo pro-p livre $\widehat{F(X)}_p$ dado no Teorema 2.4.3, e da proposição anterior. □

Citemos ainda o seguinte resultado, análogo ao caso abstrato dado no Teorema de Nielsen-Schreier 1.1.10.

Teorema 2.4.7. Sejam $\widehat{F(X)}_p$ o grupo pro-p livre sobre um espaço finito X e H subgrupo aberto de $\widehat{F(X)}_p$. Então H é um grupo pro-p livre com base finita, e

$$\text{posto}(H) = [\widehat{F(X)}_p : H](\text{posto}(\widehat{F(X)}_p) - 1) + 1.$$

Referimos ao leitor [21, Teorema 5.4.4, p. 82] ou [16, Teorema 3.6.2, p. 118] para demonstrações do resultado acima. Tal teorema, assim como diversas outras conexões entre grupos abstratos e grupos pro-p, são devidos à ligação entre ambos os casos via completamentos. O Teorema 2.4.6 evidencia mais ainda tal ligação, e assim alguns resultados do cenário abstrato podem ser traduzidos, com uma certa adequação ao contexto, ao cenário pro-p.

Proposição 2.4.8. Todo grupo pro-p é quociente de um grupo pro-p livre.

Demonstração. Seja G um grupo pro-p arbitrário e fixe $X \subseteq G$ um subespaço profinito tal que $\overline{\langle X \rangle} = G$, e denote $f : X \hookrightarrow G$ a inclusão. Considere $\widehat{F(X)}_p$ o grupo pro-p livre com base X. Pela universalidade, existe um homomorfismo contínuo $\varphi : \widehat{F(X)}_p \to G$ que estende f. Como $\widehat{F(X)}_p$ é compacto e $\langle X \rangle$ é denso em G e φ é homomorfismo contínuo, segue-se que φ é sobrejetiva. □

Assim como no caso abstrato, graças à proposição acima podemos formalizar as noções de apresentações e apresentações finitas de grupos pro-p.

Definição 2.4.9. Dados G um grupo pro-p, X um espaço profinito e $R \subset \widehat{F(X)}_p$ um subconjunto do grupo pro-p livre com base X, dizemos que o par (X, R) é uma *apresentação* do grupo pro-p G quando $G \cong \widehat{F(X)}_p/N$, no qual $N = \overline{\langle R^{\widehat{F(X)}_p} \rangle}$ é o menor subgrupo normal fechado de $\widehat{F(X)}_p$ contendo R. Nesse caso, os elementos de X são ditos os *geradores* de G, e os elementos de R são ditas as *relações* na apresentação dada, e denotamos $G = \overline{\langle X \mid R \rangle}_{\hat{p}}$ para dizer que (X, R) é uma apresentação do grupo pro-p G.
Equivalentemente, dados G um grupo pro-p, X espaço profinito e $\pi : \widehat{F(X)}_p \twoheadrightarrow G$ um epimorfismo contínuo do grupo pro-p livre com base X sobre G, dizemos que π é uma *apresentação* de G. Nesse caso, tomando-se um subconjunto $R \subset \widehat{F(X)}_p$ tal que $\ker \pi = \overline{\langle R^{\widehat{F(X)}_p} \rangle}$, retorna-se à notação acima e diz-se que o par (X, R) é uma apresentação de G.

Definição 2.4.10. Um grupo pro-p G é dito *finitamente apresentável* quando admite alguma apresentação $G = \overline{\langle X \mid R \rangle}_{\hat{p}}$ tal que X e R sejam ambos finitos.

Definição 2.4.11. Dado N subgrupo normal fechado de um grupo pro-p G, definimos $d_G(N)$ a ser a menor cardinalidade dentre os subconjuntos de G que geram N como subgrupo normal fechado de G. Em outras palavras, se $R \subset G$ é um conjunto de cardinalidade mínima tal que $N = \overline{\langle R^G \rangle}$, então $d_G(N) = |R|$ (podendo ser $|R| = \infty$).
Em particular, se $\pi : \widehat{F(X)}_p \twoheadrightarrow G$ é uma apresentação de um grupo pro-p G, então o *número de relações* em tal apresentação é $d_{\widehat{F(X)}_p}(\ker \pi)$.

Motivados pela ligação entre o grupo livre abstrato F_X e o grupo pro-p livre $\widehat{F(X)}_p$, estabelecemos o seguinte:

Teorema 2.4.12. Se G é um grupo abstrato com apresentação finita $\langle X \mid R\rangle$, então o completamento pro-p $G_{\hat{p}}$ admite apresentação (finita) $\overline{\langle X \mid R\rangle}_{\hat{p}}$, como grupo pro-$p$.

Demonstração. Basta checar a propriedade universal do completamento pro-p (2.2.13) para o grupo $\overline{\langle X \mid R\rangle}_{\hat{p}}$, observando que a própria construção de $\widehat{F(X)}_p$ é feita via o completamento pro-p de F_X, como na prova do Teorema 2.4.3. □

Formalmente, o resultado acima nos permite construir diversos grupos pro-p através de apresentações finitas de grupos abstratos, bem como traduzir algumas propriedades de grupos abstratos finitamente apresentáveis – com um certo cuidado topológico – para o cenário pro-p. Daqui em diante utilizaremos tal construção livremente, sem maiores comentários.

Exemplo 2.4.13. O grupo aditivo dos inteiros p-ádicos $\mathbb{Z}_p$ é finitamente apresentável, com $\mathbb{Z}_p = \overline{\langle 1 \mid \varnothing\rangle}_{\hat{p}}$.

Exemplo 2.4.14. Mais geralmente, todo grupo pro-p livre é finitamente apresentável. Como no caso abstrato, tais grupos são os únicos a admitirem apresentações sem relações.

Exemplo 2.4.15. Todo p-grupo finito é finitamente apresentável, visto como grupo pro-p (cf. [21, p. 239]).

Prosseguiremos com alguns resultados acerca de apresentações finitas de grupos pro-p, com particular interesse na quantidade de relações a partir da quantidade de geradores numa apresentação dada.

As próximas proposições são análogas ao que ocorre no caso abstrato: certos subgrupos de índice finito e extensões de grupos pro-p finitamente apresentáveis também são finitamente apresentáveis.

Proposição 2.4.16. Sejam $G = \overline{\langle X \mid R\rangle}_{\hat{p}}$ grupo pro-p finitamente apresentável com $|X| = d$ e $|R| = r$, e $H \leq_o G$ com índice n. Então H admite apresentação finita com $d_1 = n(d-1)+1$ geradores e $r_1 = nr$ relações.

Demonstração. Replicaremos a demonstração dada no caso abstrato (cf. Proposição 1.3.2).

Denote $F = \widehat{F(X)}_p$, $\pi : F \twoheadrightarrow G$ o epimorfismo proveniente da apresentação $G = \overline{\langle X \mid R\rangle}_{\hat{p}} \cong F/N$, $\ker\pi = N = \overline{\langle R^F\rangle}$. Denote por $F_1 = \pi^{-1}(H) \leq_o F$. Tem-se $\text{posto}(F_1) = d_1$ e, pelo Teorema 2.4.7, F_1 é grupo pro-p livre e vale que $\text{posto}(F_1) = d_1 = [F : F_1](d-1)+1$. Sendo $[G : H] = n$, vem $[F : F_1] = n$, ou seja, $d_1 = n(d-1)+1$.

Como o índice de F_1 em F é n, podemos tomar $T = \{t_1, \ldots, t_n\}$ conjunto finito de F tal que $F = \cup_{i=1}^n t_i F_1$. Denote $R = \{u_1, \ldots, u_r\}$. Para cada $f \in F$, existe (único) j tal que $f \in t_j F_1$, digamos $f = t_j \tilde{f}$. Com isso, $f^{-1}u_i f = \tilde{f}^{-1}t_j^{-1}u_i t_j \tilde{f} \in \{t_j^{-1}u_i t_j\}^{F_1}$. Logo, $R \subseteq \ker\pi = \pi^{-1}(\{1\}) \subset \pi^{-1}(H) = F_1$. Mais ainda, $\overline{\langle R^F\rangle} = \overline{\langle (\cup_{j=1}^n R^{t_j})^{F_1}\rangle}$, de modo que o conjunto $R_0 = \cup_{j=1}^n R^{t_j}$ gera (topologicamente) o núcleo da restrição $\pi_1 = \pi|_{F_1} : F_1 \twoheadrightarrow H$. Logo, $r_1 = |R_0| = \sum_{j=1}^n |R^{t_j}| = n \cdot |R| = nr$. □

Proposição 2.4.17. Sejam G um grupo pro-p e $K \lhd_c G$. Se K e G/K são finitamente apresentáveis, então G é finitamente apresentável.

Demonstração. Basta replicar a prova dada no caso abstrato (cf. Proposição 1.3.3), bastando readequar os conceitos: grupos abstratos por grupos pro-p, homomorfismos por homomorfismos contínuos, e subgrupos por subgrupos fechados. □

Os próximos lemas visam a demonstração da próxima proposição, que estabelece relações entre o número de geradores e relações em apresentações distintas de um mesmo grupo pro-p.

Lema 2.4.18. Sejam F um grupo pro-p livre sobre um conjunto finito X, F_1 subgrupo fechado gerado por $X_1 \subset X$ e $N_1 \lhd_c F_1$. Denote N o menor subgrupo normal fechado de F contendo $N_1 \cup (X \setminus X_1)$. Se $d_{F_1}(N_1) < \infty$, então $d_F(N) = d_{F_1}(N_1) + |X \setminus X_1|$.

Demonstração. Provando-se o caso em que $X \setminus X_1 = \{y\}$ é unitário, o caso geral segue-se por aplicação iterada de tal resultado.

Denote $d_{F_1}(N_1) = m$, isto é, N_1 é gerado, como subgrupo normal (fechado) de F_1, por m elementos. Então N é gerado, como subgrupo normal fechado de F, por até $m+1$ elementos, ou seja, $d_F(N) \leq m+1$.

Suponha, por absurdo, que $d_F(N) < m+1$. Então $p^{m+1} > |N/\Phi(N)| = |N/\overline{[N,N]N^p}| \geq |N/\overline{[N,F]N^p}|$. Seja $K = \overline{\langle y^F \rangle}$. Como $X \setminus X_1 = \{y\}$, vale $F = F_1K$, e assim $N_1K \lhd_c F$, pois ambos são normais (fechados), e vale ainda $N_1K = N$. Da propriedade universal de F, existe um único epimorfismo contínuo $\theta : F \twoheadrightarrow F_1$ tal que $\theta(x) = x$, $\forall x \in X_1$ e $\theta(y) = 1$. Com isso, $\theta(N) = N_1$. Considere a composição $\varphi : N \xrightarrow{\theta|_N} N_1 \longrightarrow\!\!\!\!\!\rightarrow N_1/\overline{[N_1,F_1]N_1^p}$. Tem-se que $\overline{K[N,F]N^p} \subseteq \ker\varphi$, pois $\overline{K[N_1,F_1]N_1^p} \subseteq \ker\varphi$ e $\varphi(\overline{K[N,F]N^p}) = \varphi(\overline{K[N_1K,F_1K](N_1K)^p}) \subseteq \varphi(\overline{[N_1,F_1]N_1^p})$. Como também vale $\overline{[N,F]N^p} \leq \overline{K[N,F]N^p}$, obtem-se epimorfismos contínuos $N \twoheadrightarrow N/\overline{[N,F]N^p} \twoheadrightarrow N/\overline{K[N,F]N^p} \twoheadrightarrow N_1/\overline{[N_1,F_1]N_1^p}$ induzidos pelas projeções naturais e por φ. Logo,

$$[N : \overline{[N,F]N^p}] \geq [N : \overline{K[N,F]N^p}] \geq [N_1 : \overline{[N_1,F_1]N_1^p}] = p^m.$$

Agora, se fosse $[N : \overline{[N,F]N^p}] = p^m$, as projeções acima implicariam $K \subseteq \overline{[N,F]N^p} \subseteq \overline{[F,F]F^p} = \Phi(F)$, o que não pode ocorrer pois $y \in X$ e o subgrupo de Frattini de $F = \widehat{F(X)}_p$ é o conjunto de seus não-geradores. Logo, $[N : \overline{[N,F]N^p}] > p^m$. Sendo $N/\overline{[N,F]N^p}$ um quociente abeliano (finitamente gerado) de p-torção de N, tem-se que $[N : \overline{[N,F]N^p}] \geq p^{m+1}$. Ou seja,

$$p^{m+1} > \left|\frac{N}{\overline{[N,N]N^p}}\right| \geq \left|\frac{N}{\overline{[N,F]N^p}}\right| \geq p^{m+1},$$

uma contradição. Portanto, $d_F(N) = m+1$, como queríamos. □

Lema 2.4.19. Seja G um grupo pro-p finitamente apresentável, digamos com apresentação finita $\pi : \widehat{F(X)}_p \twoheadrightarrow G$, e denote $F = \widehat{F(X)}_p$, $N = \ker\pi$. Se H é um grupo pro-p e $K \lhd_c H$ é tal que $G \cong H/K$, então K é finitamente gerado como subgrupo normal fechado de H (i.e., $d_H(K) < \infty$) e $d(F) - d_F(N) \leq d(H) - d_H(K)$.

Demonstração. Denote $d = d(G)$ e $\sigma : H \twoheadrightarrow G$ o epimorfismo contínuo tal que $\ker\sigma = K$. Tem-se que $|G/\Phi(G)| = p^d$, e assim podemos escolher $X = \{x_1, \ldots, x_{d(F)}\} \subset F$ base de F tal que $G/\Phi(G)$ é gerado pela imagem de $X_1 = \{x_1, x_2, \ldots, x_d\} \subseteq X$ pela composta $F \twoheadrightarrow G \twoheadrightarrow G/\Phi(G)$. Denote

F_1 o subgrupo pro-p livre de F com base X_1. Como $\Phi(G)$ é o conjunto dos não-geradores de G, tem-se que a restrição $\pi|_{F_1} : F_1 \to G$ é sobrejetiva, e assim $F = F_1N$. Para cada $i = 1, \dots, d$, escolha h_i num conjunto gerador de H tal que $\sigma(h_i) = \pi(x_i)$, e considere $H_1 = \overline{\langle h_1, \dots, h_d \rangle} \leq_c H$. Similarmente, $\sigma|_{H_1} : H_1 \to G$ é sobrejetiva e $H = H_1K$. Da propriedade universal de F_1, existe um único epimorfismo contínuo $\tau : F_1 \twoheadrightarrow H_1$ tal que $\tau(x_i) = h_i$, e assim $\pi|_{F_1} = \sigma|_{H_1} \circ \tau$. Como τ é sobrejetiva e $\ker \sigma|_{H_1} = H_1 \cap K$ e $\ker \pi|_{F_1} = F_1 \cap N$, segue-se que $\tau(F_1 \cap N) = H_1 \cap K$ e

$$d_{H_1}(H_1 \cap K) \leq d_{F_1}(F_1 \cap N).$$

Agora, considere $\overline{\sigma} : H/\Phi(H) \twoheadrightarrow G/\Phi(G)$ o epimorfismo induzido por $\sigma : H \twoheadrightarrow G$. Como $\sigma(h_i) = \pi(x_i)$ e $H_1 = \overline{\langle h_1, \dots, h_d \rangle}$ e a imagem de $\{\pi(x_1), \dots, \pi(x_d)\}$ em $G/\Phi(G)$ gera tal quociente, segue-se que a restrição de $\overline{\sigma}$ a $\frac{H_1\Phi(H)}{\Phi(H)}$ é uma bijeção, e assim $|\frac{H_1\Phi(H)}{\Phi(H)}| = p^d$. Logo, por ser $H = H_1K$, podemos tomar $S = \{s_1, s_2, \dots, s_m\} \subset K$ tal que

$$H/\Phi(H) = \langle h_1\Phi(H), \dots, h_d\Phi(H), s_1\Phi(H), \dots, s_m\Phi(H) \rangle,$$

no qual $m = d(H) - d$. Denote $K_0 = \overline{\langle S^H \rangle} \lhd_c H$. Tem-se então que $K_0 \leq_c K$, $H = H_1K_0$ e $K = (H_1 \cap K)K_0$, donde

$$d_H(K) \leq d_{H_1}(H \cap K) + d(H) - d.$$

De modo análogo, obtem-se que $d_F(N) \leq d_{F_1}(F_1 \cap N) + d(F) - d$. Mas, como F é livre e N é o menor subgrupo normal fechado de F contendo $F_1 \cap N$ e $X \setminus X_1$, segue-se do Lema 2.4.18 que tal desigualdade é de fato uma igualdade. Assim,

$$d(F) - d_F(N) = d - d_{F_1}(F_1 \cap N) \leq d - d_{H_1}(H \cap K) \leq d(H) - d_H(K).$$

□

Proposição 2.4.20. Seja G um grupo pro-p finitamente apresentável. São válidos:

i. O número inteiro $\mathrm{def}(G) := d(\widehat{F(X)}_p) - d_{\widehat{F(X)}_p}(\ker \pi)$ é um invariante de G, isto é, independe da apresentação $\pi : \widehat{F(X)}_p \twoheadrightarrow G$ (tal número é chamado a *deficiência* de G);

ii. Se $G = \overline{\langle X \mid R \rangle}_p$ com $|X| = n$ e $|R| = r$, então G também admite apresentação com $d(G)$ geradores e $r - (n - d(G))$ relações;

iii. Se G admite apresentação com $n = d(G) + m$ geradores e $r = m$ relações, $m \geq 0$, então G é um grupo pro-p livre.

Demonstração. **i**. Sejam F_1 e F_2 dois grupos pro-p livres com epimorfismos contínuos $\pi_1 : F_1 \twoheadrightarrow G$ e $\pi_2 : F_2 \twoheadrightarrow G$. Então, pelo Lema 2.4.19, $d(F_1) - d_{F_1}(\ker \pi_1) \leq d(F_2) - d_{F_2}(\ker \pi_2) \leq d(F_1) - d_{F_1}(\ker \pi_1)$.

ii. Considere $\pi_1 : \widehat{F(X)}_p \twoheadrightarrow G$ a apresentação de G dada no enunciado, com $\ker \pi_1 = \overline{\langle R^{\widehat{F(X)}_p} \rangle}$. Tome $\pi_2 : F \twoheadrightarrow G$ uma apresentação de G com F um grupo pro-p livre com $\mathrm{posto}(F) = d(G)$. O número de relações em tal apresentação é $d_F(\ker \pi_2)$. Pelo item anterior, $d(G) - d_F(\ker \pi_2) = n - r$, e o resultado segue-se.

iii. Basta notar que, pelo item **(i)**, G é um grupo pro-p livre se, e só se, $\mathrm{def}(G) = d(G)$.

□

2.4.1 Álgebra de Grupo Completa, Séries de Potências e o Grupo Pro-p Livre

Esta seção tem caráter objetivo, e por tal razão evitaremos nos estender nos conceitos e fatos aqui apresentados. Nosso interesse é apresentar uma importante caracterização do grupo pro-p livre com base finita, através do estudo de R-álgebras (R anel com unidade), álgebras de grupos, e álgebras de séries formais de potência, no caso pro-p.

Serão dadas algumas definições e resultados que traduzem para os casos profinito e pro-p as noções de álgebra de grupo e módulo profinito. Demonstrações dos resultados aqui enunciados podem ser vistas em [21] e [16].

Recordamos o leitor que um anel $(R, +, \cdot)$ é dito um anel topológico quando R é também um espaço topológico tal que o grupo abeliano $(R, +)$ é um grupo topológico e o produto $\cdot : R \times R \to R$ é contínuo. Seguindo as definições 2.1.16 e 2.2.1, um anel topológico R é profinito quando é o limite inverso de aneis finitos, munidos da topologia discreta. De modo inteiramente análogo à caracterização para grupos, tem-se o resultado abaixo, cuja demonstração omitiremos.

Teorema 2.4.21. Seja R um anel topológico. São equivalentes:

i. R é profinito;

ii. R é compacto, Hausdorff e totalmente desconexo;

iii. R é compacto e o elemento nulo $0 \in R$ admite um sistema fundamental de vizinhanças abertas que consiste nos ideais abertos de R.

