Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Existência de Subgrupos Livres Em Grupos Finitamente Apresentados Com Mais Geradores do que Relações

por

Michell Lucena Dias

sob orientação da

Profª. Drª. Aline Gomes da Silva Pinto

Brasília - DF
2016

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Michell Lucena Dias

Existência de Subgrupos Livres Em Grupos Finitamente Apresentados Com Mais Geradores do que Relações

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

Profª. Drª. Aline Gomes da Silva Pinto

Orientadora

Brasília, 8 de Março de 2016.

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

Lucena Dias, Michell
LD536e Existência de Subgrupos Livres em Grupos Finitamente Apresentados Com Mais Geradores do que Relações / Michell Lucena Dias; orientador Aline Gomes da Silva Pinto. -- Brasília, 2016.
81 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2016.

1. Grupos finitamente apresentados. 2. Grupos livres. 3. Grupos pro-p. I. Gomes da Silva Pinto, Aline, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Existência de Subgrupos Livres Em Grupos Finitamente Apresentados com mais Geradores do que Relações

por

MICHELL LUCENA DIAS *

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

MESTRE EM MATEMÁTICA

Brasília, 08 de março de 2016.

Comissão Examinadora:

Aline Gomes S Pinto

Profa. Dra. Aline Gomes da Silva Pinto – MAT/UnB
(Orientadora)

Martino Garonzi

Prof. Dr. Martino Garonzi – MAT/UnB (Membro)

Antônio Pereira Brandão Jr

Prof. Dr. Antônio Pereira Brandão Júnior – UFCG (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

Os senhores todos conhecem a pergunta famosa universalmente repetida: "que livro escolheria para levar consigo, se tivesse de partir para uma ilha deserta?". Vêm os que acreditam em exemplos célebres e dizem naturalmente: "uma história de Napoleão". Mas uma ilha deserta nem sempre é um exílio. Pode ser um passatempo.

O Livro da Solidão, Cecília Meireles.

Aos meus pais, Mairon e Socorro.

Resumo

Neste trabalho mostramos a existência de subgrupos livres em grupos finitamente apresentados com mais geradores do que relações, e cujo posto coincide com a deficiência da apresentação correspondente. Apresentamos a demonstração no caso abstrato utilizando a imersão de Magnus e imersões de anéis de grupos em anéis com divisão, e no caso pro-p, indicando as modificações e introduzindo o conceito de filtração. Também mostramos como o primeiro caso pode ser deduzido a partir do segundo utilizando completamento pro-p.

Palavras-Chave: grupos finitamente apresentados, grupos livres, grupos pro-p.

Abstract

In this work we show the existence of free subgroups in finitely presented groups with more generators than relations, and such that its rank is equal to the deficiency of the corresponding presentation. We present the proof in the abstract case using the Magnus embedding and embedding of group rings in skew-fields, and in the pro-p case, indicating the modifications and introducing the concept of filtration. We also show as the first case can be deduced from second case using the pro-p completion.

Keywords: finitely presented groups, free groups, pro-p groups.

Sumário

Introdução

Na Teoria de Grupos, a ferramenta clássica que permite definir um grupo de modo breve e inteligível é chamada *apresentação*, que identifica-o a partir do conjunto de seus *geradores* e de um outro conjunto que descreve igualdades entre seus elementos, ditas *relações*. Por esta razão, investigações têm sido desenvolvidas tendo hipóteses relacionadas à cardinalidade destes dois conjuntos, quando finitos.

Não obstante, ressaltamos que, quando interpretados adequadamente, estes apontamentos também inspiram investigações em um universo particular na Teoria de Grupos, chamado de *Grupos Profinitos*, os quais foram concebidos originalmente como grupos de Galois de extensões algébricas de corpos. Equivalentemente, eles podem ser definidos como *limites inversos* de grupos finitos. Assim, estas investigações surgem como tentativa de reproduzir propriedades de uma classe conveniente de grupos finitos por "passagem ao limite", como o caso especial dos *grupos pro-p* (definidos como limite inverso de p-grupos finitos).

O objetivo principal desta dissertação é apresentar as demonstrações dos seguintes resultados dados por John S. Wilson em [15]:

Teorema Principal (Caso Abstrato) Seja G um grupo que tem uma apresentação com n geradores $x_1, x_2, \ldots, x_n$ e m relações $r_1, r_2, \ldots, r_m$, onde $n > m$, e seja Y um conjunto qualquer de geradores de G. Então existem $n - m$ elementos de Y que geram livremente um subgrupo livre de G.

Teorema Principal (Caso Pro-p) Seja G um grupo pro-p que tem apresentação (como grupo pro-p) com n geradores $x_1, x_2, \ldots, x_n$ e m relações $r_1, r_2, \ldots, r_m$, onde $n > m$, e seja Y um conjunto qualquer de geradores topológicos de G. Então existem $n - m$ elementos de Y que geram livremente um subgrupo pro-p livre de G.

As suas demonstrações ancoram-se

i) na Álgebra Linear, considerando-se espaços vetoriais sobre anéis com divisão (à direita);

ii) na imersão de Magnus.

A linha do tempo destes resultados tem início por volta de 1930, quando Magnus [5] publicou seu Freiheitssatz, que é essencialmente o Teorema Principal (Caso Abstrato) onde $Y = \{x_1, x_2, \ldots, x_n\}$ e $m = 1$. Em 1978, Romanovskii [10] generalizou a hipótese de Magnus onde $Y = \{x_1, x_2, \ldots, x_n\}$ e m é qualquer inteiro menor do que n, e em 1986 obteve em [11] o Teorema Principal (Caso Pro-p) de modo independente e utilizando um complicado argumento indutivo.

A partir das contribuições de Romanovskii, em 2004, Wilson [14] deduziu o Caso Abstrato do Teorema Principal do Caso Pro-p utilizando completamento pro-p. Apresentamos esta demonstração na Seção 4.1. O desfecho desta cronologia dá-se conforme uma publicação de Wilson [15], onde as provas do Caso Abstrato e do Caso Pro-p do Teorema Principal foram elaboradas de modo direto e correlacionado. Apresentamos estas demonstrações na Seção 2.3 e na Seção 4.3, respectivamente.

Dispusemos esta dissertação em 4 capítulos.

No Capítulo 1, definimos grupos livres e grupos abelianos livres, e selecionamos alguns resultados que descrevem suas propriedades básicas. Definimos também a apresentação de um grupo por meio de geradores e de relações e selecionamos alguns resultados sobre grupos que têm uma apresentação finita. Além disso, encerramos o capítulo apresentando um resultado dado por Magnus que tem correlação com o Teorema Principal (Caso Abstrato). Seguimos [3], [9] e [12] como referências.

No Capítulo 2, introduzimos alguns resultados sobre derivações, sobre a imersão de Magnus para grupos abstratos e sobre a imersão de anéis de grupos em anéis com divisão. Além disso, apresentamos a demonstração do Teorema Principal (Caso Abstrato). Seguimos [15] como referência.

No Capítulo 3, selecionamos algumas definições da Topologia Geral e destacamos alguns resultados que descrevem propriedades básicas de espaços topológicos. Definimos também grupos pro-p via limite inverso e selecionamos resultados sobre o completamento pro-p, sobre grupos pro-p livres e sobre grupos pro-p que têm uma apresentação finita. Por fim, encerramos

o capítulo definindo módulos profinitos, módulos profinitos livres e álgebras de grupo completas e comentando alguns resultados que descrevem suas propriedades. Seguimos [6], [8] e [13] como referências.

No Capítulo 4, apresentamos uma nova demonstração para o Teorema Principal (Caso Abstrato) via completamento pro-p. Introduzimos também alguns resultados sobre a imersão de Magnus para grupos pro-p e sobre filtrações. Além disso, apresentamos a demonstração do Teorema Principal (Caso Pro-p). Seguimos [14] e [15] como referências.

Capítulo 1

Grupos Livres e Apresentação de Grupos

O objetivo deste capítulo é conduzir o leitor ao entendimento de especificidades importantes dos grupos livres e da apresentação de um grupo, os quais ambientam o estudo pretendido neste documento.

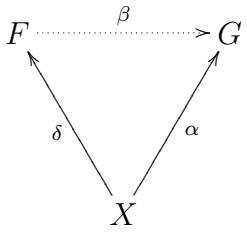
O tratamento empregado tem inclinação preliminar, sobretudo, referente ao Capítulo 2. Entretanto, além deste viés, introduziremos também alguns apontamentos inerentes aos conceitos supracitados que julgamos serem oportunos para fermentar nossa discussão, apesar de não mencioná-los posteriormente. Dentre eles, destacamos um limitante para a deficiência de um grupo (dado em função do Multiplicador de Schur) e os Teoremas de Hall (que ajudam a responder a questão se grupos finitamente gerados são finitamente apresentados) e de Magnus (que comporta-se como um caso especial do nosso principal resultado).

Este capítulo foi elaborado a partir da leitura de Johnson [3], Robinson [9] e Rotman [12], e é assumido o conhecimento básico da Teoria de Grupos por parte do leitor. Para consultar estes conceitos e resultados básicos, indicamos a referência Isaacs [2].

1.1 Grupos Livres e Grupos Abelianos Livres

1.1.1 Grupos Livres

Sejam X um subconjunto não vazio de um grupo F e $\delta : X \longrightarrow F$ uma função. Então F é dito *livre sobre* X se a seguinte propriedade universal é satisfeita: para qualquer grupo G e qualquer função $\alpha : X \longrightarrow G$, vista como aplicação entre conjuntos, existe um único homomorfismo de grupos $\beta : F \longrightarrow G$ tal que $\beta\delta = \alpha$, isto é, se o seguinte diagrama comuta:



Com a notação acima, a função $\delta : X \longrightarrow F$ é necessariamente injetiva. De fato, suponha que $\delta(x_1) = \delta(x_2)$, mas $x_1 \neq x_2$. Vamos considerar agora um grupo G, com $|G| \geqslant 2$, e $g_1, g_2 \in G$ distintos e tais que $\alpha(x_1) = g_1$ e $\alpha(x_2) = g_2$. Então $(\beta\delta)(x_1) = (\beta\delta)(x_2)$. Portanto, $\alpha(x_1) = \alpha(x_2)$, ou seja, $g_1 = g_2$; uma contradição com a hipótese.

Além disso, a existência de grupos livres não é um fato óbvio. De modo geral, a sua construção se dá conforme a definição de uma relação de equivalência sobre o conjunto cujos elementos são escritos como uma justaposição finita de elementos de X, que é a ideia por trás da demonstração do teorema abaixo.

Teorema 1.1.1 *Se X é um conjunto não vazio, então existem um grupo F e uma função $\delta : X \longrightarrow F$ tais que F é livre sobre X e $F = \langle Im\delta \rangle$.*

Demonstração: Consultar Robinson [9], Teorema 2.1.1. ∎

Sendo δ injetiva, podemos considerá-la sem perda de generalidade como sendo a inclusão. Neste caso, identificaremos X com sua imagem $\delta(X)$, e portanto assumiremos que $F = \langle X \rangle$. Diremos também que X é uma *base livre* (ou *conjunto de geradores livres*) de F.

Corolário 1.1.2 *Todo grupo é quociente de algum grupo livre.*

Demonstração: Sejam G um grupo e $X = \{x_g \mid g \in G\}$ um conjunto. Assim, $\alpha : X \longrightarrow G$ dada por $x_g \mapsto g$ é bijeção. Neste caso, considerando F o grupo livre sobre X, temos que existe um homomorfismo sobrejetivo $\phi : F \longrightarrow G$ (estendendo α), e assim $G \cong F/ker\phi$. ■

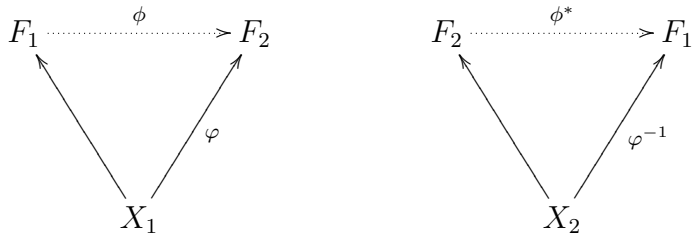
Conforme o Teorema 1.1.1, estabelecemos a existência dos grupos livres. A seguir, mostraremos no Teorema 1.1.3 que eles são determinados pela cardinalidade do seu conjunto de geradores livres. Para tanto, é oportuno esclarecermos que se F é livre sobre X, então podemos realizar a associação biunívoca abaixo, para qualquer grupo G.

$$\left\{ \begin{array}{c} \text{Homomorfismos} \\ \text{de } F \text{ em } G \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Aplicações} \\ \text{de } X \text{ em } G \end{array} \right\}$$

Com efeito, dado um homomorfismo de F em G, podemos exibir uma aplicação de X em G tomando-se, por exemplo, a sua restrição. A recíproca deste fato e a injetividade da associação acima decorrem imediatamente da propriedade universal na definição de grupo livre.

Teorema 1.1.3 *Sejam F_1 livre sobre X_1 e F_2 livre sobre X_2. Então $F_1 \cong F_2$ se, e somente se, X_1 e X_2 têm a mesma cardinalidade.*

Demonstração: Suponha $\varphi : X_1 \longrightarrow X_2$ uma bijeção. Então φ determina uma aplicação de X_1 em F_2 (que por simplicidade também será indicada por φ). Assim, existe um único homomorfismo $\phi : F_1 \longrightarrow F_2$ estendendo φ. Analogamente, a inversa $\varphi^{-1} : X_2 \longrightarrow X_1$ de φ também determina um único homomorfismo $\phi^* : F_2 \longrightarrow F_1$ estendendo $\varphi^{-1} : X_2 \longrightarrow F_1$.



A composição $\phi^*\phi : F_1 \longrightarrow F_1$ é um homomorfismo tal que

$$\phi^*\phi(x) = \phi^*(\varphi(x)) = \varphi^{-1}\varphi(x) = Id_{F_1}(x)$$

para todo $x \in X_1$. Neste caso, $\phi^*\phi$ estende a inclusão de X_1 em F_1. Uma vez que esta extensão é única, temos que $\phi^*\phi = Id_{F_1}$. Analogamente, $\phi\phi^* = Id_{F_2}$, donde concluímos que ϕ é isomorfismo e $F_1 \cong F_2$.

Reciprocamente, suponha $F_1 \cong F_2$. Conforme foi discutido, os homomorfismos de F_1 em G estão em correspondência biunívoca com as aplicações de X_1 em G, para todo grupo G. Em particular, para $G = \mathbb{Z}_2$ tem-se $2^{|X_1|}$ homomorfismos de F_1 em $\mathbb{Z}_2$. Agora, denotando por $Hom(F_i, \mathbb{Z}_2)$ o conjunto de todos os homomorfismos de F_i em $\mathbb{Z}_2$, para $i = 1, 2$, ressaltamos a seguinte igualdade

$$\mid Hom(F_1, \mathbb{Z}_2) \mid = \mid Hom(F_2, \mathbb{Z}_2) \mid$$

pois $F_1 \cong F_2$. Assim, este número é invariante por isomorfismos de F_1. Neste caso, temos em especial $2^{|X_1|} = 2^{|X_2|}$, e portanto $\mid X_1 \mid = \mid X_2 \mid$. ∎

Definimos o *posto* de um grupo livre como sendo a cardinalidade de uma base livre. Assim, o teorema anterior além de determinar a unicidade dos grupos livres sobre um conjunto, a menos de isomorfismo, esclarece também que o seu posto não depende da escolha da base, e portanto está bem definido.

Teorema 1.1.4 (Nielsen-Schreier) *Todo subgrupo de um grupo livre é livre.*

Demonstração: Consultar Rotman [12], Teorema 11.44. ∎

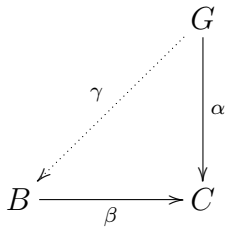
Se F é um grupo livre e $H \leqslant F$, em geral, não podemos garantir que o posto de H é menor do que o posto de F. Na verdade, muitas vezes ele se comporta de maneira completamente inesperada. Por exemplo, se F tem posto 2, o seu subgrupo comutador F' tem posto infinito (Rotman [12], Teorema 11.48). O teorema abaixo nos dá condições em que podemos determiná-lo.

Teorema 1.1.5 *Se F é um grupo livre de posto finito n, e H é um subgrupo de índice finito m, então H tem posto igual a $m(n-1)+1$.*

Demonstração: Consultar Rotman [12], Teorema 11.45. ∎

Um grupo G é dito ser *projetivo* se dados um epimorfismo $\beta : B \longrightarrow C$ e um homomorfismo $\alpha : G \longrightarrow C$, para quaisquer grupos B e C, existe um

homomorfismo $\gamma : G \longrightarrow B$ tal que $\beta\gamma = \alpha$, isto é, se o seguinte diagrama comuta:



Apesar de ser concebido como uma propriedade básica dos grupos livres (que é evidenciado na proposição a seguir), este fato terá lugar sutil, mas esclarecedor, durante a demonstração do nosso principal resultado.

Proposição 1.1.6 (Propriedade Projetiva dos Grupos Livres) *Todo grupo livre é projetivo.*

Demonstração: Sejam F, B e C grupos, com F livre sobre um conjunto X, $\alpha : F \longrightarrow C$ e $\beta : B \longrightarrow C$ homomorfismos, com β sobrejetivo. Dado $x \in X$, podemos encontrar $b_x \in B$ tal que $\alpha(x) = \beta(b_x)$. Assim, defina um homomorfismo $\gamma : F \longrightarrow B$ por meio da relação $\gamma(x) = b_x$, e observe que está bem definida. Então $(\beta\gamma)(x) = \beta(b_x) = \alpha(x)$, e portanto $\beta\gamma = \alpha$. ■

1.1.2 Grupos Abelianos Livres

Um grupo abeliano F é um *grupo abeliano livre* se F é uma soma direta de grupos cíclicos infinitos, ou seja, se existe um subconjunto $X \subset F$ de elementos de ordem infinita, chamado de *base livre*, com $F = \bigoplus_{x \in X} \langle x \rangle$. Se $X = \varnothing$, definimos $F = 0$.

Observe que se F é um grupo abeliano livre sobre X, então cada elemento $g \in F$ tem única expressão da forma

$$g = \sum_{x \in X} m_x x,$$

com $m_x \in \mathbb{Z}$ e $m_x \neq 0$ apenas para um número finito de índices de x. Observe também que $\langle X \rangle = \bigoplus_{x \in X} \langle x \rangle = F$. Ademais, grupos cíclicos infinitos estão na interseção dos grupos abelianos livres com os grupos livres.

Teorema 1.1.7 *Sejam F um grupo abeliano livre com base X, G um grupo abeliano arbitrário e $f : X \longrightarrow G$ uma função. Então existe um único homomorfismo $\phi : F \longrightarrow G$ estendendo f.*

Demonstração: Se $g \in F$, então a unicidade da expressão $g = \sum_{x \in X} m_x x$, onde $m_x \neq 0$ somente para um número finito de índices de X, mostra que $\phi : F \longrightarrow G$ dada por $\phi(g) = \sum_{x \in X} m_x f(x)$ está bem definida. Ademais, é homomorfismo e estende f. Agora, se $\overline{\phi} : F \longrightarrow G$ é um homomorfismo com as mesmas propriedades de ϕ, então eles são iguais pois coincidem numa base de F. ∎

O teorema anterior esclarece que os grupos abelianos livres são os grupos livres na categoria dos grupos abelianos. Portanto, convidamos o leitor a interpretar o conceito de posto e enunciar o Corolário 1.1.2 (Rotman [12], Corolário 10.12) e o Teorema 1.1.3 (Rotman [12], Teorema 10.14) no contexto desta categoria. De modo especial, aqui podemos provar que o posto respeita a hierarquia na estrutura de grupo (isto é, subgrupos têm posto menor ou igual ao posto do correspondente grupo), representando portanto uma particularidade do Teorema de Nielsen-Schreier para grupos abelianos livres (Rotman [12], Teorema 10.18).

Proposição 1.1.8 *Se F é um grupo livre sobre X, então F/F' é um grupo abeliano livre sobre $\overline{X} = \{xF' \mid x \in X\}$.*

Demonstração: Considere A um grupo abeliano e $\overline{f} : \overline{X} \longrightarrow A$ uma função. Defina agora $f : X \longrightarrow A$ por $x \longmapsto \overline{f}(xF')$. Como F é livre sobre X, então existe um homomorfismo $\varphi : F \longrightarrow A$ estendendo f. Uma vez que $F/ker\varphi$ é isomorfo a um subgrupo de A, que é abeliano, então $F' \leqslant ker\varphi$ e assim o homomorfismo $\overline{\varphi} : F/F' \longrightarrow A$ dado por $wF' \longmapsto \varphi(w)$ está bem definido, e estende $\overline{f}$. De fato, tem-se

$$\overline{\varphi}(xF') = \varphi(x) = f(x) = \overline{f}(xF')$$

para todo $x \in X$.

Vamos mostrar agora que $\overline{\varphi}$ é único com esta propriedade.

Suponha $\theta : F/F' \longrightarrow A$ um homomorfismo satisfazendo $\theta(xF') = \overline{f}(xF')$. Se $\pi : F \longrightarrow F/F'$ é o epimorfismo natural, então a composição $\theta\pi : F \longrightarrow A$ é tal que

$$\theta(\pi(x)) = \theta(xF') = \overline{f}(xF') = \overline{\varphi}(\pi(x)).$$

Portanto, θ e $\overline{\varphi}$ coincidem em $\pi(X) = \overline{X}$; e como π é sobrejetiva e X é uma base livre de F, então $\theta = \overline{\varphi}$. ∎

O Lema abaixo caracteriza os grupos abelianos livres de acordo com a propriedade projetiva.

