**Universidade de Brasília**
**Instituto de Ciências Exatas**
**Departamento de Matemática**

# Torção no Completamento Pro-finito de Grupos Livres de Torção

por

**Heisler Nadir Rangel Rodrigues**

**Brasília**
**2007**

À minha filha
*Isabela Rangel Pires Rodrigues*

# Agradecimentos

Agradeço a Deus, pois sem ele nada sou.

Agradeço a minha família, por todo apoio e incentivo nos momentos mais difíceis que passei. Em especial, à Isaura, minha esposa, por tudo.

Agradeço a todos os amigos que, de uma forma ou de outra, me incentivaram durante este trabalho.

Agradeço a minha orientadora, Aline G. S. Pinto, pela dedicação e paciência.

Agradeço a todos os meus professores de graduação. Em especial, aos professores Lineu, Helder, Hemar, Rui e Alfredo.

Agradeço aos amigos de graduação Diogo e Monique pela amizade.

Agradeço aos amigos de pós-graduação pelo companherimos e amizade. Em especial, Manuela, Ricardo, Anyelle, Tertuliano, Anderson, Porfírio, Vagner, Evander, Ivonildes.

Agradeço aos funcionários do Departamento de Matemática da UnB, que muito contribuíram para o desenvolvimento deste trabalho, em especial ao Manuel.

Finalmente, agradeço ao CNPq pelo apoio financeiro.

# RESUMO

A finalidade deste trabalho é estudar a torção no completamento pro-finito de grupos residualmente finitos e livres de torção. Consideramos os casos de grupos abelianos e grupos metabelianos, baseados em [6]. No primeiro caso, o completamento é livre de torção. No segundo, se o grupo é finitamente gerado o completamento também é livre de torção, o que não é verdade sem hipótese de ser finitamente gerado. Exibimos exemplos feitos em [3] que mostram que, sem esta última hipótese, o completamento contém um elemento de ordem finita.

# Abstract

The purpose of this work is to study the torsion in the pro-finite completion of residually finite and torsion free groups. We consider the cases of abelian groups and metabelian groups, based on [6]. In the first case, the completion is torsion free. In the second one, if the group is finitely generated the completion is also torsion free, what is not true without the finitely generation condition. We give the examples done in [3] where without the last hypothesis the completion has an element of finite order.

# CONTEÚDO

# Introdução

Neste trabalho estudamos o completamento pro-finito de grupos metabelianos. Em [2] Crawley-Boevey, Kropholler e Linnell observaram que era uma questão em aberto se o completamento pro-finito de um grupo residualmente finito e livre de torção é necessariamente livre de torção. Em tal trabalho sobre a conjectura do divisor de zero, a saber *" Se G é um grupo livre de torção e K é um corpo, então KG é um domínio"*, mostraram esta conjectura para anéis de grupos solúveis livres de torção e também o seguinte corolário *" O completamento pro-finito de grupos metabelianos por finito, finitamente gerado e livre de torção é livre de torção"*.

Evans [3], mais tarde foi o primeiro a mostrar que tais completamentos poderiam conter elementos não triviais de ordem finita. Apresentou em seu trabalho dois exemplos onde isso ocorre, que serão os Teoremas:

*Teorema 3.7. Para cada primo p, existe um grupo H livre de torção e residualmente p-grupo finito que o seu completamento pro-p contém um elemento de ordem p.*

*Teorema 3.8. Para cada primo p existe um grupo G metabeliano, enumerável, livre de torção e residualmente finito tal que seu completamento pro-finito contém um elemento de ordem p.*

Observamos que o primeiro teorema não responde a pergunta, mas dá uma idéia de que se o grupo não é finitamente gerado o completamento pro-finito poderá ter um elemento de ordem finita.

Posteriormente Lubotzky, em [7], observa que o completamento pro-finito $\widehat{G}$ pode ter

torção mesmo que $G$ seja finitamente gerado (é claro que não pode ser o grupo metabeliano enunciado em [2]). De fato, ele apresentou o seguinte teorema *"Existe um grupo $G$ finitamente gerado, residualmente finito e livre de torção, cujo completamento pro-finito contém uma cópia isomorfa de todo grupo pro-finito separável. Em particular $\widehat{G}$ contém o produto cartesiano $\prod_i F_i$, onde $F_i$ percorre todos os grupos finitos (classes de isomorfismos de grupos finitos)*". A prova do teorema não será tratada neste trabalho, mas é baseada no problema do subgrupo de congruência e algumas de suas propriedades relacionadas.

Baseado em todas estas indagações, Kropholler e Wilson em [6] estudaram alguns resultados positivos. Mostraram que não existem contra-exemplos entre os grupos abelianos por nilpotentes finitamente gerados, abelianos residualmente finitos e grupos solúveis minimax. Entretanto entre grupos nilpotentes de classe dois (necessariamente não finitamente gerado) e grupos centro por metabeliano finitamente gerado há contra-exemplo, como mostrado por Kropholler e Wilson em [6] e por Quick em [8]. Nós vamos nos restringir aos grupos abelianos residualmente finitos, abelianos por abelianos finitamente gerados, onde mostraremos:

*Teorema 3.3. Seja $G$ um grupo abeliano e residualmente finito. Então $\overline{t(G)} \supseteq t(\widehat{G})$.*

*Teorema 3.6. Se $G$ é finitamente gerado abeliano por abeliano, então $\overline{t(G)} = t(\widehat{G})$.*

Os resultados apresentados nesta dissertação estão exatamente na direção de estudar quando o completamento de grupos metabelianos residualmente finitos é livre de torção. Nossas demonstrações são baseadas em [6].

No Capítulo 1 apresentaremos as definições e os resultados sobre grupos abelianos livres, grupos abelianos finitamente gerados, grupos livres, produtos livres, produtos livres com subgrupos amalgamados, grupos p-nilpotentes e módulos. Recapturaremos também alguns resultados sobre estes grupos e demonstraremos teoremas essenciais para melhor entendermos os grupos usados no Capítulo 3, destes se destacam os teoremas:

*Teorema 1.47. Se $p$ é um primo e $F$ é um grupo livre, então $F$ é residualmente $p$-grupo finito.*

*Teorema 1.50. Seja $G$ o produto livre de dois grupos residualmente $p$-grupos finitos. Então $G$ é residualmente $p$-grupo finito.*

No Capítulo 2 apresentaremos os conceitos de limite inverso (ou projetivo) e completamento pro-$\mathcal{C}$ (onde $\mathcal{C}$ é uma classe de grupos) e provaremos um resultado interessante para grupos p-nilpotentes, que será o Teorema:

*Teorema 2.25. Seja G um grupo p-nilpotente. Então o completamento pro-p de G pode ser identificado com um p-subgrupo de Sylow do completamento pro-finito.*

Fechamos esta dissertação com o Capítulo 3, provando os resultados mencionados, onde veremos que a hipótese de um grupo ser finitamente gerado faz com que em geral o completamento pro-finito tenha torção.

# CAPÍTULO 1

# Preliminares

Descrevemos, neste capítulo, alguns pré-requisitos necessários para melhor entendermos os grupos trabalhados no Capítulo 3. Para isto, apresentaremos os conceitos de grupo abeliano livre, grupo abeliano finitamente gerado, grupo livre, produto livre, produto livre com subgrupo amalgamado, grupo p-nilpotente, módulos e também estudaremos algumas propriedades importantes referentes a estes grupos. Entre estas propriedades podemos destacar uma muito importante, encontrada em [4], que afirma que o produto livre de grupos residualmente p-grupo é residualmente p-grupo. Para módulos, se um A-módulo Noetheriano é simples, então ele é residualmente finito.

## 1.1 Grupos Abelianos

### 1.1.1 Soma Direta

Sejam $K$ um conjunto qualquer e $\{A_k : k \in K\}$ uma família de grupos abelianos.