Similarmente, dizemos que um anel profinito é pro-p quando seus ideais abertos têm índice (vistos como subgrupos aditivos) potências de p.

De agora em diante, ***assumiremos que todo anel*** R ***admite elemento unidade*** $1 \in R$, e que homomorfismos (contínuos) entre aneis (topológicos) $f : R_1 \to R_2$ preservam o elemento neutro multiplicativo, isto é, $f(1_{R_1}) = 1_{R_2}$.

Diferentemente do que ocorre no caso de um anel topológico geral R, no qual seu grupo das unidades $\mathcal{U}(R)$ não é necessariamente um grupo topológico (com a topologia do subespaço), o grupo das unidades de um anel *profinito* R é um subespaço fechado e é um grupo *profinito*. Isso segue do fato de que R é o limite inverso $R = \varprojlim R/J_i$ sendo J_i seus ideais abertos, de modo que $\mathcal{U}(R) = \varprojlim \mathcal{U}(R/J_i)$ é limite inverso de grupos finitos. A título de referência, enunciamos abaixo tal resultado, cuja demonstração pode ser vista em [21, Lema 7.1.1].

Proposição 2.4.22. Seja R um anel profinito. Então seu grupo das unidades $\mathcal{U}(R)$ é fechado, e é um grupo profinito, com a topologia do subespaço.

Prosseguiremos agora com a noção de álgebras sobre um anel dado.

Definição 2.4.23. Seja R um anel comutativo com elemento unidade. Dizemos que um par (A, i) é uma R-álgebra quando A é um anel e $i : R \to \mathrm{Z}(A)$ é um homomorfismo (de aneis) de R no centro de A.

Como de costume, omitimos a aplicação $i : R \to \mathrm{Z}(A)$ e dizemos simplesmente que o anel A é uma R-álgebra.

Exemplo 2.4.24. Todo anel A é uma $\mathrm{Z}(A)$-álgebra via a inclusão $\mathrm{Z}(A) \hookrightarrow A$.

Exemplo 2.4.25. Mais geralmente, A é uma R-álgebra, para qualquer R subanel de $\mathrm{Z}(A)$.

Exemplo 2.4.26. Seja $\mathbb{F}$ um corpo de característica zero. Então o anel $\mathrm{M}_n(\mathbb{F})$ das matrizes $n \times n$ sobre $\mathbb{F}$ é uma $\mathbb{F}$-álgebra, via a bijeção $\mathbb{F} \longleftrightarrow \mathrm{Z}(\mathrm{M}_n(\mathbb{F})) = \{\alpha \cdot I_n \mid \alpha \in \mathbb{F}\}$.

Se (A, i) é uma R-álgebra podemos, em um certo sentido, visualizar R como uma família de *escalares* agindo sobre o anel A, via a identificação dada pelo homomorfismo $i : R \to \mathrm{Z}(A)$. Com isso, para $r \in R$ e $a \in A$, denotamos um produto $i(r) \cdot a$ $(= a \cdot i(r)\ )$ simplesmente por ra $(= ar)$.

Dadas A, B duas R-álgebras, dizemos que um homomorfismo (de aneis) $f : A \to B$ é um *homomorfismo de R-álgebras* quando $f(r \cdot a) = r \cdot f(a),\ \forall r \in R$.

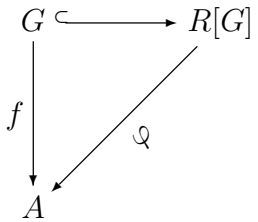
Definição 2.4.27. Dados G um grupo e R um anel comutativo, a *álgebra de grupo*[5] $R[G]$ do grupo G sobre o anel R é o anel das somas formais

$$R[G] = \left\{ \sum r_g g \mid r_g \in R \text{ e } r_g = 0 \text{ exceto para uma quantidade finita de elementos } g \in G \right\},$$

com as operações de soma e produto naturais, isto é,

- $\sum r_g g + \sum s_g g = \sum (r_g + s_g) g$ (soma dos coeficientes termo-a-termo);
- $(\sum r_g g) \cdot (\sum s_h h) = \sum_{g,h} (r_g s_h)(gh)$ (somatório duplo dado pela distributividade e o produto em G).

Note que há inclusões naturais $G \hookrightarrow R[G]$ e $R \hookrightarrow R[G]$ dadas por $g \mapsto 1_R \cdot g$ e $r \mapsto r \cdot 1_G$, respectivamente. Com isso, o grupo (multiplicativo) das unidades $\mathcal{U}(R[G])$ contem G como subgrupo, e $R[G]$ contem R como subanel. Mais ainda, $R[G]$ é de fato uma R-álgebra. Veja que o anel $R[G]$ é comutativo se, e somente se, G é um grupo abeliano.



Observamos ainda que $R[G]$ pode ser caracterizado pela seguinte propriedade universal: para toda R-álgebra A e para qualquer $f : G \to \mathcal{U}(A)$ homomorfismo do grupo G no grupo das unidades $\mathcal{U}(A)$, existe um único homomorfismo de R-álgebras $\varphi : R[G] \to A$ tal que $\varphi|_G = f$. Dizemos então que φ é o homomorfismo (de R-álgebras) que estende o homomorfismo (de grupos) f.

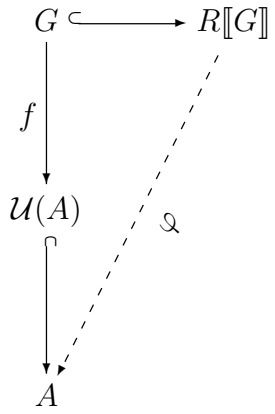
Exemplo 2.4.28. Tome $R = \mathbb{Z}$ o anel dos inteiros e $G = \langle x \rangle \cong \mathbb{Z}$ o grupo cíclico infinito gerado por $\{x\}$. Então $\mathbb{Z}[G] = \bigoplus_{n \in \mathbb{Z}} \mathbb{Z} x^n = \mathbb{Z}\left[x, \frac{1}{x}\right]$ é o Anel de Polinômios de Laurent.

É a partir da propriedade universal dada acima que baseia-se o análogo à álgebra de grupos para o caso profinito, a ser dado na sequência.

[5] Alguns autores denotam RG ou $[RG]$.

Definição 2.4.29. Seja R um anel profinito comutativo. Dizemos que um par (A, i) é uma R-álgebra *profinita* quando A é um anel profinito e $i : R \to \mathrm{Z}(A)$ é um homomorfismo contínuo (de aneis topológicos) de R no centro do anel profinito A.

Definição 2.4.30. Dados G um grupo profinito e R um anel profinito, a *álgebra de grupo completa* $R[\![G]\!]$ do grupo G sobre o anel R é a R-álgebra profinita tal que $G \subset \mathcal{U}(R[\![G]\!])$ e que satisfaz a seguinte propriedade universal:



para toda R-álgebra profinita A e para qualquer $f : G \to \mathcal{U}(A)$ homomorfismo contínuo do grupo profinito G no grupo das unidades $\mathcal{U}(A)$, existe um único homomorfismo contínuo de R-álgebras $\varphi : R[\![G]\!] \to A$ tal que $\varphi|_G = f$. Dizemos então que φ é o homomorfismo contínuo (de R-álgebras) que estende o homomorfismo contínuo (de grupos) f.

Alguns comentários acerca de tal definição devem ser feitos. Primeiramente, observamos que o conceito acima de fato está bem definido, isto é, faz sentido falar *da* álgebra de grupo completa (e em particular fixar sua notação $R[\![G]\!]$), pois como de praxe a propriedade universal nos garante a unicidade (a menos de isomorfismo contínuo de R-álgebras) do objeto universal em questão. Em segundo lugar, lembramos que $\mathcal{U}(A)$ é na verdade um grupo profinito, com a topologia do subespaço, pela Proposição 2.4.22.

O resultado natural a ser considerado, tendo em vista a definição, é o seguinte.

Teorema 2.4.31. **i**. A inclusão $G \hookrightarrow R[\![G]\!]$ estende-se a um mergulho $R[G] \hookrightarrow R[\![G]\!]$ da álgebra de grupo na álgebra de grupo completa, sendo a imagem de $R[G]$ densa em $R[\![G]\!]$;

ii. Para quaisquer G grupo profinito e R anel profinito comutativo, existe a álgebra de grupo completa $R[\![G]\!]$, que é construída como $R[\![G]\!] = \varprojlim_{N \trianglelefteq_o G} R[G/N]$;

iii. Para todo H subgrupo normal de G, a projeção canônica $\pi : G \twoheadrightarrow G/H$ induz um epimorfismo entre as álgebras de grupo completas $\pi_H : R[\![G]\!] \twoheadrightarrow R[\![G/H]\!]$, cujo núcleo é o fecho do ideal I_H de $R[\![G]\!]$ gerado pelo conjunto $\{r(h-1) \mid r \in R,\ h \in H\}$.

Assim como o completamento de um grupo abstrato é seu "correspondente" na classe dos grupos profinitos, a álgebra de grupo completa é o correspondente profinito à álgebra de um grupo. De fato, no teorema acima a construção da álgebra de grupo completa é análoga à do completamento

de grupos visto anteriormente. A analogia se estende também ao fato de que a álgebra $R[G]$ é densa em sua álgebra completa $R[\![G]\!]$. A verificação das propriedades acima pode ser vista em [21, Proposição 7.1.2].

Trataremos agora de módulos no caso profinito.

Definição 2.4.32. Sejam R um anel topológico e $(M, +)$ um grupo abeliano topológico. Dizemos que M é um R-módulo topológico (à direita) quando existe uma aplicação contínua

$$\begin{aligned} M \times R &\longrightarrow M \\ (m, r) &\longmapsto mr \end{aligned}$$

tal que, $\forall m, m_1, m_2 \in M,\ r, r_1, r_2 \in R$, valem:

i. $(m_1 + m_2)r = m_1 r + m_2 r$;

ii. $m(r_1 + r_2) = mr_1 + mr_2$;

iii. $m(r_1 r_2) = (mr_1)r_2$;

iv. $m1 = m$.

Em outras palavras, o anel R age continuamente (à direita) sobre o grupo abeliano $(M, +)$ respeitando a distributividade. De modo análogo define-se R-módulos topológicos à esquerda.

Exemplo 2.4.33. Todo espaço vetorial real de dimensão finita é um $\mathbb{R}$-módulo topológico.

Definição 2.4.34. Seja R um anel profinito com elemento unidade. Dizemos que M é um R-módulo profinito quando M é o limite inverso de R-módulos finitos.

Assim como no caso de grupos, tem-se uma caracterização simples de R-módulos profinitos através de sua topologia.

Teorema 2.4.35. Sejam R um anel profinito e M um grupo abeliano profinito. Se M é também um R-módulo (abstrato), então as seguintes afirmações são equivalentes:

i. M é um R-módulo profinito;

ii. M é um R-módulo topológico;

iii. o conjunto de submódulos abertos de M forma uma base de vizinhanças abertas do $0 \in M$.

A demonstração do teorema acima se dá de modo análogo ao teorema 2.2.7, atentando-se à construção de R e M como limites inversos e fazendo uso de propriedades como as vistas na Proposição 2.1.15.

Exemplo 2.4.36. Semelhante ao que ocorre no item **(vi)** da Proposição 2.2.12, o completamento profinito $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ de $\mathbb{Z}$ age contínua e homomorficamente sobre qualquer grupo abeliano profinito A via a "potenciação", $a \in A \mapsto a^z,\ z \in \widehat{\mathbb{Z}}$. Com tal ação, todo grupo abeliano profinito é um $\widehat{\mathbb{Z}}$-módulo. Similarmente, todo grupo abeliano profinito que é também grupo pro-p é um $\mathbb{Z}_p$-módulo.

Exemplo 2.4.37. Todo ideal fechado I de um anel profinito R é um R-módulo profinito.

Definição 2.4.38. Dado R um anel *arbitrário*, dizemos que um R-módulo (à direita) M é finitamente gerado quando existem $m_1, \ldots, m_n \in M$ tais que $M = \{\sum_{i=1}^{n} m_i r_i \mid r_i \in R\}$. Análogo para módulos à esquerda.

Veja que a definição acima engloba tanto os casos de módulos topológicos quanto módulos profinitos. Diferentemente do caso de geradores (topológicos) de um grupo profinito, não há necessidade de exigir que o submódulo gerado por $m_1, \ldots, m_n$ seja denso no módulo profinito M, fato que se deve ao seguinte resultado, cuja demonstração é dada em [21, Lema 7.2.2].

Proposição 2.4.39. Sejam R um anel profinito, M um R-módulo profinito, e $\{m_1, \ldots, m_n\} \subset M$. Então:

i. $N = \{\sum_{i=1}^{n} m_i r_i \mid r_i \in R\}$ é um submódulo fechado de M;

ii. M finitamente gerado $\implies$ todo homomorfismo $f : M \to L$ de R-módulos é contínuo, no qual L é R-módulo profinito.

Como toda álgebra de grupo completa $R[\![G]\!]$ é, em particular, um anel profinito, podemos naturalmente considerar módulos sobre tais álgebras. A título de referência, citamos a útil proposição abaixo, cujo resultado é natural e nos diz que homomorfismos contínuos que preservam as ações de G e R em um $R[\![G]\!]$-módulo são de fato homomorfismos de $R[\![G]\!]$-módulos (cf. [21, Proposição 7.2.5]).

Proposição 2.4.40. Sejam G um grupo profinito e R um anel profinito comutativo. Suponha que M e N sejam $R[\![G]\!]$-módulos e que uma função $f : M \to N$ seja:

- contínua;
- homomorfismo de R-módulos;
- homomorfismo de G-módulos.

Então f é um homomorfismo de $R[\![G]\!]$-módulos.

Passemos, finalmente, ao estudo das álgebras de séries de potências em nosso caso de interesse.

Definição 2.4.41. Seja R um anel comutativo com elemento unidade. Dado $T = \{t_1, \ldots, t_d\}$ conjunto finito, considere M_T o conjunto dos monômios sobre as incógnitas ***não***-comutativas $t_1, \ldots, t_d$, isto é, M_T é o subconjunto do grupo livre F_T formado por elementos da forma $t = 1$ e $t = t_{i_1}^{\alpha_1} \cdots t_{i_m}^{\alpha_m}$, no qual $t_{i_j} \in T$ e $\alpha_j \geq 1$, qualquer que seja $1 \leq j \leq d$.
Uma *série formal de potências* sobre as incógnitas *não-comutativas* $t_1, \ldots, t_d$ é uma expressão da forma $\sum_{t \in M_T} r_t t$, no qual $r_t \in R$. Denotamos por $R[\![t_1, \ldots, t_d]\!]$ o *conjunto das séries formais de potências* sobre as incógnitas não-comutativas $t_1, \ldots, t_d$.

A primeira observação acerca da definição acima é a mais natural possível: como R é um anel comutativo com elemento unidade, podemos tornar facilmente $R[\![t_1, \ldots, t_d]\!]$ um anel, com as operações de soma usual (compatível, portanto, com a soma de R), e o produto dado pelo produto de séries de potências, isto é, induzido pela distributividade. Note que tal produto é compatível com o produto de R, e a multiplicação de monômios no produto de séries é induzida pelo produto do grupo livre F_T com base $T = \{t_1, \ldots, t_d\}$. Mais ainda, tem-se a inclusão natural $R \hookrightarrow R[\![t_1, \ldots, t_d]\!]$ dada por $r \mapsto r \cdot 1_{M_T}$, e assim $R[\![t_1, \ldots, t_d]\!]$ torna-se uma R-álgebra.

A segunda observação também consiste de um resultado esperado:

Proposição 2.4.42. Se R é profinito, então $R[\![t_1, \ldots, t_d]\!]$ é uma R-álgebra profinita.

Demonstração. Este resultado é garantido por construção análoga à feita no exemplo dos inteiros p-ádicos (cf. Teorema 2.2.14) e na prova de existência das álgebras completas (cf. Teorema 2.4.31), fundadas na noção de completamentos.

Considere o anel profinito de polinômios $R[t_1, \ldots, t_d]$ nas incógnitas *não-comutativas* $t_1, \ldots, t_d$. Para cada $k \geq 1$, defina $I_k = (\{t_{i_1}^{\alpha_1} \cdots t_{i_m}^{\alpha_m} \in M_T \mid \alpha_1 + \cdots + \alpha_m \geq k\})$ o ideal de $R[t_1, \ldots, t_d]$ gerado pelos monômios de graus maiores ou iguais a k. Note que $I_1 = (t_1, \ldots, t_d) \supset I_2 \supset \cdots \supset I_k \supset \cdots$, ficando definidas as projeções naturais $\varphi_{ij} : \frac{R[t_1,\ldots,t_d]}{I_i} \to \frac{R[t_1,\ldots,t_d]}{I_j}$, $i \geq j$, e podemos considerar $\varprojlim R[t_1, \ldots, t_d]/I_k$. Então o anel (abstrato) $R[\![t_1, \ldots, t_d]\!]$ é isomorfo ao anel $\varprojlim R[t_1, \ldots, t_d]/I_k$, através do isomorfismo

$$\sum_{t \in M_T} r_t t \overset{\varphi}{\longmapsto} \left(\sum_{s \in M_T} r_s s + I_k \right)_{k \in \mathbb{N}},$$

no qual $t = t_{i_1}^{\alpha_1} \cdots t_{i_m}^{\alpha_m} \in M_T$, e os monômios correspondentes $s = t_{i_1}^{\alpha_1} \cdots t_{i_m}^{\alpha_m}$ no segundo membro são aqueles para os quais $\alpha_1 + \cdots + \alpha_m < k$.

Com isso, para que $R[\![t_1, \ldots, t_d]\!]$ torne-se anel topológico, basta definir sua topologia como sendo a topologia proveniente da bijeção φ, isto é, $A \subset R[\![t_1, \ldots, t_d]\!]$ é aberto se, e somente se, $\varphi(A) \subset \varprojlim R[t_1, \ldots, t_d]/I_k$ é aberto, definindo também as operações $u + v = \varphi^{-1}(\varphi(u) + \varphi(v))$, $u \cdot v = \varphi^{-1}(\varphi(u) \cdot \varphi(v))$. Como tais operações estendem naturalmente a soma e produto de R, as mesmas coincidem com a soma e produto usuais de séries de potências.

Por fim, da construção acima vemos que $R[\![t_1, \ldots, t_d]\!]$ é limite inverso das R-álgebras profinitas $R[t_1, \ldots, t_d]/I_k$, e portanto $R[\![t_1, \ldots, t_d]\!]$ é também R-álgebra profinita. □

Façamos algumas observações importantes. Devido à natureza da construção dada acima, algumas propriedades de $R[\![t_1, \ldots, t_d]\!]$ carregam certa semelhança com o anel dos inteiros p-ádicos $\mathbb{Z}_p$. Similarmente ao que ocorre em $\mathbb{Z}_p$ com os ideais $p^k\mathbb{Z}_p$, definimos para cada $k \geq 1$ os ideais $I_k = (\{t_{i_1}^{\alpha_1} \cdots t_{i_m}^{\alpha_m} \in M_T \mid \alpha_1 + \cdots + \alpha_m \geq k\})$, agora em $R[\![t_1, \ldots, t_d]\!]$, gerados pelos monômios de grau maior ou igual a k. Tem-se que tais ideais são abertos (portanto fechados) por serem os núcleos das projeções φ_k do limite inverso construído na Proposição 2.4.42. Com isso, $\{I_k\}_{k \in \mathbb{N}}$ forma um sistema fundamental de vizinhanças abertas do $0 \in R[\![t_1, \ldots, t_d]\!]$ (compare com alguns resultados da Proposição 2.2.12). Particularizando para o anel $I_1 = (t_1, \ldots, t_d)$ gerado pelas incógnitas de $R[\![t_1, \ldots, t_d]\!]$, tem-se que $R[\![t_1, \ldots, t_d]\!]/I_1 = R[\![t_1, \ldots, t_d]\!]/\ker \varphi_1 \cong R$. Mais ainda, cada quociente $R[\![t_1, \ldots, t_d]\!]/I_k$ é um R-módulo finitamente gerado.