Lema 1.1.9 *Um grupo abeliano é projetivo se, e somente se, é abeliano livre.*

Demonstração: Suponha G projetivo e considere um epimorfismo $\alpha : F \longrightarrow G$, onde F é um grupo abeliano livre. Aplicando a propriedade projetiva, obtemos um homomorfismo $\beta : G \longrightarrow F$ tal que $\alpha\beta = Id_G$. Se $g \in Ker\beta$, então $g = \alpha(\beta(g)) = \alpha(1) = 1$, e portanto $Ker\beta = \{1\}$. Assim, $G \cong Im\beta \leqslant F$, donde concluímos que G é abeliano livre.

A recíproca é idêntica a Proposição 1.1.6. ■

Proposição 1.1.10 *Se G é um grupo abeliano e H é um subgrupo tal que G/H é abeliano livre, então $G = H \oplus K$ para algum subgrupo K.*

Demonstração: É conveniente utilizarmos aqui a notação aditiva. Sejam $F = G/H$ e $\alpha : G \longrightarrow F$ o homomorfismo canônico. Como F é projetivo, existe um homomorfismo $\beta : F \longrightarrow G$ de sorte que $\alpha\beta = Id_F$. Se $g \in G$, então $\alpha(g - \beta(\alpha(g))) = \alpha(g) - \alpha(g) = 0$, e portanto $g - \beta(\alpha(g)) \in ker\alpha$. Logo, $g = g - \beta(\alpha(g)) + \beta(\alpha(g)) \in ker\alpha + Im\beta$, e assim $G = ker\alpha + Im\beta$. Além disso, se $g \in ker\alpha \cap Im\beta$, então $g = \beta(x)$ para algum $x \in F$. Portanto, $x = \alpha(\beta(x)) = 0$, donde $g = 0$, e assim $ker\alpha \cap Im\beta = \{0\}$. Então $G = ker\alpha \oplus Im\beta$. Por fim, $H = ker\alpha$. ■

Proposição 1.1.11 *Todo grupo abeliano finitamente gerado livre de torção é abeliano livre.*

Demonstração: Consultar Rotman [12], Teorema 10.19. ■

Teorema 1.1.12 (Teorema Fundamental) *Se A é um grupo abeliano finitamente gerado, então $A \cong T \oplus B$, onde T é finito e B é abeliano livre de posto finito.*

Demonstração: Consultar Rotman [12], Teorema 10.20. ■

Vamos denotar por

$$d(A)$$

o número mínimo de geradores de A, e por

$$\rho(A)$$

o posto de B (considerando a notação do teorema anterior).

As observações a seguir exprimem propriedades básicas destes números. Faremos menção a elas durante a Seção 1.2.3.

Observação 1.1.13 *Se A é um grupo abeliano finitamente gerado (como acima), então um conjunto de geradores para A contém um subconjunto que gera uma cópia isomorfa de B. Portanto, tem-se $\rho(A) \leqslant d(A)$. Ademais, $\rho(A) = d(A)$ se, e somente se, A é livre; e $\rho(A) = 0$ se, e somente se, A é de torção.*

Sejam $G_1, G_2, \ldots, G_n$ grupos cíclicos. Para cada $i \in \{1, 2, \ldots, n\}$, denote por 1_i o elemento neutro de G_i e considere $g_i \in G_i$ tal que $G_i = \langle g_i \rangle$. Então $G = G_1 \times G_2 \times \cdots \times G_n$ é um grupo abeliano finitamente gerado e os elementos

$$(g_1, 1_2, 1_3, \ldots, 1_n), (1_1, g_2, 1_3, \ldots, 1_n), \ldots, (1_1, 1_2, 1_3, \ldots, g_n)$$

constituem um conjunto gerador para G.

Sejam agora $m \in \mathbb{N}$, com $m \geqslant 2$, e $G_i = C_m$ um grupo cíclico finito de ordem m, para todo $i \in \{1, 2, \ldots, n\}$, isto é, $G = \underbrace{C_m \times \cdots \times C_m}_{n}$. Observe que $| G | = m^n$. Pelo que observamos acima, devemos ter $d(G) \leqslant n$. Supondo agora $d(G) = k < n$, tomemos $\{h_1, h_2, \ldots, h_k\}$ um conjunto gerador de G com exatamente k elementos. Como $o(h_i) \leqslant m$ para todo $i \in \{1, 2, \ldots, k\}$, temos

$$| G | \leqslant o(h_1)o(h_2) \cdots o(h_k) \leqslant m^k < m^n,$$

um absurdo. Assim, devemos ter $d(G) = n$.

Por analogia, denotando por $\mathbb{Z}^n$ o produto direto $\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n}$ de n cópias do grupo aditivo dos inteiros $\mathbb{Z}$, temos que $d(\mathbb{Z}^n) \leqslant n$. Suponhamos agora que $d(\mathbb{Z}^n) < n$. Tomando o subgrupo $N = (2\mathbb{Z})^n$ de $\mathbb{Z}^n$, temos $\mathbb{Z}^n / N \cong \mathbb{Z}_2^n$ e assim $d(\mathbb{Z}_2^n) \leqslant d(\mathbb{Z}^n) < n$. Mas pelo que mostramos, deveríamos ter $d(\mathbb{Z}_2^n) = n$, o que nos dá uma contradição. Logo, $d(\mathbb{Z}^n) = n$.

Observação 1.1.14 *Se A e B são grupos abelianos finitamente gerados, com B livre, então $d(A \oplus B) = d(A) + d(B)$.*

Temos que $A \oplus B = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_n} \times \mathbb{Z}^m$, onde $n, m \geqslant 0$, d_i divide d_{i+1} para todo $i \in \{1, 2, \ldots, n-1\}$, e $d_1 \geqslant 2$. Temos que $d(A \oplus B) = n + m$. De fato, é imediato que $d(A \oplus B) \leqslant n + m$. Considerando agora p um

divisor primo de d_1 e H_i o subgrupo de $\mathbb{Z}_{d_i}$ tal que $\mid \mathbb{Z}_{d_i} : H_i \mid = p$, para $i \in \{1, 2, \ldots, n\}$, temos

$$\frac{\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_n} \times \mathbb{Z}^m}{H_1 \times H_2 \times \cdots \times H_n \times p\mathbb{Z}^m} \cong \mathbb{Z}_p^{n+m}.$$

Assim, se $N = H_1 \times H_2 \times \cdots \times H_n \times p\mathbb{Z}^m$, então $d(A \oplus B/N) = n + m$. Logo,

$$n + m = d(A \oplus B/N) \leqslant d(A \oplus B) \leqslant n + m,$$

e portanto $d(A \oplus B) = n + m$.

Observação 1.1.15 *Se A é um grupo abeliano finitamente gerado e $H \leqslant A$, então $\rho(A) = \rho(A/H) + \rho(H)$.*

Se A é de torção, então identifica-se $\rho(A) = \rho(A/H) = \rho(H) = 0$. Neste caso, suponhamos que A tem uma parte livre. Nos resta então analisar a estrutura de H. Se H é de torção, então $\rho(H) = 0$ e $\rho(A/H) = \rho(A)$. Se H tem uma parte livre é imediato que $\rho(A/H) = \rho(A) - \rho(H)$.

1.2 A Apresentação de um Grupo

1.2.1 Geradores e Relações

Mostramos anteriormente que todo grupo G pode ser obtido como imagem de um grupo livre F sobre um epimorfismo $\delta : F \longrightarrow G$, ou seja, $G \cong F/R$ com $R = ker\delta$. Neste contexto, dizemos que δ é uma *apresentação* de G, e utilizamos a notação

$$G = (X \mid S)$$

onde X é um conjunto de geradores livres de F e $S \subset F$ é tal que $S^F = R$ (isto é, R é gerado como subgrupo normal por S). Quando for conveniente, por razão de organização observacional, utilizaremos a notação

$$R \rightarrowtail F \twoheadrightarrow G.$$

Os elementos de X são ditos *geradores* e os elementos de R são ditos *relações definidoras* (ou simplesmente *relações*) da apresentação.

Neste sentido, cometemos o abuso de notação de nos referirmos aos elementos de X e de S como elementos de G (subentendendo-se a sua identificação). Observe que as relações de G são os elementos de F que determinam

de modo não trivial a identidade de G. Observe também que a apresentação de um grupo não é única pois depende da escolha dos conjuntos X e S. Apesar disso, ela pode ser entendida como uma maneira breve de especificar um grupo. Vejamos alguns exemplos.

Se F é livre sobre X, então F não possui relações definidoras, e por este motivo usamos a notação $F = (X \mid \varnothing)$.

Os grupos cíclicos infinitos (os quais são cópias isomorfas de $\mathbb{Z}$) coincidem com os grupos abelianos livres de posto 1. Portanto, uma apresentação para $\mathbb{Z}_6 \cong \mathbb{Z}/6\mathbb{Z}$ é $(x \mid x^6)$. Observe também que $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, e assim podemos apresentá-lo por $(a, b \mid a^2, b^3, [a, b])$, onde o comutador de a e b foi introduzido no conjunto de relações para exprimir o fato de que suas imagens comutam.

O grupo dos quatérnios tem geradores x e y e relações definidoras $x^4 = 1$, $x^2 = y^2$ e $y^{-1}xy = x^{-1}$. Para maior aprofundamento e outros exemplos, indicamos consultar Johnson [3].

Observe que se um grupo é finitamente gerado, então ele pode ser visto como um quociente de um grupo livre de posto finito. Contudo, esta informação não determina por si sobre a cardinalidade do conjunto de relações. Com este espírito, introduziremos na próxima seção alguns apontamentos acerca desta questão.

1.2.2 Grupos Finitamente Gerados e Grupos Finitamente Apresentados

Dizemos que um grupo G é *finitamente apresentável* se existe uma apresentação com um número finito de geradores e de relações.

Claramente, exemplos de grupos finitamente apresentados incluem grupos cíclicos e grupos livres de posto finito. O próximo resultado ampliará sobremaneira o horizonte de nossos exemplos.

Proposição 1.2.1 *Todo grupo finito admite uma apresentação finita.*

Demonstração: Sejam G um grupo finito, digamos de ordem n, $X \subseteq G$ um conjunto de geradores (podemos tomar $X = G$, por exemplo) e $\theta' : F \longrightarrow G$, o homomorfismo do grupo livre F sobre X que estende a inclusão. Pelo Teorema 1.1.5, temos que $ker\theta'$ é gerado por um conjunto B de cardinalidade $n(r-1)+1$, onde $\mid X \mid = r$. Como $\langle B \rangle = ker\theta' \lhd F$, então $G = (X \mid B)$. ■

Fatalmente, todo grupo finitamente apresentado é finitamente gerado. Entretanto, a recíproca é falsa. Mostraremos adiante que o produto entrelaçado de dois grupos cíclicos infinitos, denotado por $\mathbb{Z} \wr \mathbb{Z}$, é 2-gerado e no entanto não possui uma apresentação finita.

O produto entrelaçado de dois grupos é definido da seguinte forma.

Sejam D e Q grupos, Ω um Q-conjunto finito, e seja $\{D_\omega \mid \omega \in \Omega\}$ uma família de cópias isomorfas de D indexada por Ω. Então o *produto entrelaçado* de D por Q, denotado por $D \wr Q$, é o produto semidireto de K por Q, onde $K = \prod_{\omega \in \Omega} D_\omega$ e Q age em K por $q \cdot (d_\omega) = (d_{q \cdot \omega})$, para quaisquer $q \in Q$ e $(d_\omega) \in K$.

Um caso especial da construção do produto entrelaçado é quando consideramos $\Omega = Q$ visto como Q-conjunto agindo sobre si por multiplicação à esquerda. Assim, $K = \prod_{x \in Q} D_x$ é o produto direto de $\mid Q \mid$ cópias de D, e $q \in Q$ envia uma $\mid Q \mid$-upla $(d_x) \in \prod_{x \in Q} D_x$ em $(d_{q \cdot x})$.

Agora, para estendermos esta ideia ao caso geral onde podemos considerar inclusive grupos infinitos, a construção do produto entrelaçado é feita da seguinte forma. Sejam N e G grupos quaisquer. Para cada $x \in G$, seja N_x uma cópia isomorfa de N via a aplicação $a \longmapsto a_x$ e consideremos o produto cartesiano $B = \prod_{x \in G} N_x$. Se $b \in B$ e $g \in G$, defina b^g pela correspondência $(b^g)_x = b_{xg^{-1}}$. Assim, esta ação de G em B define o produto semidireto $G \ltimes B$, o qual chamamos de *produto entrelaçado* de G por N.

A fim de introduzir os Teoremas 1.2.6 e 1.2.7, devidos a P. Hall, é conveniente destacarmos agora os seguintes pontos.

Teorema 1.2.2 (von Dick) *Sejam G e H grupos com apresentações $\varepsilon : F \longrightarrow G$ e $\delta : F \longrightarrow H$ tais que $Ker\varepsilon \leqslant Ker\delta$. Então a função $\varepsilon(f) \longmapsto \delta(f)$ está bem definida e é um epimorfismo de G em H.*

Demonstração: Se $g \in G$, então $g = \varepsilon(f)$ para algum $f \in F$. Além disso, $\delta(f)$ é unicamente determinado por g. De fato, se $g = \varepsilon(f_1)$, então $f = f_1 k$, onde $k \in Ker\varepsilon$. Logo, $k \in Ker\delta$, e portanto $\delta(f) = \delta(f_1)$. Ademais, claramente $\varepsilon(f) \longmapsto \delta(f)$ é um epimorfismo. ∎

Teorema 1.2.3 (B. H. Neumann) *Sejam G um grupo finitamente apresentável e X um conjunto qualquer de geradores de G. Então G tem uma apresentação finita da forma $(X_0 \mid r_1 = r_2 = \cdots = r_l = 1)$, onde $X_0 \subseteq X$.*

Demonstração: Seja $(y_1, y_2, \ldots, y_m \mid s_1 = s_2 = \cdots = s_l = 1)$ uma apresentação finita de G. Se $G = \langle X \rangle$, então $G = \langle X_0 \rangle$, onde $X_0 = \{x_1, x_2, \ldots, x_n\}$

é um subconjunto finito de X. Existem, portanto, expressões para os termos y_i's em termos dos x_j's, e também existem expressões para os termos x_j's em termos dos y_i's, digamos $y_i = w_i(x)$ e $x_j = v_j(y)$. Assim, as seguintes relações em termos dos x_j's são válidas:

$$s_k(w_1(x), \ldots, w_m(x)) = 1 \qquad \text{e} \qquad x_j = v_j(w_1(x), \ldots, w_m(x))$$

onde $k = 1, \ldots, l$ e $j = 1, \ldots, n$. Observe também que existem apenas uma quantidade finita dessas relações.

Agora seja $\overline{G}$ um grupo com geradores $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}$ e com relações definidoras como acima em termos dos $\overline{x_j}$'s. Pelo Teorema 1.2.2, existe um epimorfismo de $\overline{G}$ em G dado por $\overline{x_j} \longmapsto x_j$. Defina $\overline{y_i} = w_i(\overline{x})$. Então o segundo conjunto de relações definidoras acimas mostram que $\overline{G} = \langle \overline{y_1}, \overline{y_2}, \ldots, \overline{y_m} \rangle$. Uma vez que $s_k(\overline{y}) = 1$, então novamente pelo Teorema 1.2.2, existe um epimorfismo de G em $\overline{G}$ dado por $y_i \longmapsto \overline{y_i}$. Observe também que estes epimorfismos são mutuamente inversos, então eles são isomorfismos. Assim, G é gerado pelos elementos $x_1, x_2, \ldots, x_n$ sujeito apenas as relações definidoras nos x_j's listadas acima. ∎

Observação 1.2.4 *Se F é um grupo livre sobre o conjunto $\{x_1, x_2, \ldots, x_n\}$, então $F'/\gamma_3 F$ é abeliano livre e os elementos $[x_i, x_j]\gamma_3 F$ formam um conjunto de geradores livres, com $i < j = 2, \ldots, n$.*

Primeiramente, lembre que $\gamma_i F$ é o i-ésimo termo da série central inferior de F. Note que o subgrupo $\gamma_3 F$ não impõe torção ao quociente $F/\gamma_3 F$, e portanto este último é livre de torção. Neste caso, $F'/\gamma_3 F$ é abeliano finitamente gerado livre de torção, isto é, abeliano livre (Proposição 1.1.11). Ademais, qualquer elemento tem expressão única em termos de $[x_i, x_j]\gamma_3 F$.

Observação 1.2.5 *Sejam $R \rightarrowtail F \twoheadrightarrow G$ uma apresentação de um grupo G. Se A é o grupo de todos os automorfismos α de F tais que $\alpha(R) = R$, então existe um homomorfismo canônico $A \longrightarrow Aut(G)$.*

Dado $\alpha \in A$, podemos induzir um homomorfismo $\overline{\alpha} : F/R \longrightarrow F/R$ definido por $\overline{\alpha}(xR) = \alpha(x)R$. Para $x_1, x_2 \in F$, note que $x_1 R = x_2 R$ implica $x_1 x_2^{-1} \in R$, donde $\alpha(x_1 x_2^{-1}) \in R$, e portanto $\overline{\alpha}(x_1 R) = \overline{\alpha}(x_2 R)$, isto é, $\overline{\alpha}$ está bem definida. Além disso, observe que $\overline{\alpha} \in Aut(G)$.

No próximo teorema, trabalharemos com os grupos nilpotentes livres que podem ser entendidos como grupos livres na categoria dos grupos nilpotentes. Outra menção importante sobre a classe dos grupos finitamente gerados é o seguinte Teorema de B. H. Neumann: *existem* $2^{\aleph_0}$ *grupos* 2*-gerados não isomorfos*. Assim, quando construirmos um grupo 2-gerado dado por um quociente G/H de um grupo livre G de posto finito, saberemos que certamente existem, no máximo, $2^{\aleph_0}$ maneiras de escolher o subgrupo H.

Teorema 1.2.6 (P. Hall) *Se A é um grupo abeliano enumerável, então existem $2^{\aleph_0}$ grupos 2-gerados não isomorfos G tais que $[G'', G] = 1$, $Z(G) \cong A$ e $G/Z(G)$ tem centro trivial.*

Demonstração: Sejam Y um grupo nilpotente livre de classe 2 sobre $\{y_i \mid i \in \mathbb{Z}\}$. Então $Y \cong F/\gamma_3 F$, onde F é um grupo livre de posto infinito enumerável. Assim $Y' = F'/\gamma_3 F$, e portanto Y' é um grupo abeliano livre cuja base é formada pelos elementos $c_{ij} = [y_i, y_j]$, com $i < j$ (Observação 1.2.4).

Agora, vamos considerar K o subgrupo de Y' gerado pelos elementos da forma $c_{ij}^{-1} c_{i+1,j+1}$. Temos $[Y', Y] = 1$ (pois Y é de classe 2), donde $[K, Y] = 1$, ou seja, $K \subseteq Z(Y)$. Logo, $K \trianglelefteq Y$, e assim podemos definir o quociente $X = Y/K$. Escrevendo $x_i = y_i K$, temos que $\{x_i \mid i \in \mathbb{Z}\}$ é um conjunto gerador de X sujeito as relações

$$[x_i, x_j, x_k] = 1 \quad \text{e} \quad [x_{i+k}, x_{j+k}] = [x_i, x_j], \tag{1.1}$$

pois $\overline{c_{ij}^{-1} c_{i+1j+1}} = 1$ em X.

Suponha por absurdo que X é abeliano. Então $Y' \leqslant K$, e portanto $Y' = K$. Assim, cada c_{ij} pode ser escrito da seguinte forma

$$c_{ij} = (c_{i_1 j_1}^{-1} c_{i_1+1, j_1+1})(c_{i_2 j_2}^{-1} c_{i_2+1, j_2+1}) \dots (c_{i_k j_k}^{-1} c_{i_k+1, j_k+1}).$$

Mas como os elementos c_{ij}'s formam uma base livre de Y', então existe $l \in \{1, 2, \dots, k\}$ para o qual

$$c_{i_l j_l} = 1,$$

o que é um absurdo. Portanto, X é um grupo nilpotente livre de torção (pois K não impõe finitude às ordens dos elementos em Y) de classe 2. Além disso, temos que $X' = Y'/K$ é abeliano livre.

Por (1.1), vem $[x_{i+k}, x_{(j+k)+r}] = [x_{i+k}, x_{(j+r)+k}] = [x_i, x_{j+r}]$. Logo, os elementos da forma

$$d_r = [x_i, x_{i+r}]$$

(com $i = 1, 2, \dots$) independem de i e com isto formam uma base livre para X'.

Agora, note que a aplicação $x_i \longmapsto x_{i+1}$ preserva o conjunto de relações (1.1). Assim, da Observação 1.2.5, existe um automorfismo α de X tal que $\alpha(x_i) = x_{i+1}$, e α tem ordem infinita. Com isto, podemos definir o produto semidireto

$$H = T \ltimes X,$$

onde $T = \langle t \rangle$ e t age sobre X conforme α (isto é, $x_i^t = x_{i+1}$). Então

$$d_r^t = [x_0, x_r]^t = [x_0^t, x_r^t] = [x_1, x_{r+1}] = d_r$$

donde $X' \leqslant Z(H)$, e assim podemos tomar o quociente $\overline{H} = H/X'$. Uma vez que $\overline{H}$ é metabeliano (pois não é comutativo e qualquer comutador de tamanho 3 é trivial), então $H'' \leqslant X'$, e daí $[H'', H] = 1$. Além disso, fica estabelecido que H pode ser gerado por t e x_0 pois $x_i^t = x_{i+1}$.