**Definição 1.1.** *O produto direto restrito,*

$$C = \mathbf{Dr}_{k \in K} A_k,$$

*consiste do grupo formado por todos os "vetores" $(a_k)$ com k-componente $a_k$ em $A_k$, tal que $a_k = 1_k$ para quase todos os $k$, onde a operação é definida coordenada a coordenada, o elemento identidade de $C$ é $(1_k)$ e $(a_k)^{-1} = (a_k^{-1})$.*

Se os grupos $A_k$ tiver em notação aditiva, o produto direto restrito dos $A_k's$ é chamado de **Soma Direta** e denotado por $\bigoplus_{k\in K} A_k$, onde os elementos são da forma $\sum_{k\in K} a_k$.

Nas seções que se referem a grupos abelianos, nos usaremos a notação de soma direta.

**Proposição 1.2.** *Seja $\{A_k : k \in K\}$ uma família de subgrupos do grupo abeliano $G$, onde $K$ é um conjunto qualquer. Então são equivalentes:*

*a)* $G \cong \bigoplus_{k\in K} A_k$.

*b) Cada $g \in G$ tem um única expressão da forma*

$$g = \sum_{k\in K} a_k,$$

*onde $a_k \in A_k$, os $k$ são distintos, e $a_k \neq 0$ somente para um número finito de $k$.*

*c)* $G = \langle \bigcup_{k\in K} A_k \rangle$ *e, para cada $j \in K$, temos* $A_j \cap \langle \bigcup_{k\neq j} A_k \rangle = 0$.

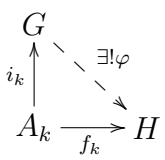
**Demonstração:** Mostraremos que *a*) implica *b*). Temos que $g = \Sigma_{k\in K} a_k$ para um número finito de $k$. Basta mostrar que esta forma é única. Suponha $g = \Sigma_{k\in K} \tilde{a_k}$. Como $G$ é grupo $-\Sigma_{k\in K}\tilde{a_k} \in G$, e então $0 = g - g = \Sigma_{k\in K} a_k - \Sigma_{k\in K}\tilde{a_k}$. Com isso,

$$\tilde{a_k} = \tilde{a_k} - 0 = \tilde{a_k} - (\tilde{a_k} - a_k) = a_k, \forall k \in K.$$

Agora *b*) implica *c*). Suponha, por contradição, que $A_j \cap \langle \bigcup_{k\neq j} A_k \rangle \neq 0$. Com isso, teremos um elemento de $G$ escrito de duas formas distintas, o que é absurdo. E como cada elemento de $G$ tem uma única expressão da forma $g = \sum_{k\in K} a_k$, $G = \langle \bigcup_{k\in K} A_k \rangle$.

Finalmente *c*) implica *a*). Definamos $\varphi : G \to \bigoplus_{k\in K} A_k$ por $\varphi(a_k) = (0, \ldots, a_k, \ldots, 0)$. Assim $\varphi$ é um epimorfismo com núcleo $\bigcap_{k\in K} A_k$, como $A_j \cap \langle \bigcup_{k\neq j} A_k \rangle = 0$, teremos $G \cong \bigoplus_{k\in K} A_k$. ■

**Teorema 1.3.** *Sejam $G$ um grupo abeliano, $\{A_k : k \in K\}$ uma família de grupos abelianos e $\{i_k : A_k \to G : k \in K\}$ uma família de homomorfismos. Então $G \cong \bigoplus_{k\in K} A_k$ se, e somente se, dado algum grupo abeliano $H$ e uma família de homomorfismos $\{f_k : A_k \to H : k \in K\}$, existe um único homomorfismo $\varphi : G \to H$ de forma que o diagrama comute para todo $k$ ($\varphi i_k = f_k$):*



**Demonstração:** Suponhamos $G \cong \bigoplus_{k\in K} A_k$. Defina $i_k : A_k \hookrightarrow G$ pela inclusão. Pelo Proposição 1.2, cada $g \in G$ tem uma única expressão da forma $g = \Sigma_{k\in K} a_k$. Defina $\psi : G \to H$ por $\psi(g) = \Sigma_{k\in K} f_k(a_k)$, com isso, $\psi$ é um homomorfismo e faz o seguinte diagrama comutar para todo $k$:

$$\begin{array}{ccc} G & & \\ {\scriptstyle i_k}\uparrow & \searrow^{\psi} & \\ A_k & \xrightarrow[f_k]{} & H. \end{array}$$

Supondo outra $\bar{\psi}$ com a mesma propriedade ($\bar{\psi} i_k = f_k$), teremos $\psi = \bar{\psi}$, pois $\langle \bigcup_{k\in K} i_k(A_k) \rangle = G$ .

Agora a recíproca. Troque $H$ por $\bigoplus_{k\in K} A_k$ e $f_k$ por $i_k$. Por hipótese, existe um única aplicação $\varphi : G \to \bigoplus_{k\in K} A_k$. Similarmente, façamos a troca de $G$ por $\bigoplus_{k\in K} A_k$ no diagrama, e $H = G$. Por hipótese existe uma única aplicação $\psi : \bigoplus_{k\in K} A_k \to G$. Assim, temos o seguinte diagrama:

$$\begin{array}{ccc} & & G \\ & {\scriptstyle i_k}\nearrow & {\scriptstyle \psi}\uparrow\downarrow{\scriptstyle \varphi} \\ A_i & \xrightarrow[i_k]{} & \bigoplus_{k\in K} A_k \end{array}$$

Finalmente, vamos mostrar que $\psi\varphi$ e $\varphi\psi$ são identidades. De fato, pois $\psi\varphi$ e $1_G$ fazem o digrama comutar

$$\begin{array}{ccc} G & & \\ {\scriptstyle i_k}\uparrow & \searrow^{1_G} & \\ A_k & \xrightarrow[i_k]{} & G \end{array}$$

e então $\psi\varphi = 1_G$. Analogamente temos que $\varphi\psi = 1_{\oplus_{k\in K} A_k}$. ■

### 1.1.2 Grupos Abelianos Livres

**Definição 1.4.** *Um grupo abeliano $F$ é abeliano livre se é uma soma direta de grupos cíclicos infinitos. Mais precisamente, existe um subconjunto $X \subset F$ de elementos de ordem infinita, chamada de base de $F$, com $F = \bigoplus_{x\in X} \langle x \rangle$, isto é, $F \cong \bigoplus \mathbb{Z}$.*

Admitimos a possibilidade $X = \varnothing$, o que resulta em $F = 0$. Notemos que, se um grupo $G$ é uma soma direta de grupos cíclicos infinitos, ele é abeliano livre.

**Proposição 1.5.** *Se $F$ é um grupo abeliano livre em $X$, cada elemento $0 \neq u \in F$ tem uma única expressão da forma $u = \Sigma m_x x$, onde $m_x \in \mathbb{Z}$, e $m_x \neq 0$ somente para um número finito de $x$.*

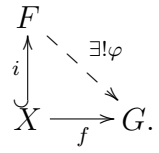
**Demonstração:** Segue da Proposição 1.2. ■

Se $X$ é finito e tem $n$ elementos, dizemos que $F$ tem posto $n$.