Com tais noções em mente, passamos ao nosso caso de interesse, o da álgebra (profinita) das séries formais de potências sobre o corpo $\mathbb{F}_p$ de ordem prima p. Note que, nesse caso, o ideal $I_1 = (t_1, \ldots, t_d) \subseteq \mathbb{F}_p[\![t_1, \ldots, t_d]\!]$ satisfaz $\mathbb{F}_p[\![t_1, \ldots, t_d]\!]/I_1 \cong \mathbb{F}_p$, sendo portanto maximal. Além disso, cada quociente $\mathbb{F}_p[\![t_1, \ldots, t_d]\!]/I_k$ é um $\mathbb{F}_p$-espaço vetorial de dimensão finita. O resultado seguinte afirma que tal álgebra sempre contem um grupo pro-p, diferente, evidentemente, do próprio p-grupo finito $\mathbb{F}_p$.

Proposição 2.4.43. Seja $\mathbb{F}_p$ o corpo de ordem prima p. Então a classe lateral $G = 1 + I_1$ do ideal $I_1 = (t_1, \ldots, t_d)$ de $\mathbb{F}_p[\![t_1, \ldots, t_d]\!]$ é um grupo pro-p com relação à multiplicação no anel $\mathbb{F}_p[\![t_1, \ldots, t_d]\!]$.

Demonstração. Primeiro, G é fechado para o produto de $\mathbb{F}_p[\![t_1, \ldots, t_d]\!]$, pela distributividade e por ser I_1 ideal. Em segundo lugar, construamos o inverso multiplicativo de $1 + f \in 1 + I_1$ arbitrário. Para cada $n \in \mathbb{N}$, defina $s_n = \sum_{i=1}^{n-1}(-f)^i = -f + f^2 - f^3 + \cdots + (-f)^{n-1}$. Tem-se então que $(1 + f)(1 + s_n) = 1 - f^n$. Como $f \in I_1 = (t_1, \ldots, t_d)$, tem-se $f^n \in I_n$, para todo $n \in \mathbb{N}$. Defina $s = \lim_{n\to\infty} s_n$. Pela continuidade da soma e do produto,

$$(1 + f)(1 + s) = (1 + f)(1 + \lim s_n) = \lim(1 + f)(1 + s_n) = \lim(1 - f^n) = 1 - 0 = 1.$$

Portanto, $G = 1 + I_1$ é grupo multiplicativo.

Para ver que G é pro-p, considere as projeções $\varphi_k : \mathbb{F}_p[\![t_1, \ldots, t_d]\!] \to F_k := \mathbb{F}_p[t_1, \ldots, t_d]/I_k$ dadas pelo limite inverso na Proposição 2.4.42. Tem-se que cada $\mathbb{F}_p[t_1, \ldots, t_d]/I_k$ tem dimensão finita sobre $\mathbb{F}_p$, digamos p^{j_k}. Além disso, $\varphi_k(I_1)$ é ideal de $F_k = \mathbb{F}_p[t_1, \ldots, t_d]/I_k$ com $F_k/\varphi_k(I_1) \cong \mathbb{F}_p$, pela definição de I_1. Como $\varphi_k(G) = \varphi_k(1 + I_1) = 1 + \varphi_k(I_1)$, obtem-se $|\varphi_k(G)| = p^{j_k}/p = p^{j_k-1}$. Sendo $G = \varprojlim \varphi_k(G)$ por construção, segue-se que G é pro-p. □

Antes de provar o resultado principal desta seção, enunciamos o seguinte lema, cuja demonstração pode ser encontrada em [21, pp. 120 e 121].

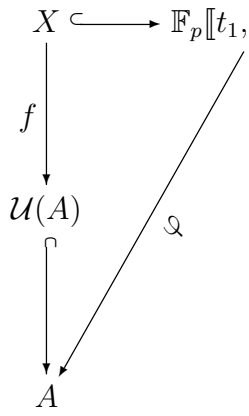
Lema 2.4.44. **i**. Se A é uma R-álgebra profinita e $a_1, \ldots, a_d \in A$ são tais que $a_{i_1} \cdot a_{i_2} \cdots a_{i_n} = 0$, para algum $n \in \mathbb{N}$ e para quaisquer $i_j \in \{1, \ldots, d\}$, então existe um único homomorfismo contínuo de R-álgebras $\varphi : R[\![t_1, \ldots, t_d]\!] \to A$ tal que $\varphi(t_i) = a_i,\ \forall i = 1, \ldots, d$;

ii. Dado p um número primo, se R é um anel finito com cardinalidade $|R| = p^n$ e $G \leq \mathcal{U}(R)$ é um p-subgrupo, então $(g_1 - 1) \cdot (g_2 - 1) \cdots (g_n - 1) = 0,\ \forall g_1, \ldots, g_n \in G$.

Provemos então o seguinte: todo grupo pro-p livre com base finita pode ser mergulhado numa álgebra de séries formais de potências com coeficientes inteiros módulo p.

Teorema 2.4.45. Sejam $d \in \mathbb{N}$, e considere $F_p[\![t_1, \ldots, t_d]\!]$ a álgebra de séries formais de potências sobre o corpo de ordem prima p. Defina $x_i = 1+t_i$, para $1 \leq i \leq d$. Então o subgrupo multiplicativo fechado $G = \overline{\langle x_1, \ldots, x_d \rangle} \leq_c \mathcal{U}(F_p[\![t_1, \ldots, t_d]\!])$ é o grupo pro-p livre com base $X = \{x_1, \ldots, x_d\}$. Mais ainda, $\mathbb{F}_p[\![t_1, \ldots, t_d]\!] = \mathbb{F}_p[\![G]\!]$.

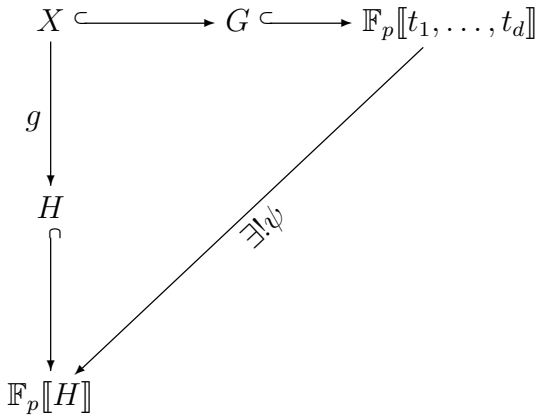
Demonstração. Pela Proposição 2.4.43, como $X \subset 1 + I_1$, segue-se que $G = \overline{\langle x_1, \ldots, x_d \rangle} \subset 1 + I_1$ é um grupo pro-p. Mostremos que $\mathbb{F}_p[\![t_1, \ldots, t_d]\!] = \mathbb{F}_p[\![G]\!]$. Sejam A uma $\mathbb{F}_p$-álgebra profinita, e $f : X \to \mathcal{U}(A)$ contínua. Observe que basta considerar o caso em que A é finita, pelo Teorema 2.4.31, pois a álgebra $\mathbb{F}_p[\mathcal{U}(A)]$ mergulha num conjunto denso da álgebra completa $\mathbb{F}_p[\![\mathcal{U}(A)]\!]$. Nesse caso, A tem cardinalidade p^m para algum $m \in \mathbb{N}$, e assim $\mathcal{U}(A)$ é um p-grupo, digamos $|\mathcal{U}(A)| = p^k$. Tem-se então que $(a_1 - 1) \cdots (a_k - 1) = 0$, para quaisquer $a_1, \ldots, a_k \in \mathcal{U}(A)$, pelo item **(ii)** do Lema 2.4.44. Em particular, $(f(x_{i_1}) - 1) \cdots (f(x_{i_k}) - 1) = 0$, para $1 \leq i_1, \ldots, i_k \leq d$, donde existe $\varphi : \mathbb{F}_p[\![t_1, \ldots, t_d]\!] \to A$ homomorfismo contínuo tal que $\varphi(t_i) = f(x_i) - 1$ para todo i, pelo item **(i)** do Lema 2.4.44. Como $x_i = 1 + t_i$,



tem-se $\varphi(x_i) = \varphi(1 + t_i) = \varphi(1) + \varphi(t_i) = 1 + f(x_i) - 1 = f(x_i)$, ou seja, $\varphi|_G = f$.

Agora, dado $f : G \to \mathcal{U}(A)$ homomorfismo contínuo, A álgebra profinita, pode-se estender $f|_X$ via o argumento acima a um homomorfismo contínuo de $\mathbb{F}_p$-álgebras profinitas $\varphi : \mathbb{F}_p[\![t_1, \ldots, t_d]\!] \to A$, que evidentemente estende f pois $G = \overline{\langle x_1, \ldots, x_d \rangle}$. Tal homomorfismo é único, pois $\varphi(t_i) = f(x_i) - 1$, para todo i, o que garante que φ é unicamente determinado nos monômios que geram (topologicamente) a álgebra de séries de potências $\mathbb{F}_p[\![t_1, \ldots, t_d]\!]$.

Por fim, o fato de G ter a propriedade universal do grupo livre pro-p sobre X segue por aplicação da propriedade universal de $\mathbb{F}_p[\![G]\!]$ obtida acima. De fato, se H é grupo pro-p e $g : X \to H$ é função contínua, estende-se g unicamente a um homomorfismo contínuo ψ de $\mathbb{F}_p[\![t_1, \ldots, t_d]\!]$ na álgebra de grupo completa $\mathbb{F}_p[\![H]\!]$, de modo que existe um único homomorfismo contínuo de G em H que estende g, a saber, a restrição $\psi|_G$.



□

Capítulo 3

A Desigualdade de Golod-Šafarevič para Apresentações de Grupos Pro-p e Abstratos

O famigerado teorema publicado por E. Golod e I. Šafarevič em 1964 [7] teve seu reconhecimento evidenciado por se relacionar à solução de 3 importantes problemas em aberto.

Em Álgebra Comutativa e Teoria Algébrica dos Números, Golod e Šafarevič solucionaram o problema proposto por P. Furtwängler sobre as titulares torres de corpos de classes, que se perguntava se a torre de corpos de classes de Hilbert de um dado corpo numérico $\mathbb{K}$ seria sempre finita [15, p. 413]. Após quase 4 décadas em aberto [17, p. 232], Golod e Šafarevič foram capazes de construir uma torre infinita de corpos de classes de Hilbert [7], mostrando que o problema, em geral, tem resposta negativa.

Em 1941, A. Kuroš propôs, no contexto de álgebras associativas, problemas análogos aos problemas de Burnside da teoria de grupos, apresentando soluções para casos específicos, focando em aneis comutativos (cf. [11, p. 240]). Mais de 20 anos depois, o trabalho de Golod e Šafarevič [7] permitiu solucionar (negativamente) um dos problemas no caso Não-Comutativo, através da construção de nil álgebras associativas de dimensão infinita, finitamente geradas, e cujos elementos são algébricos [6].

Os supracitados problemas de W. Burnside, propostos pelo mesmo no começo do século XX, têm até hoje grande impacto na Teoria de Grupos pela ampla quantidade de trabalhos desenvolvidos na área visando suas respectivas soluções. Um dos questionamentos, conhecido como o Problema Geral de Burnside, é formulado para grupos abstratos como segue: "*Seria finito todo grupo finitamente gerado e de torção?*"

Sabemos que a resposta é afirmativa, por exemplo, no caso de grupos abelianos, devido à Classificação dos Grupos Abelianos Finitamente Gerados. Porém, a resposta final para tal problema foi dada também devido ao trabalho de Golod e Šafarevič ([7], [6]), após mais de 60 anos e diversas tentativas de solução definitva. Golod mostrou como construir p-grupos infinitos, de torção, e finitamente gerados, [6] usando as técnicas dadas por ele e Šafarevič [7], concluindo ser falsa, portanto, a resposta para a pergunta acima.

Enunciemos então o Teorema, que responde – ao menos parcialmente, para o caso de grupos

pro-p *finitos* – o número de relações que deve ocorrer em certas apresentações finitas:

Desigualdade de Golod-Šafarevič [7]. Se G é um p-grupo finito, com número mínimo de relações $r(G)$ e número mínimo de geradores $d(G)$ (no sentido pro-p), então[1]

$$r(G) \geq \frac{d(G)^2}{4}. \qquad (\textbf{G-Š})$$

As consequências do resultado acima, mencionadas anteriormente, advêm de implicações estruturais nos grupos (e nas álgebras) para os quais a desigualdade é estabelecida. As ferramentas desenvolvidas por Golod e Šafarevič, bem como construções mais gerais envolvendo desigualdades com certas séries (reais) de potências, que implicam em particular no resultado acima, foram ativamente estudadas nas últimas 4 décadas. Referimos ao leitor o *survey* de M. Ershov [5], por exemplo, para a definição, propriedades e resultados importantes dos chamados *Grupos de Golod-Šafarevič*.

É natural questionar quais outras classes de grupos pro-p satisfazem a desigualdade acima, ou ao menos alguma forma da mesma. Pode-se questionar, também, se grupos abstratos finitamente apresentáveis também possuem relação com alguma forma da desigualdade acima enunciada. Um dos trabalhos desenvolvidos em meados das últimas 4 décadas, relativo à Desigualdade e a Grupos de Golod-Šafarevič, foi o artigo "*Finite presentations of pro-p groups and discrete groups*", de J. S. Wilson [20], do início da década de 90. Em tal trabalho, Wilson estende a desigualdade (**G-Š**) para uma ampla classe de grupos pro-p, explicitando uma propriedade estrutural satisfeita por grupos para o qual *não* vale a desigualdade. Tais grupos pro-p são também grupos de Golod-Šafarevič e são, obrigatoriamente, infinitos. A questão sobre o "tamanho" dos grupos de Golod-Šafarevič foi tornada mais precisa com o importante teorema de Zelmanov [23], a ser mencionado ao fim da Subseção 3.2.1. Em [20], Wilson apresenta, também, uma versão da desigualdade para o caso de grupos abstratos, obtida graças à noção de completamento pro-p.

Neste capítulo desenvolveremos, de maneira relativamente objetiva, as ferramentas que visam a demonstração do teorema de Wilson. Em seguida, explicitaremos certas classes de grupos pro-p para os quais vale a desigualdade a ser obtida, e mostraremos algumas aplicações da teoria aqui desenvolvida, tanto no cenário pro-p, quanto no cenário abstrato. A construção da desigualdade, como aqui exposta, segue as linhas dadas em [21]. As aplicações para grupos abstratos seguem o artigo [20].

3.1 Grupos pro-p finitamente apresentáveis

Nosso objetivo nesta seção é apresentar a Desigualdade de Golod-Šafarevič estendida para grupos pro-p finitamente apresentáveis, atentando-nos à estrutura de grupos para o qual não vale a desigualdade – tais grupos são, em particular, infinitos.

Seguindo notação tradicional da teoria de aneis e corpos, dados R um anel e um subconjunto $Y \subset R$, denotaremos $(Y) \subseteq R$ o ideal (bilateral) gerado por Y, i.e., o menor ideal de R que contem o conjunto Y. Se R for anel topológico, $\overline{(Y)}$ denota o menor ideal fechado de R que contem Y.

[1] A forma da Desigualdade aqui dada possui uma ligeira melhoria comparada à original em [7], creditada a trabalhos independentes de È. Vinberg e W. Gaschütz (cf. [17]).

Daqui em diante, **denotaremos $P = \mathbb{F}_p[\![t_1, \ldots, t_d]\!]$ a álgebra das séries formais de potências em d incógnitas *não*-comutativas**, estudada ao fim da Seção 2.4.1. Recordemos que, para cada $k \geq 1$, definimos $I_k \subset P$ o ideal gerado por monômios de grau maior ou igual a k, que são abertos (e fechados).

Lema 3.1.1. Para todo $v \in I_1$, existem únicos $u_1, \ldots, u_d \in P$ tais que $v = \sum_{i=1}^{d} u_i t_i$.

Demonstração. Seja $v = \sum_{i=1}^{d} a_i t_i b_i \in I_1,\ a_i, b_i \in P$, um elemento arbitrário de I_1. Como $I_1 = (t_1, \ldots, t_d)$, podemos reescrever $\sum_{i=1}^{d} a_i t_i b_i \in I_1$ como uma soma *finita* $v = \sum_{w \in W} c_w w$, no qual $c_w \in P$ e $w \in W = \cup W_i$ sendo cada $W_i = \{t_{j_1} \cdots t_{j_r} \mid r \geq 1,\ t_{j_r} = t_i\}$ o conjunto dos monômios cujo último termo é t_i. Dessa forma,

$$v = \sum_{w \in W} c_w w = \sum_{i=1}^{d} \sum_{w \in W_i} c_w w = \sum_{i=1}^{d} \left(\sum_{w = t_{j_1} \cdots t_{j_{r-1}} t_i \in W_i} c_w t_{j_1} \cdots t_{j_{r-1}} \right) t_i.$$

Basta definir $u_i = \displaystyle\sum_{w = t_{j_1} \cdots t_{j_{r-1}} t_i \in W_i} c_w t_{j_1} \cdots t_{j_{r-1}} \in P$. A unicidade dos coeficientes u_i segue-se do fato de serem únicos os coeficientes $a_i, b_i \in P$ em $\sum_{i=1}^{d} a_i t_i b_i = v = \sum_{w \in W} c_w w$. □

Como a família $\{I_k\}_{k \geq 1}$ forma um sistema fundamental de vizinhanças abertas do $0 \in P$, podemos estabelecer a:

Definição 3.1.2. A *função grau* de P é a função $\delta : I_1 \setminus \{0\} \to \mathbb{N}$ que associa a cada $v \in I_1 \setminus \{0\}$ o (único) número natural k tal que $v \in I_k \setminus I_{k+1}$. Convenciona-se ainda que $\delta(0) = \infty$, de modo que $\delta(0) \geq \delta(v),\ \forall v \in I_1$.

Com a definição acima, os elementos de I_1 são aqueles de grau pelo menos 1, os elementos de I_2 possuem grau maior ou igual a 2, e assim por diante.

O seguinte resultado, creditado a È. B. Vinberg, fornece a base para os teoremas que virão a seguir.

Teorema 3.1.3. Sejam $S \subset I_1$ e $J = \overline{(S)}$ o ideal (fechado) de P gerado por S. Para cada $k \in \mathbb{N}$, considere $S_k = \{v \in S \mid \delta(v) = k\}$. Se $|S_k| < \infty,\ \forall k \in \mathbb{N}$, então:

i. $c_k - 1 \geq d c_{k-1} - \displaystyle\sum_{j=1}^{k} |S_j| c_{k-j},\ \forall k \geq 1$, no qual $c_k = \dim_{\mathbb{F}_p} \left(\dfrac{P}{J + I_{k+1}} \right)$;

ii. $I_n \subseteq J$ para algum $n \implies 1 - dy + \sigma_S(y) > 0$ para qualquer $y \in [0, 1)$ tal que a série (real) de potências $\sigma_S(y) = \displaystyle\sum_{k=1}^{\infty} |S_k| y^k$ converge.

Demonstração. **i**. A ideia da prova consiste em construir certos espaços vetoriais sobre $\mathbb{F}_p$ e obter a desigualdade calculando as dimensões de tais espaços.

Para cada $k \in \mathbb{N}$, considere a união (disjunta) $\cup_{j\leq k} S_j$. Como cada S_j é finito, podemos ordenar tal conjunto, digamos $\cup_{j\leq k} S_j = \{v_1, \ldots, v_m\}$, de modo que se tenha $\delta(v_{i+1}) \geq \delta(v_i)$ para $1 \leq i \leq m$. Denote $k_i = \delta(v_i)$. Por definição, $m = \sum_{j=1}^{k} |S_j|$ e $k_i = j$ se $v_i \in S_j$.