Em $\overline{H}$ temos que os comutadores em x_i são suprimidos. Em virtude disto, denotando agora $tX' = \overline{t}$ e $x_iX' = \overline{x_i}$, concluímos que os elementos $\overline{t}$ e $\overline{x_0}$ geram $\overline{H}$ são tais que

$$[\overline{x_i}, \overline{x_j}] = 1 \quad \text{e} \quad \overline{x_i}^{\overline{t}} = \overline{x_{i+1}}.$$

Vem,

$$\overline{H} \cong \langle tX', x_0X' \rangle = \langle tX', x_iX' \mid i \in \mathbb{Z} \rangle \cong \langle tX' \rangle \ltimes \prod_{i \in \mathbb{Z}} \langle x_iX' \rangle.$$

Logo, $\overline{H} \cong \mathbb{Z} \wr \mathbb{Z}$, donde $Z(\overline{H}) = 1$. Consequentemente, $Z(H) = X'$.

Como X' é um grupo abeliano livre de posto infinito enumerável e A é abeliano enumerável, então $A \cong X'/M$ para algum $M \leqslant X'$. Temos $M \lhd H$ (pois $X' = Z(H)$), e podemos definir

$$G_M = \frac{H}{M}.$$

Pelo que já foi discutido, devemos ter $[G_M'', G_M] = 1$ e G_M é 2-gerado (pois H é 2-gerado). Com isto,

$$Z(G_M) = \frac{Z(H)}{M} = \frac{X'}{M} \cong A$$

e

$$\frac{G_M}{Z(G_M)} = \frac{H/M}{X'/M} \cong \frac{H}{X'} = \overline{H}.$$

Assim, $Z(G_M/Z(G_M)) = 1$.

Finalmente, nos resta mostrar que $2^{\aleph_0}$ grupos não isomorfos podem ser obtidos variando M em X', sempre respeitando a condição $X'/M \cong A$. Em primeiro lugar, observamos que existem $2^{\aleph_0}$ candidatos a M disponíveis. Assim, suponha por absurdo que os correspondentes G_M determinem uma quantidade enumerável de classes de isomorfismo. Então para algum M existe uma quantidade não enumerável de isomorfismos $\theta_\lambda : G_{M_\lambda} \longrightarrow G_M$.

Se $\alpha_\lambda : H \longrightarrow G_{M_\lambda}$ é o homomorfismo natural, com $ker\alpha_\lambda = M_\lambda$, então vamos considerar a composição $\theta_\lambda\alpha_\lambda : H \longrightarrow G_M$. Se $\theta_\lambda\alpha_\lambda = \theta_\mu\alpha_\mu$, então $M_\lambda = ker(\theta_\lambda\alpha_\lambda) = ker(\theta_\mu\alpha_\mu) = M_\mu$. Assim, o conjunto dos homomorfismos $\theta_\lambda\alpha_\lambda$ (do grupo 2-gerado H no grupo enumerável G_M) é não enumerável o que é um absurdo. ■

Teorema 1.2.7 (P. Hall) *Sejam G um grupo finitamente gerado, $N \lhd G$ e suponha que G/N é finitamente apresentado. Então N é o fecho normal em G de um subconjunto finito.*

Demonstração: Sejam $\theta : F \longrightarrow G$ uma apresentação de G, onde F é um grupo livre de posto finito, e S a pré-imagem de N com respeito a θ, isto é, $S = \theta^{-1}(N)$. Então $S \rightarrowtail F \twoheadrightarrow G/N$ é uma apresentação para o grupo finitamente gerado G/N. Portanto, pelo Teorema 1.2.3, S é o fecho normal em F de algum subconjunto finito. Consequentemente, $N = \theta(S)$ é o fecho normal em G de algum subconjunto finito, como queríamos. ■

Vamos conectar agora os Teoremas 1.2.6 e 1.2.7 para mostrar um conhecido exemplo que encerrará nossa discussão sobre grupos finitamente gerados e grupos finitamente apresentados.

Teorema 1.2.8 *O produto entrelaçado de dois grupos cíclicos infinitos $\mathbb{Z} \wr \mathbb{Z}$ é um grupo metabeliano 2-gerado que não é finitamente apresentado.*

Demonstração: Seja H o grupo construído durante a prova do Teorema 1.2.6, para o qual tínhamos $H/X' \cong \mathbb{Z} \wr \mathbb{Z}$. Se este grupo fosse finitamente apresentado, pelo Teorema 1.2.7 teríamos X' finitamente gerado pois $X' = Z(H)$, e portanto

$$X'^H = X',$$

isto é, o conceito de ser gerado como subgrupo normal e de ser gerado como subgrupo coincidem. Todavia, isto é um absurdo. ■

Para uma leitura complementar, indicamos consultar a referência De Cornulier [1], na qual o autor estabelece condições necessárias e suficientes para que o produto entrelaçado de dois grupos seja finitamente apresentável.

1.2.3 A Deficiência de um Grupo

Seja G um grupo finitamente apresentado e suponha que exista uma apresentação de G com n geradores e r relações. O inteiro $n - r$ é chamado de *deficiência da apresentação*. Neste contexto, sabemos que é possível introduzir novas relações em G como consequências das anteriores. Com isso, obtemos novas apresentações com deficiências menores do que as antecedentes. Com este espírito, surge a ideia de investigarmos apresentações com deficiência tão grande quanto possível. Definimos então a *deficiência de um grupo* G, denotada por

$$def(G)$$

como sendo o máximo entre as deficiências das apresentações finitas.

Mostraremos adiante que é possível determinar um limitante superior para a deficiência de um grupo. Para tanto, utilizaremos o *multiplicador de Schur* de G, denotado por $M(G)$, e definido por

$$M(G) = \frac{R \cap F'}{[F, R]}$$

onde F é livre e $F/R \cong G$. O multiplicador de Schur depende apenas de G, e não da escolha de F e R (Robinson [9], Teorema 11.4.15). Observe que se G e H são grupos isomorfos, então indubitavelmente eles têm a mesma apresentação. Por esta razão, devemos ter $M(G) = M(H)$, isto é, o multiplicador de Schur é invariante por isomorfismos.

Vamos destacar agora duas definições que serão fortemente úteis durante esta seção.

Por uma *sequência exata* de grupos entende-se uma sequência de grupos e homomorfismos de grupos

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} G_n$$

tais que $Im\varphi_i = ker\varphi_{i+1}$ para todo i.

Com respeito a esta notação, vamos ressaltar os seguintes pontos. Quando φ_1 for injetiva, poderemos escrever a sequência como

$$1 \longrightarrow G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} G_n$$

e quando φ_n for sobrejetiva, poderemos escrever a sequência como

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} G_n \longrightarrow 1.$$

Ademais, se E é uma extensão de G por N, então indicaremos por $N \rightarrowtail E \twoheadrightarrow G$ como já feito anteriormente. Neste caso, por simplicidade, fixaremos sem perda de generalidade a imersão $N \rightarrowtail E$ como sendo a inclusão.

Por um *morfismo* entre sequências exatas, entende-se um conjunto de homomorfismos $(\theta_1, \theta_2, \ldots, \theta_n)$ definidos de modo que o seguinte diagrama comuta.

$$\begin{array}{ccccccc}
G_1 & \xrightarrow{\varphi_1} & G_2 & \xrightarrow{\varphi_2} & \cdots & \xrightarrow{\varphi_{n-1}} & G_n \\
\downarrow{\scriptstyle \theta_1} & & \downarrow{\scriptstyle \theta_2} & & & & \downarrow{\scriptstyle \theta_n} \\
\overline{G_1} & \xrightarrow{\overline{\varphi_1}} & \overline{G_2} & \xrightarrow{\overline{\varphi_2}} & \cdots & \xrightarrow{\overline{\varphi_{n-1}}} & \overline{G_n}
\end{array}$$

Limitando a Deficiência de um Grupo

Lema 1.2.9 *Seja G um grupo finitamente apresentado, digamos $(x_1, x_2, \ldots, x_n \mid y_1, y_2, \ldots, y_r)$. Vamos considerar $G \cong F/R$, onde F é livre sobre $\{x_1, x_2, \ldots, x_n\}$ e R é o subgrupo normal de F gerado por $\{y_1, y_2, \ldots y_r\}$. Então $R/[F,R]$ é um grupo abeliano finitamente gerado e $d(R/[F,R]) \leqslant r$.*

Demonstração: Como $R \lhd F$, observe que $[F,R]$ é um subgrupo normal de R contendo $[R,R] = R'$. Portanto, $R/[F,R]$ é um grupo abeliano. É suficiente mostrar que $R/[F,R]$ pode ser gerado pelas classes dos y_i's. Todo elemento de R é um produto de elementos da forma fsf^{-1}, onde s pertence ao subgrupo gerado pelos y_i's. Mas $fsf^{-1}s^{-1} \in [F,R]$, e assim $fsf^{-1} \equiv s \; mod [F,R]$. ∎

Usaremos a notação G_{ab} para indicar o quociente G/G'.

Teorema 1.2.10 *Seja G um grupo finitamente apresentado, digamos $(x_1, x_2, \ldots, x_n \mid y_1, y_2, \ldots, y_r)$. Então*

$$n - r \leqslant \rho(G_{ab}) - d(M(G)).$$

Demonstração: Seja F um grupo livre sobre $\{x_1, x_2, \ldots, x_n\}$ e R o seu subgrupo normal gerado por $\{y_1, y_2, \ldots, y_r\}$. Temos a seguinte cadeia de subgrupos normais de F

$$[F, R] \lhd R \cap F' \lhd R \lhd F'R \lhd F.$$

Pelo Lema 1.2.9, $R/[F, R]$ é um grupo abeliano finitamente gerado com, no máximo, r geradores. Existe uma sequência exata de grupos abelianos

$$0 \longrightarrow (R \cap F')/[F, R] \longrightarrow R/[F, R] \longrightarrow R/R \cap F' \longrightarrow 0.$$

Logo, $d(M(G)) = d((R \cap F')/[F, R]) \leqslant r$. Uma vez que $R/R \cap F' \cong F'R/F' \subset F_{ab}$, então o grupo $R/R \cap F'$ é abeliano livre pois F_{ab} é abeliano livre (Proposição 1.1.8). Daí,

$$\frac{R}{R \cap F'} \cong \frac{R/[R, F]}{R \cap F'/[R, F]} = \frac{R/[R, F]}{M(G)}$$

é abeliano livre e $M(G)$ é um somando direto de $R/[R, F]$ (Teorema 1.1.10), isto é, $R/[R, F] \cong M(G) \oplus (R/R \cap F')$. Pela Observação 1.1.14, vem

$$d(R/[R, F]) = d(M(G)) + d(R/R \cap F').$$

Considerando agora a seguinte sequência exata

$$0 \longrightarrow F'R/F' \longrightarrow F_{ab} \longrightarrow F/F'R \longrightarrow 0,$$

a Observação 1.1.15 esclarece que $\rho(F_{ab}) = \rho(F'R/F') + \rho(F/F'R)$. Recordando agora que F_{ab} e seu subgrupo $F'R/F'$ são abelianos livres e pela Observação 1.1.13 temos

$$d(F'R/F') = d(F_{ab}) - \rho(F/F'R) = n - \rho(F/F'R).$$

Concluímos assim a desigualdade

$$r \geqslant d(R/[F, R]) = n - \rho(F/F'R) + d(M(G)).$$

Note que $G_{ab} \cong F/F'R$. ∎

Teorema de Magnus - Um Caso Especial

O objetivo desta seção é apresentar um fecundo teorema creditado a Magnus, o qual tem forte interseção com o Caso Abstrato do Teorena Principal. De modo breve, lembre que este atesta sobre a existência de um subgrupo livre em um grupo finitamente apresentado com mais geradores do que relações, dado qualquer conjunto de geradores, e cujo posto coincide com a deficiência da apresentação.

Na verdade, sob certo ponto de vista, este Teorema de Magnus (Teorema 1.2.13) trata-se de um caso especial, onde fixamos o conjunto de geradores e usamos mão da comutatividade, como veremos a seguir.

Antes disso, vamos mostrar que podemos relacionar qualquer extensão de grupos com uma determinada sequência exata, conhecida na literatura como *Sequência de Homologia Cinco Termos*. Ratificamos que esta importante ferramenta, que surgiu no contexto da Cohomologia, será decisiva na demonstração do Teorema de Magnus adiante.

Teorema 1.2.11 (Sequência de Homologia Cinco Termos) *Dada uma extensão de grupos $N \rightarrowtail E \twoheadrightarrow G$, existe uma sequência exata*

$$M(E) \longrightarrow M(G) \longrightarrow N/[E,N] \longrightarrow E_{ab} \longrightarrow G_{ab} \longrightarrow 1.$$

Esta sequência é natural no seguinte sentido: dado um morfismo (α, β, γ) de $N \rightarrowtail E \twoheadrightarrow G$ em $\overline{N} \rightarrowtail \overline{E} \twoheadrightarrow \overline{G}$, existem homomorfismos induzidos $(\alpha_*, \beta_*, \gamma_*)$ fazendo o seguinte diagrama comutar.

$$\begin{array}{ccccccccc}
M(E) & \longrightarrow & M(G) & \longrightarrow & N/[E,N] & \longrightarrow & E_{ab} & \longrightarrow & G_{ab} & \longrightarrow & 1 \\
\downarrow{\scriptstyle \beta_*} & & \downarrow{\scriptstyle \gamma_*} & & \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \beta_*} & & \downarrow{\scriptstyle \gamma_*} & & \\
M(\overline{E}) & \longrightarrow & M(\overline{G}) & \longrightarrow & \overline{N}/[\overline{E},\overline{N}] & \longrightarrow & \overline{E}_{ab} & \longrightarrow & \overline{G}_{ab} & \longrightarrow & 1
\end{array}$$

Demonstração: Dada a extensão

$$1 \longrightarrow N \longrightarrow E \xrightarrow{\varepsilon} G \longrightarrow 1$$

vamos verificar a existência da sequência exata abaixo.

$$M(E) \xrightarrow{\xi_4} M(G) \xrightarrow{\xi_3} N/[E,N] \xrightarrow{\xi_2} E_{ab} \xrightarrow{\xi_1} G_{ab} \longrightarrow 1.$$

As aplicações

$$\begin{array}{rccc} \xi_2: & N/[E,N] & \longrightarrow & E_{ab} \\ & x[E,N] & \longmapsto & xE' \end{array} \quad \text{e} \quad \begin{array}{rccc} \xi_1: & E_{ab} & \longrightarrow & G_{ab} \\ & xE' & \longmapsto & \varepsilon(x)G' \end{array}$$

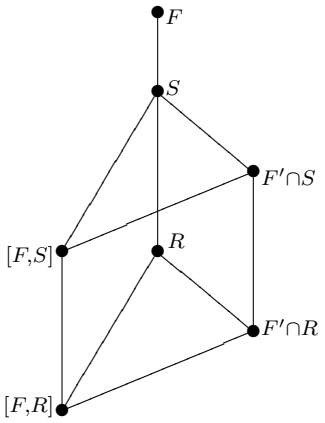
são definidas de modo natural e são tais que $Im\xi_2 = NE'/E' = Ker\xi_1$. Assim, a sequência é exata em E_{ab}. Ademais, como ε é sobrejetiva, segue que ξ_2 também é sobrejetiva, e portanto a sequência é exata em G_{ab}.

Agora, nossa meta será construir as aplicações ξ_3 e ξ_4.

Seja $\pi : F \longrightarrow E$ uma apresentação de E com núcleo R. Então a composição $\varepsilon\pi : F \longrightarrow G$ é uma apresentação de G. Denotando $ker\varepsilon\pi = S$, temos

$$M(E) \cong F' \cap R/[F,R] \quad \text{e} \quad M(G) \cong F' \cap S/[F,S].$$

Além disso, $\pi(S) = N$. Logo, $R \leq S$ e $S/R \cong N$. Note que os subgrupos em destaque constituem o seguinte reticulado.



Definindo

$$\begin{array}{rccc} \xi_3: & M(G) & \longrightarrow & N/[E,N] \\ & x[F,S] & \longmapsto & \pi(x)[E,N] \end{array}$$

verifica-se que $Im\xi_3 = E' \cap N/[E,N] = ker\xi_2$, estabelecendo assim a exatidão em $N/[E,N]$.

Finalmente, considerando $\xi_4 : M(E) \longrightarrow M(G)$ como o homomorfismo natural, temos $Im\xi_4 = (F' \cap R)[F,S]/[F,S] = ker\xi_3$, donde concluímos que a sequência é exata em $M(G)$, como queríamos.

Vamos estabelecer agora sua naturalidade.

Seja (α, β, γ) um morfismo de $N \rightarrowtail E \twoheadrightarrow G$ em $\overline{N} \rightarrowtail \overline{E} \twoheadrightarrow \overline{G}$. Nosso objetivo é construir aplicações convenientes entre as sequências de homologia

cinco termos dessas extensões de modo que o diagrama resultante comute. Para tanto, vamos considerar inicialmente $\pi : F \longrightarrow E$ e $\overline{\pi} : \overline{F} \longrightarrow \overline{E}$ apresentações de E e $\overline{E}$ com núcleos R e $\overline{R}$, respectivamente. Segue então o seguinte diagrama.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R & \longrightarrow & F & \xrightarrow{\pi} & E & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \overline{\beta}} & & \downarrow{\scriptstyle \beta} & & \\ 1 & \longrightarrow & \overline{R} & \longrightarrow & \overline{F} & \xrightarrow{\overline{\pi}} & \overline{E} & \longrightarrow & 1 \end{array}$$

Dado $x \in F$, podemos encontrar $y_x \in \overline{F}$ tal que $\beta\pi(x) = \overline{\pi}(y_x)$. Assim, vamos induzir um homomorfismo $\overline{\beta} : F \longrightarrow \overline{F}$ por meio da relação $\overline{\beta}(x) = y_x$. Neste caso, temos que $\overline{\beta}(R) \leqslant \overline{R}$, e assim podemos definir

$$\begin{array}{rccc} \beta_* : & M(E) & \longrightarrow & M(\overline{E}) \\ & x[F,R] & \longmapsto & y_x[\overline{F},\overline{R}]. \end{array}$$

De modo análogo, como $\varepsilon : E \longrightarrow G$ e $\overline{\varepsilon} : \overline{E} \longrightarrow \overline{G}$ são sobrejeções, então $\varepsilon\pi : F \longrightarrow E$ e $\overline{\varepsilon\pi} : \overline{F} \longrightarrow \overline{E}$ são apresentações de G e $\overline{G}$ com núcleos S e $\overline{S}$, respectivamente. Segue então o seguinte diagrama:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & S & \longrightarrow & F & \xrightarrow{\varepsilon\pi} & G & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \overline{\gamma}} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & \overline{S} & \longrightarrow & \overline{F} & \xrightarrow{\overline{\varepsilon\pi}} & \overline{G} & \longrightarrow & 1 \end{array}$$

Dado $x \in F$, podemos encontrar $z_x \in \overline{F}$ tal que $\gamma\varepsilon\pi(x) = \varepsilon\overline{\pi}(z_x)$. Assim, vamos induzir um homomorfismo $\overline{\gamma} : F \longrightarrow \overline{F}$ por meio da relação $\overline{\gamma}(x) = z_x$. Neste caso, temos que $\overline{\gamma}(S) \leqslant \overline{S}$, e assim podemos definir

$$\begin{array}{rccc} \gamma_* : & M(G) & \longrightarrow & M(\overline{G}) \\ & x[F,R] & \longmapsto & z_x[\overline{F},\overline{S}]. \end{array}$$

Ademais, como foi estabelecido que a aplicação injetiva $\overline{N} \rightarrowtail \overline{E}$ é a inclusão, observe que α torna-se a restrição de β a N. Portanto, definimos simplesmente

$$\begin{array}{rccc} \alpha_*: & N/[E,N] & \longrightarrow & \overline{N}/[\overline{E},\overline{N}] \\ & x[E,N] & \longmapsto & \alpha(x)[\overline{E},\overline{N}], \end{array} \qquad \begin{array}{rccc} \beta_*: & E_{ab} & \longrightarrow & \overline{E}_{ab} \\ & xE' & \longmapsto & \beta(x)E' \end{array}$$

e por fim

$$\begin{array}{rccc} \gamma_*: & G_{ab} & \longrightarrow & \overline{G}_{ab} \\ & x[E,N] & \longmapsto & \gamma(x)G'. \end{array}$$

A comutatividade do diagrama decorre da maneira como estas funções foram definidas pois a terna (α, β, γ) é um morfismo. ∎

Lema 1.2.12 *Seja $(\theta_1, \theta_2, \theta_3)$ um morfismo entre as sequências exatas abaixo.*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_1 & \xrightarrow{\alpha} & G_2 & \xrightarrow{\beta} & G_3 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \theta_1} & & \downarrow{\scriptstyle \theta_2} & & \downarrow{\scriptstyle \theta_3} & & \\ 1 & \longrightarrow & H_1 & \xrightarrow[\alpha']{} & H_2 & \xrightarrow[\beta']{} & H_3 & \longrightarrow & 1 \end{array}$$

Se θ_1 e θ_3 são isomorfismos, então θ_2 também é um isomorfismo.

Demonstração: Primeiramente, vamos mostrar a injetividade. Se $x \in \ker\theta_2$ então $1 = \beta'(\theta_2(x)) = \theta_3(\beta(x))$, e assim $\beta(x) = 1$ pois o diagrama é comutativo e θ_3 é isomorfismo. Logo, $x \in \ker\beta = Im\alpha$, e então $x = \alpha(y)$ para algum $y \in G_1$. Logo, $1 = \theta_2(x) = \theta_2(\alpha(y)) = \alpha'(\theta_1(y))$, donde $\theta_1(y) = 1$ pois a sequência é exata. Logo, $y = 1$ pois θ_1 também é isomorfismo, e portanto $x = 1$.