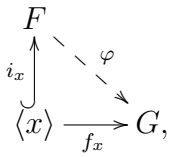
**Definição 1.6.** *Sejam $F$ e $G$ abelianos livres em $\{x_i, i \in I\}$ e $\{y_j, j \in J\}$, respectivamente. Então $F$ e $G$ têm o mesmo posto se $I$ e $J$ têm o mesmo número de elementos.*

**Definição 1.7.** *A base de um grupo abeliano livre $F$ é chamada de um conjunto livre de geradores de $F$.*

**Teorema 1.8.** *Sejam $F$ um grupo abeliano livre com base $X$, $G$ um grupo abeliano arbitrário e $f : X \longrightarrow G$ alguma função. Então existe um único homomorfismo $\varphi : F \longrightarrow G$ tal que $\varphi(x) = f(x)$, para todo $x \in X$.*




**Demonstração:** Se $u \in F$, então há uma única expressão $u = \Sigma m_x x$. Defina $f_x : \langle x \rangle \longrightarrow G$ por $f_x(mx) = mf(x)$. Temos que $f_x$ é um homomorfismo para todo $x \in X$. Como $\langle x \rangle \leq F$ e $F = \bigoplus_{x \in X} \langle x \rangle$ temos, pelo Teorema 1.3, o seguinte diagrama:




onde $i_x$ é a aplicação inclusão. Assim $\varphi$ estende cada $f_x$, logo estende $f$, pois $f(x) = f_x(x) = \varphi(i_x(x)) = \varphi(x)$. ■

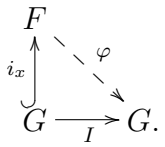
**Corolário 1.9.** *Cada grupo abeliano $G$ é um quociente de um grupo abeliano livre.*

**Demonstração:** Seja $X$ um conjunto qualquer. Afirmamos que existe um grupo abeliano livre $F$ que tem $X$ como base.

Se $X$ é um conjunto que tem $x$ como um único elemento, podemos construir o grupo cíclico infinito $\langle x \rangle$ que tem $x$ como gerador, assim temos um grupo abeliano livre.

Se $X$ é um conjunto com infinitos elementos distintos, teremos $X = \{x_k : k \in K\}$ onde cada $x_k$ gerará um grupo cíclico infinito $\langle x_k \rangle$. Com isso fazemos $F = \bigoplus \langle x_k \rangle$, portanto temos um grupo abeliano livre $F$ com base $X$.

Seja então $F$ um grupo abeliano livre com base $G$, onde $G$ é um grupo abeliano qualquer. Assim, a aplicação identidade $I : G \longrightarrow G$ nos dá o seguinte diagrama:




Pelo Teorema 1.8, $\varphi$ é única tal que $\varphi(g) = I(g)$, com isso $\varphi$ é sobrejetiva. Então $F/Ker(\varphi) = G$. ■

**Teorema 1.10.** *Sejam $F = \bigoplus_{x \in X} \langle x \rangle$ e $G = \bigoplus_{y \in Y} \langle y \rangle$ grupos abelianos livres de posto finito. Então $F \cong G$ se, e somente se, $|X| = |Y|$, onde $X$ e $Y$ são finitos.*

**Demonstração:** Suponhamos $F \cong G$. Temos que $F \cong \bigoplus_{x \in X} \mathbb{Z}_x \subset \bigoplus_{x \in X} \mathbb{Q}_x = V$, onde $V$ é um espaço de vetores sobre $\mathbb{Q}$. Similarmente, $G \cong \bigoplus_{y \in Y} \mathbb{Z}_y \subset \bigoplus_{y \in Y} \mathbb{Q}_y = W$, onde $W$ é um espaço de vetores sobre $\mathbb{Q}$.

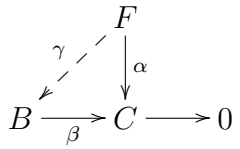
Portanto o isomorfismo $f : F \longrightarrow G$ induz a função $\tilde{f} : V \longrightarrow W$, definida por $\tilde{f}(\Sigma q_i x) = \Sigma q_i f(x)$ onde $q_i \in \mathbb{Q}$ e $\langle x \rangle = \mathbb{Z}_x$. Assim, $\tilde{f}$ é um isomorfismo entre $V$ e $W$, portanto $V$ e $W$ têm a mesma dimensão. Então $|X| = |Y|$.

Agora a recíproca. Como $|X| = |Y|$, existe uma bijeção $f : X \longrightarrow Y \subset G$, que podemos considerar $f : X \longrightarrow G$. Já que $F$ é livre com base $X$, existe um único homomorfismo $\varphi : F \longrightarrow G$ estendendo $f$. Analogamente, existe um único homomorfismo $\psi : G \longrightarrow F$ estendendo $f^{-1} : Y \longrightarrow X$. A composição $\psi\varphi : F \longrightarrow F$ é um homomorfismo que fixa $X$ ponto a ponto, isto é, $\psi\varphi$ estende a função inclusão $i : X \hookrightarrow F$. Mas o homomorfismo identidade $1_F$ também estende $i$, e então, pela unicidade da extensão, temos que $\psi\varphi = 1_F$. Da mesma forma, concluímos que $\varphi\psi = 1_G$, e portanto $\varphi : F \longrightarrow G$ é um isomorfismo. ■

Observamos que o teorema acima, também vale para grupos abelianos de posto infinito, com demonstração similar.

**Teorema 1.11 (Propriedade Projetiva).** *Seja $\beta : B \to C$ um homomorfismo sobrejetor de grupos abelianos. Se $F$ é um grupo abeliano livre e $\alpha : F \to C$ é um homomorfismo, então*

*existe um homomorfismo $\gamma : F \to B$ de maneira que o diagrama comute ($\beta\gamma = \alpha$):*

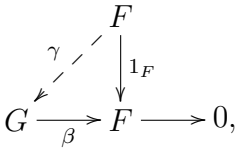


**Demonstração:** Seja $X$ uma base de $F$. Para cada $x \in X$, existe um elemento $b_x \in B$ com $\beta(b_x) = \alpha(x)$, pois $\alpha(x) \in C$ e $\beta$ é sobrejetiva.

Portanto, temos a função $f : X \to B$ definida por $f(x) = b_x$. Pelo Teorema 1.8, existe um único homomorfismo $\gamma : F \to B$ com $\gamma(x) = b_x$ para todo $x \in X$. Assim, temos que $\beta\gamma(x) = \beta(b_x) = \alpha(x)$. ■

**Corolário 1.12.** *Se $H \leq G$ e $G/H$ é abeliano livre, então $H$ é um somando direto de $G$, isto é, $G = H \oplus K$, onde $K \leq G$ e $K \cong G/H$.*

**Demonstração:** Sejam $F = G/H$ e $\beta : G \to F$ a aplicação natural. Considere o diagrama:



onde $1_F$ é a aplicação identidade. Como $F$ tem a propriedade projetiva, existe um homomorfismo $\gamma : F \to G$ com $\beta\gamma = 1_F$, isso implica que $\gamma$ é injetiva. Seja $K = Im(\gamma)$, logo temos $F/Ker(\gamma) \cong K$, então $F \cong K$.

Agora definamos $H = Ker(\beta)$ e vamos mostrar que $G = H \oplus K$.

(i) $Ker(\beta) \cap K = 0$: Seja $g \in Ker(\beta) \cap K$, isso implica $g \in Ker(\beta)$ e $g \in K$. Temos $\beta(g) = 0$ e existe $x \in F$ tal que $\gamma(x) = g$. Por este último temos $x = 1_F(x) = \beta\gamma(x) = \beta(g) = 0$. Então $g = \gamma(0) = 0$.

(ii) $G = Ker(\beta) + K$: Todo elemento de G pode ser escrito da forma

$$g = \underbrace{g - \gamma\beta(g)}_{\in Ker(\beta)} + \underbrace{\gamma\beta(g)}_{\in K}.$$

Com (i) e (ii) temos $G = H \oplus K$. ■

**Teorema 1.13** ([11, Teorema 10.18])**.** *Todo subgrupo $H$ de um grupo abeliano livre $F$ é abeliano livre.*

### 1.1.3 Grupos Abelianos Finitamente Gerados

Daremos agora teoremas que caracterizam melhor os grupos abelianos finitamente gerados.