Defina

$$\overline{A}_k = \bigoplus_{i=1}^{m} \left(\frac{P}{J + I_{k-k_i+1}} \right) \text{ e } \overline{B}_k = \underbrace{\frac{P}{J+I_k} \bigoplus \cdots \bigoplus \frac{P}{J+I_k}}_{d \text{ cópias}}.$$

Tem-se que $\overline{A}_k$ e $\overline{B}_k$ são $\mathbb{F}_p$-espaços vetoriais de dimensão finita, sendo

$$\dim_{\mathbb{F}_p} \overline{B}_k = d \cdot \left(\dim_{\mathbb{F}_p} \frac{P}{J+I_k} \right) = dc_{k-1}, \text{ e}$$

$$\begin{aligned} \dim_{\mathbb{F}_p} \overline{A}_k &= \sum_{i=1}^{m} \dim_{\mathbb{F}_p} \left(\frac{P}{J + I_{k-k_i+1}} \right) = \sum_{i=1}^{m} c_{k-k_i} = \\ &= c_{k-1} \cdot |S_1| + c_{k-2} \cdot |S_2| + \cdots + c_{k-k} \cdot |S_k| = \sum_{j=1}^{k} |S_j| c_{k-j}. \end{aligned}$$

Como I_1 é o ideal de P gerado por monômios de grau maior ou igual a 1, tem-se $\mathbb{F}_p \cong P/I_1$. Como $P/I_1 \cong \dfrac{P/(J+I_{k+1})}{I_1/(J+I_{k+1})}$, obtem-se que

$$1 = \dim_{\mathbb{F}_p}(P/I_1) = \dim_{\mathbb{F}_p} \left(\frac{P}{J+I_{k+1}} \right) - \dim_{\mathbb{F}_p} \left(\frac{I_1}{J+I_{k+1}} \right) = c_k - \dim_{\mathbb{F}_p} \left(\frac{I_1}{J+I_{k+1}} \right).$$

Logo, das observações acima, precisamos mostrar que

$$\dim_{\mathbb{F}_p} \overline{A}_k + \dim_{\mathbb{F}_p} \left(\frac{I_1}{J+I_{k+1}} \right) \geq \dim_{\mathbb{F}_p} \overline{B}_k.$$

Sejam então

$$A_k = \underbrace{P \bigoplus \cdots \bigoplus P}_{m \text{ cópias}} \text{ e } B = \underbrace{P \bigoplus \cdots \bigoplus P}_{d \text{ cópias}}.$$

Para cada $(a_1, \ldots, a_m) \in A_k$, considere o elemento $\sum_{j=1}^{m} a_j v_j \in I_1$. Pelo Lema 3.1.1, existem únicos $w_1, \ldots, w_d \in P$ tais que

$$\sum_{j=1}^{m} a_j v_j = \sum_{i=1}^{d} w_i t_i.$$

Fica portanto bem-definida a aplicação

$$\begin{aligned} \Phi : A_k &\longrightarrow B \\ (a_1, \ldots, a_m) &\longmapsto (w_1, \ldots, w_d), \end{aligned}$$

no qual os w_i são como acima. Tal aplicação é uma transformação linear de $\mathbb{F}_p$-espaços vetoriais, pois a unicidade dos coeficientes dados no Lema 3.1.1 faz com que

$$\Phi((a_1,\ldots,a_m)+\alpha\cdot(a_1',\ldots,a_m'))=\Phi((a_1,\ldots,a_m))+\alpha\cdot\Phi((a_1',\ldots,a_m')),$$

para quaisquer $a_j, a_j' \in P,\ 1\leq j\leq m$, e qualquer $\alpha\in\mathbb{F}_p$. Defina agora

$$\begin{aligned}\Psi : B &\longrightarrow I_1\\ (u_1,\ldots,u_d) &\longmapsto \sum_{i=1}^{d} u_i t_i.\end{aligned}$$

É imediato que Ψ é linear e sobrejetiva. Tem-se então um diagrama

$$\begin{array}{ccccc} A_k & \xrightarrow{\Phi} & B & \xrightarrow{\Psi} & I_1 \\ \downarrow{\scriptstyle q_1} & & \downarrow{\scriptstyle q_2} & & \downarrow{\scriptstyle q_3} \\ \overline{A}_k & & \overline{B}_k & & \dfrac{I_1}{J+I_{k+1}} \end{array}$$

no qual q_1, q_2, q_3 são as projeções canônicas. A próxima etapa desta demonstração consiste em obter aplicações lineares $\varphi : \overline{A}_k \to \overline{B}_k$ e $\psi : \overline{B}_k \to I_1/(J+I_{k+1})$ de modo a fechar o diagrama acima, tornando-o comutativo.

Por definição, tem-se

$$\ker q_1 = \bigoplus_{j=1}^{m}(J+I_{k-k_j+1}),\ \ker q_2 = \underbrace{(J+I_k)\bigoplus\cdots\bigoplus(J+I_k)}_{d\text{ cópias}} \text{ e } \ker q_3 = J+I_{k+1}.$$

Afirmamos que $\ker q_1 \subset \ker q_2 \circ \Phi$. Seja $(a_1,\ldots,a_m)\in\ker q_1$. Como $\{v_1,\ldots,v_m\}\subset I_1$, segue-se do Lema 3.1.1 que existem decomposições únicas $v_j=\sum_{i=1}^{d} w_{ij}t_i$ no qual $w_{ij}\in P$ para quaisquer i,j. Assim,

$$\sum_{j=1}^{m} a_j v_j = \sum_{j=1}^{m} a_j\left(\sum_{i=1}^{d} w_{ij}t_i\right) = \sum_{i=1}^{d}\left(\sum_{j=1}^{m} a_j w_{ij}\right)t_i.$$

Com isso,

$$\Phi((a_1,\ldots,a_m)) = (\sum_{j=1}^{m} a_j w_{1j},\ldots,\sum_{j=1}^{m} a_j w_{dj}). \qquad (*)$$

Sendo $(a_1,\ldots,a_m)\in\ker q_1$, escreva $a_j=\lambda_j+\mu_j$, no qual $\lambda_j\in J$ e $\mu_j\in I_{k-k_j+1}$, de modo que

$$\sum_{j=1}^{m} a_j w_{ij} = \sum_{j=1}^{m}\lambda_j w_{ij} + \sum_{j=1}^{m}\mu_j w_{ij}.$$

Agora, $\sum_{j=1}^m \lambda_j w_{ij} \in J$ pois $\lambda_j \in J$ para todo j, e $\sum_{j=1}^m \mu_j w_{ij} \in I_k$ pois caso contrário teria-se $\delta(\sum_{j=1}^m \mu_j w_{ij}) < k$, o que implicaria

$$\begin{aligned} k+1 &> \delta\left(\sum_{j=1}^m \mu_j w_{ij}\right) + 1 \geq \delta\left(\sum_{i=1}^d \sum_{j=1}^m \mu_j w_{ij} t_i\right) \\ &= \delta\left(\sum_{j=1}^m \mu_j \sum_{i=1}^d w_{ij} t_i\right) = \delta\left(\sum_{j=1}^m \mu_j v_j\right) \\ &\geq k - k_j + 1 + k_j = k+1, \end{aligned}$$

o que não pode ocorrer. Logo, $\sum_{j=1}^m a_j w_{ij} \in J + I_k$, e assim $\Phi((a_1, \ldots, a_m)) \in \ker q_2$, como queríamos. Por ser $\ker q_1 \subset \ker q_2 \circ \Phi$, a aplicação

$$\begin{aligned} \varphi : \overline{A}_k &\longrightarrow \overline{B}_k \\ q_1((a_1, \ldots, a_m)) &\longmapsto q_2 \circ \Phi((a_1, \ldots, a_m)) \end{aligned}$$

é bem-definida, linear, e por construção satisfaz $\varphi \circ q_1 = q_2 \circ \Phi$.

Afirmamos também que $\ker q_2 \subset \ker q_3 \circ \Psi$. Seja $(u_1, \ldots, u_d) \in \ker q_2$ e escreva $u_i = \lambda_i + \mu_i$ com $\lambda_i \in J$, $\mu_i \in I_k$. Tem-se $u_i t_i = \lambda_i t_i + \mu_i t_i \in J + I_{k+1}$ e assim $\Psi((u_1, \ldots, u_d)) = \sum_{i=1}^d u_i t_i \in J + I_{k+1} = \ker q_3$, como queríamos. Por raciocínio análogo ao anterior, induz-se uma aplicação linear $\psi : \overline{B}_k \to I_1/(J + I_{k+1})$ tal que $\psi \circ q_2 = q_3 \circ \Psi$.

Tem-se então o diagrama comutativo

$$\begin{array}{ccccc} A_k & \xrightarrow{\Phi} & B & \xrightarrow{\Psi} & I_1 \\ \downarrow{\scriptstyle q_1} & & \downarrow{\scriptstyle q_2} & & \downarrow{\scriptstyle q_3} \\ \overline{A}_k & \xrightarrow{\varphi} & \overline{B}_k & \xrightarrow{\psi} & \dfrac{I_1}{J + I_{k+1}} \end{array}$$

Mostremos agora que $\operatorname{Im} \varphi = \ker \psi$ e $\operatorname{Im} \psi = \dfrac{I_1}{J + I_{k+1}}$.

Primeiramente, ψ é sobrejetiva pois Ψ e q_3 são sobrejetivas e o diagrama comuta.

Tem-se $\operatorname{Im} \varphi \subset \ker \psi$ pois, dado $\overline{a} \in \overline{A}_k$, podemos escrever $\overline{a} = q_1((a_1, \ldots, a_m))$, para algum $(a_1, \ldots, a_m) \in A_k$, e então, usando a igualdade (*),

$$\begin{aligned} \psi \circ \varphi \circ q_1((a_1, \ldots, a_m)) &= \psi \circ q_2 \circ \Phi((a_1, \ldots, a_m)) = q_3 \circ \Psi \circ \Phi((a_1, \ldots, a_m)) = \\ &= q_3 \circ \Psi\left(\sum_{j=1}^m a_j w_{1j}, \ldots, \sum_{j=1}^m a_j w_{dj}\right) = q_3\left(\sum_{i=1}^d \left(\sum_{j=1}^m a_j w_{ij}\right) t_i\right), \end{aligned}$$

no qual os w_{ij} são os (únicos) elementos de P tais que $\sum_{j=1}^{m} a_j v_j = \sum_{i=1}^{d} \left(\sum_{j=1}^{m} a_j w_{ij}\right) t_i$, como explicitados anteriormente. Como $v_j \in S \subset J + I_{k+1}$, segue-se que

$$\psi \circ \varphi \circ q_1((a_1, \ldots, a_m)) = q_3 \left(\sum_{j=1}^{m} a_j v_j \right) = 0 \in \frac{I_1}{J + I_{k+1}}.$$

Resta verificar que $\ker \psi \subset \operatorname{Im} \varphi$.

Façamos antes uma observação. Considere J_1 o ideal (abstrato) de P gerado por $\{v_j t_i \mid 1 \leq j \leq m,\ 1 \leq i \leq d\}$, e denote por $\sum_{j=1}^{m} Pv_j$ o conjunto $\{\sum_{j=1}^{m} a_j v_j \mid a_j \in P\}$. Então

$$\ker q_3 = J + I_{k+1} = \sum_{j=1}^{m} Pv_j + J_1 + I_{k+1}.$$

Para provar tal afirmação, considere inicialmente $\widetilde{J}$ o ideal *abstrato* de P gerado por S. Tem-se que $J + I_{k+1} = \widetilde{J} + I_{k+1}$, pois a $\mathbb{F}_p$-álgebra quociente P/I_{k+1} é finita (e portanto discreta), o que implica que as imagens de J e $\widetilde{J}$ em P/I_{k+1} coincidem. Veja que podemos reescrever $\widetilde{J} + I_{k+1} = \widetilde{J}_k + I_{k+1}$, no qual $\widetilde{J}_k$ é o sub-ideal de $\widetilde{J}$ gerado por $\cup_{j \leq k} S_j = \{v_1, \ldots, v_m\} \subset S$. Tal reescrita é possível pois S é a união disjunta dos S_j e $I_{k+1} \supset \cup_{j \geq k+1} S_j$, por definição. Sendo $\widetilde{J}_k$ ideal (abstrato) gerado por $\{v_1, \ldots, v_m\}$, podemos explicitar

$$\widetilde{J}_k = \left\{ \sum_{j=1}^{m} \alpha_j m_j v_j m'_j \mid \alpha_j \in \mathbb{F}_p,\ m_j, m'_j \in M_T \right\}$$

(no qual, lembremos, M_T é o conjunto dos monômios sobre $\{t_1, \ldots, t_d\}$). Vale então a decomposição $\widetilde{J}_k = \sum_{j=1}^{m} Pv_j + J_1$. De fato, dado $\sum_{j=1}^{m} \alpha_j m_j v_j m'_j \in \widetilde{J}_k$, se $m'_j = 1$ tem-se $\alpha_j m_j v_j \in Pv_j$. Caso contrário, m'_j é monômio pertencente a I_1, e podemos escrever $v_j m'_j = (v_j t_i) l_{ij}$, no qual $l_{ij} \in M_T$. Isso significa que $m'_j \neq 1$ implica $\alpha_j m_j v_j m'_j = \alpha_j m_j (v_j t_i) l_{ij} \in J_1$, pela definição de J_1. Obtivemos portanto as igualdades

$$\ker q_3 = J + I_{k+1} = \widetilde{J} + I_{k+1} = \widetilde{J}_k + I_{k+1} = \sum_{j=1}^{m} Pv_j + J_1 + I_{k+1}.$$

Seja então $\overline{b} \in \overline{B}_k$ tal que $\psi(\overline{b}) = 0$. Podemos escrever $\overline{b} = q_2((u_1, \ldots, u_d))$, para algum $(u_1, \ldots, u_d) \in B$. Tem-se

$$0 = \psi(\overline{b}) = \psi \circ q_2((u_1, \ldots, u_d)) = q_3 \circ \Psi((u_1, \ldots, u_d)) = q_3 \left(\sum_{i=1}^{d} u_i t_i \right),$$

isto é,

$$\sum_{i=1}^{d} u_i t_i \in \ker q_3 = \sum_{j=1}^{m} Pv_j + J_1 + I_{k+1}.$$

Escreva

$$\sum_{i=1}^{d} u_i t_i = \sum_{j=1}^{m} a_j v_j + f,$$

no qual $a_j \in P$ e $f \in J_1 + I_{k+1}$. Como $I_1 \supset J_1 + I_{k+1}$, segue-se do Lema 3.1.1 que existem únicos $b_1, \ldots, b_d \in P$ tais que

$$f = \sum_{i=1}^{d} b_i t_i \in J_1 + I_{k+1}.$$

Afirmamos que $b_i \in J + I_k$ para todo $i = 1, \ldots, d$. Primeiramente, escreva $f = \alpha + \beta$, com $\alpha \in J_1$ e $\beta \in I_{k+1}$. Como $I_1 \supset I_{k+1}$, aplicando-se o Lema 3.1.1, reescreva $\beta = \sum_{i=1}^{d} \beta_i t_i$. Mas $I_k \supset I_{k+1}$ e I_k é o ideal gerado pelos monômios de grau maior ou igual a k, de modo que os termos β_i acima podem ser tomados em I_k, ou seja,

$$\beta = \sum_{i=1}^{d} \beta_i t_i \text{ com } \beta_i \in I_k, \text{ para todo } i = 1, \ldots, d.$$

Em segundo lugar, por serem $\alpha \in J_1$ e J_1 o ideal gerado pelos elementos $v_j t_i$, tem-se

$$\alpha = \sum_{i,j} \delta_{ij} v_j t_i \eta_{ij}, \text{ para certos } \delta_{ij}, \eta_{ij} \in P.$$

Como $I_1 \supset J = \overline{(S)}$, aplicando-se mais uma vez 3.1.1 podemos reescrever

$$\alpha = \sum_{i,j} \alpha_{ij} v_j t_i + \sum_{i,j} \widetilde{\alpha}_{ij} v_j m_{ij} t_i, \text{ em que } \alpha_{ij}, \widetilde{\alpha}_{ij}, m_{ij} \in P.$$

Já que cada v_j é elemento do ideal J, tem-se que os termos $\alpha_{ij} v_j, \widetilde{\alpha}_{ij} v_j m_{ij}$ pertencem a J. Com isso,

$$f = \sum_i b_i t_i = \sum_i (\sum_j \alpha_{ij} v_j) t_i + \sum_i (\sum_j \widetilde{\alpha}_{ij} v_j m_{ij}) t_i + \sum_i \beta_i t_i,$$

donde $b_i = (\sum_j \alpha_{ij} v_j + \sum_j \widetilde{\alpha}_{ij} v_j m_{ij}) + \beta_i \in J + I_k$, $\forall i = 1, \ldots, d$. Obtivemos assim a igualdade

$$\sum_{i=1}^{d} (u_i - b_i) t_i = \sum_{j=1}^{m} a_j v_j, \text{ no qual } b_i \in J + I_k \text{ para todo } i = 1, \ldots, d.$$

Tomando-se o elemento $(a_1, \ldots, a_m) \in A_k$, vale que $\Phi((a_1, \ldots, a_m)) = (u_1 - b_1, \ldots, u_d - b_d)$. Como $\ker q_2 = \underbrace{(J + I_k) \bigoplus \cdots \bigoplus (J + I_k)}_{d \text{ cópias}}$, vale $(b_1, \ldots, b_d) \in \ker q_2$, e assim

$$\overline{b} = q_2((u_1, \ldots, u_d)) = q_2((u_1 - b_1, \ldots, u_d - b_d)) = q_2 \circ \Phi((a_1, \ldots, a_m)) = \varphi \circ q_1((a_1, \ldots, a_m)),$$

ou seja, $\overline{b} \in \operatorname{Im} \varphi$, como queríamos.

Tem-se portanto a seguinte sequência exata de transformações lineares

$$\overline{A}_k \xrightarrow{\varphi} \overline{B}_k \xrightarrow{\psi} \frac{I_1}{J + I_{k+1}},$$

isto é, $\operatorname{Im}\varphi = \ker\psi$ e $\operatorname{Im}\psi = I_1/(J+I_{k+1})$. Pelo Teorema do Isomorfismo,

$$\dim_{\mathbb{F}_p}\overline{B}_k = \dim_{\mathbb{F}_p}\ker\psi + \dim_{\mathbb{F}_p}\operatorname{Im}\psi = \dim_{\mathbb{F}_p}\operatorname{Im}\varphi + \dim_{\mathbb{F}_p}\left(\frac{I_1}{J+I_{k+1}}\right),$$

$$\dim_{\mathbb{F}_p}\overline{A}_k = \dim_{\mathbb{F}_p}\ker\varphi + \dim_{\mathbb{F}_p}\operatorname{Im}\varphi.$$

Portanto,

$$\dim_{\mathbb{F}_p}\overline{A}_k + \dim_{\mathbb{F}_p}\left(\frac{I_1}{J+I_{k+1}}\right) - \dim_{\mathbb{F}_p}\ker\varphi = \dim_{\mathbb{F}_p}\overline{B}_k,$$

isto é, $\dim_{\mathbb{F}_p}\overline{A}_k + \dim_{\mathbb{F}_p}\left(\frac{I_1}{J+I_{k+1}}\right) \geq \dim_{\mathbb{F}_p}\overline{B}_k$, como queríamos demonstrar.

ii. Seja $b_0 = 1 \in \mathbb{R}$ e para cada $k \in \mathbb{N}$ defina $b_k = c_k - c_{k-1}$. Considere a série (real) de potências $\beta(y) = \sum_{k=0}^{\infty} b_k y^k$. Como $I_n \subset J$ para algum $n \in \mathbb{N}$, as dimensões $c_k = \dim_{\mathbb{F}_p}\left(\frac{P}{J+I_{k+1}}\right)$ estabilizam, de modo que $b_k = 0$ a partir de um certo índice. Ou seja, $\beta(y)$ é um polinômio em $\mathbb{R}$. Considere agora a série (real) de potências $\gamma(y) = \sum_{k=0}^{\infty} c_k y^k$. Como $b_k = c_k - c_{k-1}$ para todo $k \in \mathbb{N}$, tem-se $c_k = \sum_{i=0}^{k} b_i$. Com isso, dado qualquer $y \in [0,1)$, vale

$$\gamma(y) = \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} b_i\right)y^k = \sum_{k=0}^{\infty}\sum_{i=0}^{k} b_i y^i y^{k-i} = \left(\sum_{k=0}^{\infty} y^k\right)\left(\sum_{l=0}^{\infty} b_l y^l\right) = \frac{\beta(y)}{1-y},$$

pela convergência da série geométrica. Logo, $\gamma(y)$ converge para todo $y \in [0,1)$.