Agora a sobrejetividade. Seja $a \in H_2$. Então $\beta'(a) = \theta_3(b)$ para algum $b \in G_3$, pois θ_3 é isomorfismo. Assim, $\beta'(a) = \theta_3(\beta(c))$, para algum $c \in G_2$ pois a sequência é exata. Portanto, $\beta'(a) = \beta'(\theta_2(c))$ e assim $a \equiv \theta_2(c)$ $\mathrm{mod}(ker\beta' = Im\alpha')$. Neste caso, $a = \theta(c)\alpha'(d)$, para algum $d \in H_1$. Por sua vez, $d = \theta_1(e)$ para algum $e \in G_1$, pois θ_1 é isomorfismo. Logo,

$$a = \theta_2(c)\alpha'(d) = \theta_2(c)\alpha'(\theta_1(e)) = \theta_2(c)\theta_2(\alpha(e)),$$

isto é, $a = \theta_2(c\alpha(e))$. ∎

Citamos agora um fato amplamente conhecido sobre a série central inferior de um grupo livre que será introduzido na demonstração do Teorema de Magnus sem maiores comentários: *se F é um grupo livre, então a interseção de todos os termos da série central inferior de F é trivial.*

Teorema 1.2.13 (Magnus) *Seja G um grupo tendo uma apresentação finita com $n+r$ geradores e r relações. Se G_{ab} pode ser gerado por n elementos*

$$x_1G', x_2G', \ldots, x_nG'$$

então $x_1, x_2, \ldots, x_n$ geram um subgrupo livre de posto n e eles formam um conjunto de geradores livres.

Demonstração: Pelo Teorema 1.2.10, temos as seguintes desigualdades

$$n = n + r - r \leqslant def(G) \leqslant \rho(G_{ab}) - d(M(G)) \leqslant n - d(M(G)).$$

Assim, $d(M(G)) = 0$ e $\rho_0(G_{ab}) = n$. Portanto, $M(G) = 0$ e G_{ab} é grupo abeliano finitamente gerado e livre de torção, uma vez que

$$\rho(G_{ab}) = n \leqslant d(G_{ab}) \leqslant n \quad \text{implica} \quad \rho(G_{ab}) = d(G_{ab}) = n.$$

Então G_{ab} abeliano livre de posto n.

Sejam agora F um grupo livre sobre $\{y_1, y_2, \ldots, y_n\}$ e $\theta : F \longrightarrow G$ o homomorfismo definido por $\theta(y_i) = x_i$. Assim, é suficiente mostrar que θ é injetiva.

Como os elementos x_iG' geram G_{ab}, então θ induz um isomorfismo de F_{ab} em G_{ab}. Denotando agora os seguintes quocientes

$$F_i = \frac{F}{\gamma_{i+1}F} \quad \text{e} \quad G_i = \frac{G}{\gamma_{i+1}G},$$

vamos supor, por hipótese de indução, que θ determina um isomorfismo de F_i em G_i (para $i = 1$ recaímos no caso comentado acima). Considere o diagrama comutativo abaixo.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \gamma_{i+1}F & \longrightarrow & F & \longrightarrow & F_i & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \\
1 & \longrightarrow & \gamma_{i+1}G & \longrightarrow & G & \longrightarrow & G_i & \longrightarrow & 1
\end{array}$$

Aqui, as aplicações para baixo à esquerda e à direita são induzidas por θ (e serão igualmente denotadas por θ, por simplicidade). Aplicando agora a

sequência de homologia cinco termos (Teorema 1.2.11), obtemos o correspondente diagrama comutativo abaixo:

$$\begin{array}{ccccccccc}
1 = M(F) & \longrightarrow & M(F_i) & \xrightarrow{\alpha} & \frac{\gamma_{i+1}F}{\gamma_{i+2}F} & \xrightarrow{\beta} & F_{ab} & \xrightarrow{\gamma} & (F_i)_{ab} \longrightarrow 1 \\
\downarrow{\scriptstyle \theta_*} & & \downarrow{\scriptstyle \theta_*} & & \downarrow{\scriptstyle \theta_*} & & \downarrow{\scriptstyle \theta_*} & & \downarrow{\scriptstyle \theta_*} \\
1 = M(G) & \longrightarrow & M(G_i) & \xrightarrow{\alpha'} & \frac{\gamma_{i+1}G}{\gamma_{i+2}G} & \xrightarrow{\beta'} & G_{ab} & \xrightarrow{\gamma'} & (G_i)_{ab} \longrightarrow 1
\end{array}$$

Temos que $M(F) = 1$, pois F é livre. Como $\theta : F_i \longrightarrow G_i$ é isomorfismo, podemos induzir um isomorfismo $\theta_* : M(F_i) \longrightarrow M(G_i)$. Observe também que $\theta_* : (F_i)_{ab} \longrightarrow (G_i)_{ab}$ é isomorfismo.

Pelo Lema 1.2.12, deduzimos que $\theta : \gamma_{i+1}F/\gamma_{i+2}F \longrightarrow \gamma_{i+1}G/\gamma_{i+2}G$ é isomorfismo. Neste caso, considerando o diagrama comutativo:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \frac{\gamma_{i+1}F}{\gamma_{i+2}F} & \longrightarrow & \frac{F}{\gamma_{i+2}F} & \longrightarrow & \frac{F}{\gamma_{i+1}F} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \theta_*} & & \vdots{\scriptstyle \theta_*} & & \downarrow{\scriptstyle \theta_*} & & \\
1 & \longrightarrow & \frac{\gamma_{i+1}G}{\gamma_{i+2}} & \longrightarrow & \frac{G}{\gamma_{i+2}} & \longrightarrow & \frac{G}{\gamma_{i+1}G} & \longrightarrow & 1
\end{array}$$

o Lema 1.2.12 nos esclarece novamente que $\theta_* : F_{i+1} \longrightarrow G_{i+1}$ é bijetiva.

Segue por indução em i que $\theta_* : F_{i+1} \longrightarrow G_{i+1}$ é isomorfismo, como queríamos. Observe agora que $ker\theta \leqslant \gamma_{i+1}F$ para todo i, donde $\ker\theta \leqslant \bigcap_{i\in\mathbb{N}} \gamma_{i+1}F$, e assim $ker\theta = 1$ e $\theta : F \longrightarrow G$ é injetiva, como queríamos. ∎

Corolário 1.2.14 *Seja G um grupo que admite uma apresentação finita com $n + r$ geradores e r relações. Se G pode ser gerado com n elementos, então G é um grupo livre de posto n.*

O Corolário anterior indica que é plausível imaginar que as relações do grupo podem ser usadas para eliminar r dos seus $n + r$ geradores, e que os n geradores restantes não estão sujeitos a quaisquer relações.

Capítulo 2

O Teorema Principal - Caso Abstrato

Neste capítulo, apresentamos a demonstração do Teorema Principal (Caso Abstrato) dada por John S. Wilson em [15].

Teorema Principal (Caso Abstrato) Seja G um grupo que tem uma apresentação com n geradores $x_1, x_2, \ldots, x_n$ e m relações $r_1, r_2, \ldots, r_m$, onde $n > m$, e seja Y um conjunto qualquer de geradores de G. Então existem $n - m$ elementos de Y que geram livremente um subgrupo livre de G.

A demonstração tem como pilares a imersão de Magnus, que é uma aplicação injetiva de um determinado quociente de um grupo livre em uma extensão split, e a imersão de anéis de grupos ordenáveis em anéis com divisão (à direita).

2.1 A Imersão de Magnus e Derivações

Seja H um grupo, M um $\mathbb{Z}H$-módulo (à direita) e considere a extensão split $G = H \ltimes M$. Por refinamento estético, vamos introduzir uma notação matricial clássica para a extensão split G dada por $\begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix}$. Observe que a matriz multiplicação

$$\begin{pmatrix} h_1 & 0 \\ m_1 & 1 \end{pmatrix} \begin{pmatrix} h_2 & 0 \\ m_2 & 1 \end{pmatrix} = \begin{pmatrix} h_1 h_2 & 0 \\ m_1 h_2 + m_2 & 1 \end{pmatrix}$$

reflete de modo conveniente o fato de que $(h_1m_1)(h_2m_2) = (h_1h_2)(m_1^{h_2}m_2)$ em G. Neste contexto, podemos considerar também M como sendo um $\mathbb{Z}G$-módulo, onde a ação de G em M é dada por $m_1^{hm} = m_1^h$, onde $hm \in G = H \ltimes M$ e $m_1 \in M$.

De forma geral, uma *derivação* de G em M é qualquer aplicação $d : G \longrightarrow M$ tal que

$$d(xy) = d(x)y + d(y),$$

onde a adição denota a operação de M, e o produto $d(x)y$ denota a ação de y em $d(x)$.

Observe que a aplicação δ que leva $g \in G$ na sua componente em M é então uma derivação de G em M. De fato, dados

$$g_1 = \begin{pmatrix} h_1 & 0 \\ m_1 & 1 \end{pmatrix} \qquad \text{e} \qquad g_2 = \begin{pmatrix} h_2 & 0 \\ m_2 & 1 \end{pmatrix}$$

temos

$$g_1g_2 = \begin{pmatrix} h_1h_2 & 0 \\ m_1h_2 + m_2 & 1 \end{pmatrix}.$$

Portanto, $\delta(g_1g_2) = m_1h_2 + m_2$. Além disso, temos de modo claro $\delta(g_1) = m_1$ e $\delta(g_2) = m_2$. Observe também que (utilizando a notação clássica)

$$m_1^{g_2} = m_1^{h_2m_2} = m_1^{h_2}$$

pois M é abeliano (como grupo aditivo), e assim m_2 age em m_1 de modo trivial. Logo, $\delta(g_1g_2) = \delta(g_1)g_2 + \delta(g_2)$, e portanto δ é um derivação, como foi afirmado.

Vamos introduzir no lema a seguir uma propriedade importante das derivações.

Lema 2.1.1 *Seja $\delta : H \longrightarrow W$ uma derivação de um grupo H em um $\mathbb{Z}H$-módulo W. Se $H = \langle Z \rangle$ então o subconjunto δH está contido no $\mathbb{Z}H$-submódulo W_1 gerado por δZ.*

Demonstração: Note que $\delta(1) = \delta(1)1 + \delta(1) = 2\delta(1)$, e assim $\delta 1 = 0$. Daí, $1 = \delta(hh^{-1}) = \delta(h)h^{-1} + \delta h^{-1}$, e portanto $\delta(h^{-1}) = -(\delta(h))h^{-1}$. Neste caso, para $h_1, h_2 \in Z$, vem $\delta(h_1h_2^{-1}) = \delta(h_1)h_2^{-1} + \delta(h_2^{-1}) = \delta(h_1)h_2^{-1} - \delta(h_2)h_2^{-1} \in W_1$. Generalizando esta ideia, temos que se $h = h_1^{\epsilon_1}h_2^{\epsilon_2}\ldots h_n^{\epsilon_n} \in H$, com

$h_i \in Z, \epsilon_i = \pm 1$, e $i = 1, 2, \ldots, n$, a sua imagem com respeito a δ é uma H-combinação linear de $\delta h_1, \delta h_2, \ldots \delta h_n$, e que pertence a W_1. ∎

A *imersão de Magnus* para grupos abstratos é o homomorfismo j de F/R' em $H \ltimes M$ dado pelo lema a seguir.

Lema 2.1.2 *Sejam F um grupo livre sobre $\{x_1, x_2, \ldots, x_n\}$, R um subgrupo normal de F e $H = F/R$. Seja M um $\mathbb{Z}H$-módulo e $t_1, t_2, \ldots, t_n \in M$.*

(a) A correspondência

$$x_i \longmapsto \begin{pmatrix} x_i R & 0 \\ t_i & 1 \end{pmatrix}$$

determina um homomorfismo

$$\mu : F \longrightarrow \begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix}.$$

(b) $R' \leqslant ker\mu \leqslant R$.

(c) Seja j a aplicação de F/R' em $\begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix}$ induzida por μ. Se M é o $\mathbb{Z}H$-módulo livre sobre $\{t_1, t_2, \ldots, t_n\}$, então j é injetiva.

Demonstração: O ítem (a) é claro, pois F é livre sobre $\{x_1, x_2, \ldots, x_n\}$. Também é claro que $ker\mu \leqslant R$ pois

$$\mu(f) = \begin{pmatrix} fR & 0 \\ \delta(f) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

implica em especial $f \in R$. Além disso, a imagem de R com respeito a μ é abeliana. De fato, sejam $r_1, r_2 \in R$, e sejam

$$\mu(r_1) = \begin{pmatrix} 1 & 0 \\ m_1 & 1 \end{pmatrix} \quad \text{e} \quad \mu(r_2) = \begin{pmatrix} 1 & 0 \\ m_2 & 1 \end{pmatrix}.$$

Então

$$\begin{aligned}
\mu(r_1)\mu(r_2) &= \begin{pmatrix} 1 & 0 \\ m_1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ m_2 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ m_1 1 + m_2 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ m_1 + m_2 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ m_2 + m_1 & 1 \end{pmatrix} \\
&= \mu(r_2)\mu(r_1).
\end{aligned}$$

Portanto temos $R' \leqslant Ker\mu$, o que completa a prova do item (b).

Nota A prova do item (c) a seguir é apresentada no artigo de John S. Wilson [15] onde ele cita Romanovskii como autor.

Para verificarmos o item (c), vamos primeiro construir uma imersão θ de F/R' em um grupo da forma $\begin{pmatrix} H & 0 \\ N & 1 \end{pmatrix}$. Para isso, considere o grupo abeliano N constituído de todas as funções $b : H \longrightarrow R/R'$ (com respeito a operação ponto a ponto).

Afirmação 1 Dada a correspondência

$$\begin{array}{ccc} N \times H & \longrightarrow & N \\ (b, h) & \longmapsto & bh \end{array}$$

definida por $(bh)(x) = b(xh^{-1})$ para todo $x \in H$, temos que N é um $\mathbb{Z}H$-módulo.

Temos que $(b1)(x) = b(x1) = b(x)$ para todo $b \in N$ e $x \in H$, e $b(h_1h_2)(x) = b(xh_2^{-1}h_1^{-1}) = (bh_1)(xh_2^{-1}) = (bh_1)(h_2)(x)$ para todo $b \in N$ e quaisquer $h_1, h_2, x \in H$. Logo, a correspondência definida acima é uma ação (à direita) de H em N, e assim podemos considerar a extensão split $H \ltimes N$, a qual induz em N a estrutura de $\mathbb{Z}H$-módulo.

Neste contexto, note também que a ação de H em N induz uma ação

$$\begin{array}{ccc} N \times F/R' & \longrightarrow & N \\ (b, g) & \longmapsto & b^g \end{array}$$

onde $b^g(x) = (bq(g))(x)$, para todo $x \in H$, e $q : F/R' \longrightarrow H$ é o epimorfismo $fR' \longmapsto fR$.

Agora, para construir a imersão $\theta : F/R' \longrightarrow H \ltimes N$ considere uma função $\sigma : F/R \longrightarrow F/R'$ cuja composta com $q : F/R' \longrightarrow F/R$ é a aplicação identidade de F/R. Para cada $fR' \in F/R'$, defina $\delta(fR') \in N$ por

$$(\delta(fR'))(uR) = \sigma(uf^{-1}R) \cdot fR' \cdot (\sigma(uR))^{-1}$$

para todo $uR \in H$.

Afirmação 2 Temos $\delta(\overline{f_1 f_2}) = (\delta\overline{f_1})^{\overline{f_2}}(\delta\overline{f_2})$ para quaisquer $\overline{f_1}, \overline{f_2} \in F/R'$. Além disso, se $\overline{f} \in R/R'$ é tal que $\delta\overline{f}$ é o elemento identidade de N, então $\overline{f}$ é o elemento identidade de R/R'.

Com efeito,

$$(\delta\overline{f_1})^{\overline{f_2}}(uR) = (\delta\overline{f_1})(uf_2^{-1}R) = \sigma(u(f_1 f_2)^{-1}R) \cdot f_1 R' \cdot (\sigma(uf_2^{-1}R))^{-1}$$

e também

$$(\delta(f_2 R'))(uR) = \sigma(uf_2^{-1}R) \cdot f_2 R' \cdot (\sigma(uR))^{-1}.$$

Portanto

$$(\delta\overline{f_1})^{\overline{f_2}}(\delta\overline{f_2})(uR) = \sigma(u(f_1 f_2)^{-1}R) \cdot f_1 f_2 R' \cdot (\sigma(uR))^{-1} = \delta(\overline{f_1 f_2})(uR)$$

para todo $uR \in F/R$. Além disso, se $\delta\overline{f}$ é o elemento identidade de N, com $\overline{f} \in R/R'$, então $(\delta\overline{f}\delta\overline{f_1})(uR) = \delta\overline{f_1}(uR)$ para todo $uR \in F/R$. Logo, $\delta\overline{f}(uR) = R'$, isto é,

$$R' = \sigma(uf^{-1}R) \cdot fR' \cdot (\sigma(uR))^{-1} = \sigma(uR) \cdot fR' \cdot (\sigma(uR))^{-1} = fR'$$

donde concluímos que $\overline{f}$ é o elemento identidade em R/R', como queríamos.

Defina

$$\theta : F/R' \longrightarrow \begin{pmatrix} H & 0 \\ N & 1 \end{pmatrix} \quad \text{por} \quad \theta(fR') = \begin{pmatrix} fR & 0 \\ \delta(fR') & 1 \end{pmatrix}.$$

Da Afirmação 2, tem-se

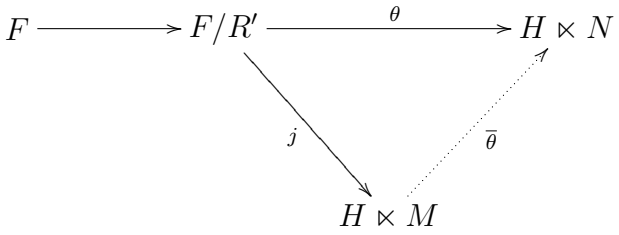
$$\begin{aligned}
\theta(\overline{f_1 f_2}) &= \begin{pmatrix} f_1 f_2 R & 0 \\ \delta(\overline{f_1 f_2}) & 1 \end{pmatrix} \\
&= \begin{pmatrix} f_1 f_2 R & 0 \\ (\delta\overline{f_1})^{\overline{f_2}}(\delta\overline{f_2}) & 1 \end{pmatrix} \\
&= \begin{pmatrix} f_1 R & 0 \\ \delta(\overline{f_1}) & 1 \end{pmatrix}\begin{pmatrix} f_2 R & 0 \\ \delta(\overline{f_2}) & 1 \end{pmatrix} \\
&= \theta(\overline{f_1})\theta(\overline{f_2}),
\end{aligned}$$

para quaisquer $f_1, f_2 \in F$, e portanto θ é homomorfismo. Além disso, se

$$\theta(fR') = \begin{pmatrix} fR & 0 \\ \delta(fR') & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

então $f \in R$ e $\delta(fR') = 1$, e assim pela Afirmação 2 tem-se $f \in R'$. Portanto, θ é um homomorfismo injetivo, como queríamos.

Finalmente, para provar (c), vamos mostrar que o diagrama



pode ser completado com uma aplicação $\overline{\theta}$ de tal forma que $\overline{\theta} j = \theta$. Como θ é injetiva, segue que j também é injetiva, o que completa a prova do item (c).

Defina $v_i \in N$ por

$$\theta(x_i R') = \begin{pmatrix} x_i R & 0 \\ v_i & 1 \end{pmatrix}.$$

Como M é $\mathbb{Z}H$-módulo livre com base $t_1, t_2, \ldots, t_n$, seja $\kappa : M \longrightarrow N$ o único $\mathbb{Z}H$-homomorfismo definido pela correspondência $t_i \longmapsto v_i$. Então $\overline{\theta}$ dada por

$$\begin{pmatrix} h & 0 \\ m & 1 \end{pmatrix} \longmapsto \begin{pmatrix} h & 0 \\ \kappa(m) & 1 \end{pmatrix}$$

possui a propriedade que desejamos. De fato, dado $x_iR' \in F/R$, temos

$$j(x_iR') = \begin{pmatrix} x_iR & 0 \\ t_i & 1 \end{pmatrix}.$$

Portanto,

$$\overline{\theta}j(x_iR') = \begin{pmatrix} x_iR & 0 \\ \kappa(t_i) & 1 \end{pmatrix} = \begin{pmatrix} x_iR & 0 \\ v_i & 1 \end{pmatrix} = \theta(x_iR'),$$

donde concluímos $\overline{\theta}j = \theta$. ∎

A existência da aplicação $\theta : F/R' \longrightarrow \begin{pmatrix} H & 0 \\ N & 1 \end{pmatrix}$ vista na demonstração do item (c) segue também do Teorema de Kaloujnine-Krasner (consultar [4]), onde determina-se que a extensão split $H \ltimes N$ é o produto entrelaçado $R/R' \wr F/R$, isto é, o produto semidireto $F/R \ltimes B$, onde B é o produto de $\mid F/R \mid$ cópias de R/R' (e que também pode ser deduzida de Wilson [13], Teorema 4.4.1).

2.2 Imersão de Anéis de Grupos em Anéis com Divisão

Um grupo G é dito *ordenável* se ele tem uma ordem total $\leqslant$ tal que se $a, b \in G$ e $a \leqslant b$ então $xay \leqslant xby$ para quaisquer $x, y \in G$. Neste caso, o par $(G, \leqslant)$ é dito ser um *grupo ordenado*.

Podemos encontrar com facilidade na literatura exemplos de grupos ordenados. Por exemplo, podemos citar o grupo numérico dos reais $\mathbb{R}$ (visto aditivamente), com sua ordem usual, como exemplo trivial de grupos ordenados. Além disso, subgrupos de grupos ordenados são ordenados (indutivamente).

O nosso horizonte de exemplos pode ser ampliado com a seguinte ideia. Dado um grupo ordenado G e X um conjunto bem ordenado qualquer, então o conjunto de todas as funções de X em G é também um grupo ordenado, considerando a operação ponto-a-ponto. Utilizaremos esta ideia de modo mais específico no Lema 2.2.4.

O lema a seguir indica condições em que podemos definir uma ordem em uma extensão split que seja compatível com sua operação.