**Definição 1.14.** *Seja $G$ um grupo, o* **subgrupo de torsão** *de $G$ é:*

$$t(G) = \{g \in G : ng = 0 \text{ para algum inteiro } n \text{ diferente de zero}\}.$$

**Definição 1.15.** *Um grupo $G$ é dito de* **torção** *se $t(G) = G$; e* **livre de torção** *se $t(G) = 0$.*

**Teorema 1.16.** *O grupo quociente $G/t(G)$ é livre de torção, e assim, todo grupo $G$ é uma extensão de um grupo de torção por um grupo livre de torção.*

**Demonstração:** Seja $g + t(G) \in G/t(G)$. Suponha que, para algum inteiro $n \neq 0$, tenhamos $n(g + t(G)) = 0$. Então $ng \in t(G)$, portanto existe um inteiro $m \neq 0$ tal que $m(ng) = 0$. Como $mn \neq 0$, temos que $g \in t(G)$, e assim, $g + t(G) = t(G)$. Logo $G/t(G)$ é livre de torção. ■

**Teorema 1.17.** *Cada grupo abeliano finito $G$ é uma soma direta de grupos cíclicos finitos.*

**Demonstração:** Escolhamos $n$ o menor número natural tal que $G$ pode ser gerado por um conjunto de $n$ elementos. Entre todos os conjuntos de geradores $\{x_1, \ldots, x_n\}$ de tamanho $n$, escolha o que contém um elemento $x_1$ de menor ordem e seja $k$ esta ordem.

Agora vamos fazer indução sobre os geradores. Se $n = 1$, temos $G = \langle x_1 \rangle$ e, com isso $\langle x_1 \rangle$ é finito. Suponha que vale para os $n - 1$ geradores de $G$. Assim, um subgrupo $H = \langle x_2, \ldots, x_n \rangle$ de $G$ é uma soma direta de grupos cíclicos, pela hipótese de indução. Vamos mostrar que $G = \langle x_1 \rangle \oplus H$. Para isso, é suficiente mostrar que $\langle x_1 \rangle \cap H = 0$, porque $\langle x_1 \rangle + H = \langle x_1, \ldots, x_n \rangle = G$.

Suponhamos, por contradição, que $\langle x_1 \rangle \cap H \neq 0$. Seja $z \in \langle x_1 \rangle \cap H$, então $z = a_1 x_1 = \Sigma_{i=2}^{n} a_i x_i$, para $a_1, \ldots, a_n \in \mathbb{Z}$ e $0 < a_1 < k$. Agora seja $d$ o mdc de $a_1, \ldots, a_n$ e defina $g = -(a_1/d)x_1 + \Sigma_{i=2}^{n}(a_i/d)x_i$. Primeiro note que $g \neq 0$. De fato, o Lema [[11], 6.8] diz: " Se $G = \langle x_1, \ldots, x_n \rangle$ e $a_1, \ldots, a_n$ são inteiros co-primos, então existe um conjunto de geradores de $G$ com $n$ elementos $\{y_1, \ldots, y_n\}$ onde $y_1 = \Sigma_{i=1}^{n} a_i x_i$". Então, como $a_1/d, \ldots, a_n/d$ são co-primos, temos assim um conjunto de geradores de $G$ de $n$ elementos, onde $g$ pertence a ele. Então $g \neq 0$, pois caso contrário teríamos um conjunto gerador de $G$ com $n - 1$ elementos, contradição. Agora observe que a ordem de $g$ é menor do que $k$, pois $dg = 0$ e $d \leq a_1 < k$. Aplicando o Lema [[11], 6.8] novamente, vemos que isso contradiz a minimalidade de $k$. ■

**Teorema 1.18.** *Cada grupo abeliano finitamente gerado livre de torção é abeliano livre.*

**Demonstração:** Provaremos por indução sobre $n$, onde $G = \langle x_1, \ldots, x_n \rangle$. Se $n = 1$, temos $G = \langle x_1 \rangle$, logo abeliano livre.

Defina $H = \{g \in G : mg \in \langle x_n \rangle \text{ para algum inteiro positivo } m\}$. Agora $H$ é um subgrupo de $G$ e $G/H$ é livre de torção. O primeiro fato não é difícil de ver, já o segundo será mais detalhado. Seja $x \in G$ tal que $k(x + H) = 0$, para algum $k$. Então $kx \in H$, o que implica $m(kx) \in \langle x_n \rangle$, assim $x \in H$. Portanto $G/H$ é abeliano livre, pois pelo Teorema 1.19, $G/H$ é uma soma direta de cíclicos infinitos.

Pelo Corolário 1.12, $G = H \oplus G/H$. Agora é suficiente provar que H é cíclico infinito, pois, caso seja $H$ vai satisfazer a Definição 1.4. Note que $H$ é finitamente gerado, porque é um somando direto do grupo $G$ que é finitamente gerado.

Se $0 \neq g \in H$, então $mg = kx_n$ para inteiros $m$ e $k$ diferentes de zero. Defina $\varphi : H \to \mathbb{Q}$ por $\varphi(g) = k/m$. É fácil checar que $\varphi$ define um homomorfismo injetor, assim $H$ é isomorfo a um subgrupo finitamente gerado de $\mathbb{Q}$. Seja $H = \langle a_1/b_1, \ldots, a_t/b_t \rangle$. Se $b = \Pi_{i=1}^{t} b_i$, então a aplicação $\psi : H \to \mathbb{Z}$ dada por $\psi(h) = bh$, é injetiva. Portanto, $H$ é isomorfo a um subgrupo de $\mathbb{Z}$, sendo então cíclico infinito. ■

**Teorema 1.19.** *Cada grupo $G$ abeliano finitamente gerado é uma soma direta finita de grupos cíclicos finitos e infinitos, e o número de somandos diretos depende somente de $G$.*

**Demonstração:** Pelo Teorema 1.18, temos que $G/t(G)$ é abeliano livre. Assim, pelo Corolário 1.12, temos $G = t(G) \oplus F$, onde $F \cong G/t(G)$. Como $t(G)$ é finitamente gerado e, todos os elementos têm ordem finita, $t(G)$ é finito. Pelo Teorema 1.17, $t(G)$ é uma soma direta de grupos cíclicos finitos.

O número de somandos de $t(G)$ depende de sua ordem e o número de cíclicos infinitos depende do posto de $G/t(G)$, assim depende somente de $G$. ■

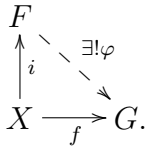
Quando $G$ não é finitamente gerado, o teorema acima pode ainda ser verdadeiro, como podemos ver na proposição abaixo.

**Definição 1.20.** *Seja $G$ um grupo abeliano. Dizemos que $G$ tem expoente finito se existir algum inteiro positivo $n$ tal que $nG=0$, ou seja, $n$ é um inteiro que anula todos os elementos de $G$.*

**Proposição 1.21** ([11, Corolário 10.37])**.** *Se um grupo abeliano $G$ tem expoente finito. Então $G$ é uma soma direta de grupos cíclicos finitos.*

## 1.2 Grupos Livres

**Definição 1.22.** *Seja $F$ um grupo e $X$ um subconjunto de $F$. $F$ é dito um* **grupo livre** *com base $X$ se, para todo grupo $G$ e toda aplicação $f : X \longrightarrow G$, existe um único homomorfismo $\varphi : F \longrightarrow G$ tal que $\varphi(x) = f(x)$, para todo $x \in X$, ou seja, de maneira que o diagrama abaixo comuta*




A definição acima é formal e abstrata, e não nos permite garantir a existência. Por isso, faremos uma construção explícita de um grupo livre com base $X$. Faremos isso provando que, dado um conjunto $X$, existe um grupo livre $F$ cuja base é $X$.

Seja $X$ um conjunto e seja $X^{-1}$ um conjunto disjunto de $X$, para o qual existe uma bijeção $X \longrightarrow X^{-1}$, que denotaremos por $x \longrightarrow x^{-1}$. Chamaremos os elementos de $X$ de **símbolo**.