Fixe então $y \in [0,1)$ tal que $\sigma_S(y) = \sum_{k=1}^{\infty} |S_k| y^k$ convirja em y. Multiplicando-se a desigualdade do item **(i)** por y^k, obtem-se

$$c_k y^k - y^k \geq d c_{k-1} y^k - \sum_{j=1}^{k} |S_j| c_{k-j} y^k,$$

donde

$$\begin{aligned}\sum_{k=0}^{\infty} c_k y^k - \sum_{k=0}^{\infty} y^k &\geq \left(\sum_{k-1=0}^{\infty} d c_{k-1} y^{k-1} y\right) - \sum_{k=0}^{\infty}\left(\sum_{j=1}^{k} |S_j| y^j c_{k-j} y^{k-j}\right) \\ &= dy\sum_{l=0}^{\infty} c_l y^l - \left(\sum_{i=0}^{\infty} |S_i| y^i\right)\left(\sum_{j=0}^{\infty} c_j y^j\right),\end{aligned}$$

isto é, $\gamma(y) - \frac{1}{1-y} \geq dy\gamma(y) - \sigma_S(y)\gamma(y)$ ou, equivalentemente, $1 - dy + \sigma_S(y) \geq (\gamma(y)\cdot(1-y))^{-1}$. O resultado segue-se da continuidade de $\gamma(y)$ e $(1-y)^{-1}$ em $[0,1)$.

□

Corolário 3.1.4. Sejam $(e_k)_{k\in\mathbb{N}}$ uma sequência em $I_1 \subset P$, e $y \in [0,1)$. Dados $S \subset I_1$, $J = \overline{(S)}$ e $\sigma_S(y) = \sum_{k=1}^{\infty} |S_k| y^k$ como no teorema anterior, se $\sigma_S(y)$ converge em y e $1 - dy + \sigma_S(y) < 0$, então existe K ideal fechado de P tal que:

i. $I_n \not\subseteq K$ qualquer que seja $n \in \mathbb{N}$;

ii. $J \subseteq K$;

iii. P/K é infinito;

iv. $e_k + K \in P/K$ é nilpotente para todo $k \in \mathbb{N}$.

Demonstração. Pela continuidade de $\sigma_S(y)$ e $1/(1-y)$ em $y \in [0,1)$, podemos tomar $q \in \mathbb{N}$ suficientemente grande de modo que

$$1 - dy + \sigma_S(y) + \frac{1}{q(1-y)} < 0.$$

Sendo $y \in [0,1)$, dado $n \in \mathbb{N}$, vale que

$$\begin{aligned} q\sum_{k=1}^{n} y^{qk} &= \underbrace{y^q + \cdots + y^q}_{q \text{ fatores}} + \cdots + \underbrace{y^{nq} + \cdots + y^{nq}}_{q \text{ fatores}} \\ &\leq (\underbrace{1 + \cdots + y^{q-1}}_{q \text{ fatores}}) + (y^q + \cdots + y^{2q-1}) + \cdots + (y^{nq-q} + \cdots + y^{nq-1}) = \frac{1-y^{nq}}{1-y}. \end{aligned}$$

Logo,

$$\sum_{k=1}^{\infty} y^{qk} = \lim_{n\to\infty}\left(\sum_{k=1}^{n} y^{qk}\right) \leq q^{-1}\lim_{n\to\infty}\left(\frac{1-y^{nq}}{1-y}\right) = q^{-1}(1-y)^{-1},$$

e com isso

$$1 - dy + \sigma_S(y) + \sum_{k=1}^{\infty} y^{qk} \leq 1 - dy + \sigma_S(y) + \frac{1}{q(1-y)} < 0.$$

Defina $R = S \cup \{e_k^{qk} \mid k \in \mathbb{N}\}$. Tem-se $S \subseteq R \subseteq I_1$. Como $\delta(e_k) \geq 1$, vale $\delta(e_k^{qk}) \geq qk$, donde

$$1 - dy + \sum_{k=1}^{\infty} |S_k| y^k + \sum_{k=1}^{\infty} y^{\delta(e_k^{qk})} \leq 1 - dy + \sigma_S(y) + \sum_{k=1}^{\infty} y^{qk} < 0.$$

Agora, por construção, cada conjunto $R_k := \{v \in R \mid \delta(v) = k\}$ é finito. Além disso,

$$R_{\delta(e_k^{qk})} = \{e_k^{qk}\} \cup \{v \in S \mid \delta(v) = \delta(e_k^{qk})\} = \{e_k^{qk}\} \cup S_{\delta(e_k^{qk})}.$$

Logo, definindo-se a série (real) de potências $\sigma_R(y) = \sum_{k=1}^{\infty} |R_k| y^k$, vale $\sigma_R(y) = \sigma_S(y) + \sum_{k=1}^{\infty} y^{\delta(e_k^{qk})}$, com $\sigma_R(y)$ convergindo em $y \in [0,1)$. Substituindo-se na desigualdade acima, tem-se $1 - dy + \sigma_R(y) < 0$.

Tome então K o ideal fechado de P gerado por R. Por definição, $J \subseteq K$. Pelo item **(ii)** do Teorema 3.1.3, $\nexists n \in \mathbb{N}$ tal que $I_n \subseteq K$, o que implica também que P/K é infinito. Por fim, denotando-se $\pi : P \twoheadrightarrow P/K$ a projeção canônica, segue-se que $\pi(e_k)$ é nilpotente para todo $k \in \mathbb{N}$, pois por construção $e_k^{qk} \in R \subset K$. □

A próxima proposição está intimamente relacionada ao Teorema A dado por Wilson em [20]. Antes de prová-la, precisaremos do lema abaixo. Daqui em diante, denotaremos $F = \widehat{F(X)}_p$ o grupo pro-p livre de posto d, em que $X = \{x_1, \ldots, x_d\}$, e o identificaremos como subgrupo multiplicativo da álgebra de séries formais de potências $P = \mathbb{F}_p[\![t_1, \ldots, t_d]\!]$ via o homomorfismo contínuo tal que $x_i \mapsto 1 + t_i$, como no Teorema 2.4.45.

Lema 3.1.5. Sejam K um ideal fechado de P e F o grupo pro-p livre com base $\{x_1, \ldots, x_d\}$, mergulhado em P via $x_i \mapsto 1 + t_i$. Denote $q : P \twoheadrightarrow P/K$ a projeção canônica. Então $q(F) \subset P/K$ é finito se, e somente se, $I_n \subseteq K$ para algum n.

Demonstração. Suponha $I_n \subseteq K$ para algum n, e considere o homomorfismo (contínuo) canônico $P/I_n \twoheadrightarrow P/K$. Tem-se que P/I_n é finito, de modo que P/K também é finito, e portanto $q(F) \subset P/K$ é finito.

Reciprocamente, se $q(F)$ é finito, considere V o $\mathbb{F}_p$-subespaço vetorial (abstrato) de P/K gerado por $q(F)$. Então V é finito. Mais precisamente, V é uma $\mathbb{F}_p$-subálgebra finita, sendo portanto fechado em P/K. Mas, pelo Teorema 2.4.45, P é a álgebra de grupo completa de F, e assim a $\mathbb{F}_p$-álgebra P/K é gerada (topologicamente) por $q(F)$. Logo, $V = P/K$. Daí que $K = q^{-1}(\{0\})$ é aberto em P. Como $\{I_n\}_{n\in\mathbb{N}}$ é um sistema fundamental de vizinhanças abertas do $0 \in P$, segue-se que existe $n \in \mathbb{N}$ tal que $I_n \subseteq K$. □

Proposição 3.1.6. Sejam $S \subset I_1$, $J = \overline{(S)}$ e $\sigma_S(y)$ como no Teorema 3.1.3, e F o grupo pro-p livre com base $\{x_1, \ldots, x_d\}$, mergulhado em P via $x_i \mapsto 1+t_i$. Denote por $\pi : P \twoheadrightarrow P/J$ a projeção canônica. Então ou $1 - dy + \sigma_S(y) \geq 0\ \forall y \in [0, 1)$, ou todo subgrupo abstrato, denso e enumerável $G \leq \pi(F)$ admite um grupo de p-torção infinito como imagem homomórfica, isto é, existem H grupo e $\varphi : G \twoheadrightarrow H$ epimorfismo tais que H é infinito e a ordem de h é uma potência de p, para todo $h \in H$.

Demonstração. Suponha que exista $y \in [0, 1)$ tal que $1 - dy + \sigma_S(y) < 0$, e seja $G \leq \pi(F)$ um subgrupo abstrato, denso e enumerável. Como $F \subset 1 + I_1$, existe um conjunto enumerável $E = \{1 + e_k \mid k \in \mathbb{N}\} \subset 1 + I_1$ tal que $\pi(E) = G$. Como $(e_k)_{k\in\mathbb{N}} \in I_1$ e $1 - dy + \sigma_S(y) < 0$, segue-se do Corolário 3.1.4 que existe $K \subseteq P$ ideal fechado tal que $J \subseteq K$, P/K é infinito e $q(e_k)$ é nilpotente para todo $k \in \mathbb{N}$, no qual $q : P \twoheadrightarrow P/K$ é a projeção canônica. Considere o epimorfismo (contínuo) canônico

$$\begin{aligned} \widetilde{\varphi} : P/J &\longrightarrow\!\!\!\!\!\rightarrow P/K \\ a + J &\longmapsto a + K. \end{aligned}$$

Pondo $H = \widetilde{\varphi}(G)$ e $\varphi = \widetilde{\varphi}|_G : G \to H$, obter-se-á o resultado. De fato, dado $g = (1 + e_k) + J \in G$, existe $n \in \mathbb{N}$ tal que $e_k^n \in K$, pois $q(e_k) \in P/K$ é nilpotente. Assim,

$$(1 + e_k)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} e_k^i = 1 + e_k^{p^n} \in 1 + K,$$

pois $p \geq 2$ é primo e os coeficientes binomiais são calculados em $\mathbb{F}_p \subset P = \mathbb{F}_p[\![t_1, \ldots, t_d]\!]$. Com isso, $\varphi(g)^{p^n} = \widetilde{\varphi}((1 + e_k) + J)^{p^n} = 1 + K = 1_H \in H \subset P/K$, ou seja, H é um grupo de p-torção.

Agora, $q(F) \subset P/K$ é infinito, pois caso contrário teria-se $I_n \subseteq K$ para algum n, pelo Lema 3.1.5, o que não pode ocorrer devido ao Corolário 3.1.4. Como G é denso em $\pi(F) \subset P/J$, segue-se que $H = \widetilde{\varphi}(G)$ é denso em $q(F)$, e portanto H é também infinito. □

Antes de estabelecer o teorema principal desta seção, voltaremos a considerar o subgrupo de Frattini.

Lema 3.1.7. Seja F o grupo pro-p livre com base $\{x_1, \ldots, x_d\}$, mergulhado em P via $x_i \mapsto 1 + t_i$. Sejam ainda $\Phi(F)$ o subgrupo de Frattini de F e I_2 o ideal de P gerado pelos monômios de grau maior que 1. São válidos:

i. $\Phi(F) \subset 1 + I_2$;

ii. Se G é um grupo pro-p com $d(G) = d$ e tal que $G \cong F/N$, com $N \lhd_c F$, então $N \subset 1 + I_2$.

Demonstração. **i**. Tem-se $\Phi(F) \lhd_o F \subset 1 + I_1$. Observemos primeiro que P/I_2 é comutativo. De fato, sejam $u, v \in P$ e considere suas imagens $\overline{u}, \overline{v} \in P/I_2$. Como $P = \mathbb{F}_p + I_1$, é suficiente mostrar o resultado para $u, v \in I_1$. Nesse caso, vale $uv - vu \in I_2$ pois $\delta(u), \delta(v) \geq 1$, o que implica $\delta(uv) = \delta(vu) \geq 2$. Logo, $\overline{uv} - \overline{vu} = \overline{0} \in P/I_2$.

Dados então $g, h \in F$, escreva $g = 1 + u$ e $h = 1 + v$, no qual $u, v \in I_1$. O comutador $[g, h]$ satisfaz

$$[g,h] + I_2 = (1+u)(1+v)(1+u)^{-1}(1+v)^{-1} + I_2 = (1+u)(1+u)^{-1}(1+v)(1+v)^{-1} + I_2 = 1 + I_2,$$

pela comutatividade de P/I_2. Além disso,

$$g^p = (1+u)^p = \sum_{i=0}^{p} \binom{p}{i} u^i = 1 + u^p \in 1 + I_2,$$

pois $\binom{p}{i} \in \mathbb{F}_p$ e $\delta(u^p) = p \cdot \delta(u) \geq 2$. Como $\Phi(F) = \overline{[F,F]F^p}$, pelo item **(iii)** do Teorema 2.3.11, segue-se que $\Phi(F) \subset 1 + I_2$.

ii. Pelo item **(ii)** do Teorema 2.3.11, $[F : \Phi(F)] = p^d = [G : \Phi(G)] = [F/N : \Phi(F/N)]$. Denotando-se $\pi : F \to F/N$ o epimorfismo (contínuo) canônico, obtem-se $\frac{\Phi(F)N}{N} = \pi(\Phi(F)) = \pi(\overline{[F,F]F^p}) = \overline{[\pi(F), \pi(F)]\pi(F)^p} = \Phi(F/N)$. Com isso,

$$p^d = [F : \Phi(F)] = [F/N : \Phi(F/N)] = [F/N : (\Phi(F)N)/N] = [F : \Phi(F)N],$$

donde $N \subseteq \Phi(F)N \subseteq \Phi(F) \subset 1 + I_2$.

□

Estamos agora em condições de generalizar a Desigualdade de Golod-Šafarevič para uma ampla classe de grupos pro-p.

Teorema 3.1.8. [20, *Theorem* A] Seja G um grupo pro-p com uma apresentação finita com $n \geq 1$ geradores e $r \geq 1$ relações, e suponha $d = d(G) > 1$. Então ou

$$r \geq n + \frac{1}{4}d^2 - d$$

ou, para todo subgrupo abstrato, denso e enumerável A de G, existe $K \triangleleft_c G$ tal que $\frac{AK}{K}$ é um grupo de p-torção infinito.

Demonstração. Denote $d(G) = d$.

Dada uma apresentação de G com n geradores e r relações, a Proposição 2.4.20 nos diz que existe também apresentação de G com $\widetilde{n} = d$ geradores e $\widetilde{r} = r - n + d$ relações. Assim, se $\widetilde{r} \geq \frac{d^2}{4}$, vem $r - n + d \geq d^2/4$, isto é, $r \geq n + d^2/4 - d$. Basta então provar o resultado para o caso de $n = d$ geradores, ou seja, mostrar que $r \geq d^2/4$.

Tome $G = \overline{\langle x_1, \ldots, x_d \mid z_1, \ldots, z_r \rangle}_{\hat{p}}$ apresentação de G, com $F = \widehat{F(X)}_p$ o grupo pro-p livre com base $X = \{x_1, \ldots, x_d\}$ e $R = \{z_1, \ldots, z_r\} \subset F$. Denote $N = \overline{\langle R^F \rangle}$ e mergulhe F em $P = \mathbb{F}_p[\![t_1, \ldots, t_d]\!]$ via $x_i \mapsto 1 + t_i$.

Suponha que G não satisfaça a Desigualdade, isto é, $r < d^2/4$. Considere o polinômio $f : \mathbb{R} \to \mathbb{R},\ f(y) = ry^2 - dy + 1$. Tem-se $d^2 - 4r > 0$, daí que

$$0 < \frac{d}{2r} + \frac{\sqrt{d^2 - 4r}}{2r} \quad \text{e} \quad (0,1) \bigcap \left(\frac{d}{2r} - \frac{\sqrt{d^2 - 4r}}{2r} \ , \ \frac{d}{2r} + \frac{\sqrt{d^2 - 4r}}{2r} \right) \neq \varnothing.$$

Logo, existe $y \in [0, 1)$ tal que $f(y) = 1 - dy + ry^2 < 0$. Como $G = F/N$, vale $N \subset 1 + I_2$, pelo Lema 3.1.7. Em particular, $\delta(z_i - 1) \geq 2,\ \forall z_i \in R$. Tome $S = \{z_1 - 1, \ldots, z_r - 1\}$ e considere J o ideal fechado de P gerado por S e $\sigma_S(x)$ a série (real) de potências como no Teorema 3.1.3. Então $\sigma_S(x) = \sum_{i=1}^{r} x^{\delta(z_i - 1)}$ é um polinômio. Em particular, para $x = y \in [0, 1)$ como acima,

$$1 - dy + \sigma_S(y) = 1 - dy + y^{\delta(z_1 - 1)} + \cdots + y^{\delta(z_r - 1)} \leq 1 - dy + \underbrace{y^2 + \cdots + y^2}_{r \text{ fatores}} = 1 - dy + ry^2 < 0.$$

Denote $\pi : P \twoheadrightarrow P/J$ a projeção canônica. Como $G = F/N$ e $1 + N \subset J$, tem-se o epimorfismo (contínuo) canônico $q : G \twoheadrightarrow \pi(F) \subset P/J$. Segue-se da Proposição 3.1.6 que todo subgrupo abstrato, denso e enumerável de G possui um grupo de p-torção infinito como imagem homomórfica. □

Observamos que a estimativa dada acima para apresentações finitas é boa, visto que existem apresentações de grupos pro-p que atingem o limitante inferior da Desigualdade. De fato, tome $G = \mathbb{Z}_p \oplus \mathbb{Z}_p = \overline{\langle x, y \mid [x, y] \rangle}_{\hat{p}}$. Em tal apresentação, $n = d(G) = 2$ e $r = 1$, e portanto $r = n + d(G)^2/4 - d(G)$.

3.2 Aplicações

Nesta seção apresentamos algumas aplicações da teoria desenvolvida na seção anterior, incluindo grupos satisfazendo a Desigualdade, consequências à estrutura de certos subgrupos de grupos que a satisfazem, e alguns resultados para grupos abstratos.

3.2.1 Aplicações para grupos pro-p

É natural questionar quais outras classes de grupos pro-p satisfazem a desigualdade dada no Teorema 3.1.8, e se a mesma de fato generaliza a Desigualdade (**G-Š**). Vejamos algumas classes de grupos pro-p para o qual a mesma é válida e verifiquemos o caso finito em seguida.

Lema 3.2.1. Seja G um grupo abstrato ou profinito. Se G é um grupo de torção finitamente gerado e solúvel, então G é finito.

Demonstração. Considere $G' = [G, G]$ o subgrupo derivado e G/G' a abelianização de G (ou $G' = \overline{[G, G]}$, no caso profinito, pois aqui devemos considerar subgrupos fechados para preservar a topologia profinita em G/G'). Como todos os elementos de G têm ordem finita, os elementos de G/G' possuem a mesma propriedade. Logo, por ser abeliano e finitamente gerado, G/G' é um grupo finito, pela Classificação de Grupos Abelianos Finitamente Gerados. Ou seja, o índice $[G : G']$ é finito, e portanto G' é finitamente gerado (note que, no caso profinito, $G' = \overline{[G, G]}$ é aberto). Considerando-se $G'' = G^{(2)} = [G', G']$ (ou $G^{(2)} = \overline{[G', G']}$), obtem-se de modo análogo que $G^{(2)}$ é finitamente gerado. Podemos aplicar tal processo iteradamente sobre a série derivada, obtendo-se que todos os subgrupos derivados de G são finitamente gerados. Como G é solúvel, digamos, de classe n, obtem-se que $G^{(n-1)} = G^{(n-1)}/\{1\} \cong G^{(n-1)}/G^{(n)}$ é grupo finito. Com isso, o $(n-2)$-ésimo subgrupo derivado $G^{(n-2)} \triangleright G^{(n-1)}$ é também finito, por ser união disjunta de finitas cópias do subgrupo finito $G^{(n-1)}$. Indutivamente sobre os fatores da série derivada, obtem-se que G é finito. □

Definição 3.2.2. Diz-se que um grupo profinito G satisfaz a *Condição Maximal para Subgrupos Normais* (abreviadamente max-n) quando toda família não-vazia $\mathcal{N}$ de subgrupos normais fechados de G admite elemento maximal $N \in \mathcal{N}$ (com respeito à inclusão).