Lema 2.2.1 *Se $G = H \ltimes A$ é uma extensão split dos grupos ordenados $(H, \leqslant_H)$ e $(A, \leqslant_A)$, e se, para $a \in A$ e $h \in H$,*

$$1 \leqslant_A a \quad \textit{implica} \quad 1 \leqslant_A a^h,$$

então podemos definir em G uma ordem total da seguinte forma: $h_1a_1 \leqslant h_2a_2$ quando $h_1 <_H h_2$ ou $h_1 = h_2$ e $a_1 \leqslant_A a_2$. Munido desta ordem, $(G, \leqslant)$ é um grupo ordenado.

Demonstração: É claro que a relação $\leqslant$ definida em G é uma relação de ordem. Vamos mostrar que ela é compatível com a sua operação. Sejam $h_ia_i \in G$, com $i = 1, 2, 3$, tais que $h_1a_1 \leqslant h_2a_2$. Logo, temos duas possibilidades: $h_1 <_H h_2$ ou $h_1 = h_2$ e $a_1 \leqslant_A a_2$. Se $h_1 <_H h_2$, então $h_3h_1 <_H h_3h_2$ pois $(H, \leqslant_H)$ é ordenado, e assim

$$h_3a_3h_1a_1 = h_3h_1a_3^{h_1}a_1 \leqslant h_3h_2a_3^{h_2}a_2 = h_3a_3h_2a_2.$$

Caso contrário, devemos ter $h_1 = h_2$ e $a_1 <_A a_2$, donde $a_3^{h_1} = a_3^{h_2}$, e portanto $a_3^{h_1}a_1 <_A a_3^{h2}a_2$, pois $(A, \leqslant_A)$ é ordenado. Assim, $h_3a_3h_1a_1 \leqslant h_3a_2h_1a_2$.

Resta-nos agora verificar que o produto à direita também preserva $\leqslant$. Observe que se $h_1 <_H h_2$, então o argumento é análogo ao que foi apresentado acima. Para a segunda situação, devemos ter $1 \leqslant_A a_1^{-1}a_2$. Agora, por hipótese, tem-se $1 \leqslant_A (a_1^{-1}a_2)^{h_3}$, e assim $a_1^{h_3} \leqslant_A a_2^{h_3}$, o que nos dá

$$h_1a_1h_3a_3 = h_1h_3a_1^{h_3}a_3 \leqslant h_2h_3a_2^{h_3}a_3 = h_2a_2h_3a_3.$$

■

Lema 2.2.2 *Todo grupo G tem um único subgrupo normal minimal K tal que G/K é ordenável.*

Demonstração: Sejam $(K_\lambda)_{\lambda\in\Lambda}$ a família dos núcleos dos homomorfismos de G em grupos ordenados e $K = \cap_{\lambda\in\Lambda}K_\lambda$. Note que, para cada $\lambda \in \Lambda$, G/K_λ é isomorfo a um subgrupo de um grupo ordenado. Vamos então fixar uma ordem em cada grupo G/K_λ e vamos considerar Λ como sendo bem ordenado. Agora, podemos definir uma ordem em G/K da seguinte forma: $aK < bK$ se para algum $\mu \in \Lambda$ temos $aK_\mu < bK_\mu$ e $aK_\lambda = bK_\lambda$ para todo $\lambda < \mu$. ■

Um *anel com divisão ordenado* é um anel com divisão Q junto com uma ordem $\leqslant$ tais que Q com a adição e o conjunto $U_+(Q) = \{h \in Q \mid h > 0\}$ com a multiplicação são grupos ordenados com respeito a $\leqslant$.

Proposição 2.2.3 *Seja H um grupo ordenado. Então $\mathbb{Z}H$ pode ser mergulhado em um anel com divisão ordenado Q de modo que a ordem em Q induz uma imersão de H (como grupo ordenado) em $U_+(Q)$.*

Demonstração: A prova desta proposição pode ser encontrada em Neumann [7]. Em linhas gerais, um candidato a Q é o anel com divisão constituído das séries formais $q = \sum_{h \in H} \lambda_h h$ (munido das operações usuais de soma e multiplicação), com $\lambda_h \in \mathbb{Q}$ para todo $h \in H$, e com suporte $\{h \in H \mid \lambda_h \neq 0\}$ inversamente bem-ordenado. Então $U_+(Q)$ é o conjunto dos elementos q tal que $\lambda_m > 0$, onde $m \in H$ é o maior elemento do suporte de q. ∎

Para finalizar a seção, conectamos o Lema 2.2.1 e a Proposição 2.2.3 conforme abaixo.

Lema 2.2.4 *Sejam H um grupo ordenado, Q um anel com divisão ordenado contendo $\mathbb{Z}H$ e V um Q-espaço vetorial (à direita) de dimensão finita; assim, V é naturalmente um $\mathbb{Z}H$-módulo. Então a extensão split $H \ltimes V$ é ordenável.*

Demonstração: Primeiramente, podemos considerar V como sendo o espaço $Q^{(n)}$ cujos elementos são n-uplas de elementos de Q. Vamos definir uma ordem $\leqslant_V$ em V da seguinte forma: $(x_1, x_2, \ldots, x_n) \leqslant_V (y_1, y_2, \ldots, y_n)$ se $0 < y_i - x_i$ para a primeira diferença $y_i - x_i$ não nula. Assim, se $0 <_V v$, com $v = (v_1, v_2, \ldots, v_n) \in V$ e $h \in H$, seja v_i a primeira entrada não nula, a qual satisfaz $0 < v_i$ em Q. Então $0 < v_i h$, pois Q é ordenado. Logo, $0 < vh$. Portanto, pelo Lema 2.2.1 $H \ltimes V$ é ordenável. ∎

2.3 Prova do Teorema

Teorema Principal (Caso Abstrato) Seja G um grupo que tem uma apresentação com n geradores $x_1, x_2, \ldots, x_n$ e m relações $r_1, r_2, \ldots, r_m$, onde $n > m$, e seja Y um conjunto qualquer de geradores de G. Então existem $n - m$ elementos de Y que geram livremente um subgrupo livre de G.

Demonstração: Considere $F/R \cong G$ uma apresentação de G, onde F é um grupo livre gerado livremente por $x_1, x_2, \ldots, x_n$, e cujo núcleo R pode ser gerado como subgrupo normal pelo conjunto constituído dos elementos $r_1, r_2, \ldots, r_m$, onde $m < n$.

Pelo Lema 2.2.2, existe um menor subgrupo normal S de F contendo R para o qual $\overline{G} = F/S$ é ordenável.

Aplicando a Proposição 2.2.3, seja Q um anel com divisão ordenável contendo $\mathbb{Z}\overline{G}$. Sejam V o espaço vetorial (à direita) sobre Q com base $\{t_1, t_2, \ldots, t_n\}$ e M o $\mathbb{Z}\overline{G}$-módulo gerado por $t_1, t_2, \ldots, t_n$. Uma vez que existe uma imersão natural de M em V, então todo elemento de M é escrito de maneira única em termos de $t_1, t_2, \ldots, t_n$. Portanto, M é um $\mathbb{Z}\overline{G}$-módulo livre com base livre $\{t_1, t_2, \ldots, t_n\}$.

Considere o homomorfismo dado pelo Lema 2.1.2

$$\begin{aligned} \mu : F &\longrightarrow \begin{pmatrix} \overline{G} & 0 \\ M & 1 \end{pmatrix} \\ x_i &\longmapsto \begin{pmatrix} x_i S & 0 \\ t_i & 1 \end{pmatrix} \end{aligned}$$

e considere a derivação $\delta : F \longrightarrow M$ que leva $f \in F$ na componente em M de $\mu(f)$, conforme indicado abaixo

$$\mu(f) \longmapsto \begin{pmatrix} fS & 0 \\ \delta(f) & 1 \end{pmatrix}.$$

Seja U o subespaço de V gerado por $\delta(r_1), \delta(r_2), \ldots, \delta(r_m)$ e considere o espaço quociente $W = V/U$. Temos que $dim W = r \geq n - m$. Além disso, considere

$$\begin{aligned} \overline{\delta} : F &\longrightarrow (M+U)/U \\ f &\longmapsto \delta(f) + U \end{aligned}$$

uma derivação induzida por δ. Como $\{t_1, t_2, \ldots, t_n\}$ é uma base de V, e $\delta(x_i) = t_i$ para todo $i = 1, 2, \ldots, n$, então $\{\overline{\delta}(x_1), \overline{\delta}(x_2), \ldots, \overline{\delta}(x_n)\}$ gera W.

Considere agora o homomorfismo

$$\varphi : \begin{pmatrix} \overline{G} & 0 \\ M & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} \overline{G} & 0 \\ \frac{M+U}{U} & 1 \end{pmatrix}$$

e defina

$$\psi : F \longrightarrow \begin{pmatrix} \overline{G} & 0 \\ \frac{M+U}{U} & 1 \end{pmatrix}$$

como sendo a composição $\psi = \varphi\mu$.

Pelo Lema 2.2.4, temos que $\overline{G} \ltimes (M+U)/U$ é ordenável. Assim, $F/ker\psi$ é ordenável. Por um lado, temos claramente $ker\psi \leq S$. Por outro lado, para todo $i = 1, 2, \ldots, m$, temos $r_i S = S$ (pois $R \leq S$) e $\overline{\delta} r_i = 0$ (pois U é gerado por $\{\delta(r_1), \delta(r_2), \ldots, \delta(r_n)\}$). Logo, $R \leq ker\psi$. Pela minimalidade de S, segue que $S = ker\psi$. Portanto, ψ induz uma imersão

$$j : \overline{G} \longrightarrow \begin{pmatrix} \overline{G} & 0 \\ W & 1 \end{pmatrix}.$$

Seja $Y \subseteq F$ um conjunto gerador de F/R. Por simplicidade, vamos escrever $F/R = \langle Y \rangle$, identificando Y com sua imagem em F/R. Vamos induzir também a derivação $\overline{\delta} : F \longrightarrow W$ ao quociente F/R. Aplicando o Lema 2.1.1, temos que

$$\overline{\delta}(F/R) \subseteq \langle \overline{\delta}(Y) \rangle \subseteq \overline{\delta}(F/R).$$

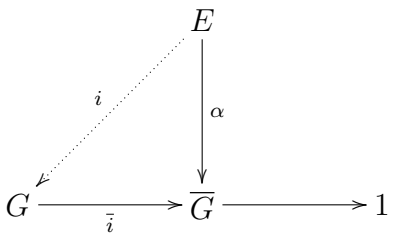
Portanto, $\overline{\delta}(F/R) = \langle \overline{\delta}(Y) \rangle \leqslant W$. Observe também que $\overline{\delta}(x_i) \in \overline{\delta} Y$. De fato, se algum $x_i \in R$, então $\overline{\delta}(x_i) = 0$ pois $R \leqslant Ker\psi$. Caso contrário, $x_i \in \langle Y \rangle$ e assim $\overline{\delta}(x_i) \in \langle \overline{\delta}(Y) \rangle$. Um vez que $W = \langle \overline{\delta}(x_i), \overline{\delta}(x_2), \ldots, \overline{\delta}(x_n) \rangle$ temos que $W = \langle \overline{\delta}(Y) \rangle$.

Considere então $\{\overline{\delta} y_1, \overline{\delta} y_2, \ldots, \overline{\delta} y_r\}$ uma base de W e E o grupo livre com base livre $\{y_1, y_2, \ldots, y_r\}$. Defina o homomorfismo $\alpha : E \longrightarrow \overline{G}$ por $y_i \longmapsto y_i S$ e seja $N = ker\alpha$.

Pelo Lema 2.1.2, o homomorfismo

$$\beta : y_i \longmapsto \begin{pmatrix} y_i S & 0 \\ \overline{\delta} y_i & 1 \end{pmatrix}$$

definido como sendo a composição $\beta = j\alpha$ tem núcleo N'. Mas j é injetiva, e portanto obtemos $N = N'$. Todavia, N é subgrupo de um grupo livre; logo, N é livre e, como $N = N'$, segue que $N = 1$. Assim, o subgrupo $\langle y_1, y_2, \ldots, y_n \rangle$ de F é livre módulo S. Pela propriedade projetiva dos grupos livres (Proposição 1.1.6), existe uma aplicação $i : E \longrightarrow G$ tal que o seguinte diagrama comuta, onde $\overline{i} : G \longrightarrow \overline{G}$ é o epimorfismo natural.



Neste contexto, como α é injetiva, temos que i também é injetiva, e isto conclui a demonstração.

■

Capítulo 3

Grupos Profinitos

O objetivo deste capítulo é apresentar um arcabouço de definições e resultados conhecidos sobre Grupos Profinitos com caráter preliminar referente ao Capítulo 4. Consciente ao Teorema Principal (Caso Pro-p), consideramos por conveniência restringir nosso estudo a classe dos p-grupos finitos.

Apresentamos um prelúdio topológico e introduzimos a definição de grupo pro-p baseando-se no conceito de limite inverso. Destacamos propriedades importantes do completamento pro-p, dos grupos pro-p livres e dos grupos pro-p finitamente apresentados. Apresentamos também especificidades dos módulos profinitos, dos módulos profinitos livres e das álgebras de grupo completas.

Este capítulo foi elaborado a partir da leitura Munkres [6], Ribes-Zalesskii [8] e Wilson [13].

3.1 Preliminares Topológicas

Nesta seção, selecionamos com síntese alguns conceitos elementares associados aos espaços topológicos, e introduzimos as definições de grupos e anéis topológicos, objetos matemáticos que reúnem características tanto topológicas quanto algébricas e que são o alicerce do estudo que apresentaremos a partir deste ponto. Cabe ressaltar que esta seção não tem caráter didático e não objetiva explorar com profundidade os assuntos tratados, mas deve preencher eventuais lacunas.

Para maior aprofundamento, indicamos consultar Munkres [6].

3.1.1 Espaços Topológicos e Aplicações Contínuas

Espaços Topológicos

Definimos um *espaço topológico* (ou simplesmente *espaço*) como sendo um conjunto X com uma família de subconjuntos, ditos *conjuntos abertos* (ou simplesmente *abertos*), satisfazendo as seguintes condições:

i) Os conjuntos vazio $\varnothing$ e X são abertos;

ii) A interseção de quaisquer dois abertos (e portanto a interseção de uma quantidade finita de abertos) é um aberto;

iii) a união de qualquer coleção de abertos é um aberto.

O conjunto dos abertos de X é dito uma *topologia*.

Qualquer conjunto pode ser visto como espaço topológico, por exemplo, com respeito à topologia em que cada subconjunto é um aberto. Esta topologia é dita *topologia discreta*, e neste caso X é dito ser um *espaço discreto*. Todavia, é oportuno observar que nem toda coleção de subconjuntos representa uma topologia (pois esta coleção arbitrária pode não conter uma união de seus subconjuntos).

Um subconjunto Y de X é dito ser *conjunto fechado* (ou simplesmente *fechado*) se o seu complementar em X é aberto. A interseção de todos os subconjuntos fechados de X contendo Y é dito o *fecho* de Y, e denotado por $\overline{Y}$. Se $X = \overline{Y}$, então Y é dito ser *denso* em X .

Aplicando as identidades de DeMorgan nos itens (i), (ii) e (iii) na definição de topologia acima, temos que em um espaço topológico X o conjunto vazio $\varnothing$ e o próprio X são fechados, a união de quaisquer dois fechados (e portanto a união de uma quantidade finita de fechados) é um fechado, e a interseção de qualquer coleção de fechados é um fechado. Em especial, temos que $\overline{Y}$ é fechado.

Uma *base* de uma topologia em X é uma coleção $(U_\lambda \mid \lambda \in \Lambda)$ de abertos de X de sorte que se $Y \subseteq X$ é um aberto, então $Y = \cup_{\lambda \in \Lambda_*} U_\lambda$, onde $\Lambda_* \subseteq \Lambda$.

Uma *vizinhança aberta* (ou simplesmente *vizinhança*) de um elemento $x \in X$ é um aberto de X que contém x. Um *sistema fundamental de vizinhanças* de um ponto $x \in X$ é um conjunto $\mathscr{V}$ de vizinhanças de x de sorte que se $x \in V \subseteq X$ e V é um aberto em X, então existe $W \in \mathscr{V}$ tal que $W \subseteq V$.

Aplicações Contínuas

Sejam X e Y espaços topológicos e $f : X \longrightarrow Y$ uma aplicação. Então f é dita ser *contínua* se para todo aberto U de Y a sua imagem inversa

$$f^{-1}(U) = \{x \in X \mid f(x) \in U\}$$

é um aberto em X. f é dita ser um *homeomorfismo* se f é uma bijeção contínua com inversa f^{-1} contínua.

3.1.2 Espaços Compactos, Conexos e Hausdorff

Seja X um espaço topológico. X é dito ser *compacto* se para qualquer família de abertos $\{U_\lambda \mid \lambda \in \Lambda\}$ de X tal que $X = \cup_{\lambda\in\Lambda} U_\lambda$ (dita *cobertura aberta* de X), existe uma quantidade finita de índices $\lambda_1, \lambda_2, \ldots, \lambda_n \in \Lambda$ tais que $X = \cup_{i=1}^{n} U_{\lambda_i}$.

X é dito ser *Hausdorff* se para quaisquer elementos $x, y \in X$ existem vizinhanças V e W de x e y, respectivamente, tais que $V \cap W = \varnothing$.

X é dito ser *conexo* se não pode ser decomposto como uma união disjunta de dois abertos não vazios. X é dito ser *totalmente desconexo* se todo subespaço conexo tem no máximo um elemento.

Os conceitos de compacidade, conexidade e Hausdorff têm destaque nesta dissertação. Um espaço topológico compacto Hausdorff totalmente desconexo é dito um *espaço profinito*.

Proposição 3.1.1 *Seja X um espaço topológico compacto. Então todo subconjunto fechado é compacto.*

Demonstração: Seja Y um subconjunto fechado de X. Dada uma cobertura aberta $\mathscr{A}$ de Y, temos que $\mathscr{B} = \mathscr{A} \cup \{X - Y\}$ é uma cobertura aberta de X. Assim, existe alguma subcoleção finita de abertos em $\mathscr{B}$ que cobre X. Se esta subcoleção contém $X - Y$, descarte-o. Com isto, obtemos uma subcoleção finita de $\mathscr{A}$ que cobre Y. ∎

Proposição 3.1.2 *Sejam $f, g : X \longrightarrow Y$ aplicações entre espaços topológicos. Se f e g são contínuas e Y é Hausdorff, então $\{x \in X \mid f(x) = g(x)\}$ é fechado em X.*

Demonstração: Escreva $N = \{x \in X \mid f(x) \neq g(x)\}$. Sejam $y \in N$ e U, V vizinhanças disjuntas de $f(y)$ e $g(y)$ em Y, respectivamente. Claramente, $N_y = f^{-1}(U) \cap g^{-1}(V)$ é um aberto contido em N e contendo y. Portanto, $N = \cup_{y\in N} N_y$ é um aberto. ∎

3.1.3 Subespaço Topológico, Topologia Quociente e Topologia Produto

Ao longo do texto, será recorrente o uso de alguns tipos de topologias. Vamos descrevê-las abaixo.

Subespaço Topológico

Se Y é um subconjunto de um espaço topológico X, então a coleção de todos os subconjuntos da forma $Y \cap U$, onde U é um aberto em X, é uma topologia em Y, chamada de *topologia induzida*. Neste caso, Y é dito ser um *subespaço* de X.

Topologia Quociente

Seja ρ uma relação de equivalência em um espaço topológico X, e escreva X/ρ para o conjunto quociente e $q : X \longrightarrow X/\rho$ para a aplicação quociente que leva cada elemento na sua classe de equivalência. A *topologia quociente* em X/ρ é a topologia cujos abertos são os subconjuntos V de X/ρ tais que $q^{-1}(V)$ é um aberto em X. Portanto, se consideramos em X/ρ a topologia quociente, temos que q é naturalmente contínua.

Produto Topológico

O *produto cartesiano* (ou simplesmente *produto*) de uma família $(X_\lambda \mid \lambda \in \Lambda)$ é o conjunto $\prod_{\lambda\in\Lambda} X_\lambda$ cujos elementos x são aplicações de Λ em $\cup_{\lambda\in\Lambda} X_\lambda$ de sorte que $x(\lambda) \in X_\lambda$ para todo $\lambda \in \Lambda$. Assim, um elemento em $\prod_{\lambda\in\Lambda} X_\lambda$ será escrito como (x_λ) o qual corresponde à função que associa λ a x_λ.

A aplicação $\pi_\lambda : \prod_{\lambda\in\Lambda} X_\lambda \longrightarrow X_\lambda$ dada por $(x_\lambda) \longmapsto x_\lambda$ para cada $x(\lambda) \in X_\lambda$ é dita *projeção*.

Se cada X_λ é um espaço topológico, então o produto $\prod_{\lambda\in\Lambda} X_\lambda$ pode ser considerado como um espaço topológico com respeito à topologia cujos abertos são todas as uniões de conjuntos da forma

$$\pi_{\lambda_1}^{-1}(U_1) \cap \pi_{\lambda_2}^{-1}(U_2) \cap \cdots \cap \pi_{\lambda_n}^{-1}(U_n)$$

com $n \in \mathbb{N}$ e U_{λ_i} aberto em X_{λ_i} para cada $\lambda_i \in \Lambda$.

Proposição 3.1.3 *Seja $(X_\lambda \mid \lambda \in \Lambda)$ uma família de espaços topológicos. Se cada X_λ é compacto Hausdorff totalmente desconexo, então o produto $\prod_{\lambda\in\Lambda} X_\lambda$ é compacto Hausdorff totalmente desconexo.*

Demonstração: Consultar Wilson [13]. Teorema 0.2.1. ∎

3.1.4 Grupos e Anéis Topológicos

Grupos Topológicos

Um *grupo topológico* é um conjunto G que possui ambas as estruturas de grupo e de espaço topológico, e cuja aplicação $(x, y) \longmapsto xy^{-1}$ de $G \times G$ (com a topologia produto) em G é contínua.