**Definição 1.23.** *a) Uma* **palavra** *sobre $X$ é uma expressão da forma $w = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$, onde os símbolos $x_i \in X$, $e_i \in \{+1, -1, 0\}$ e $e_n = \pm 1$. A palavra que não contenha símbolos em $X$ é dita a palavra vazia e é denotada por 1.*

*b) O comprimento de $w = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$ é definido como sendo $n$ e o comprimento da palavra vazia é definido como sendo 0.*

*c) Se $w = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$ é uma palavra sobre $X$, então sua inversa é a palavra $w^{-1} = x_n^{-e_n} x_{n-1}^{-e_{n-1}} \dots x_1^{-e_1}$.*

Notemos que, se o comprimento de uma palavra $w$ é $n$, sua inversa $w^{-1}$ também é.

**Definição 1.24.** *Uma palavra $w$ sobre $X$ é dita* **reduzida** *se $w$ é vazia ou escrita na forma $w = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$, onde $x_i \in X$, todos os $e_i = \pm 1$, e $x_i, x_i^{-1}$ não são adjacentes.*

**Exemplo 1.25.** *Seja $X = \{x_1, x_2, x_3\}$. A palavra $u = x_3 x_1 x_2^{-1} x_1$ é reduzida sobre $X$, enquanto a palavra $v = x_2 x_3 x_3^{-1} x_1$ não é reduzida sobre $X$.*

**Definição 1.26.** *Uma sub-palavra de $w = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$ é a palavra vazia ou uma palavra da forma $v = x_i^{e_i} \dots x_j^{e_j}$, onde $1 \leq i \leq j \leq n$.*

Podemos definir uma multiplicação de palavras: se $w = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$ e $u = y_1^{d_1}y_2^{d_2}\dots y_m^{d_m}$, então $wu = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}y_1^{d_1}y_2^{d_2}\dots y_m^{d_m}$. Agora esta multiplicação não define um produto no conjunto de todas as palavras reduzidas sobre $X$, pois o produto $wu$ não é necessariamente uma palavra reduzida sobre $X$. Mas podemos definir uma nova multiplicação de palavras $w$ e $u$ como sendo a palavra reduzida obtida de $wu$, após todos os possíveis cancelamentos. Mais precisamente, se existe uma sub-palavra (possivelmente vazia) $v$ de $w$ com $w = w'v$ tal que $v^{-1}$ é uma sub-palavra de $u$, com $u = v^{-1}u'$, de tal maneira que $w'u'$ é reduzida, então definimos o produto $wu$ como sendo:

$$wu = w'u'.$$

Esta multiplicação é chamada de **justaposição**.

**Exemplo 1.27.** *: Se* $w = x_2x_3x_1x_2^{-1}$ *e* $u = x_2x_1^{-1}x_2x_3x_3x_2$*, então*

$$wu = (x_2x_3x_1x_2^{-1})(x_2x_1^{-1}x_2x_3x_3x_2)$$

$$= x_2x_3(x_1(x_2^{-1}x_2)x_1^{-1})x_2x_3x_3x_2 = x_2x_3x_2x_3x_3x_2.$$

Agora estamos prontos para provar que, dado um conjunto $X$, existe um grupo livre cuja base é $X$. Para isto, vamos utilizar o truque de **Van der Waerden**, que consiste em mostrar que o conjunto de todas as palavras reduzidas $F$ podem ser imersas, via isomorfismo, no grupo das permutações de $F$. E, assim, provaremos que $F$ é um grupo com a operação de **justaposição**.

**Teorema 1.28.** *Dado um conjunto X, existe um grupo livre F com base X.*

**Demonstração:** Seja $F$ o conjunto de todas as palavras reduzidas sobre $X$. Para cada $x \in X$, consideremos as funções $|x| : F \longrightarrow F$ e $|x^{-1}| : F \longrightarrow F$, definidas como segue: para $e = \pm 1$,

$$|x^e|(x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}) = \begin{cases} x_2^{e_2}\dots x_n^{e_n}, & \text{se} \quad x^e = x_1^{-e_1} \\ x^e x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}, & \text{se} \quad x^e \neq x_1^{-e_1} \end{cases}$$

Como as compostas $|x^e||x^{-e}|$ e $|x^{-e}||x^e|$ são ambas iguais à função identidade de $F$, temos que $|x^e|$ é uma permutação de $F$ cuja permutação inversa é $|x^{-e}|$. Seja $S_F$ o grupo simétrico sobre $F$, e seja $\overline{F}$ o subgrupo de $S_F$ gerado pelo conjunto $\overline{X} = \{|x| : x \in X\}$. Observe que existe uma bijeção $\xi : \overline{X} \longrightarrow X$, dada por $|x| \longmapsto x$.

Afirmamos que $\overline{F}$ é um grupo livre com base $\overline{X}$.

Se $1 \neq g \in \overline{F}$, então temos que $g$ possui uma fatoração

$$g = |x_1^{e_1}||x_2^{e_2}|\dots|x_n^{e_n}|$$

onde $e_i = \pm 1$ e $|x_i^{e_i}|$ e $|x_i^{-e_i}|$ nunca são adjacentes, pois, do contrário, poderíamos cancelá-los. Uma tal fatoração de $g$ é única, pois $g(1) = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$, e já observamos que a ortografia de uma palavra reduzida é única.

Usemos a definição de grupos livres dada anteriormente para provarmos que $\overline{F}$ é um grupo livre com base $\overline{X}$. Suponhamos que $G$ é um grupo e que $f : \overline{X} \longrightarrow G$ é um função. Já que a fatoração (1) é única, a função $\varphi : \overline{F} \longrightarrow G$, dada por $\varphi(|x_1^{e_1}||x_2^{e_2}|\dots|x_n^{e_n}|) = f(|x_1^{e_1}|)f(|x_2^{e_2}|)\dots f(|x_n^{e_n}|)$, está bem definida e estende $f$. Já que $\overline{X}$ gera $\overline{F}$, é suficiente mostrarmos que $\varphi$ é um homomorfismo, pois, para provarmos que $\varphi$ é único, basta observarmos que dois homomorfismos coincidindo sobre um mesmo conjunto gerador devem ser iguais.

Sejam $w$ e $u$ palavras reduzidas sobre $\overline{X}$. É claro que $\varphi(wu) = \varphi(w)\varphi(u)$ sempre que a palavra $wu$ é reduzida. Se a palavra $wu$ não for reduzida, escrevemos $w = w'v$ e $u = v^{-1}u'$, como na definição de justaposição, e teremos:

$$\varphi(wu) = \varphi((w'v)(v^{-1}u')) = \varphi(w'u') = \varphi(w')\varphi(u') =$$

$$= \varphi(w')\varphi(v)\varphi(v)^{-1}\varphi(u') = \varphi(w'v)\varphi(v^{-1}u') = \varphi(w)\varphi(u).$$

E então, de fato, $\varphi$ é um homomorfismo. Até agora, mostramos que $\overline{F}$ é um grupo livre com base $\overline{X}$. Finalizando, consideremos a aplicação $\overline{\xi} : \overline{F} \longrightarrow F$, definida por

$$|x_1^{e_1}||x_2^{e_2}|\dots|x_n^{e_n}| \longmapsto x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}.$$

$\overline{\xi}$ é uma bijeção com $\overline{\xi}(\overline{X}) = \xi(X) = X$, e portanto podemos considerar $F$ como um grupo isomorfo a $\overline{F}$ e então $F$ é um grupo livre com base $X$. ■

**Corolário 1.29.** *Todo grupo $G$ é um quociente de um grupo livre.*

**Demonstração:** Seja $G$ um grupo qualquer e consideremos o conjunto $X = \{x_g \mid g \in G\}$. Assim, a aplicação $f : X \to G$ definida por $f(x_g) = g$ é uma bijeção. Pelo Teorema 1.28, existe um grupo livre $F$ cuja base é $X$, logo existe um homomorfismo $\varphi : F \to G$ estendendo $f$, como $f$ é sobrejetiva, temos que $\varphi$ também é. Portanto, $G \cong F/Ker(\varphi)$. ■

Daremos agora uma descrição do grupo livre a partir de sua apresentação.