Devido ao Lema de Zorn tem-se, em particular, que se G satisfaz max-n, então toda cadeia ascendente

$$N_1 \leq_c N_2 \leq_c \cdots \leq_c N_k \leq_c \cdots$$

de subgrupos normais fechados de G admite elemento maximal, i.e., exite um índice i tal que $N_i \geq N_k$, para todo k.

Lema 3.2.3. Sejam $S \subset I_1$, $J = \overline{(S)}$ e $\sigma_S(y)$ como no Teorema 3.1.3, e F o grupo pro-p livre com base $\{x_1, \ldots, x_d\}$, mergulhado em P via $x_i \mapsto 1 + t_i$. Denote por $\pi : P \twoheadrightarrow P/J$ a projeção canônica. Se o grupo $\pi(F)$ é solúvel ou satisfaz max-n, então $1 - dy + \sigma_S(y) \geq 0$, $\forall y \in [0, 1)$.

Demonstração. Suponha $\pi(F)$ solúvel, e suponha por absurdo que $1 - dy + \sigma_S(y) < 0$ para algum $y \in [0, 1)$. Como $F = \overline{\langle 1 + t_1, \ldots, 1 + t_d \rangle}$, o subgrupo abstrato $A = \langle 1 + \pi(t_1), \ldots, 1 + \pi(t_d) \rangle \leq \pi(F)$ é denso e enumerável. Logo, pela Proposição 3.1.6, existe epimorfismo $\varphi : A \twoheadrightarrow B$ tal que B é um grupo de p-torção infinito. Mas $\pi(F)$ é solúvel e finitamente gerado, e assim A e B também são solúveis e finitamente gerados. Logo, pelo Lema 3.2.1, B é finito. Uma contradição. Portanto, $1 - dy + \sigma_S(y) \geq 0$, $\forall y \in [0, 1)$.

Antes de prosseguir com a segunda etapa da demonstração, uma definição: diremos que um grupo H é um *contra-exemplo* se existe $R \subset I_1$ satisfazendo as hipóteses do Teorema 3.1.3 tal que

$H \cong q(F)$ e $1 - dy + \sigma_R(y) < 0$ para *algum* $y \in [0,1)$, no qual K é o ideal fechado de P gerado por R, $q : P \twoheadrightarrow P/K$ é a projeção canônica e a série (real) $\sigma_R(y)$ é como no Teorema 3.1.3.

Suponha então que $G = \pi(F)$ satistaz max-n, e suponha por absurdo que $1 - dy + \sigma_S(y) < 0$ para algum $y \in [0,1)$. Nesse caso, G é um *contra-exemplo*.

Note agora que, como G satisfaz max-n, então existe um grupo pro-p quociente $C = G/N$ tal que *nenhum* quociente próprio de C é contra-exemplo. De fato, considere a família $\mathcal{N}$ de subgrupos normais fechados de G tais que G/N é contra-exemplo, para cada $N \in \mathcal{N}$. Por max-n, existe $N \in \mathcal{N}$, $N \lhd_c G$, o maior subgrupo normal fechado de G para o qual $C = G/N$ é contra-exemplo. Portanto, qualquer quociente próprio de C *não* é contra-exemplo.

Assim podemos, sem perda de generalidade, supor que $C = G$ acima, isto é, supor que *nenhum* quociente próprio de G é contra-exemplo (pois caso contrário basta passar a um quociente próprio adequado de G e fazer a construção a partir daí).

Lembremos que $F \subset 1 + I_1$. Seja $v \in F \setminus (1 + J)$ arbitrário. Tem-se $\pi(v) = \pi(v - 1 + 1) \neq 1_G$. Defina $R = S \cup \{v - 1\}$ e considere K o ideal fechado de P gerado por R, $q : P \twoheadrightarrow P/K$ a projeção canônica e $H = q(F)$ a imagem de F em P/K. Considere ainda o epimorfismo (contínuo) canônico $\widetilde{\varphi} : P/J \twoheadrightarrow P/K$. Tem-se $H = \widetilde{\varphi} \circ \pi(F) = \widetilde{\varphi}(G)$ e $\widetilde{\varphi} \circ \pi(v) = q(v) = q(v - 1 + 1) = 1_H$, de modo que $H = q(F) \subset P/K$ é um quociente próprio de $G = \pi(F) \subset P/J$. Como nenhum quociente próprio de G é *contra-exemplo*, vale que $1 - dx + \sigma_R(x) \geq 0$, $\forall x \in [0,1)$. Em particular, para $x = y$, vem $1 - dy + \sigma_R(y) \geq 0$. Mas $R = S \cup \{v - 1\}$, donde $\sigma_R(y) = \sigma_S(y) + y^{\delta(v-1)}$ e assim $1 - dy + \sigma_S(y) + y^{\delta(v-1)} \geq 0$. Como $\lim_{n\to\infty} y^n = 0$, podemos fixar $m \in \mathbb{N}$ o maior inteiro positivo tal que

$$1 - dy + \sigma_S(y) + y^m \geq 0.$$

Logo, $\delta(v - 1) > m$. Como a escolha de $v \in F \setminus 1 + J$ é arbitrária, segue-se que $v - 1 \in J$ para qualquer $v \in F$ satisfazendo $\delta(v - 1) > m$.

Agora, para qualquer $u \in F$, vale que $(u - 1)^{p^m} = \sum_{i=0}^{p^m} \binom{p^m}{i} (-1)^{p^m - i} u^i = u^{p^m} - 1$, donde $\delta(u^{p^m} - 1) = p^m \cdot \delta(u - 1) \geq p^m \cdot 1 > m$. Logo, $u^{p^m} - 1 \in J$, $\forall u \in F$, ou seja, G é um grupo de p-torção.

Dados $u_1, u_2 \in F$, escreva $u_1 = 1 + w_1$, $u_2 = 1 + w_2$ com $w_1, w_2 \in I_1$. Tem-se $u_1^{-1} = 1 + s_1$, $u_2^{-1} = 1 + s_2$, no qual $s_1 = \sum_{k\geq 1} (-w_1)^k$, $s_2 = \sum_{l \geq 1} (-w_2)^l \in I_1$ como no Teorema 2.4.45. Tem-se que o comutador de u_1 e u_2 satisfaz

$$\begin{aligned}
[u_1, u_2] &= (1 + w_1)(1 + w_2)(1 + s_1)(1 + s_2) = (1 + (1 + w_1)w_2(1 + s_1))(1 + s_2) \\
&= 1 + s_2 + (w_2 + w_1 w_2)(1 + s_1 + s_2 + s_1 s_2) \\
&= (1 + s_2 + w_2 + w_2 s_2) + w_2 s_1 + w_2 s_1 s_2 + w_1 w_2 + w_1 w_2 s_1 + w_1 w_2 s_2 + w_1 w_2 s_1 s_2 \\
&= 1 + w_2 s_1 + w_2 s_1 s_2 + w_1 w_2 + w_1 w_2 s_1 + w_1 w_2 s_2 + w_1 w_2 s_1 s_2 \\
&\equiv 1 \mod I_2,
\end{aligned}$$

isto é, $\delta([u_1, u_2] - 1) \geq 2$. Indutivamente, considerando-se um comutador (normado à esquerda) $[u_1, \ldots, u_n]$ de $n \geq 3$ elementos de F, se $\delta([u_1, \ldots, u_{n-1}] - 1) \geq n - 1$ então, denotando-se $u_n = 1 + w_n$

com $w_n \in I_1$ e $\lambda = [u_1, \ldots, u_{n-1}] - 1 \in I_{n-1}$, $s_n = \sum_{k\geq 1}(-w_n)^k \in I_1$, $\sigma = \sum_{l\geq 1}(-\lambda)^l \in I_{n-1}$, vem

$$\begin{aligned}[u_1, \ldots, u_{n-1}, u_n] &= [1+\lambda, u_n] = (1+\lambda)(1+u_n)(1+\sigma)(1+s_n) \\ &= 1 + w_n\sigma + w_n\sigma s_n + \lambda w_n + \lambda w_n\sigma + \lambda w_n s_n + \lambda w_n\sigma s_n \\ &\equiv 1 \mod I_n.\end{aligned}$$

Ou seja, $u_1, \ldots, u_n \in F$ implica $\delta([u_1, \ldots, u_n] - 1) \geq n$. Em particular, o comutador de $m+1$ elementos $u_1, \ldots, u_{m+1}$ quaisquer de F é tal que $[u_1, \ldots, u_{m+1}] - 1 \in J$. Logo, G é um grupo nilpotente (de classe no máximo m), e portanto solúvel.

Com isso, pelo Lema 3.2.1, $G = \pi(F) \subset P/J$ é finito, donde existe n tal que $I_n \subseteq J$, pelo Lema 3.1.5. Consequentemente, $1 - dy + \sigma_S(y) > 0$, pelo Teorema 3.1.3. Uma contradição. Portanto, $1 - dy + \sigma_S(y) \geq 0,\ \forall y \in [0, 1)$. □

Teorema 3.2.4. Seja G um grupo pro-p finitamente apresentável, com uma apresentação com $n \geq 1$ geradores e $r \geq 1$ relações, e suponha $d(G) \geq 2$. Se G é solúvel ou G satisfaz max-n, então

$$r \geq n + \frac{1}{4}d(G)^2 - d(G).$$

Demonstração. Denote $d(G) = d$. Novamente pela Proposição 2.4.20, G admite apresentação com $\widetilde{n} = d$ geradores e $\widetilde{r} = r - n + d$ relações, e portanto basta mostrar que $r \geq d^2/4$.

Tome $G = \overline{\langle x_1, \ldots, x_d \mid z_1, \ldots, z_r\rangle}_{\hat{p}}$ apresentação de G, com $F = \widehat{F(X)}_p$ o grupo pro-p livre com base $X = \{x_1, \ldots, x_d\}$ e $R = \{z_1, \ldots, z_r\} \subset F$. Denote $N = \overline{\langle R^F\rangle}$ e mergulhe F em $P = \mathbb{F}_p[\![t_1, \ldots, t_d]\!]$ via $x_i \mapsto 1 + t_i$.

Suponha, por absurdo, que $r < d^2/4$. Considere $f : \mathbb{R} \to \mathbb{R}$, $f(y) = ry^2 - dy + 1$. Como $d^2 - 4r > 0$, existe $y \in [0, 1)$ tal que $f(y) = 1 - dy + ry^2 < 0$. Sendo $G = F/N$, vale $N \subset 1 + I_2$ pelo Lema 3.1.7. Em particular, $\delta(z_i - 1) \geq 2,\ \forall z_i \in R$. Tome $S = \{z_1 - 1, \ldots, z_r - 1\}$ e considere J o ideal fechado de P gerado por S e $\sigma_S(x)$ a série (real) de potências como no Teorema 3.1.3. Para $x = y \in [0, 1)$ como acima, obtem-se $1 - dy + \sigma_S(y) = 1 - dy + y^{\delta(z_1-1)} + \cdots + y^{\delta(z_r-1)} \leq 1 - dy + ry^2 < 0$.

Denote $\pi : P \twoheadrightarrow P/J$ a projeção canônica. Como $G = F/N$ e $1 + N \subset J$, tem-se o epimorfismo (contínuo) canônico $q : G \twoheadrightarrow \pi(F) \subset P/J$. Agora, G é solúvel ou satisfaz max-n, e portanto $\pi(F)$ é solúvel ou satisfaz max-n. Logo, pelo Lema 3.2.3, $1 - dy + \sigma_S(y) \geq 0,\ \forall y \in [0, 1)$. Uma contradição. Portanto $r \geq d^2/4$. □

O Teorema de Golod-Šafarevič originalmente enunciado torna-se uma consequência direta do resultado acima.

Exemplo 3.2.5. Todo p-grupo finito G com $d(G) \geq 2$, visto como grupo pro-p, satisfaz a Desigualdade de Golod-Šafarevič. De fato, como p-grupos finitos são solúveis (por serem nilpotentes) e finitamente apresentáveis (como grupos pro-p), a afirmação segue-se do Teorema 3.2.4. Em particular, numa apresentação de G com número mínimo de geradores $d(G)$ e número mínimo de relações $r(G)$, vale

$$r(G) \geq \frac{d(G)^2}{4}.$$

O próximo corolário aqui apresentado afirma que a Desigualdade também é válida para grupos pro-p de posto finito, com pelo menos dois geradores. Resultados básicos sobre grupos pro-p de posto finito podem ser encontrados no Anexo I.

Corolário 3.2.6. Seja G um grupo pro-p de posto finito com $d(G) \geq 2$. Para qualquer apresentação de G com $n \geq 1$ geradores e $r \geq 1$ relações, vale

$$r \geq n + \frac{1}{4}d(G)^2 - d(G).$$

Demonstração. Como G tem posto finito, G é finitamente apresentável, pelo Teorema I.0.25. Agora, todo grupo pro-p de posto finito satisfaz max-n, pelo Corolário I.0.28. O resultado segue-se do Teorema 3.2.4. □

Nos próximos corolários obteremos propriedades de certos subgrupos de grupos pro-p satisfazendo o Teorema 3.2.4. Tais resultados abrangem os dados por Wilson em [20, *Corollary* A], sobre **(i)** o crescimento do número de geradores de subgrupos abertos em certos grupos pro-p finitamente apresentáveis e **(ii)** sobre os núcleos de aplicações de tais grupos sobre o grupo pro-p livre com 1 gerador, $\mathbb{Z}_p$.

Recordamos o leitor que todo subgrupo de um grupo solúvel é também solúvel. Consequentemente, todo subgrupo aberto, com pelo menos 2 geradores, de um grupo pro-p finitamente apresentável e solúvel também satisfaz a Desigualdade de Golod-Šafarevič. Podemos obter o mesmo resultado para grupos pro-p que satisfazem max-n. De fato, Wilson mostra em [22], em particular, que a condição maximal para subgrupos normais é herdada por subgrupos de índice finito, e tal propriedade traduz-se para subgrupos abertos de grupos profinitos, bastando considerar subgrupos fechados e ações contínuas. Com isso, podemos provar o seguinte:

Corolário 3.2.7. Seja G um grupo pro-p finitamente apresentável que é solúvel ou satisfaz max-n. Então existe uma constante $c > 0$ tal que $d(H) < c[G : H]^{\frac{1}{2}}$, para todo subgrupo aberto H de G.

Demonstração. Considere uma apresentação $G = \overline{\langle X \mid R\rangle}_{\hat{p}}$ com $|X| = n$ geradores e $|R| = r$ relações. Seja H subgrupo aberto de G com $[G : H] = h$. Suponha inicialmente $d(H) \geq 2$. Pela Proposição 2.4.16, H admite apresentação com $d_1 = h(n-1)+1$ geradores e $r_1 = hr$ relações. Como G é solúvel ou satisfaz max-n, o mesmo vale para H. Logo, pelo Teorema 3.2.4,

$$hr \geq h(n-1)+1+\frac{1}{4}d(H)^2 - d(H) = h(n-1)+\frac{1}{4}d(H)^2 - \frac{4}{4}d(H)+\frac{4}{4} = h(n-1)+\frac{1}{4}(d(H)-2)^2,$$

ou seja, $(d(H)-2)^2 \leq 4(r-n+1)h$. Com isso,

$$d(H) \leq 2(r-n+1)^{1/2}h^{1/2}+2 < 2(r-n+1)^{1/2}h^{1/2}+2h^{1/2} = (2(r-n+1)^{1/2}+2)h^{1/2}.$$

Basta pôr $c = 2(r-n+1)^{1/2}+2 > 0$. Caso seja $d(H) = 1$, tem-se também $d(H) = 1 < c \cdot 1^{1/2} \leq c[G : H]^{1/2}$. □

Exemplo 3.2.8. O corolário anterior nos dá uma condição necessária para que um grupo pro-p seja imagem homomórfica (contínua) de um grupo pro-p finitamente apresentável e solúvel. Daremos exemplo de um grupo pro-p que não pode ser uma tal imagem.

Seja T um grupo pro-p procíclico infinito, isto é, $T \cong \mathbb{Z}_p$, e seja $R = \mathbb{F}_p[\![T]\!]$. Evidentemente, R é um $\mathbb{F}_p[\![T]\!]$-módulo livre de posto 1. Como $T \cong \mathbb{Z}_p$, seus subgrupos $T^{p^r},\ r \in \mathbb{N}$, satisfazem $[T : T^{p^r}] = p^r$. Além disso, podemos considerar um conjunto $X = \{x_1, x_2, \ldots, x_{p^r}\} \subset T$ tal que $T = \cup_{i=1}^{p^r} x_i T^{p^r}$.

Afirmamos que R é o $\mathbb{F}_p[\![T^{p^r}]\!]$-módulo livre com base X. De fato, sejam M um $\mathbb{F}_p[\![T^{p^r}]\!]$-módulo topológico e $f : X \to M$ função. Note que f é contínua, pois X é discreto. Como $T = \cup_{i=1}^{p^r} x_i T^{p^r}$, fica bem definida a aplicação contínua $\tilde{f} : T \to M$ dada por $\tilde{f}(x_i g) = f(x_i)g,\ \forall x_i \in X,\ g \in T^{p^r}$. Agora, a álgebra de grupos $\mathbb{F}_p[T]$ é um $\mathbb{F}_p$-módulo livre com base T, de modo que $\tilde{f}$ estende-se unicamente a um homomorfismo $\tilde{\varphi} : \mathbb{F}_p[T] \to M$, e como $\mathbb{F}_p[T]$ é denso em $R = \mathbb{F}_p[\![T]\!]$, obtem-se um único homomorfismo contínuo $\varphi : R \to M$ tal que $\varphi(x_i) = f(x_i)$ para todo $x_i \in X$. Por fim, como a base X é finita, segue-se que R é de fato o $\mathbb{F}_p[\![T^{p^r}]\!]$-módulo livre (topológico) com base X.

Com isso, podemos escrever $R = \mathbb{F}_p[\![T^{p^r}]\!]x_1 \oplus \cdots \oplus \mathbb{F}_p[\![T^{p^r}]\!]x_{p^r}$. Considere o submódulo $(T^{p^r} - 1)R = \{at^{p^r} - a \mid a \in R,\ t \in T\}$. Tem-se que a ação do grupo T^{p^r} sobre o $\mathbb{F}_p[\![T^{p^r}]\!]$-módulo $\frac{R}{(T^{p^r}-1)R}$ é trivial, e assim $\frac{R}{(T^{p^r}-1)R}$ é um espaço vetorial sobre $\mathbb{F}_p$, de dimensão p^r.

Seja então o grupo pro-p $\mathcal{G} = R \rtimes T$, induzido pela ação natural de T sobre R. Por construção, seus subgrupos fechados $R \rtimes T^{p^r},\ r \in \mathbb{N}$, têm respectivos índices $[\mathcal{G} : R \rtimes T^{p^r}] = p^r$, sendo portanto abertos. Considere ainda a projeção canônica $R \rtimes T^{p^r} \twoheadrightarrow \frac{R}{(T^{p^r}-1)R} \rtimes T^{p^r}$. Como a ação de T^{p^r} sobre $\frac{R}{(T^{p^r}-1)R}$ é trivial, vem $\frac{R}{(T^{p^r}-1)R} \rtimes T^{p^r} \cong \frac{R}{(T^{p^r}-1)R} \times T^{p^r}$, e como $\frac{R}{(T^{p^r}-1)R}$ é um $\mathbb{F}_p$-espaço vetorial de dimensão p^r, segue-se que $d(R \rtimes T^{p^r}) \geq d(\frac{R}{(T^{p^r}-1)R} \times T^{p^r}) \geq p^r + 1$.