Proposição 3.1.4 *Sejam G um grupo topológico e $H \leqslant G$.*

(a) H é um grupo topológico com respeito à topologia induzida.

(b) Se $H \lhd G$, então G/H é um grupo topológico com respeito à topologia quociente.

Demonstração: Consultar Wilson [13], Lema 0.3.1(e). ∎

Seja $(G_\lambda \mid \lambda \in \Lambda)$ uma família de grupos topológicos. Defina no produto $\prod_{\lambda\in\Lambda} G_\lambda$ a operação ponto-a-ponto $(x_\lambda)(y_\lambda) = (x_\lambda y_\lambda)$. Assim, $\prod_{\lambda\in\Lambda} G_\lambda$ munido desta operação e da topologia produto, é um grupo topológico.

Anéis Topológicos

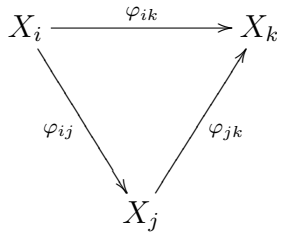
Um *anel topológico* é um anel R que, visto aditivamente, é um grupo topológico, e cuja multiplicação dada por $(x, y) \longmapsto xy$ de $R \times R$ (com a topologia produto) em R é uma aplicação contínua.

3.2 Limite Inverso

Um conjunto I munido de uma relação de ordem parcial $\preceq$ é dito ser *dirigido* se para quaisquer $i, j \in I$ existe algum $k \in I$ tal que $i, j \preceq k$.

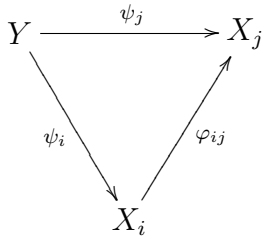
Um *sistema inverso* de espaços topológicos sobre um conjunto dirigido I consiste de uma coleção de espaços topológicos $\{X_i \mid i \in I\}$ e de uma coleção de aplicações contínuas $\varphi_{ij} : X_i \longrightarrow X_j$, definidas quando $i \succeq j$ e tais que o

seguinte diagrama comuta (isto quando $i, j, k \in I$ e $i \succeq j \succeq k$):

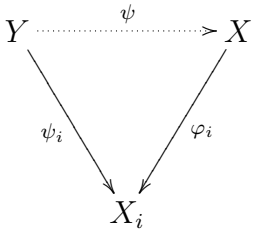


Vamos denotar um sistema inverso, como acima, por $\{X_i, \varphi_{ij}, I\}$. Se cada aplicação φ_{ij} é sobrejetora, então $\{X_i, \varphi_{ij}, I\}$ é dito *sistema inverso sobrejetor*.

Sejam Y um espaço topológico, $\{X_i, \varphi_{ij}, I\}$ um sistema inverso de espaços topológicos sobre um conjunto dirigido I, e $\psi_i : Y \longrightarrow X_i$ aplicações contínuas para cada $i \in I$. Então as aplicações ψ_i são ditas *compatíveis* se $\varphi_{ij}\psi_i = \psi_j$, sempre que $j \preceq i$, isto é, se o seguinte diagrama comuta:



Dizemos que um par (X, φ_i) constituído de um espaço topológico X junto com uma família de aplicações contínuas compatíveis $\varphi_i : X \longrightarrow X_i$ é um *limite inverso* de um sistema inverso $\{X_i, \varphi_{ij}, I\}$ se a seguinte propriedade universal é satisfeita: para qualquer espaço topológico Y e qualquer família de aplicações contínuas compatíveis $\psi_i : Y \longrightarrow X_i$ $(i \in I)$, existe uma única aplicação contínua $\psi : Y \longrightarrow X$ tal que $\varphi_i\psi = \psi_i$, para todo $i \in I$, isto é, se o diagrama abaixo comuta:



Neste contexto, dizemos então que ψ é *induzida* ou *determinada* pela família $(\psi_i)_{i\in I}$. Dizemos também que as aplicações $\varphi_i : X \longrightarrow X_i$ são *projeções.*

Proposição 3.2.1 *Seja $\{X_i, \varphi_{ij}, I\}$ um sistema inverso de espaços topológicos. Então existe um limite inverso de $\{X_i, \varphi_{ij}, I\}$. Além disso, este limite é único no seguinte sentido: se (X, φ_i) e (Y, ψ_i) são dois limites inversos de $\{X_i, \varphi_{ij}, I\}$, então existe um único homeomorfismo $\varphi : X \longrightarrow Y$ tal que $\psi_i\varphi = \varphi_i$, para todo $i \in I$.*

Demonstração: Defina X como o subespaço de $\prod_{i\in I} X_i$ formado pelos elementos $(x_i)_{i\in I}$ que satisfazem

$$\varphi_{ij}(x_i) = x_j$$

para $i \succeq j$.

Seja $\varphi_i : X \longrightarrow X_i$ a restrição da projeção canônica $\pi_i : \prod_{i\in I} X_i \longrightarrow X_i$. Então φ_i é uma aplicação contínua compatível para todo $i \in I$ e (X, φ_i) é um limite inverso. De fato, suponha que $\{\psi_i : Y \longrightarrow X_i\}$ é uma família de aplicações compatíveis. Defina

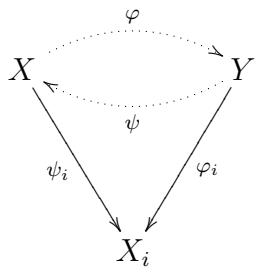
$$\begin{array}{rccc} \overline{\psi}: & Y & \longrightarrow & \prod_{i\in I} X_i \\ & y & \longmapsto & \overline{\psi}(y) = (\psi_i(y)). \end{array}$$

Assim, $\pi_i\overline{\psi} = \psi_i$ para cada i, e $\overline{\psi}$ é contínua (pois a sua composta com cada projeção é contínua). Além disso, se $i \succeq j$, então

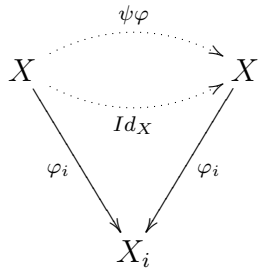
$$\pi_j\overline{\psi} = \psi_i = \varphi_{ij}\psi_i = \varphi_{ij}\pi_i\overline{\psi}$$

e portanto $\overline{\psi} : Y \longrightarrow X$.

Suponha agora (X, φ_i) e (Y, ψ_i) dois limites inversos do sistema $\{X_i, \varphi_i, I\}$.



Como as aplicações $\psi_i : Y \longrightarrow X_i$ são compatíveis, a propriedade universal do limite inverso (X, φ_i) mostra que existe uma única aplicação contínua $\psi : Y \longrightarrow X$ tal que $\varphi_i\psi = \psi_i$ para todo $i \in I$. Analogamente, como as aplicações $\varphi_i : X \longrightarrow X_i$ são compatíveis e (Y, ψ_i) é um limite inverso, existe uma única aplicação contínua $\varphi : X \longrightarrow Y$ tal que $\psi_i\varphi = \varphi_i$ para todo $i \in I$. Com isto, observamos que o diagrama abaixo comuta para todo $i \in I$.



Por definição, existe uma única aplicação satisfazendo esta propriedade, e portanto $\psi\varphi = Id_X$. Analogamente, tem-se $\varphi\psi = Id_Y$. Assim, φ é um homeomorfismo. ■

Se $\{X_i, \varphi_{ij}, I\}$ é um sistema inverso de espaços topológicos, denotaremos seu limite inverso por

$$\varprojlim_{i\in I} X_i.$$

Observação 3.2.2 *Sejam $\{X_i, \varphi_{ij}, I\}$ um sistema inverso e $X = \varprojlim_{i\in I} X_i$. Considerando $\alpha_i : X \to X_i$ projeções, e $\overline{\varphi_{ij}}$ a restrição de φ_{ij} a $\alpha_i(X)$, então obtemos um sistema inverso sobrejetor $\{\alpha_i(X), \overline{\varphi_{ij}}, I\}$ com o mesmo limite inverso.*

Proposição 3.2.3 *Seja $\{X_i, \varphi_{ij}, I\}$ um sistema inverso de espaços topológicos compactos Hausdorff totalmente desconexos. Então $\varprojlim_{i\in I} X_i$ é compacto Hausdorff totalmente desconexo.*

Demonstração: Pela Proposição 3.1.3, temos que $\prod_{i\in I} X_i$ é compacto Hausdorff totalmente desconexo. Além disso, dos argumentos apresentados na Proposição 3.2.1 podemos identificar o limite inverso de $\{X_i, \varphi_{ij}, I\}$ com um subconjunto do produto $\prod_{i\in I} X_i$ dado por

$$\varprojlim_{i\in I} X_i = \bigcap_{i\succeq j} D_{ij}$$

onde $D_{ij} = \{c \in \prod_{i\in I} X_i \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\}$ $(i \succeq j)$ e π_i são projeções (para quaisquer $i, j \in I$). Agora, pela Proposição 3.1.2, observamos que cada conjunto D_{ij} é fechado, e portanto $\varprojlim_{i\in I} X_i$ é fechado. Assim, segue da Proposição 3.1.1 que $\varprojlim_{i\in I} X_i$ é compacto. As proriedades de ser Hausdorff e totalmente desconexo são induzidas do produto $\prod_{i\in I} X_i$. ■

Admitindo as hipóteses da proposição acima, enfatizamos que o limite inverso $\varprojlim_{i\in I} X_i$ é um subespaço fechado de $\prod_{i\in I} X_i$. A proposição a seguir esclarece que podemos enfraquecer estas hipóteses sobre o sistema inverso $\{X_i, \varphi_{ij}, I\}$ e ainda assim termos $\varprojlim_{i\in I} X_i$ fechado em $\prod_{i\in I} X_i$.

Proposição 3.2.4 *Se $\{X_i, \varphi_{ij}, I\}$ é um sistema inverso de espaços topológicos Hausdorff, então $\varprojlim_{i\in I} X_i$ é um subespaço fechado de $\prod_{i\in I} X_i$.*

Demonstração: Seja $(x_i) \in (\prod_{i\in I} X_i) - (\varprojlim_{i\in I} X_i)$. Então existem índices $r, s \in I$, com $r \succeq s$ e $\varphi_{rs}(x_r) \neq x_s$. Neste caso, podemos escolher vizinhanças abertas disjuntas U e V de $\varphi_{rs}(x_r)$ e x_s em X_s, respectivamente. Seja U' uma vizinhança aberta de x_r em X_r tal que $\varphi_{rs}(U') \subseteq U$. Considere o subconjunto $W = \prod_{i\in I} V_i$ de $\prod_{i\in I} X_i$, onde $V_r = U', V_s = V$ e $U_i = X_i$ para $i \neq r, s$. Temos que W é uma vizinhança aberta de (x_i) em $\prod_{i\in I} X_i$ disjunta de $\varprojlim_{i\in I} X_i$. ■

Proposição 3.2.5 *Seja $\{X_i, \varphi_{ij}, I\}$ um sistema inverso de espaços topológicos compactos Hausdorff não vazios. Então $\varprojlim_{i\in I} X_i$ é não vazio.*

Demonstração: Para $i \succeq j$, temos que D_{ij} é fechado (Proposição 3.1.2) e $\prod_{i\in I} X_i$ é compacto (Proposição 3.1.3). Se $\varprojlim X_i = \varnothing$, então $\cap_{r=1}^{n} D_{i_r j_r} = \varnothing$, $n \in \mathbb{N}$. Como I é dirigido, existe $k \in I$ tal que $k \succeq i_r$ para todo r. Escolha $x_k \in X_k$, defina $x_l = \varphi_{kl}(x_k)$, para $l \succeq k$, e defina x_l arbitrariamente para todos os outros elementos de I. Portanto,

$$(x_i) \in \bigcap_{r=1}^{n} D_{i_r j_r},$$

uma contradição. ■

Convidamos o leitor a definir sistema inverso e limite inverso para grupos topológicos e anéis topológicos. Nestes casos, aplicações contínuas são

substituídas por homomorfismos contínuos de grupos e por homomorfismos contínuos de anéis, respectivamente. Esclarecemos também que os resultados apresentados nesta seção continuam sendo válidos nestes casos, uma vez que dependem apenas da topologia das estruturas referidas.

Por exemplo, sejam $I = \mathbb{N}, p$ um primo e $G_i = \mathbb{Z}/p^i\mathbb{Z}$ para cada i; e para $i \geqslant j$, as aplicações $\varphi_{ij} : G_i \longrightarrow G_j$ definidas por

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

para cada $n \in \mathbb{Z}$. Então (G_i, φ_{ij}, I) é um sistema inverso.

De modo mais geral, sejam G um grupo e I uma família de subgrupos normais com a propriedade de que para quaisquer $U_1, U_2 \in I$, existe $V \in I$ tal que $V \leqslant U_1 \cap U_2$. Neste caso, podemos considerar I como sendo um conjunto dirigido com respeito a ordem $U \leqslant' V$ se V é subgrupo de U. Assim, defina $q_{VU} : G/V \longrightarrow G/U$ por

$$q_{VU}(Vg) = Ug$$

para todo $g \in G$. Então $(G/V, q_{VU}, I)$ é um sistema inverso de grupos.

3.3 Grupos Pro-p

Seja $\mathscr{C}$ uma *classe* não vazia de grupos finitos com a propriedade de ser fechada com respeito a imagens isomórficas (isto é, se $G_1 \in \mathscr{C}$ e $G_1 \cong G_2$, então $G_2 \in \mathscr{C}$). G é dito *$\mathscr{C}$-grupo* se $G \in \mathscr{C}$. G é dito *grupo pro-$\mathscr{C}$* se $G = \varprojlim G_i$, onde $\{G_i, \varphi_{ij}, I\}$ é um sistema inverso sobrejetor de $\mathscr{C}$-grupos (munidos da topologia discreta).

Observe que um grupo pro-$\mathscr{C}$, como acima, é um grupo topológico, cuja topologia é induzida da topologia produto em $\prod_{i \in I} G_i$. Observe também que $\mathscr{C}$-grupos são grupos pro-$\mathscr{C}$ decorrentes de sistemas inversos sobre conjuntos dirigidos com apenas um elemento.

Claramente, as propriedades dos grupos pro-$\mathscr{C}$ dependem do tipo de classe de grupos finitos que estamos considerando. Em especial, assumiremos a partir deste ponto $\mathscr{C}$ como sendo a classe dos p-grupos finitos em virtude da finalidade do nosso estudo. Neste caso, um grupo pro-$\mathscr{C}$ será chamado de *grupo pro-p*.

Temos, neste caso, que $\mathscr{C}$ é fechada para quocientes (isto é, se $G \in \mathscr{C}$ e $K \lhd G$, então $G/K \in \mathscr{C}$) e fechada para produtos finitos (isto é, se G é um grupo finito com subgrupos normais N_1 e N_2 tais que $G/N_1, G/N_2 \in \mathscr{C}$, então $G/(N_1 \cap N_2) \in \mathscr{C}$).

Os grupos pro-p podem ser caracterizado de várias maneiras, elencadas segundo a proposição a seguir.

Proposição 3.3.1 *Seja $\mathscr{C}$ a classe dos p-grupos finitos. Então as seguintes condições para um grupo topológico G são equivalentes.*

(a) G é um grupo pro-p.

(b) G é compacto Hausdorff totalmente desconexo, e para cada subgrupo normal aberto U de G, tem-se $G/U \in \mathscr{C}$.

(c) G é compacto e o elemento identidade 1 de G admite um sistema fundamental $\mathscr{U}$ de vizinhanças abertas U tais que $\cap_{U\in\mathscr{U}} U = 1$ e cada U é um subgrupo normal aberto de G com $G/U \in \mathscr{C}$.

(d) O elemento identidade 1 de G admite um sistema fundamental $\mathscr{U}$ de vizinhanças abertas U tais que cada U é um subgrupo normal de G, com $G/U \in \mathscr{C}$ e

$$G = \varprojlim_{U\in\mathscr{U}} G/U.$$

Demonstração: Consultar Ribes-Zalesskii [8], Teorema 2.1.3. ∎

Proposição 3.3.2 *Seja $\mathscr{C}$ a classe dos p-grupos finitos.*

(a) Todo grupo quociente G/K de um grupo pro-p, onde $K \lhd G$ é fechado, é um grupo pro-p. Além disso, todo subgrupo fechado de G é um grupo pro-p.

(b) O produto direto $\prod_{i\in I} G_i$ de qualquer coleção $\{G_i \mid i \in I\}$ de grupos pro-p com a topologia produto é um grupo pro-p.

(c) O limite inverso $\varprojlim_{i\in I} G_i$ de um sistema inverso sobrejetivo $\{G_i, \varphi_{ij}, I\}$ de grupos pro-p é um grupo pro-p.

Demonstração: Consultar Ribes-Zalesskii [8], Proposição 2.2.1. ∎

Sejam G um grupo pro-p e X um subconjunto de G. Dizemos que X *gera G como grupo topológico* se o subgrupo abstrato $\langle X\rangle$ de G gerado por X é denso em G. Neste caso, X é dito um *conjunto de geradores (topológicos)* de G, e escrevemos $G = \overline{\langle X\rangle}$. Se X é finito, G é dito *(topologicamente) finitamente gerado*, e denotamos por

$$d(G) = min\{|\ X\ |;\ X \subseteq G,\ X \text{ gera } G \text{ topologicamente}\}$$

para o número mínimo de elementos (possivelmente infinito) necessários para gerar G topologicamente. Temos que $d(G) = dim_{\mathbb{F}_p} G/\Phi_p(G)$, onde $\Phi_p(G) = \overline{G^p[G,G]}$ é o subgrupo de Frattini de G.

3.4 Completamento Pro-p

Sejam G um grupo, $\mathscr{C}$ a classe dos p-grupos finitos e $\mathscr{N} = \mathscr{N}_{\mathscr{C}}(G)$ uma coleção não vazia de subgrupos de G dada por

$$\mathscr{N} = \{N \lhd_f G \mid G/N \in \mathscr{C}\},$$

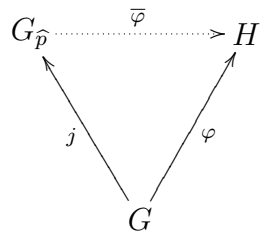
onde $N \lhd_f G$ denota o fato de N ser subgrupo normal de G de índice finito. Temos que $\mathscr{N}$ é não vazia (pois $G \in \mathscr{N}$) e possui a seguinte propriedade: para quaisquer $N_1, N_2 \in \mathscr{N}$, existe $N \in \mathscr{N}$ tal que $N \leqslant N_1 \cap N_2$ (pois podemos escolher $N = N_1 \cap N_2$). Assim, G pode ser interpretado como um espaço topológico se considerarmos $\mathscr{N}$ como um sistema fundamental de vizinhanças da identidade de G.

Definindo agora a relação $\preceq$ em $\mathscr{N}$ dada por $N \preceq M$ se M é subgrupo de N, temos que $\mathscr{N}$ torna-se um conjunto dirigido. Neste contexto, se considerarmos $\varphi_{MN} : G/N \longrightarrow G/M$ como o epimorfismo natural (definido para $M \succeq N$), então $\{G/M, \varphi_{MN}, \mathscr{N}\}$ é um sistema inverso sobrejetor de $\mathscr{C}$-grupos, e

$$\varprojlim_{N \in \mathscr{N}} G/N$$

é dito o *completamento pro-p* de G, o qual será denotado por $G_{\widehat{p}}$.

Observe que a existência e unicidade do completamento pro-p decorrem da existência e unicidade do limite inverso. Observe também que, naturalmente, existe um homomorfismo de grupos contínuo $j : G \longrightarrow G_{\widehat{p}}$ induzido pelos epimorfismos $G \longrightarrow G/N$ $(N \in \mathscr{N})$ e definido por $g \longmapsto gN$ para todo $g \in G$. Ademais, $G_{\widehat{p}}$ definido como acima, possui a seguinte propriedade universal: para qualquer homomorfismo de grupos contínuo $\varphi : G \longrightarrow H$ em um grupo pro-p H, existe um único homomorfismo de grupos contínuo $\overline{\varphi} : G_{\widehat{p}} :\longrightarrow H$ tal que $\overline{\varphi} j = \varphi$, isto é, o seguinte diagrama comuta:



É suficiente verificar a propriedade universal acima apenas para p-grupos, e assim seguirá automaticamente para grupos pro-p (uma vez que são limites

inversos de p-grupos). Para maiores esclarecimentos, indicamos consultar Ribes-Zalesskii [8], Lema 3.2.1.

Um caso especial é quando consideramos o grupo $\mathbb{Z}$ dos inteiros. O completamento pro-p de $\mathbb{Z}$ é denotado por $\mathbb{Z}_p$ e expresso por

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \{(x_n) \mid x_n \in \mathbb{Z}, x_n \equiv x_m (\text{mod } p^m), m \leqslant n\}.$$

Este completamento é conhecido na literatura como anel dos inteiros p-ádicos.

Proposição 3.4.1 *Sejam $G_{\widehat{p}} = \varprojlim_{N\in\mathscr{N}} G/N$ o completamento pro-p de um grupo G e $j : G \longrightarrow G_{\widehat{p}}$ definido por $g \longmapsto gN$ (com $N \in \mathscr{N}$).*

(a) Imj é denso em $G_{\widehat{p}}$.

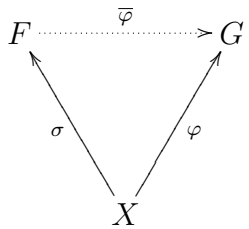
(b) $kerj = \cap_{N\in\mathscr{N}} N$.

Demonstração: Consultar Wilson [13], Proposição 1.4.4. ∎

Observe que podemos generalizar naturalmente o conceito de completamento pro-p e a proposição acima à coleção de todos os subgrupos normais de índice finito de um grupo G.