**Definição 1.30.** *Sejam $X$ um conjunto e $\Delta$ uma família de palavras sobre $X$. Um grupo $G$ tem geradores $X$ e relações $\Delta$ se $G \cong F/R$, onde $F$ é o grupo livre com base $X$ e $R$ é o subgrupo normal de $F$ gerado por $\Delta$. O par ordenado $(X|\Delta)$ é chamado de apresentação de $G$.*

**Exemplo 1.31.** *O grupo cíclico de ordem 4: $C_4 = \{1, x, x^2, x^3\}$, pode ser visto como o quociente entre o grupo livre sobre um gerador $\langle x \rangle$ e o subgrupo normal gerado por $x^4$. Assim, $C_4 \cong \langle x \rangle / \langle x^4 \rangle$ e uma apresentação de $C_4$ é $(x|x^4)$.*

**Exemplo 1.32.** *Um grupo livre é um grupo que tem uma apresentação da forma $(X|\varnothing)$, ou seja, ele não possui relação(não trivial).*

Duas conseqüências imediatas são:

(i) Um grupo livre é livre de torção, ou seja, ele não possui elementos de ordem finita.

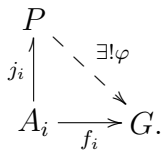
(ii) Os geradores de um grupo livre não comutam. Logo, se F é um grupo livre com base X, então o centro $\mathbf{Z}(F)$ de F é não trivial se, e somente se, $|X| = 1$.

**Teorema 1.33** ([10, 6.1.1])**.** *Todo subgrupo $H$ de um grupo livre $F$ é livre.*

## 1.3 Produto Livre

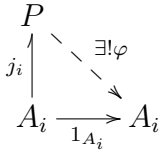
Definiremos, nesta seção, o conceito de produto livre de grupos, que será definido como uma solução para que um certo diagrama comute. Uma vez estabelecidas a existência e unicidade de produtos livres, daremos uma descrição concreta destes grupos em termos de seus elementos e de sua apresentação.

**Definição 1.34.** *Seja $\{A_i : i \in I\}$ uma família de grupos, onde $I$ é um conjunto de índices quaisquer. Um* **produto livre** *dos $A_i$ é um grupo $P$ e uma família de homomorfismos $j_i : A_i \longrightarrow P$ tais que, para todo grupo $G$ e toda família de homomorfismos $f_i : A_i \longrightarrow G$, existe um único homomorfismo $\varphi : P \longrightarrow G$ com $\varphi j_i = f_i$, para todo $i$, ou seja, de maneira que o diagrama abaixo comuta:*



**Lema 1.35.** *Se $P$ é um produto livre de $\{A_i : i \in I\}$, então os homomorfismos $j_i$ são injetivos.*

**Demonstração:** Para um índice $i$ fixo, consideremos o diagrama em que $G = A_i$, $f_i$ é o homomorfismo identidade e, para $k \neq i$, as aplicações $f_k : A_k \longrightarrow A_i$ são triviais.

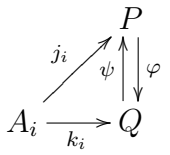



E então temos que $\varphi j_i = 1_{A_i}$. Portanto, o homomorfismo $j_i$ é injetor. ■

Por causa deste lema, as aplicações $j_i : A_i \longrightarrow P$ são chamadas de imersões.

**Teorema 1.36.** *Seja $\{A_i : i \in I\}$ uma família de grupos. Se $P$ e $Q$ são, cada um deles, produto livre dos $A_i$, então $P \cong Q$.*

**Demonstração:** Sejam $j_i : A_i \longrightarrow P$ e $k_i : A_i \longrightarrow Q$ as imersões. Já que P e Q são o produto livre dos $A_i$, existe um homomorfismo $\varphi : P \longrightarrow Q$ satisfazendo $\varphi j_i = k_i$, para todo $i$. Similarmente, existe uma aplicação $\psi : Q \longrightarrow P$ com $\psi k_i = j_i$, para todo $i$.




E assim, vemos que

$$j_i = \psi k_i = \psi(\varphi j_i) = (\psi\varphi) j_i$$

e também que

$$k_i = \varphi j_i = \varphi(\psi k_i) = (\varphi\psi) k_i.$$

Logo, $\psi\varphi = 1_P$ e $\psi\varphi = 1_Q$, e portanto, $\varphi : P \longrightarrow Q$ é um isomorfismo, já que $\psi$ é sua inversa. ■

Pelo Teorema 1.36, podemos nos referir ao produto livre $P$ de $\{A_i : i \in I\}$. Vamos denotá-lo por

$$P = *_{i \in I} A_i.$$

Se existir um número finito de grupos $A_i$, então denotaremos o produto livre por

$$P = A_1 * \ldots * A_n.$$

**Proposição 1.37.** *Assuma que os conjuntos* $\{X_i : i \in I\}$ *são dois a dois disjuntos. Se* $F_i$ *é o grupo livre com base* $X_i$*, então* $P = *_{i\in I}F_i$ *é o grupo livre com base* $\bigcup_{i\in I} X_i$*.*

**Demonstração:** Queremos provar que, dados um grupo $G$ e uma função $f : \bigcup_{i\in I} X_i \longrightarrow G$, existe um único homomorfismo $\varphi : P \longrightarrow G$ estendendo $f$, ou seja, $\varphi|_{\cup_{i\in I}X_i} = f$. Para isso, consideremos funções $f_i : X_i \longrightarrow G$ definidas por $f_i = f|_{X_i}$. Como $F_i$ é o grupo livre sobre $X_i$, existe $\varphi_i : F_i \longrightarrow G$ satisfazendo $\varphi_i|_{X_i} = f_i$. Então o homomorfismo $\varphi : P \longrightarrow G$, definido por $\varphi|_{X_i} = \varphi_i$, está unicamente determinado pelos já únicos homomorfismos $\varphi_i$. Portanto, $\varphi|_{\cup_{i\in I}X_i} = f$ e temos que $P$ é o grupo livre com base $\bigcup_{i\in I} X_i$. ■

Trataremos agora da existência de produtos livres.

**Teorema 1.38.** *Dada uma família* $\{A_i : i \in I\}$ *de grupos, o produto livre* $P = *_{i\in I}A_i$ *existe.*

**Demonstração:** A prova é similar à prova da existência de grupos livres.

Sejam $\{A_i : i \in I\}$ uma família de grupos. Suponhamos que os conjuntos $A_i^\sharp = A_i - \{1\}$ sejam dois a dois disjuntos. Chamemos $\bigcup_{i\in I} A_i^\sharp \cup \{1\}$ o *alfabeto*, chamemos seus elementos de *letras*, que formam *palavras* $w = a_1a_2 \dots a_n$, onde cada $a_i$ está em algum $A_i$. Uma palavra $w$ é *reduzida* se, $w = 1$ ou se $w = a_1a_2 \dots a_n$, onde cada letra $a_j \in A_{i_j}^\sharp$ e letras adjacentes estão em distintos $A_i^\sharp$.