Ou seja, para cada $r \in \mathbb{N}$, construímos $H \lhd_o \mathcal{G}$ tal que $d(H) \geq p^r + 1$. Portanto, não existe uma constante $c > 0$ tal que $d(H) < c[\mathcal{G} : H]^{\frac{1}{2}}$ para todos os subgrupos abertos H de $\mathcal{G}$, e assim não existe G grupo pro-p finitamente apresentável e solúvel tal que $\mathcal{G}$ é imagem homomórfica (contínua) de G, pelo corolário anterior.

Corolário 3.2.9. Seja G um grupo pro-p finitamente apresentável e solúvel. Se K é um subgrupo normal fechado de G tal que $G/K \cong \mathbb{Z}_p$, então K é finitamente gerado.

Demonstração. Notemos primeiro que G pode ser escrito como o produto semi-direto de K por um subgrupo $T \leq G$ isomorfo a $\mathbb{Z}_p$. De fato, como $G/K \cong \mathbb{Z}_p$ e $\mathbb{Z}_p$ é um grupo pro-p livre (com 1 gerador), existe único homomorfismo (contínuo) $\rho : \mathbb{Z}_p \to G$ tal que $\pi \circ \rho = id_{\mathbb{Z}_p}$, no qual $\pi : G \twoheadrightarrow \mathbb{Z}_p$ é o homomorfismo (contínuo) com $\ker \pi = K$. Ou seja, $G \cong \ker \pi \rtimes \operatorname{Im} \rho = K \rtimes T$, no qual $T = \operatorname{Im} \rho \cong \mathbb{Z}_p$.

Mostremos que K é finitamente gerado. Como $d(K) = d(K/\Phi(K))$, é suficiente mostrar que $K/\Phi(K)$ é finito. Pelo Teorema 2.3.11, $K/\Phi(K)$ é um $\mathbb{F}_p$-espaço vetorial, e por ser $G \cong K \rtimes T$ tem-se que T age continuamente (via conjugação) sobre K, induzindo-se portanto uma ação natural de $\mathbb{F}_p[\![T]\!]$ sobre $K/\Phi(K)$. Em outras palavras, $K/\Phi(K)$ é um $\mathbb{F}_p[\![T]\!]$-módulo. Considere agora $q : F \twoheadrightarrow G$ apresentação finita de G, no qual F é grupo pro-p livre de posto finito e $\ker q = \overline{\langle R^F \rangle},\ R$ finito. Seja $K_0 = q^{-1}(K) \lhd F$. Obtem-se a apresentação $\mathbb{Z}_p \cong G/K \cong (F/\ker q)/(K_0/\ker q) \cong F/K_0$. Sendo $\mathbb{Z}_p$ finitamente apresentável, tem-se $K_0 = \overline{\langle R_0^F \rangle}$, no qual R_0 é finito. Assim, $K = q(K_0) =$

$q(\overline{\langle R_0^F \rangle}) = \overline{\langle q(R_0)^G \rangle}$, com $q(R_0)$ finito. Como a ação de $T \leq G$ sobre K se dá via conjugação, segue-se que $K/\Phi(K)$ é finitamente gerado como $\mathbb{F}_p[\![T]\!]$-módulo.

Como $T \cong \mathbb{Z}_p$ é grupo pro-p livre com 1 gerador, segue-se do Teorema 2.4.45 que a álgebra de grupos completa $\mathbb{F}_p[\![T]\!]$ é isomorfa à álgebra de séries formais de potências em uma variável $\mathbb{F}_p[\![x]\!]$. De tal isomorfismo segue-se que $\mathbb{F}_p[\![T]\!]$ é um Domínio de Ideais Principais, pois $\mathbb{F}_p$ é corpo, e tem-se também que $\mathbb{F}_p[\![T]\!]/J$ é finito para qualquer ideal $J \neq \{0\}$, pois os ideais de $\mathbb{F}_p[\![x]\!]$ são da forma $(x^\alpha),\ \alpha \geq 0$. Daí que existem ideais $J_1, \ldots, J_n$ de $\mathbb{F}_p[\![T]\!]$ tais que $K/\Phi(K)$ pode ser escrito como uma soma direta

$$\frac{\mathbb{F}_p[\![T]\!]}{J_1} \oplus \cdots \oplus \frac{\mathbb{F}_p[\![T]\!]}{J_n},$$

pela Estrutura de Módulos Finitamente Gerados sobre Domínios de Ideais Principais. Por outro lado, G é um grupo pro-p finitamente apresentável e solúvel, o que implica que G não pode ter o grupo $\mathcal{G} = \mathbb{F}_p[\![T]\!] \rtimes T$ do exemplo acima como imagem homomórfica (contínua). Em particular, K não pode ter o módulo $\mathbb{F}_p[\![T]\!]$ como imagem homomórfica, de modo que nenhum fator $\frac{\mathbb{F}_p[\![T]\!]}{J_i}$ na decomposição acima pode ser isomorfo a $\mathbb{F}_p[\![T]\!]$. Equivalentemente, tem-se que $J_i \neq \{0\}$ para todo i, e portanto $K/\Phi(K)$ é finito por ser soma direta finita de fatores finitos.

□

Encerramos esta subseção com alguns comentários acerca de Grupos de Golod-Šafarevič. Tal noção passa por desigualdades relativas à série $\sigma_S(y)$ do Teorema 3.1.3 de Vinberg.

Dado $G = \overline{\langle X \mid R \rangle}_{\hat{p}}$, considere $S = R - 1 \subset I_1 \subset P$ e a série associada $\sigma_S(y)$, como na demonstração do Teorema 3.1.8. Se existe $y \in [0, 1)$ para o qual $1 - dy + \sigma_S(y) < 0$ (em particular, se G *não* satisfaz a Desigualdade de Golod-Šafarevič), dizemos que G é um *Grupo de Golod-Šafarevič* (cf. [5] e [23] para uma formulação mais geral).

Como evidenciado pela implicação estrutural dada no Teorema 3.1.8, grupos de Golod-Šafarevič são necessariamente infinitos. Em [20], Wilson se questiona sobre o "quão grandes" podem ser os grupos de Golod-Šafarevič. Em tais considerações, ele conjectura que tais grupos contêm subgrupos livres de posto maior ou igual a dois.

Um dos resultados mais significativos quanto à estrutura de grupos de Golod-Šafarevič é precisamente o seguinte:

Teorema de Zelmanov [23]. Todo grupo de Golod-Šafarevič contem um grupo pro-p livre não-abeliano.

O resultado acima, provado em [23], responde positivamente à conjectura de Wilson. Uma das consequências de tal teorema é que, se G é de Golod-Šafarevič e Γ é um p-grupo finito, então G admite subgrupo normal aberto N tal que Γ é um quociente contínuo de N [23, p. 224].

3.2.2 Aplicações para grupos abstratos

Consideraremos agora aplicações dos resultados das seções anteriores no contexto abstrato.

Exemplo 3.2.10. (A construção de Golod [6] e o Problema Geral de Burnside). A teoria desenvolvida na Seção 3.1 nos permite construir grupos finitamente gerados de p-torção com

infinitos elementos, no qual p é um número primo qualquer. Fixe n um número de geradores, e considere $\widehat{F}_p$ o grupo pro-p livre com base $\{x_1, \ldots, x_n\}$. Mergulhando $\widehat{F}_p$ em $P = \mathbb{F}_p[\![t_1, \ldots, t_n]\!]$ via $x_i \mapsto 1 + t_i$, tome $S = \varnothing \subset I_1 \subset P$. Então $J = \overline{(S)} = \{0\}$, de modo que $P/J = P$. Agora, o subgrupo abstrato $A = \langle x_1, \ldots, x_n \rangle$ é denso em $\widehat{F}_p = \overline{\langle x_1, \ldots, x_n \rangle}$, pois $\widehat{F}_p$ é o completamento pro-p de A. Além disso, A é enumerável, por possuir finitos geradores. Logo, pela Proposição 3.1.6, se tomarmos n adequado, obteremos um grupo B como imagem homomórfica de A (portanto finitamente gerado) tal que B é infinito e seus elementos têm ordens potências de p.

O próximo teorema estabelece uma versão da Desigualdade para grupos abstratos.

Teorema 3.2.11. [20, *Theorem* B] Seja G um grupo abstrato finitamente apresentável, com uma apresentação com $n \geq 1$ geradores e $r \geq 1$ relações, e denote $d = d(G/[G,G])$. Então ou

$$r \geq n + \frac{1}{4}(d^2 - 1) - d,$$

ou existe um número primo p para o qual existe $N \triangleleft G$ tal que G/N é um grupo infinito, enumerável, de p-torção e residualmente finito.

Demonstração. Como G é finitamente apresentável, o grupo abeliano $G/[G,G]$ é finitamente gerado. Logo, da Decomposição de Grupos Abelianos Finitamente Gerados, existem $m, n_1, \ldots, n_k \in \mathbb{Z}$ tais que

$$\frac{G}{[G,G]} \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{m \text{ fatores}} \oplus \frac{\mathbb{Z}}{n_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{n_k\mathbb{Z}},$$

no qual m e k são minimais e $n_1 | n_2,\ n_2 | n_3, \ldots, n_{k-1} | n_k$. Em particular, $d(G/[G,G]) = m + k$. Agora, se a torção de $G/[G,G]$ é nula, vem $G/[G,G]G^p \cong \mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p$ (m fatores) para qualquer número primo p, de modo que $d(G/[G,G]G^p) = d(G/[G,G])$. Se a torção de $G/[G,G]$ é não-nula, então $n_1 \neq 0$, e assim existe um número primo p tal que $p | n_i,\ 1 \leq i \leq k$. Logo,

$$\frac{G}{[G,G]G^p} \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}}_{m \text{ fatores}} \oplus \frac{\mathbb{Z}/n_1\mathbb{Z}}{p\mathbb{Z}/n_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}/n_k\mathbb{Z}}{p\mathbb{Z}/n_k\mathbb{Z}} \cong \underbrace{\mathbb{F}_p \oplus \cdots \mathbb{F}_p \oplus \mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p}_{m+k \text{ fatores}},$$

e tem-se novamente $d(G/[G,G]G^p) = d(G/[G,G])$. Fixe então um tal primo p como acima.

Ponha $G = \langle X \mid R \rangle$ apresentação com $|X| = n,\ |R| = r$ e considere F_X o grupo livre abstrato com base $X = \{x_1, \ldots, x_n\}$ e escreva $R = \{u_1, \ldots, u_r\} \subset F_X$. Seja ainda $\widehat{F}_p = \widehat{F(X)}_p$ o completamento pro-p de F_X, ou seja, o grupo pro-p livre com base X. Tem-se $R \subset F_X \hookrightarrow \widehat{F}_p$, e com isso $\widehat{G}_p = \overline{\langle X \mid R \rangle}_{\hat{p}} = \widehat{F}_p / \overline{\langle R^{\widehat{F}_p} \rangle}$ é o completamento pro-p de G, tendo portanto uma apresentação (como grupo pro-p) com n geradores e r relações. Do Teorema 2.3.11, o quociente de Frattini de $\widehat{G}_p$ é seu quociente maximal abeliano de expoente p, de modo que

$$d(\widehat{G}_p) = d(\widehat{G}_p/\Phi(\widehat{G}_p)) = d\left(\frac{\widehat{G}_p}{\overline{[\widehat{G}_p, \widehat{G}_p](\widehat{G}_p)^p}}\right) = \dim_{\mathbb{F}_p} \frac{G}{[G,G]G^p} = d\left(\frac{G}{[G,G]G^p}\right) = d(G/[G,G]).$$

Denote $d = d(\widehat{G}_p) = d(G/[G,G])$.

Suponha inicialmente $d = 1$. Nesse caso, $\widehat{G}_p/\Phi(\widehat{G}_p)$ é um $\mathbb{F}_p$-espaço vetorial unidimensional. Como $\widehat{G}_p = \overline{\langle X \mid R\rangle}_{\hat{p}} = \overline{\langle x_1, \ldots, x_n \mid u_1, \ldots, u_r\rangle}_{\hat{p}}$, tem-se

$$\frac{\widehat{G}_p}{\Phi(\widehat{G}_p)} \cong \frac{\mathbb{F}_p x_1 \oplus \cdots \oplus \mathbb{F}_p x_n}{\sum\limits_{1\leq i\leq r} \mathbb{F}_p u_i} =: \frac{V}{S},$$

donde $1 = \dim_{\mathbb{F}_p}(\widehat{G}_p/\Phi(\widehat{G}_p)) = \dim V - \dim S = n - \dim S \geq n - r$, ou seja, $r \geq n - 1 = n + \frac{1}{4}(d^2 - 1) - d$.

Suponha agora $d > 1$. Nesse caso, segue-se do Teorema 3.1.8 que ou $r \geq n + \frac{1}{4}d^2 - d > n + \frac{1}{4}(d^2 - 1) - d$ ou, para todo A subgrupo abstrato, denso e enumerável de $\widehat{G}_p$, existe $K \lhd_c \widehat{G}_p$ tal que $\frac{AK}{K}$ é grupo infinito de p-torção. Suponha que estejamos no segundo caso. Pelo fato de que G é subgrupo (abstrato) denso em seu completamento $\widehat{G}_p$, podemos tomar $N \lhd G$ de modo que $G/N \cong \frac{AK}{K} \leq \widehat{G}_p/K$ é um grupo infinito, enumerável e de p-torção. Resta mostrar que G/N é residualmente finito. Como $K \lhd_c \widehat{G}_p$, o quociente $\widehat{G}_p/K$ é grupo pro-p, sendo portanto residualmente p, i.e., a interseção de seus subgrupos normais cujos índices são finitos (de fato, potências de p) é o grupo trivial. Em particular, seu subgrupo $G/N \leq \widehat{G}_p/K$ é residualmente finito. □

Em particular, assim como no caso pro-p aqui apresentado, o Teorema 3.2.11 é válido para grupos abstratos solúveis finitamente apresentáveis. Consequentemente, tem-se o:

Corolário 3.2.12. [20, *Corollary* B] Seja G um grupo abstrato finitamente apresentável e suponha que não existam p primo e $A, K \leq G$ tais que $K \lhd A$ e A/K é um grupo infinito, de p-torção, enumerável e residualmente finito. Então existe uma constante $c > 0$ tal que $d(H/[H,H]) \leq c[G : H]^{\frac{1}{2}}$, para todo subgrupo H de G com índice finito.

Demonstração. Considere uma apresentação $G = \langle X \mid R\rangle$ com $|X| = n$ geradores e $|R| = r$ relações. Seja H subgrupo de G de índice finito, e denote $[G : H] = h$ e $d = d(H/[H,H])$. Suponha inicialmente $d \geq 2$. Pela Proposição 1.3.2, H admite apresentação com $d_1 = h(n-1)+1$ geradores e $r_1 = hr$ relações. Por hipótese, não existe $N \lhd H$ tal que H/N é um grupo infinito, de p-torção, enumerável e residualmente finito. Logo, pelo Teorema 3.2.11, $hr \geq h(n-1)+1+\frac{1}{4}(d^2-1)-d = h(n-1) - \frac{1}{4} + \frac{1}{4}(d^2 - 4d + 4)$, donde

$$\left(r - n + 1 + \frac{1}{4}\right) h = hr - h(n-1) + \frac{1}{4}h > hr - h(n-1) + \frac{1}{4} \geq \frac{1}{4}(d-2)^2.$$

Com isso,

$$d < 2\left(r - n + \frac{5}{4}\right)^{1/2} h^{1/2} + 2 < 2\left(r - n + \frac{5}{4}\right)^{1/2} h^{1/2} + 2h^{1/2} = \left(2\left(r - n + \frac{5}{4}\right)^{1/2} + 2\right) h^{1/2}.$$

Basta pôr $c = 2(r - n + \frac{5}{4})^{1/2} + 2 > 0$. Caso seja $d = 1$, tem-se também $d < c \cdot 1^{\frac{1}{2}} \leq c[G : H]^{\frac{1}{2}}$. □

Anexo I

Grupos Pro-p de Posto Finito

Neste anexo compilamos alguns resultados relacionados a uma classe mais restrita de grupos pro-p finitamente gerados: os grupos pro-p de posto finito[1]. Tais grupos satisfazem diversas propriedades e caracterizações fortes e, dentre grupos pro-p, são por si só ricos objetos de estudo. Referimos ao leitor o texto de Dixon, du Sautoy, Mann e Segal [4] para um tratamento mais completo sobre grupos pro-p de posto finito. As propriedades e resultados aqui enunciados visam uma aplicação do Teorema 3.2.4, sendo portanto propriedades relacionadas a geradores e relações em apresentações pro-p.

O subgrupo de Frattini $\Phi(G) = \overline{[G,G]G^p}$ de um grupo pro-p G e sua relação com a quantidade de geradores de G será novamente utilizado. Recordemos que, dado G um grupo profinito, $d(G)$ denota a cardinalidade mínima de um conjunto gerador de G (como grupo topológico).

Definição I.0.13. Seja G um grupo pro-p. Definimos o *posto* de G, denotado $\mathrm{rk}(G)$, a ser o menor $n \in \mathbb{N} \cup \{0, \infty\}$ tal que *todo* subgrupo fechado de G é gerado por n elementos. Ou seja, $\mathrm{rk}(G) = \sup\{\mathrm{d(H)} \mid \mathrm{H} \leq_{\mathrm{c}} \mathrm{G}\}$.

Exemplo I.0.14. Todo p-grupo finito, visto como grupo pro-p, tem posto finito.

Exemplo I.0.15. O anel dos inteiros p-ádicos $\mathbb{Z}_p$ tem posto finito igual a 1, pois todos os seus subgrupos (ideais) são gerados por um único elemento.

Exemplo I.0.16. É importante ressaltar a distinção entre o posto (i.e., cardinalidade da base) de um grupo pro-p livre e o posto (rk) de um grupo pro-p. Apesar de ser $\mathbb{Z}_p$ um grupo pro-p livre com $\mathrm{posto}(\mathbb{Z}_p) < \infty$, este é o único grupo pro-p livre não-trivial $F_{\hat{p}}$ com $\mathrm{posto}(F_{\hat{p}}) = m < \infty$ tal que $\mathrm{rk}(F_{\hat{p}}) < \infty$. Isso segue do fato de que, se $m \geq 2$, então o grupo livre (abstrato) F com base de cardinalidade m admite subgrupo livre cuja base é infinita, somado ao fato de que $F_{\hat{p}}$ é o completamento pro-p de F (Teorema 2.4.6).

Exemplo I.0.17. O núcleo N da aplicação natural $\mathrm{GL}_n(\mathbb{Z}_p) \to \mathrm{GL}_n(\mathbb{Z}_p/p\mathbb{Z}_p) \cong \mathrm{GL}_n(\mathbb{F}_p)$ é um grupo pro-p de posto finito (cf. [21, Proposição 8.5.1]).

[1] Não confundir com o posto de um grupo livre!

Definição I.0.18. Seja G um grupo pro-p. Dizemos que G é *p-possante*[2] quando p é ímpar e $\overline{[G,G]} \leq \overline{G^p}$ ou quando $p = 2$ e $\overline{[G,G]} \leq \overline{G^4}$. Se for $\overline{[G,G]} \leq \overline{G^{p^2}}$, dizemos que G é *extra p-possante*.

Evidentemente, se G é extra p-possante, então G é p-possante. Ambas as definições coincidem no caso $p = 2$. Vale também a seguinte caracterização:

Lema I.0.19. Seja G um grupo pro-p. São equivalentes:

i. G é p-possante;

ii. Se $p = 2$, então $G/\overline{G^4}$ é abeliano, ou, se p é ímpar, então $G/\overline{G^p}$ é abeliano.