3.5 Grupos Pro-p Livres

Sejam F um grupo pro-p, $\mathscr{C}$ a classe dos p-grupos finitos, X um espaço profinito e $\sigma : X \longrightarrow F$ uma aplicação contínua tal que $F = \overline{\langle Im\sigma \rangle}$. O par (F, σ) é dito um *grupo pro-p livre* sobre X se a seguinte propriedade universal é satisfeita: para qualquer aplicação contínua $\varphi : X \longrightarrow G$ em um grupo pro-p G tal que $\varphi(X)$ gera G, existe um único homomorfismo contínuo $\overline{\varphi} : F \longrightarrow G$ tal que $\overline{\varphi}\sigma = \varphi$, isto é, se o seguinte diagrama comuta:



Observe que é suficiente testar a propriedade universal na definição acima apenas para p-grupos finitos, e assim seguirá automaticamente para grupos pro-p (uma vez que são limites inversos de p-grupos).

A função $\sigma : X \longrightarrow F$ é necessariamente injetiva (Ribes-Zalesskii [8], Lema 3.3.1). Assim, podemos considerá-la sem perda de generalidade como sendo a inclusão. Neste caso, identificaremos X com sua imagem $\sigma(X)$, e portanto assumiremos que $F = \overline{\langle X \rangle}$ no contexto da definição acima.

Proposição 3.5.1 *Para todo espaço profinito X existe um único grupo pro-p livre sobre X.*

Demonstração: Consultar Ribes-Zalesskii, [8] Teorema 3.3.2. ∎

Dizemos que um subconjunto X de um grupo pro-p G *converge a* 1 se todo subgrupo aberto U de G contém todos a menos uma quantidade finita de elementos de X.

Proposição 3.5.2 *Seja F o grupo pro-p livre sobre um conjunto X convergindo a* 1*.*

(a) Se F é também pro-p livre sobre um conjunto Y convergindo a 1*, então X e Y têm a mesma cardinalidade.*

(b) Se $X = \{x_1, x_2, \ldots, x_n\}$ é finito, então qualquer conjunto de geradores $\{y_1, y_2, \ldots, y_n\}$ de n elementos converge a 1*.*

Demonstração: Consultar Ribes-Zalesskii [8], Lema 3.3.5. ∎

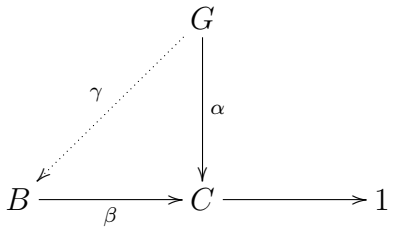
Se F é um grupo pro-p livre sobre um conjunto X convergindo a 1, definimos o *posto* de F como sendo a cardinalidade de X. Assim, a proposição anterior esclarece que o seu posto (como grupo pro-p livre) não depende da escolha da base, e portanto está bem definido e o denotamos por

$$d(F).$$

Particularmente, como o nosso Teorema Principal (Caso Pro-p) está impondo hipótese de ser finitamente gerado, não precisaremos nos preocupar com a existência de um conjunto convergindo a 1 pois um conjunto de geradores finito naturalmente já possui esta propriedade.

Um grupo pro-p G é dito *p-projetivo* se dado um epimorfismo $\beta : B \longrightarrow C$ e um homomorfismo $\alpha : G \longrightarrow C$, para quaisquer grupos pro-p B e C, existe

um homomorfismo $\gamma : G \longrightarrow B$ tal que $\beta\gamma = \alpha$, isto é, se o seguinte diagrama comuta:



Assim como mostramos no caso abstrato que a propriedade projetiva é verificada nos grupos livres, o próximo resultado atesta que o seu análogo para grupos pro-p também é verdadeiro.

Proposição 3.5.3 *Todo grupo pro-p livre é p-projetivo.*

Demonstração: Consultar Wilson [13]. Proposição 5.2.2. ■

Proposição 3.5.4 *Seja F um grupo abstrato livre sobre um conjunto finito X. Então o completamento pro-p $F_{\widehat{p}}$ de F é um grupo pro-p livre sobre X.*

Demonstração: Consultar Ribes-Zalesskii [8], Proposição 3.3.6. ■

Proposição 3.5.5 *Para todo conjunto X, a aplicação canônica $j : F \longrightarrow F_{\widehat{p}}$ do grupo abstrato livre F sobre X no grupo pro-p livre $F_{\widehat{p}}$ sobre X é injetiva.*

Demonstração: Consultar Wilson [13], Proposição 5.4.2. ■

Sejam F é um grupo abstrato livre de posto finito e $j : F \longrightarrow F_{\hat{p}}$ a aplicação natural. A Proposição 3.4.1 estabeleceu que

$$kerj = \cap_{N \in \mathscr{N}} N,$$

onde $\mathscr{N}$ é a coleção de todos os subgrupos normais de índice finito de F que determinam quocientes que são p-grupos. Assim, a proposição anterior esclarece que esta interseção é trivial. Neste caso, dizemos que F é *residualmente p*.

Observe também que $\mathbb{Z}_p$ é o grupo pro-p livre gerado por um elemento e $\mathbb{Z}$ mergulha em $\mathbb{Z}_p$.

3.6 Grupos Pro-p Finitamente Apresentados

Sejam G um grupo pro-p e $R \lhd G$. Dizemos que R é *gerado como subgrupo normal* por um conjunto X se R é o menor subgrupo normal (fechado) contendo X, e denotamos por

$$d_G(R)$$

a cardinalidade de X.

Uma *apresentação* de um grupo pro-p G é um epimorfismo contínuo $\pi : F \longrightarrow G$ de um grupo pro-p livre F em G. A apresentação é dita *finita* se ambos $d(F)$ e $d_F(ker\pi)$ são finitos. Neste caso, G é dito *finitamente apresentado*. Claramente, grupos pro-p livres finitamente gerados têm apresentações finitas.

Proposição 3.6.1 *Seja G um grupo pro-p.*

(a) Suponha que $\pi : F \longrightarrow G$ é uma apresentação finita. Então o número $d(F) - d_F(ker\pi)$ é independente de π e portanto é um invariante de G.

(b) Se $d(G) = d$ e G tem uma apresentação como grupo pro-p com $r + d$ geradores e r relações, então G é livre.

Demonstração: Consultar Wilson [13], Corolário 12.1.6. ∎

Uma questão em aberto sobre este tema é se podemos reproduzir o resultado acima para apresentações de p-grupos finitos considerados como grupos abstratos. Seja G um grupo abstrato finitamente apresentado e $\pi : F_a \longrightarrow G$ uma apresentação, onde F_a é um grupo livre (abstrato) de posto n_π e $d_{F_a}(ker\pi) = r_\pi$, digamos. Como vimos, a deficiência de G é dada por

$$defG = max\{n_\pi - r_\pi\},$$

isto é, o máximo entre todas as deficiências das apresentações. Entretanto, não se sabe se um p-grupo finito G tem uma apresentação $\pi : F_a \longrightarrow G$ que alcança esse máximo e $d(G) = n_\pi$.

Além disso, destacamos que o Teorema Principal (Caso Pro-p) é uma generalização do item (b) da Proposição 3.6.1.

Proposição 3.6.2 *Seja $\mathscr{C}$ a classe dos p-grupos finitos (que é fechada para quocientes, para produtos diretos finitos e para subgrupos normais). Se*

$$1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$$

é uma sequência exata de grupos, então

$$K_{\widehat{p}} \longrightarrow G_{\widehat{p}} \longrightarrow H_{\widehat{p}} \longrightarrow 1$$

é uma sequência exata de grupos pro-p.

Demonstração: Consultar Ribes-Zalesskii [8], Proposição 3.2.5. ∎

Seja G um grupo (abstrato) finitamente apresentado e $\pi : F \twoheadrightarrow G$ uma apresentação finita de G. Então, pela Proposição 3.6.2, π induz um epimorfismo (contínuo) $\pi_{\widehat{p}} : F_{\widehat{p}} \longrightarrow G_{\widehat{p}}$ entre os complementos pro-p de F e G. Pela Proposição 3.5.4, $F_{\widehat{p}}$ é um grupo pro-p livre de posto finito. Então $\pi_{\widehat{p}}$ é uma apresentação de $G_{\widehat{p}}$ com um número finito de geradores. Mais ainda, o núcleo de $\pi_{\widehat{p}}$ é o fecho da imagem de $Ker\pi$ via a aplicação canônica $F \longrightarrow F_{\widehat{p}}$. Com isto, vemos que uma apresentação finita para G também é uma apresentação finita para o seu completamento pro-p $G_{\widehat{p}}$, como destacamos na proposição a seguir.

Proposição 3.6.3 *Seja G um grupo abstrato. Se G tem uma apresentação como grupo abstrato com n geradores e r relações, então o completamento pro-p $G_{\widehat{p}}$ de G tem tal apresentação como grupo pro-p. Consequentemente, a deficiência de G como grupo abstrato não é maior do que a deficiência de $G_{\widehat{p}}$ como grupo pro-p*

Demonstração: Consultar Wilson [13], Proposição 12.1.7. ∎

Observe que se G é um p-grupo finito, então $G = G_{\widehat{p}}$. Entretanto, não é conhecido se suas deficiências como grupo abstrato e grupo pro-p coincidem.

3.7 Módulos Profinitos e Módulos Profinitos Livres

Anéis e Módulos Profinitos

Um *anel profinito* é um limite inverso de um sistema inverso de anéis finitos $\{R_i, \varphi_{ij}, I\}$. Assumiremos que os anéis possuem um elemento identidade, denotado por 1, e que os homomorfismos de anéis enviam elementos identidade em elementos identidade.

Os anéis profinitos possuem caracterizações análogas às de grupos profinitos (preconizados na Proposição 3.3.1) em termos dos seus ideais abertos.

Proposição 3.7.1 *Seja R um anel topológico. Então as seguintes condições são equivalentes.*

(a) R é um anel profinito.

(b) R é compacto Hausdorff totalmente desconexo.

(c) R é compacto e o elemento 0 de R admite um sistema fundamental de vizinhanças formado pelos ideais abertos de R.

(d) O elemento identidade 1 de R admite um sistema fundamental $\{T_i \mid i \in I\}$ de vizinhanças abertas tais que cada T_i é um ideal aberto de R e

$$R = \varprojlim_{i \in I} R/T_i.$$

Demonstração: Consultar Ribes-Zalesskii [8], Proposição 5.1.2. ∎

A partir deste ponto, R denota um anel profinito.

Um *R-módulo profinito à direita* é um grupo profinito abeliano M com uma aplicação contínua $M \times R \longrightarrow M$ que satisfaz as propriedades usuais de R-módulo abstrato.

Todo R-módulo profinito M tem uma base de vizinhanças abertas de 0 formada pelos subgrupos abertos de M que são invariantes sob a ação de R, ou seja, formada pelos R-submódulos abertos. Na categoria de R-módulos profinitos todos os morfismos $f : M \longrightarrow N$ entre R-módulos profinitos são homomorfismos contínuos com imagens fechadas, aos quais vamos nos referir apenas como homomorfismos. Convidamos também o leitor a definir os conceitos naturais de submódulos, núcleo e imagem de R-homomorfismos de R-módulos profinitos. Eles são análogos quando R é um anel abstrato.

Seja X um subconjunto de um R-módulo M. O R-submódulo fechado N topologicamente gerado por X é o fecho do R-submódulo abstrato gerado por X, ou seja, a interseção de todos os R-submódulos fechados de M que contêm X. Se X é um conjunto finito, N é dito *(topologicamente) finitamente gerado*. Neste caso, o lema a seguir diz que as definições de módulos profinitos topologicamente e abstratamente finitamente gerado coincidem.

Lema 3.7.2 *Sejam R um anel profinito, M um R-módulo profinito e $\{a_1, a_2, \ldots, a_n\}$ um subconjunto finito de M .*

(a) O conjunto $M_1 = \{\sum_{i=1}^{n} a_i u_i \mid u_1, u_2, \ldots, u_n \in R\}$ é um submódulo fechado.

(*b*) *Suponha que M é finitamente gerado, e seja N um R-módulo profinito. Então todo R-homomorfismo $\theta : M \longrightarrow N$ é contínuo.*

Demonstração: Consultar Wilson [13], Lema 7.2.2. ■

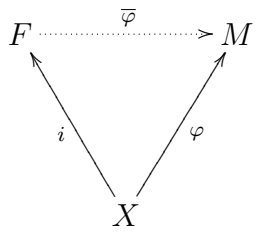
Módulos Profinitos Livres

Uma aplicação f de um conjunto X em um módulo profinito M é dita 0-*convergente* se para cada submódulo aberto N de M o conjunto

$$\{x \in X \mid f(x) \notin N \}$$

é finito.

Sejam F um R-módulo profinito, X um subconjunto de F e $i : X \longrightarrow F$ a aplicação inclusão. Então F é dito um *R-módulo profinito livre* sobre X se a aplicação inclusão i é 0-convergente e se satisfaz a seguinte propriedade universal: para qualquer aplicação 0-convergente $\varphi : X \longrightarrow M$ em um R-módulo profinito M, existe um único homomorfismo de R-módulos profinitos $\overline{\varphi}$ de F em M tal que $\overline{\varphi} i = \varphi$, isto é, o seguinte diagrama comuta:

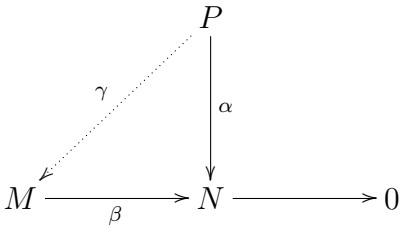


Observe que é suficiente verificar a propriedade universal na definição acima apenas para R-módulos finitos, e assim seguirá automaticamente para R-módulos profinitos (uma vez que são o limite inverso de R-módulos finitos).

O R-módulo profinito livre sobre X existe e é único a menos de isomorfismo, podendo também ser construído como o completamento do R-módulo abstrato livre sobre X (com respeito à família de submódulos U de índice finito tais que $X - U$ é finito) ou como o produto cartesiano de cópias de R indexadas pelos elementos de X. Para maiores esclarecimentos, indicamos consultar Wilson [13], Proposição 7.4.1.

Um R-módulo profinito P é dito ser *projetivo* se dado um homomorfismo sobrejetivo $\beta : M \longrightarrow N$ e um homomorfismo $\alpha : P \longrightarrow N$, para quaisquer

R-módulos M e N, existe um homomorfismo $\gamma : M \longrightarrow N$ tal que $\beta\gamma = \alpha$, isto é, se o seguinte diagrama comuta:



Todo módulo profinito livre é projetivo (Wilson [13], Proposição 7.4.2). Os módulos profinitos projetivos são precisamente os "somando diretos" dos módulos profinitos livres (Wilson [13], Proposição 7.4.7). Quando o anel profinito é *local*, ou seja, se possui um único ideal à direita aberto maximal, temos que módulos profinitos livres e projetivos coincidem (Wilson [13], Proposição 7.5.1).

3.8 A Álgebra de Grupo Completa

Álgebra de Grupo Completa

Seja R um anel comutativo. Uma *R-álgebra* é um anel Λ com um homomorfismo de anéis de R no centro de Λ. Escreveremos $r\lambda$ para o produto da imagem de $r \in R$ e $\lambda \in \Lambda$.

Uma aplicação $\theta : \Lambda \longrightarrow E$, onde E é uma R-álgebra, é dita um *homomorfismo de R-álgebras* se é um homomorfismo de anéis e satisfaz $\theta(r\lambda) = r\theta(\lambda)$, para todo $r \in R$ e $\lambda \in \Lambda$. Qualquer anel contendo R no seu centro pode ser considerado como uma R-álgebra.

Seja G um grupo. Denotamos por RG a álgebra de grupo de G sobre R, ou seja, RG é o conjunto formado por todas as somas formais $\sum_{g\in G} r_g g$, tais que $r_g \in R$ e $r_g \neq 0$ somente para um número finito de elementos de $g \in G$, munido da soma usual e produto induzido pela operação de G. Identificamos R e G com suas imagens naturais em RG. A álgebra de grupo é caracterizada pela seguinte propriedade universal: cada homomorfismo de grupos de G no grupo das unidades E^X de uma R-álgebra E estende-se unicamente a um homomorfismo de R-álgebras de RG em E.

Suponha agora que R é um anel profinito comutativo. Uma *R-álgebra profinita* é um anel profinito Λ com um homomorfismo contínuo de R no

centro de Λ. Note que o centro de Λ é um subanel fechado de Λ, já que é a interseção dos núcleos de homomorfismos da forma $\varphi_\lambda : x \longmapsto x\lambda - \lambda x$, para todo $\lambda \in \Lambda$.

Vamos destacar agora a seguinte definição.

Seja G um grupo profinito. A *álgebra de grupo completa* $[\![RG]\!]$ de G sobre R é uma R-álgebra profinita que contém G no seu grupo de unidades e que satisfaz a seguinte propriedade universal: qualquer homomorfismo contínuo de G no grupo das unidades E^X de uma R-álgebra profinita E estende-se a um único homomorfismo contínuo de R-álgebras de $[\![RG]\!]$ em E.

Temos que E^X é um grupo profinito com a topologia subespaço em E (Wilson [13], Proposição 7.1.1). A álgebra de grupo completa $[\![RG]\!]$ também pode ser dada segundo o limite inverso

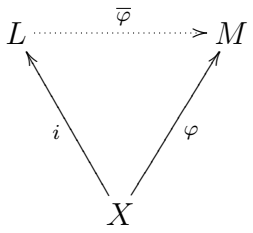
$$[\![RG]\!] = \varprojlim_{N \in \mathscr{U}} R(G/N)$$

onde $\mathscr{U}$ é a coleção de todos os subgrupos normais abertos de G. Temos que G mergulha em $[\![RG]\!]$ via a aplicação $g \longmapsto \prod_{N \in \mathscr{U}} gN$ que estende-se a um mergulho de RG em $[\![RG]\!]$ como uma subálgebra densa em $[\![RG]\!]$ (Wilson [13], Proposição 7.1.2).

Módulos Profinitos Topologicamente Livres

Consideremos agora a álgebra de grupo abstrata RG de um grupo G sobre um anel comutativo R (que é um R-módulo abstrato livre no conjunto G). Temos que a correspondente propriedade universal não vale para a álgebra de grupo completa $[\![RG]\!]$ de um grupo profinito G sobre um anel comutativo R. De fato, em geral a inclusão de G em $[\![RG]\!]$ não é 0-convergente. Isto ocorre apenas se G é finito. Para contornar este problema, apresentaremos agora a seguinte definição.

Sejam R um anel profinito, X um subconjunto fechado de um R-módulo profinito L e $i : X \longrightarrow L$ a aplicação inclusão. Então L é dito um *R-modulo profinito topologicamente livre* com base X se a seguinte propriedade universal é satisfeita: para qualquer aplicação contínua φ de X em um R-módulo profinito M existe um único homomorfismo contínuo de R-módulos $\overline{\varphi} : L \longrightarrow M$ tal que $\overline{\varphi} i = \varphi$, isto é, o seguinte diagrama comuta:



Observe que se X é finito, então as definições de módulo profinito livre e de módulo profinito topologicamente livre coincidem. Observe também que X é o limite inverso de suas imagens nos quocientes de L módulo os submódulos abertos. Portanto, X é um espaço profinito. Neste caso, seja $X = \varprojlim X_i$, onde cada X_i é um conjunto finito. Se as aplicações $\psi_i : X \longrightarrow X_i$ são sobrejetivas, então o R-módulo profinito topologicamente livre $[\![RX]\!]$ pode também ser construído, a menos de isomorfismo, como o limite inverso

$$[\![RX]\!] = \varprojlim RX_i$$

dos R-módulos profinitos livres RX_i, e a aplicação canônica de $[\![RX]\!]$ em RX_i é o único homomorfismo de R-módulos estendendo ψ_i.

G-Módulos

Seja G um grupo pro-p. Um *G-módulo pro-p (à direita)* é um grupo pro-p abeliano M com uma ação contínua $\mathbb{Z}_p$-linear $M \times G \longrightarrow M$ que satisfaz as propriedades de um módulo abstrato com coeficientes em G.

Proposição 3.8.1 *Seja M um grupo pro-p abeliano e considere $\mathbb{Z}$ identificado com sua imagem no seu completamento pro-p $\mathbb{Z}_p$. Fixe $m \in M$. A aplicação $n \longmapsto mn = \underbrace{m + \cdots + m}_{n}$ de $\mathbb{Z}$ em M é um homomorfismo contínuo. Logo, pela propriedade universal do completamento pro-p, ela se estende a um único homomorfismo contínuo $\theta_m : \mathbb{Z}_p \longrightarrow M$. Então a aplicação $\theta : M \times \mathbb{Z}_p \longrightarrow M$ definida por $(m, z) \longmapsto mz = \theta_m(z)$ é contínua. Se $m, m' \in M$ e $z, z' \in \mathbb{Z}_p$, então $m(z + z') = mz + mz'$, $mz(z') = m(zz')$ e $(m + m')z = mz + m'z$.*

Demonstração: Consultar Wilson [13], Proposição 1.5.3. ∎

A proposição anterior esclarece que todo grupo pro-p abeliano M tem uma ação natural contínua e linear de $\mathbb{Z}_p$.

Se M é um $[\![\mathbb{Z}_pG]\!]$-módulo pro-p, então M é um G-módulo pro-p, já que $\mathbb{Z}_pG$ mergulha em $[\![\mathbb{Z}_pG]\!]$. Reciprocamente, se M é um G-módulo pro-p, então M tem uma estrutura natural de $[\![\mathbb{Z}_pG]\!]$-módulo pro-p, em que a aplicação $M \times [\![\mathbb{Z}_pG]\!] \longrightarrow M$ estende $MG \longrightarrow M$ e os $[\![\mathbb{Z}_pG]\!]$-submódulos fechados de M são exatamente os G-submódulos fechados de M. Para maiores informações, indicamos consultar Wilson [13], Proposição 7.2.4. Assim, a categoria dos $[\![\mathbb{Z}_pG]\!]$-módulos pro-p e a categoria dos G-módulos pro-p coincidem.