Seja $P$ o conjunto de todas as letras de todas as palavras reduzidas sobre $\bigcup_{i\in I} A_i^\sharp \cup \{1\}$, e consideremos a operação de justaposição sobre os elementos de $P$ da seguinte maneira: assuma que as palavras $w = a_1 \dots a_n$ e $v = b_1 \dots b_m$ sejam reduzidas. Se $a_n$ e $b_1$ estão em distintos $A_i^\sharp$, definimos

$$wv = a_1 \dots a_n b_1 \dots b_m,$$

pois o lado direito da equação acima é uma palavra reduzida. Se $a_n$ e $b_1$ estão no mesmo $A_i^\sharp$ e $a_nb_1 \neq 1$, definamos

$$wv = a_1 \dots a_{n-1}(a_nb_1)b_2 \dots b_m,$$

pois novamente esta é uma palavra reduzida. Se $a_n$ e $b_1$ estão no mesmo $A_i^\sharp$ e $a_nb_1 = 1$, então cancelamos o fator $a_nb_1$ e repetimos o processo para as palavras $w' = a_1 \dots a_{n-1}$ e $u' = b_2 \dots b_m$. Como o comprimento de uma palavra reduzida é finito, temos que o processo termina com uma palavra reduzida, que será justamente o resultado da multiplicação $wu$. Claramente, 1 é a identidade de $P$ e a inversa de uma palavra reduzida é reduzida. Para verificação da associatividade, basta usarmos o truque de *Van der Waerden* como foi feito antes para grupos livres e, desta forma, está provado o teorema. ■

**Teorema 1.39 (Forma normal).** *Se $g \in P = *_{i\in I}A_i$ e $g \neq 1$, então $g$ tem uma fatoração única*

$$g = a_1 a_2 \dots a_n,$$

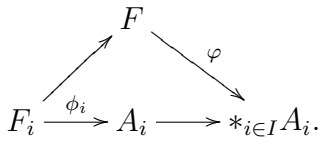
*onde os fatores adjacentes estão em diferentes $A^\sharp$.*

**Demonstração:** Na construção do produto livre feita acima, definimos seus elementos como palavras reduzidas, que naturalmente já têm a forma citada acima. ■

Assim, já temos uma descrição completa dos elementos do produto livre $*_{i\in I}A_i$ dos grupos $A_i$. Daremos agora uma descrição do produto livre a partir de sua apresentação.

**Teorema 1.40.** *Seja $\{A_i : i \in I\}$ uma família de grupos cujas apresentações são respectivamente $(X_i \mid \triangle_i)$, onde os conjuntos $X_i$ são dois a dois disjuntos. Então a apresentação de $P = *_{i\in I}A_i$ é $(\bigcup_{i\in I} X_i \mid \bigcup_{i\in I} \triangle_i)$.*

**Demonstração:** Pela Proposição 1.37, se $F_i$ é o grupo livre com base $X_i$, então $F = *_{i\in I}F_i$ é o grupo livre com base $\bigcup_{i\in I} X_i$. Assim, basta mostrar que $*_{i\in I}A_i \cong F/R$, onde $R$ é o subgrupo normal de $F$ gerado por $\bigcup_{i\in I} \triangle_i$. Pelo Corolário 1.29, temos que $A_i \cong F_i/R_i$, onde $R_i$ é o subgrupo normal gerado pelas relações $\triangle_i$, logo existem homomorfismos $\phi_i : F_i \longrightarrow A_i$ sobrejetivos com $Ker(\phi_i) = R_i$ e, pela definição de produto livre aplicado a $F$, deve existir um homomorfismo $\varphi : F \longrightarrow *_{i\in I}A_i$, estendendo todos $F_i \longrightarrow A_i \hookrightarrow *_{i\in I}A_i$ cujo núcleo é o subgrupo normal gerado por $\bigcup_{i\in I} \triangle_i$. Veja o diagrama abaixo.




■

A partir de agora, daremos a definição de **residualmente P** e provaremos alguns resultados.

**Definição 1.41.** *Seja $P$ uma propriedade referente a grupos. Dizemos que um grupo $G$ é residualmente $P$, se uma das três propriedades (equivalentes) abaixo for satisfeita:*

*(i) Para todo elemento $g \in G$, $g \neq 1$, existe um subgrupo normal $N_g \trianglelefteq G$ tal que $g \notin N_g$ e o grupo quociente $G/N_g$ satisfaz $P$.*

*(ii) Para cada elemento $g \in G$ existe um grupo $H_g$ e um homomorfismo $\psi_g : G \to H_g$ tal que $\psi_g(g) \neq 1$ e $H_g$ satisfaz $P$.*

*(iii) A interseção de todos os subgrupos normais $N \trianglelefteq G$ cujo quociente $G/N$ satisfaz $P$ é trivial.*

**Proposição 1.42.** *Sejam $H \lhd G$ e $\pi$ aplicação natural de $G$ em $G/H$. Se $K \lhd G/H$, então $\pi^{-1}(K) \lhd G$.*

**Demonstração:** Vamos mostrar que dado $g_K \in \pi^{-1}(K)$ e $g \in G$, temos $g_K^g \in \pi^{-1}(K)$. Assim, temos $\pi^{-1}(K) = \{g \in G : \pi(g) \in K\} = \{g \in G : gH \in K\}$. Portanto:

$$g^{-1}g_K g = g^{-1}H^{-1}\overbrace{Hg_K}^{\in K}HH^{-1}g = (Hg)^{-1}(Hg_K)(Hg)H^{-1} = (Hg_K)H^{-1} = g_K \in \pi^{-1}(K).$$

■

**Proposição 1.43.** *A soma direta de grupos cíclicos finitos é um grupo residualmente finito.*

**Demonstração:** Seja $G = \bigoplus_{i\in\mathbb{N}^*} C_i$, onde os $C_i$ são cíclicos finitos. Assim, dado $0 \neq g \in G$, temos que $g$ tem um número finito de entradas diferentes de zero. Defina $N$ com a soma direta dos cíclicos, onde as coordenadas de $g$ são zero. Portanto $N \leq G$, $g \notin N$ e $G/N$ é isomorfo a uma soma de cíclicos finitos, logo $G/N$ é finito. ■

Observe que, se tivermos $p$-grupos finitos, teremos que a soma direta é residualmente $p$-grupo finito.

**Proposição 1.44.** *Se $H$ tem índice finito em $G$, então $\bigcap_{x\in G} xHx^{-1}$ é um subgrupo normal em $G$ e tem índice finito.*

**Demonstração:** Vamos mostrar, que para cada $y \in G$ e $k \in K = \bigcap_{x\in G} xHx^{-1}$, temos $k^y \in K$. Notemos que

$$yKy^{-1} = \bigcap_{x\in G} yxH(yx)^{-1} = \bigcap_{g=yx\in G} gHg^{-1},$$

o que implica $k^y \in K$.

Agora, mostraremos que $K$ tem índice finito em $G$. Antes disto, mostraremos $K = \bigcap_{i=1}^n x_i H x_i^{-1}$, onde $x_i$ é um certo conjunto de representantes. É fácil ver que $K \subset \bigcap_{i=1}^n x_i H x_i^{-1}$. Seja $l \in \bigcap_{i=1}^n x_i H x_i^{-1}$, o que implica $x_i l x_i^{-1} \in H$ para todo $i = 1, \ldots, n$. Fixe $g \in G$. Assim,

$g = kx_j$ para algum $j$. Uma vez que $x_i l x_i^{-1} \in K$ para $i = 1, \ldots, n$, temos $x_j l x_j^{-1} \in K$, assim $kx_j l x_j^{-1} k^{-1} \in K$, o que implica $glg^{-1} \in K$. Então $gl \in Kg$, como $K$ é normal $gl \in gK$, assim $l \in K$.