Demonstração. Segue imediatamente do Teorema 2.3.11. □

Definição I.0.20. Dado G um grupo pro-p, definimos sua *série de Frattini* indutivamente como a seguinte cadeia de subgrupos:

$$\Phi^0(G) := G,\ \Phi^1(G) := \Phi(G) \text{ e, para } i \geq 1,\ \Phi^{i+1}(G) := \Phi(\Phi^i(G)).$$

Como o subgrupo de Frattini é normal e característico, a série acima é de fato uma série normal descendente de subgrupos fechados

$$\cdots \lhd_c \Phi^{i+1}(G) \lhd_c \Phi^i(G) \lhd_c \cdots \lhd_c \Phi^2(G) \lhd_c \Phi(G) \lhd_c G.$$

Definição I.0.21. Um grupo pro-p G é dito *p-saturável*, ou *uniformemente p-possante*, ou simplesmente *uniforme*, quando G é finitamente gerado, p-possante, e os índices da sua série de Frattini são constantes[3], isto é, $[\Phi^i(G) : \Phi^{i+1}(G)] = [G : \Phi(G)],\ \forall i \geq 0$.

Grupos pro-p uniformes não são meramente finitamente gerados, mas sim finitamente apresentáveis. Mais adiante mostraremos que todo grupo pro-p de posto finito admite apresentação finita, e utilizaremos o fato abaixo.

Proposição I.0.22. Todo grupo pro-p uniforme é finitamente apresentável.

Uma demonstração direta do resultado acima pode ser vista em [4, Proposição 4.32], utilizando uma variante do lema abaixo, que também é necessário para a prova do nosso próximo teorema.

Lema I.0.23. Se G é um grupo pro-p com posto finito $\mathrm{rk}(G) < \infty$, então existe $H \lhd_o G$ tal que, para todo $K \lhd_o G$ com $K \subseteq H$, valem:

i. K é extra p-possante;

[2] Do inglês, "*powerful pro-p groups*". Não confundir com grupos potentes – "*potent groups*"! Um grupo pro-p é dito p-potente quando o $(p-1)$-ésimo termo da sua série central descendente está contido no subgrupo das p-potências.

[3] A princípio, o conceito de grupo pro-p uniforme G exige estabilidade nos índices $[P_i(G) : P_{i+1}(G)] = [G : P_2(G)]$, no qual $P_1(G) = G$ e $P_i(G) = \overline{[P_{i-1}(G), G](P_{i-1}(G))^p}$ (cf. [4, Definição 4.1]). Porém, se G é p-possante e finitamente gerado, então $P_{i+1}(G) = \Phi^i(G)$ (cf. [4, Teorema 3.6]).

ii. $[K, H] \leq \Phi(K)$;

iii. A função $\mathrm{pot} : K \to K$ dada por $\mathrm{pot}(k) = k^p$ induz um epimorfismo

$$\overline{\mathrm{pot}} : K/\Phi(K) \longrightarrow\!\!\!\!\!\rightarrow \Phi(K)/\Phi^2(K).$$

Referimos ao leitor [21, Proposição 8.5.2] para uma demonstração completa do lema acima. O principal teorema desta seção é o seguinte:

Teorema I.0.24. Todo grupo pro-p G de posto finito $\mathrm{rk}(G) < \infty$ admite um subgrupo normal aberto uniforme.

Demonstração. Precisamos obter $U \triangleleft_o G$ finitamente gerado e p-possante tal que $[\Phi^i(U) : \Phi^{i+1}(U)] = [U : \Phi(U)],\ \forall i \geq 0$.

Como G tem posto finito, segue-se do Lema I.0.23 que existe $H \triangleleft_o G$ tal que todo $K \triangleleft_o G$ contido em H é extra p-possante, $[K, H] \leq \Phi(K)$ e existe um epimorfismo $K/\Phi(K) \longrightarrow\!\!\!\!\!\rightarrow \Phi(K)/\Phi^2(K)$, induzido pela aplicação $k \mapsto k^p$. Em particular, o próprio H é extra p-possante e $[H : \Phi(H)] \geq [\Phi(H) : \Phi^2(H)]$. Note que $[H : \Phi(H)]$ é finito, pois $H/\Phi(H)$ é um p-grupo finito.

Tome então o subgrupo de Frattini $\Phi(H) \triangleleft_o H$. Como H é normal em G e $\Phi(H)$ é um subgrupo característico de H, vale que $\Phi(H)$ também é normal em G. Como G tem posto finito, H é finitamente gerado e portanto $\Phi(H)$ é aberto em H, pelo Teorema 2.3.13. Sendo H aberto em G, segue-se que $\Phi(H) \triangleleft_o G$, contido em H, e estamos, portanto, nas hipóteses do Lema I.0.23. Tem-se então que $\Phi(H)$ é extra p-possante, e portanto p-possante, e que existe epimorfismo $\Phi(H)/\Phi^2(H) \longrightarrow\!\!\!\!\!\rightarrow \Phi^2(H)/\Phi^3(H)$. Agora, a finitude de $\mathrm{rk}(G)$ implica que $\Phi(H),\ \Phi^2(H)$ e $\Phi^3(H)$ são finitamente gerados, sendo portanto todos abertos, e satisfazendo novamente as hipóteses do Lema I.0.23. Aplicando-se os argumentos acima iteradamente sobre a série de Frattini de H, obtem-se a cadeia

$$\cdots \triangleleft_o \Phi^{i+1}(H) \triangleleft_o \Phi^i(H) \triangleleft_o \cdots \triangleleft_o \Phi^3(H) \triangleleft_o \Phi^2(H) \triangleleft_o \Phi(H) \triangleleft_o H \triangleleft_o G,$$

e a sequência não-negativa não-crescente

$$[H : \Phi(H)] \geq [\Phi(H) : \Phi^2(H)] \geq \cdots \geq [\Phi^i(H) : \Phi^{i+1}(H)] \geq \cdots \geq 0.$$

Logo, a sequência acima estabiliza, isto é, existe $n \in \mathbb{N}$ tal que $[\Phi^m(H) : \Phi^{m+1}(H)] = [\Phi^n(H) : \Phi^{n+1}(H)],\ \forall m \geq n$.

Defina $U = \Phi^n(H) = \Phi(\Phi^{(n-1)}(H))$. Por construção, $U \triangleleft_o G$ e $[\Phi^i(U) : \Phi^{i+1}(U)] = [U : \Phi(U)],\ \forall i \geq 0$. Por fim, U é finitamente gerado pois G tem posto finito. Portanto, U é uniforme. □

Face ao fato de que grupos pro-p uniformes são finitamente apresentáveis, tem-se ainda o seguinte resultado:

Teorema I.0.25. Todo grupo pro-p G de posto finito $\mathrm{rk}(G) < \infty$ é finitamente apresentável.

Demonstração. Pelo Teorema I.0.24, G admite um subgrupo normal aberto uniforme U, que é finitamente apresentável pela Proposição I.0.22. Sendo U aberto e normal, G/U é um p-grupo finito, sendo portanto finitamente apresentável. Logo, pela Proposição 2.4.17, G é finitamente apresentável. □

Recordemos que, se N é um subgrupo normal de G, $d_G(N)$ denota a menor cardinalidade $|R|$ tal que N é gerado, como subgrupo normal fechado de G, pelo conjunto R. Uma aplicação do teorema anterior relacionada à Desigualdade de Golod-Šafarevič é dada no Corolário 3.2.6, com o auxílio da próxima proposição. Antes de demonstrá-la, enunciamos o seguinte lema, cuja demonstração pode ser vista em [21, Lema 12.1.1].

Lema I.0.26. Seja G um grupo pro-p. Se $\widetilde{N} \lhd_c G$ e $N \lhd_c G$ são tais que $\widetilde{N} \leq N$ e $N = \widetilde{N}L$, no qual $L = \overline{[N,G]N^p}$, então $\widetilde{N} = N$.

Proposição I.0.27. Seja G um grupo pro-p. Então G satisfaz max-n se, e somente se, $d_G(N) < \infty,\ \forall N \lhd_c G$.

Demonstração. Suponha que G satisfaz max-n e seja $N \lhd_c G$. Considere $\mathcal{K}$ a família de todos os subgrupos normais fechados de G tais que $K \subseteq N$ e $d_G(K) < \infty$, para cada $K \in \mathcal{K}$. Por max-n, existe K elemento maximal de $\mathcal{K}$, digamos gerado por um conjunto finito X como subgrupo normal fechado de G. Afirmamos que $K = N$. Caso contrário, existiria um elemento $g \in N \setminus K$, e assim o subgrupo normal fechado gerado por $X \cup \{g\}$ seria topologicamente finitamente gerado como subgrupo normal, e inteiramente contido em N, o que contradiz a maximalidade de K. Logo, $d_G(N) < \infty$.

Reciprocamente, suponha $d_G(N) < \infty,\ \forall N \lhd_c G$, e seja $\mathcal{N} = \{N_\lambda \mid \lambda \in \Lambda\}$ uma família não-vazia de subgrupos normais fechados de G. Defina $N = \overline{\bigcup_{\lambda\in\Lambda} N_\lambda} \lhd_c G$ e $L = \overline{[N,G]N^p} \lhd_c N$. Como $d_G(N) < \infty$ por hipótese, obtem-se que N/L é um grupo finito. Assim, $[N : N_\lambda L] < \infty$ para cada $N_\lambda \in \mathcal{N}$, e sendo $N = \overline{\bigcup_{\lambda\in\Lambda} N_\lambda L}$ obtem-se que de fato vale $N = \bigcup_{\lambda\in\Lambda} N_\lambda L$, pois L e cada N_λ são fechados. Logo, existe $\eta \in \Lambda$ tal que $N = N_\eta L$. Segue-se do Lema I.0.26 que $N = N_\eta \in \mathcal{N}$. Como $N_\lambda \subseteq N$ para todo $\lambda \in \Lambda$, conclui-se que N é um elemento maximal da família $\mathcal{N}$. Ou seja, G satisfaz max-n.

□

Corolário I.0.28. Todo grupo pro-p G de posto finito $\mathrm{rk}(G) < \infty$ satisfaz max-n.

Demonstração. Segue imediatamente da Proposição I.0.27 e da definição de $\mathrm{rk}(G)$ (I.0.13). □

Em particular, o corolário acima e o Corolário 3.2.6 garantem um resultado originalmente devido a H. Koch [10]: grupos pro-p que são *p-ádicos analíticos* satisfazem a Desigualdade de Golod-Šafarevič (i.e., grupos topológicos que admitem estrutura de variedade analítica sobre $\mathbb{Z}_p$ e cujas operações de produto e tomar a inversa são analíticas sobre $\mathbb{Z}_p$ – devido a essa definição, tais grupos são às vezes chamados *grupos de Lie p-ádicos*). Tal afirmação se deve à caracterização – dentre diversas outras – de que um grupo pro-p é p-ádico analítico se, e somente se, é um grupo pro-p de posto finito (cf. [4, Corolário 8.34]). Referimos novamente ao leitor o texto [4] para essa e outras caracterizações de grupos pro-p de posto finito, e para um tratamento aprofundado de grupos p-ádicos analíticos.

Anexo II

Homologia e Cohomologia de Grupos Pro-p

Esta seção tem caráter expositivo. Este trabalho foi desenvolvido sobre o estudo de grupos pro-p finitamente gerados e finitamente apresentáveis e, como ocorre no caso de grupos abstratos, tais propriedades de finitude são intimamente ligadas ao estudo da (co)homologia de tais grupos.

A teoria de homologia e cohomologia, no caso abstrato, é desenvolvida sobre módulos para aneis associativos e tem enfoque no caso das álgebras de grupo $\mathbb{Z}[G]$, no qual $\mathbb{Z}$ é o anel dos inteiros e G é um grupo (abstrato) dado. Através de tal teoria é possível extrair propriedades de finitude do grupo G relacionando-as aos grupo (módulos) de (co)homologia de G. Referimos ao leitor os textos de Rotman [18] e Brown [2] para introduções às teorias de homologia e cohomologia.

No caso de grupos profinitos e pro-p também desenvolve-se teoria de (co)homologia, nesse caso sobre módulos profinitos e pro-p, e com a exigência de que os homomorfismos considerados sejam contínuos. No caso pro-p, o anel base em geral é o corpo $\mathbb{F}_p$ com p elementos ou o anel $\mathbb{Z}_p$ dos inteiros p-ádicos, com enfoque nas álgebras $\mathbb{F}_p[\![G]\!]$ ou $\mathbb{Z}_p[\![G]\!]$, no qual G é um grupo pro-p dado. Referimos ao leitor [16, Capítulos 6 e 7] e [21, Capítulos 9 a 11] para textos sobre homologia e cohomologia de grupos profinitos e pro-p.

Citaremos aqui alguns resultados importantes relacionados a geradores e relações para apresentações de grupos pro-p, cujas demonstrações podem ser vistas nas referências dadas. Daqui em diante, denotaremos $H^i(G) := H^i(G, \mathbb{F}_p)$ a i-ésima cohomologia do grupo pro-p G com coeficientes em $\mathbb{F}_p$.

Teorema II.0.29. [16, Teorema 7.7.4] Seja G um grupo pro-p. São equivalentes:

i. $H^2(G) = 0$;

ii. G é um grupo pro-p livre.

Teorema II.0.30. [16, Corolário 7.7.5] Todo subgrupo fechado de um grupo pro-p livre é também um grupo pro-p livre.

Recordemos que, dado G um grupo profinito, $d(G)$ denota a cardinalidade mínima de um conjunto gerador de G (como grupo topológico), e se $N \lhd_c G$ é tal que $R \subset N$ tem cardinalidade mínima com $N = \overline{\langle R^G \rangle}$, denota-se $d_G(N) = |R|$.

Teorema II.0.31. [16, Teorema 7.8.1] Se G é um grupo pro-p, então $d(G) = \dim_{\mathbb{F}_p} H^1(G)$.

Definição II.0.32. Dados G um grupo pro-p finitamente gerado e $\pi : \widehat{F(X)}_p \twoheadrightarrow G$ uma apresentação de G, com $|X| = d(G)$ e $N = \ker \pi$, definimos o *posto de relações* de G a ser a quantidade mínima de relações $rr(G) = d_{\widehat{F(X)}_p}(N)$ na apresentação dada (podendo ser ∞).

Teorema II.0.33. [16, Teorema 7.8.3] Se G é um grupo pro-p finitamente gerado, então $rr(G) = \dim_{\mathbb{F}_p} H^2(G)$.

Em particular, o teorema acima implica que o conceito de posto de relações dado em II.0.32 independe da escolha de um conjunto minimal de geradores para G. Mais ainda, um grupo pro-p G é finitamente apresentável se, e somente se, as dimensões (sobre $\mathbb{F}_p$) de suas primeiras cohomologias $H^1(G)$ e $H^2(G)$ são finitas. A deficiência de um grupo pro-p finitamente apresentável G (Proposição 2.4.20) pode ser definida alternativamente como sendo $\mathrm{def}(G) = \dim_{\mathbb{F}_p} H^1(G) - \dim_{\mathbb{F}_p} H^2(G)$.

Via dimensões cohomológicas, o Teorema de Golod-Šafarevič (**G-Š**) pode ser reescrito da seguinte forma: se G é p-grupo finito, então

$$\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) \geq \frac{(\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p))^2}{4}.$$

No caso particular de grupos pro-p finitos, tem-se ainda o seguinte:

Teorema II.0.34. [16, Proposição 7.8.4] Se G é um p-grupo finito, então $rr(G) - d(G) = d(H^3(G, \mathbb{Z}))$.

Encerramos este anexo referindo-nos ao seguinte resultado importante, devido a Michel Lazard (cf. [12, Seção 2.5 e Proposição 2.5.7.1].

Teorema II.0.35. Seja G um grupo pro-p finitamente gerado tal que o módulo graduado $\mathrm{gr}(\mathbb{F}_p[\![G]\!])$ é uma álgebra polinomial sobre $\mathbb{F}_p$. Então $H(G, \mathbb{F}_p) := \bigoplus_{i=0}^{\infty} H^i(G)$ é a álgebra exterior de $H^1(G)$.

Com relação aos resultados apresentados no Anexo I, tem-se o seguinte: como $\mathrm{gr}(\mathbb{F}_p[\![G]\!])$ é uma álgebra polinomial se, e só se, G é um grupo pro-p uniforme (cf. [21, Seção 8.7]), e também por ser $d(G) = \dim_{\mathbb{F}_p} H^1(G)$, o teorema acima implica que, se G é uniforme, então $H(G, \mathbb{F}_p)$ é a álgebra exterior de um $\mathbb{F}_p$-espaço vetorial de dimensão $d(G)$. Isso nos dá uma outra alternativa para mostrar que todo grupo pro-p de posto finito é finitamente apresentável.

Uma demonstração do Teorema II.0.35 e das observações acima podem ser vistas em [21, Seção 11.6].

Referências

[1] N. Bourbaki. *Elements of Mathematics. General Topology*. Hermann, Paris, e Addison-Wesley, Reading, MA, 1966.

[2] K. S. Brown. *Cohomology of Groups*. Springer–Verlag, Berlin–Heidelberg–New York, 1982.

[3] D. E. Cohen. *Combinatorial Group Theory: a Topological Approach*. Cambridge University Press, Cambridge, 1989.

[4] J. D. Dixon et al. *Analytic Pro-p Groups*. 2ª ed. Cambridge University Press, Cambridge, 1999.

[5] M. Ershov. "Golod-Shafarevich Groups: A Survey". Em: *International Journal of Algebra and Computation* 22.5 (2012), pp. 1–68.

[6] E. S. Golod. "On nil-algebras and finitely approximable p-groups". Em: *Izv. Akad. Nauk SSSR Ser. Mat.* (em Russo) 28.2 (1964), pp. 273–276.

[7] E. S. Golod e I. R. Šafarevič. "On the class field tower". Em: *Izv. Akad. Nauk SSSR Ser. Mat.* (em Russo) 28.2 (1964), pp. 261–272.

[8] F. Q. Gouvêa. *p-adic Numbers: An Introduction*. 2ª ed. Springer–Verlag, Berlin–Heidelberg–New York, 1997.

[9] D. L. Johnson. *Presentations of Groups*. Cambridge University Press, Cambridge, 1990.

[10] H. Koch. "Zum Satz von Golod-Schafarewitsch". Em: *Math. Nachr.* 42 (1969), pp. 321–333.

[11] A. G. Kuroš. "Ringtheoretische Probleme, die mit dem Burnsideschen Problem über periodische Gruppen in Zusammenhang stehen". Em: *Izv. Akad. Nauk SSSR Ser. Mat.* (em Russo, com Introdução em Alemão) 5.3 (1941), pp. 233–240.

[12] M. Lazard. "Groupes analytiques p-adiques". Em: *Publ. Math. Inst. Hautes. Études. Sci.* 26 (1965), pp. 389–603.

[13] W. Magnus, A. Karrass e D. Solitar. *Combinatorial Group Theory*. 2ª ed. Dover Publications, Inc., New York, 1976.

[14] J. R. Munkres. *Topology*. 2ª ed. Prentice Hall, New Jersey, 2000.

[15] J. Neukirch. *Algebraic Number Theory*. Springer–Verlag, Berlin–Heidelberg–New York, 1999.

[16] L. Ribes e P. A. Zalesskii. *Profinite Groups*. 1ª ed. Springer, Berlin, 2000.

[17] P. Roquette. "On Class Field Towers". Em: *Algebraic Number Theory*. Ed. por J. W. S. Cassels e A. Fröhlich. Academic Press, London–New York, 1967.

[18] J. J. Rotman. *An Introduction to Homological Algebra*. 1ª ed. Academic Press, San Diego, 1979.

[19] J. J. Rotman. *An Introduction to the Theory of Groups*. 4ª ed. Springer–Verlag, Berlin–Heidelberg–New York, 1995.

[20] J. S. Wilson. "Finite Presentations of Pro-p Groups and Discrete Groups". Em: *Inv. Mathematicae* 105.1 (1991), pp. 177–183.

[21] J. S. Wilson. *Profinite Groups*. Clarendon Press, Oxford, 1998.

[22] J. S. Wilson. "Some Properties of Groups Inherited by Normal Subgroups of Finite Index". Em: *Math. Z.* 114.1 (1970), pp. 19–21.

[23] E. I. Zelmanov. "On Groups Satisfying the Golod-Shafarevich Condition". Em: *New Horizons in pro-p Groups*. Ed. por M. du Sautoy, D. Segal e A. Shalev. Birkhäuser, Boston, 2000.

Índice Remissivo