Capítulo 4

O Teorema Principal - Caso Pro-p

Neste capítulo, apresentamos a demonstração do Teorema Principal (Caso Pro-p) dada por John S. Wilson em [15].

Teorema Principal (Caso Pro-p) Seja G um grupo pro-p que tem apresentação (como grupo pro-p) com n geradores $x_1, x_2, \ldots, x_n$ e m relações $r_1, r_2, \ldots, r_m$, onde $n > m$, e seja Y um conjunto qualquer de geradores topológicos de G. Então existem $n - m$ elementos de Y que geram livremente um subgrupo pro-p livre de G.

Essencialmente, a estrutura da prova vista no Teorema Principal (Caso Abstrato) será preservada. Todavia, lançamos nova luz sobre alguns argumentos. Agora, todos os subgrupos serão entendidos como subgrupos fechados, todas as aplicações deverão ser aplicações contínuas, e os módulos serão módulos sobre a álgebra de grupo completa $[\![\mathbb{Z}_p G]\!]$ de G sobre $\mathbb{Z}_p$. Essas modificações fazem-se necessárias pois precisamos garantir que, do ponto de vista topológico, ocorra o fechamento das estruturas aqui citadas.

Antes disso, apresentamos outra demonstração do Teorema Principal (Caso Abstrato) dada por John S. Wilson em [14], onde é assumido o Caso Pro-p dado originalmente por Romanovskii em [11]. Utilizamos também o Completamento Pro-p, introduzido na Seção 3.4.

4.1 Prova do Teorema Via Completamento Pro-p

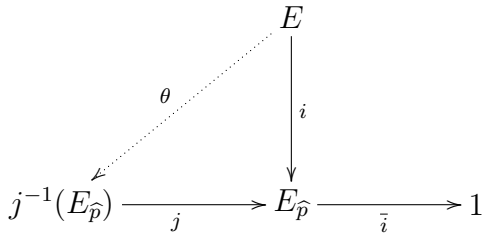
Teorema Principal (Caso Abstrato) Seja G um grupo que tem apresentação com n geradores $x_1, x_2, \ldots, x_n$ e m relações $r_1, r_2, \ldots, r_m$, onde $n > m$, e seja Y um conjunto qualquer de geradores de G. Então existem $n - m$ elementos de Y que geram livremente um subgrupo livre de G.

Demonstração: Considere $(x_1, x_2, \ldots, x_n \mid r_1, r_2, \ldots, r_m)$ uma apresentação de G, onde $m > n$. Então $(x_1, x_2, \ldots, x_n \mid r_1, r_2, \ldots, r_m)$ é também uma apresentação na categoria dos grupos pro-p para o complemento pro-p $G_{\widehat{p}}$ de G, conforme a Proposição 3.6.2.

Seja Y um conjunto qualquer de geradores de G. Considerando a aplicação $j : G \longrightarrow G_{\widehat{p}}$ dada na Proposição 3.4.1, temos que $\Gamma = j(Y)$ gera $G_{\widehat{p}}$ como grupo pro-p. Assim, como $G_{\widehat{p}}$ é um grupo pro-p com n geradores m relações, onde $m < n$, pelo Caso Pro-p do Teorema Principal, Γ contém um subconjunto Γ_1 com $\mid \Gamma_1 \mid = n - m$ que gera livremente um subgrupo pro-p livre E_Γ de $G_{\widehat{p}}$.

Considere em Y um subconjunto Y_1 satisfazendo $\mid Y_1 \mid = \mid \Gamma_1 \mid$ e $j(Y_1) = \Gamma_1$. Neste caso, temos que E_Γ é o complemento pro-p do grupo livre abstrato E sobre Y_1, isto é, $E_\Gamma = E_{\widehat{p}}$.

Uma vez que a aplicação do grupo livre abstrato E com base Y_1 no grupo pro-p livre com base Y_1 (que coincide com $E_{\widehat{p}}$) é injetiva (Proposição 3.5.5), segue que Y_1 gera um subgrupo livre abstrato de G. De fato, seja $i : E \longrightarrow E_{\widehat{p}}$ a aplicação canônica, e considere $j^{-1}(E_{\widehat{p}}) \leqslant G$. Pela propriedade projetiva dos grupos livres (Proposição 1.1.6), existe $\theta : E \longrightarrow j^{-1}(E_{\widehat{p}})$ tal que o seguinte diagrama comuta.



Neste contexto, como i é injetiva, temos que θ também é injetiva, e isto conclui a demonstração. ∎

4.2 Modificações Para o Caso Pro-p

Para introduzir as modificações com respeito à prova do Teorema Principal (Caso Abstrato) dada na Seção 2.3, vamos mostrar, de acordo com o lema a seguir, que um grupo pro-p pode ser mergulhado em uma extensão split. Para tanto, a nossa principal ferramenta será o Teorema de Kaloujnine-Krasner (consultar Rotman [12], Teorema 7.37) para grupos finitos, o qual atesta que se um grupo G é uma extensão de grupos, digamos H e K, então G é um subgrupo do produto entrelaçado $H \wr K$ (isto é, um subgrupo do produto semidireto $K \ltimes B$, onde B é o produto direto de $\mid K \mid$ cópias de H).

Lema 4.2.1 *Sejam G um grupo pro-p, A um subgrupo abeliano normal (fechado) de G e $H = G/A$. Então G pode ser imerso em um grupo pro-p $H \ltimes B$, com B abeliano, de modo que a composta da imersão com a aplicação $H \ltimes B \longrightarrow H$ é a aplicação quociente $G \longrightarrow H$.*

Demonstração: Seja $(N_\lambda)_{\lambda \in \Lambda}$ uma família de subgrupos normais abertos de G tal que $\bigcap_{\lambda \in \Lambda} N_\lambda = 1$. Para cada $\lambda \in \Lambda$, G/N_λ é uma extensão finita de G/AN_λ por AN_λ/N_λ. Logo, o Teorema de Kaloujnine-Krasner para grupos finitos nos dá imersões

$$j_\lambda : G/N_\lambda \longrightarrow (G/AN_\lambda) \wr (AN_\lambda/N_\lambda).$$

Observe que o produto entrelaçado dado acima é o produto semidireto $(G/AN_\lambda) \ltimes B_\lambda$, onde B_λ é o produto de $\mid G/AN_\lambda \mid$ cópias de AN_λ/N_λ. Observe também que B_λ é um p-grupo abeliano.

Assim, é suficiente considerar o subgrupo de $\prod_{\lambda \in \Lambda}(G/AN_\lambda \ltimes B_\lambda)$ gerado pelo subgrupo normal abeliano $\prod_{\lambda \in \Lambda} B_\lambda$ e pela imagem de G via a aplicação $\varphi : g \longmapsto (j_\lambda(gN_\lambda))$. ∎

Estabelecemos o análogo pro-p do Lema 2.1.2 conforme o lema a seguir.

Lema 4.2.2 *Sejam F um grupo pro-p livre sobre $\{x_1, x_2, \ldots, x_n\}$, R um subgrupo normal (fechado) de F e $H = F/R$. Seja M um $[\![\mathbb{Z}_p H]\!]$-módulo pro-p e $t_1, t_2, \ldots, t_n \in M$.*

(a) A correspondência

$$x_i \longmapsto \begin{pmatrix} x_i R & 0 \\ t_i & 1 \end{pmatrix}$$

determina um homomorfismo contínuo

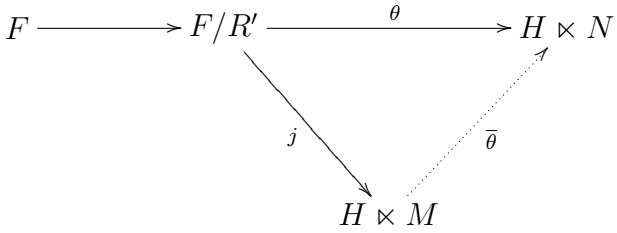
$$\mu : F \longrightarrow \begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix}.$$

(b) $R' \leqslant ker\mu \leqslant R$.

(c) *Seja* j *a aplicação de* F/R' *em* $\begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix}$ *induzida por* μ. *Se* M *é um* $[\![\mathbb{Z}_p H]\!]$*-módulo pro-p livre sobre* $\{t_1, t_2, \ldots, t_n\}$, *então* j *é injetiva.*

Demonstração: Os ítens (a) e (b) seguem por analogia ao que foi apresentado no contexto dos grupos abstratos (Lema 2.1.2).

Para provar (c), utilizaremos a imersão dada no Lema 4.2.1, que será denotada por θ, mantendo-nos atentos às seguintes modificações com respeito à notação: por G vamos considerar F/R', por A vamos considerar R/R', e por H vamos considerar então F/R. Assim, F/R' está imerso no grupo pro-p $H \ltimes N$, onde N é um grupo pro-p abeliano, e podemos então considerar o seguinte diagrama.



Neste ponto, nossa estratégia é completar o diagrama acima com uma aplicação $\overline{\theta} : H \ltimes M \longrightarrow H \ltimes N$ de tal forma que $\overline{\theta} j = \theta$. Como θ é injetiva, segue que j também é injetiva, o que completa a prova do item (c). O argumento seguirá *lipsis litteris* ao Lema 2.1.2. De fato, seja $v_i \in N$ dado por

$$\theta(x_i R') = \begin{pmatrix} x_i R & 0 \\ v_i & 1 \end{pmatrix}$$

e considere $\kappa : M \longrightarrow N$ como sendo o único $[\![\mathbb{Z}_p H]\!]$-homomorfismo definido pela correspondência $t_i \longmapsto v_i$, que é contínuo em virtude do Lema 3.7.2. Então

$$\overline{\theta} : \begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} H & 0 \\ N & 1 \end{pmatrix} \quad \text{dada por} \quad \begin{pmatrix} h & 0 \\ m & 1 \end{pmatrix} \longmapsto \begin{pmatrix} h & 0 \\ \kappa(m) & 1 \end{pmatrix}$$

é um homomorfismo contínuo e possui a propriedade que desejamos. ∎

Consoante a um profundo resultado dado por Romanovskii em [11], e que enunciaremos conforme a Proposição 4.2.4 a seguir, o leitor será capaz de perceber que não podemos usar simplesmente grupos ordenáveis como foi feito na Seção 2.3 pois precisamos, por exemplo, garantir que $U \cap M$ é fechado no $[\![\mathbb{Z}_p G]\!]$-módulo M. Para contornar este problema, apresentaremos agora a seguinte definição.

Uma *filtração*

$$A = A_{(1)} \geqslant \cdots \geqslant A_{(n)} \geqslant \cdots$$

de subgrupos normais de um grupo profinito com $\bigcap A_{(i)} = 1$ é dita *convergente* se cada vizinhança de 1 contém algum subgrupo $A_{(i)}$. Denotaremos por $\mathscr{N}$ a classe de todos os grupos pro-p finitamente gerados com uma filtração convergente com fatores centrais livres de torção.

Observação 4.2.3 *Seja G um grupo pro-p finitamente gerado, e considere K como sendo a interseção dos núcleos de todos os homomorfismos φ_λ de G em grupos pro-p nilpotentes livres de torção G_λ, isto é, $K = \ker \varphi$, onde*

$$\begin{aligned} \varphi : G &\longrightarrow \prod G_\lambda \\ g &\longmapsto \varphi(g) = (\varphi_\lambda(g)). \end{aligned}$$

Então $G/K \in \mathscr{N}$.

O próximo resultado, devido à Romanovskii, é o ponto central para estabelecer a analogia entre a demonstração apresentada na Seção 2.3 e a que apresentaremos na próximo seção. Utilizando a classe de grupos pro-p $\mathscr{N}$ definida acima, a proposição a seguir determina que se $H \in \mathscr{N}$, então existe um anel com divisão Q contendo a álgebra de grupo completa $[\![\mathbb{Z}_p H]\!]$ e a extensão $H \ltimes M \in \mathscr{N}$, onde M é o $\mathbb{Z}_p$-módulo como descrito abaixo.

Proposição 4.2.4 *Seja H um grupo pro-p em $\mathscr{N}$ e seja L a álgebra de grupo completa $[\![\mathbb{Z}_p H]\!]$. Então existe uma filtração $(H_{(i)})_{i \geqslant 1}$ com fatores centrais livres de torção e um anel com divisão $Q \geqslant L$ tais que as seguintes afirmações ocorrem: se $n \geqslant 1$ e U é um subespaço do espaço vetorial $Q^{(n)}$, então*

(i) $U \cap L^{(n)}$ é fechado em $L^{(n)}$.

(ii) O $\mathbb{Z}_p$-módulo $M = L^{(n)}/(U \cap L^{(n)})$ tem uma filtração $(M_j)_{j\geqslant 1}$ de submódulos fechados tais que $[M_j, H_i] \leqslant M_{i+j}$ e M_j/M_{j+1} é um grupo livre de torção para todo i, j.

(iii) $(H_iM_i)_{i\geqslant 1}$ é uma filtração de $H \ltimes M$ com fatores centrais livres de torção, e então $H \ltimes M \in \mathscr{N}$.

Demonstração: Consultar Romanovskii [11], Proposição 7. ∎

4.3 Prova do Teorema

Nesta seção, apresentamos a demonstração do Teorema Principal (Caso Pro-p) dada por John S. Wilson em [15], reproduzindo os argumentos que foram utilizados na demonstração dada na Seção 2.3 e acrescentando as modificações sugeridas na Seção 4.2.

Teorema Principal (Caso Pro-p) Seja G um grupo pro-p que tem apresentação (como grupo pro-p) com n geradores $x_1, x_2, \ldots, x_n$ e m relações $r_1, r_2, \ldots, r_m$, onde $n > m$, e seja Y um conjunto qualquer de geradores topológicos de G. Então existem $n - m$ elementos de Y que geram livremente um subgrupo pro-p livre de G.

Demonstração: Considere $F/R \cong G$ uma apresentação de G, onde F é um grupo pro-p livre gerado livremente por $x_1, x_2, \ldots, x_n$, e cujo núcleo R pode ser gerado como subgrupo normal pelo conjunto R constituído dos elementos $r_1, r_2, \ldots, r_m$, onde $m < n$.

Seja S/R a interseção dos núcleos de todos os homomorfismos de F/R em grupos pro-p nilpotentes livres de torção (como na Observação 4.2.3). Assim, $F/S \in \mathscr{N}$ e S é o menor subgrupo normal de F contendo R com esta propriedade. Vamos denotar $\overline{G} = F/S$.

Sejam agora Q um anel com divisão contendo $[\![\mathbb{Z}_p\overline{G}]\!]$ (como na Proposição 4.2.4), V o espaço vetorial (à direita) sobre Q com base $\{t_1, t_2, \ldots, t_n\}$ e M o $[\![\mathbb{Z}_p\overline{G}]\!]$-módulo pro-$p$ gerado por $t_1, t_2, \ldots, t_n$. Temos que M é um $[\![\mathbb{Z}_p\overline{G}]\!]$-módulo pro-$p$ livre com base livre $\{t_1, t_2, \ldots, t_n\}$.

Aplicando o Lema 4.2.2, defina o homomorfismo (contínuo)

$$\mu : F \longrightarrow \begin{pmatrix} \overline{G} & 0 \\ M & 1 \end{pmatrix} \quad \text{induzido por} \quad x_i \longmapsto \begin{pmatrix} x_iS & 0 \\ t_i & 1 \end{pmatrix}$$

e considere a derivação $\delta : F \longrightarrow M$ que leva $f \in F$ na componente em M de $\mu(f)$, conforme indicado abaixo

$$\mu(f) \longmapsto \begin{pmatrix} fS & 0 \\ \delta f & 1 \end{pmatrix}.$$

Seja U o subespaço de V gerado por $\delta r_1, \delta r_2, \ldots, \delta r_m$ e considere o espaço quociente $W = V/U$. Temos que $dim W = r \geq n - m$. Além disso, considere

$$\overline{\delta} : F \longrightarrow (M + U)/U$$

uma derivação (contínua) induzida por δ. Como $\{t_1, t_2, \ldots, t_n\}$ é uma base de V e $\delta(x_i) = t_i$ para todo $i = 1, 2, \ldots, n$, então $\{\overline{\delta}x_1, \overline{\delta}x_2, \ldots, \overline{\delta}x_n\}$ gera W.

Considere agora o homomorfismo contínuo

$$\varphi : \begin{pmatrix} \overline{G} & 0 \\ M & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} \overline{G} & 0 \\ \frac{M+U}{U} & 1 \end{pmatrix}$$

e defina

$$\psi : F \longrightarrow \begin{pmatrix} \overline{G} & 0 \\ \frac{M+U}{U} & 1 \end{pmatrix}$$

como sendo a composição $\psi = \varphi\theta$.

$$F \xrightarrow{\theta} \overline{G} \ltimes M \xrightarrow{\varphi} \overline{G} \ltimes (M + U)/U$$
$$\psi$$

Pela Proposição 4.2.4, temos que $\overline{G} \ltimes (M + U)/U \in \mathscr{N}$, e portanto $F/ker\psi \in \mathscr{N}$. Por um lado, observando agora que $ker\psi \leqslant S$ e que, por outro lado, para todo $i = 1, 2, \ldots, m$, temos $r_i S = S$ (pois $R \leqslant S$) e $\overline{\delta} r_i = 0$ (pois $U = \langle \delta r_1, \delta r_2, \ldots, \delta r_n \rangle$), então $R \leqslant ker\psi$. Pela minimalidade de S, vem $S = ker\psi$. Neste caso, ψ induz uma imersão

$$j : \overline{G} \longrightarrow \begin{pmatrix} \overline{G} & 0 \\ W & 1 \end{pmatrix}.$$

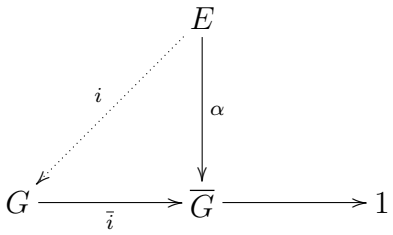
Seja Y um conjunto gerador de F/R. Com argumento análogo ao que foi apresentado na Seção 2.3, temos que $W = \langle \overline{\delta} Y \rangle$.

Considere então $\{\overline{\delta}y_1, \overline{\delta}y_2, \ldots, \overline{\delta}y_r\}$ uma base de W, e E o grupo pro-p livre com base livre $\{y_1, y_2, \ldots, y_r\}$. Defina o homomorfismo $\alpha : E \longrightarrow \overline{G}$ por $y_i \longmapsto y_i S$ e seja $N = ker\alpha$.

Pelo Lema 4.2.2, o homomorfismo

$$\beta : y_i \longmapsto \begin{pmatrix} y_i S & 0 \\ \overline{\delta}y_i & 1 \end{pmatrix}$$

definido como sendo a composição $\beta = j\alpha$ tem núcleo N'. Mas j é injetiva, e portanto devemos ter $N = N'$. Todavia, N é subgrupo de um grupo pro-p livre; logo, N é pro-p livre e devemos ter $N = 1$. Assim, E é livre módulo S. Pela propriedade p-projetiva dos grupos pro-p livres (Proposiçao 3.5.3), existe uma aplicação $i : E \longrightarrow G$ tal que o seguinte diagrama comuta, onde $\overline{i} : G \longrightarrow \overline{G}$ é o epimorfismo natural.



Neste contexto, como α é injetiva, temos que i também é injetiva, e isto conclui a demonstração. ■

Bibliografia

[1] DE CORNULIER, Y.; *Finitely Presented Wreath Product and Double Coset Decompositions.* Geom. Dedicata 102 (2006), 89 − 108.

[2] ISAACS, I. M.; *Algebra: A Graduate Course.* Graduate Studies in Mathematics. American Mathematical Society, 2009.

[3] JOHNSON, D. L.; *Presentation of Groups.* Second Edition. London Mathematical Society Student Texts 15. Cambridge University Press, 1997.

[4] KALOUJNINE, L. et M. KRASNER; *Produit Complet des Groupes de Permutations et Problème d'Extension de Groupes.* III. Acta Sci. Math. Szeged 14 (1951), 69 − 82.

[5] MAGNUS, W.; *Über Diskontinuierliche Gruppen Mit Einer Definierenden Relation.* (Der Freiheitssatz), J. Reine Angew. Math. 163 (1930), 141 − 165.

[6] MUNKRES, J. R.; *Topology.* Upper Saddle River, NJ: Pearson Education International - Prentice Hall, 2000.

[7] NEUMANN, B. H.; *On Ordered Division Rings.* Trans. Amer. Math. Soc. 66 (1949), 202 − 252.

[8] RIBES, L.; ZALESSKII, P.; *Profinite Groups.* Second Edition. Springer, Berlin, 2010.

[9] ROBINSON, D. J. S.; *A Course in the Theory of Groups.* Springer-Verlag New York Inc, New York, 1982.

[10] ROMANOVSKII, N. S.; *Free subgroups of Finitely Presented Groups.* Algebra Logic 16 (1978), 62 − 68.

[11] ROMANOVSKII, N. S.; *A Generalized Theorem on Freedom For Pro-p Groups.* Siberian Math. J. 27 (1986), 267 − 280.

[12] ROTMAN, J. J.; *An Introdution to the Theory of Groups.* Fourth Edition. Springer-Verlag New York, 1995.

[13] WILSON, J. S.; *Profinite Groups.* Clarendon Press, Oxford, 1998. 173 – 185.

[14] WILSON, J. S.; *On Growth of Groups With Few Relators.* Bull. London Math. Soc. 36 (2004), 1 – 2.

[15] WILSON, J. S.; *Free Subgroups in Groups With Few Relators.* L'Enseignement Mathématique (2) 56 (2010).