Mostraremos o prometido. Definiremos o homomorfismo $\varphi : G \to (G/x_1 H x_1^{-1}) \times \ldots \times (G/x_n H x_n^{-1})$. Portanto

$$G/\bigcap_{i=1}^{n} x_i H x_i^{-1} \cong (G/x_1 H x_1^{-1}) \times \ldots \times (G/x_n H x_n^{-1}),$$

onde cada $G/x_i H x_i^{-1}$ são finitos. Como o lado esquerdo é finito, temos, o que queríamos. ■

**Proposição 1.45.** *Se $G \geq H \geq K \geq 1$ é uma série de subgrupos, onde cada um é normal no seu precedente e $G/H$, $H/K$ são $p$-grupos finitos, então $K$ contém um subgrupo $L$ normal em $G$ e $G/L$ é $p$-grupo finito.*

**Demonstração:** Seja $L = \bigcap_{g \in G} gKg^{-1}$ e observe que $[G : K] = [G : H][H : K]$, agora a demonstração é análoga a da Proposição 1.44. ■

**Lema 1.46.** *Seja $H$ um subgrupo normal de $G$ tal que $G/H$ é $p$-grupo finito e $H$ é residualmente $p$-grupo finito. Então $G$ é residualmente $p$-grupo finito.*

**Demonstração:** Para cada $1 \neq g \in G$, devemos encontrar um subgrupo $K_g$ tal que $g \notin K_g$ e $G/K_g$ é $p$-grupo finito. Se $g \notin H$, seja $K_g = H$. Por outro lado, se $g \in H$, podemos encontrar $K$ normal em $H$, tal que $g \notin K$ e $H/K$ é $p$-grupo finito. Pela Proposição 1.45, $K$ contém $L$ normal em G, tal que $G/L$ é $p$-grupo finito, assim podemos escolher $K_g = L$. ■

**Teorema 1.47.** *Se $p$ é um primo e $F$ é um grupo livre, então $F$ é residualmente $p$-grupo finito.*

**Demonstração:** Seja $A = \mathcal{M}_{(n+1)(n+1)}(\mathbb{Z}/p^\alpha\mathbb{Z})$ o anel das matrizes de dimensão $n+1$ sobre o anel $\mathbb{Z}/p^\alpha\mathbb{Z}$ dos inteiros módulo $p^\alpha$, onde $p$ é um primo e $\alpha \geq 1$.

Consideremos

$$J = \left\{ \begin{bmatrix} 0 & & \bigstar \\ \vdots & \ddots & \\ 0 & \ldots & 0 \end{bmatrix} \right\} \subset A.$$

Assim, $J$ é um sub-anel. Além disso, notemos que para $M \in J$, temos

$$M = \begin{bmatrix} 0 & a_{12} & \dots & a_{1(n+1)} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & a_{n(n+1)} \\ 0 & \dots & \dots & 0 \end{bmatrix},$$

assim,

$$M^2 = \begin{bmatrix} 0 & 0 & c_{13} & \dots & c_{1(n+1)} \\ & & \ddots & & \vdots \\ \vdots & & & \ddots & c_{n(n+1)} \\ & & & & 0 \\ 0 & & \dots & & 0 \end{bmatrix}.$$

Então $M^{n+1} = 0$, para todo $M \in J$.

Agora vamos mostrar que $\mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$, é um $p$-grupo finito. Todos os elementos de $\mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$ são da forma $I + N$, onde $N \in J$ e $I$ é matriz identidade, ou seja, são todas as matrizes $(n+1) \times (n+1)$ triangulares superiores com 1 na diagonal principal. É um grupo pela respectiva multiplicação de anel:

i) $(I + N)(I + M) = I + (N + M + NM) \in \mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$

ii) $(I + N)^{-1} = I + (-N + N^2 - \ldots + (-1)^n N^n) \in \mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$.

Aqui é muito relevante o fato de $N^{n+1} = 0$.

Seja $(I + M) \in \mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$. Assim, pela multiplicação acima definida:

$$(I + M)^{p^\alpha} = I + p^\alpha M + \frac{p^\alpha(p^\alpha - 1)M}{2} + \ldots + M^{p^\alpha} = I + M^{p^\alpha}$$

pois, para todo $a \in \mathbb{Z}/p^\alpha\mathbb{Z}$ temos $p^\alpha a = 0$.

Se $n > p^\alpha$, faça

$$((I + M)^{p^\alpha})^{p^\alpha} = (I + M)^{p^{2\alpha}} = I + M^{p^{2\alpha}},$$

e assim por diante até $n < p^{k\alpha}$, para algum $k$, o que implica $(I + M)^{p^{k\alpha}} = I$.

Logo, para todo $(I + M) \in \mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$, $o(I + M) | p^{t\alpha}$ para algum $t \geq 1$. Portanto todo elemento de $\mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$ tem ordem potência de $p$ e, como $A$ é finito, temos que $\mathcal{U}(J, \mathbb{Z}/p^\alpha\mathbb{Z})$ é um $p$-grupo finito.

Observe que $\mathcal{U}(J,A) =< \mathcal{D} >$, onde $\mathcal{D} \subseteq \mathcal{M}_{(n+1)(n+1)}(\mathbb{Z}/p^{\alpha}\mathbb{Z})$ e é o seguinte conjunto:

$$\left\{ M_1 = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ & 1 & 0 & & \vdots \\ & & 1 & \ddots & \\ & 0 & & \ddots & 0 \\ & & & & 1 \end{bmatrix}, M_2 = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ & 1 & 1 & \ddots & \vdots \\ & & 1 & & 0 \\ & 0 & & \ddots & 0 \\ & & & & 1 \end{bmatrix}, \dots, M_n = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ & 1 & 0 & \ddots & \vdots \\ & & 1 & & 0 \\ & 0 & & \ddots & 1 \\ & & & & 1 \end{bmatrix} \right\},$$

pois conseguimos gerar $a_{ij} = 1$ para todo $i \leq j$, fazendo a multiplicação dos elementos de $\mathcal{D}$. Logo $\mathcal{D}$ gera todos os elementos de $\mathcal{U}(J, \mathbb{Z}/p^{\alpha}\mathbb{Z})$.

Finalmente, usaremos convenientemente as propriedades do grupo $\mathcal{U}(J,A)$, para mostrar que todo grupo livre é residualmente $p$-grupo finito. Seja $F$ livre gerado por $X = \{x_1, \dots, x_n\}$. Assim para $1 \neq x \in F$, temos $x = x_{i_1}^{m_1} \dots x_{i_r}^{m_r}$, onde $x_i \in X$, $m_l \neq 0$, onde $l = 1 \dots r$, e $i_u \neq i_{u+1}$. Escolhemos um inteiro positivo $m$ tal que $p^m$ não divide $m_1 \dots m_r$. Logo, seja $B = \mathbb{Z}/p^m\mathbb{Z}$ temos assim $\mathcal{U}(J,B)$ é um $p$-grupo finito gerado por $\mathcal{D}$.

Definamos a função $\varphi : X \to \mathcal{U}(J,B)$ por $\varphi(x_i) = M_i$ para $i = 1, \dots, n$. Como $F$ é livre em $X$, $\varphi$ se estende a um único homomorfismo $\tilde{\varphi} : F \to \mathcal{U}(J,B)$ tal que $\tilde{\varphi}|_X = \varphi$. Com isso $Im(\tilde{\varphi}) = \mathcal{U}(J,B)$, pois $\tilde{\varphi}$ é sobrejetiva. O que implica

$$F/Ker(\tilde{\varphi}) \cong \mathcal{U}(J,B).$$

Portanto, $F$ é residualmente $p$-grupo finito pois, $x \notin Ker(\tilde{\varphi})$ pelo fato de que

$$\tilde{\varphi}(x) = \tilde{\varphi}(x_{i_1})^{m_1} \dots \tilde{\varphi}(x_{i_r})^{m_r} = M_{i_1}^{m_1} \dots M_{i_r}^{m_r} \neq 1$$

pois, $p^m$ não divide $m_1 \dots m_n$. ■

**Teorema 1.48** ([10, 6.3.1])**.** *[Kurosh, 1934] Seja $A_i$ uma família de grupos. Se $H \leq *_{i \in I} A_i$, então $H = F * (*_{\lambda \in \Lambda} H_\lambda)$ para algum conjunto (pode ser vazio) de índices $\Lambda$, onde $F$ é um grupo livre e cada $H_\lambda$ é da forma $H_\lambda = H \cap A_i^{a_i}$, onde os $a_i$ percorrem um certo conjunto de representantes de classes duplas em $H \setminus H/A_i$.*

**Teorema 1.49.** *Sejam $G_1$ e $G_2$ $p$-grupos finitos. Então $G_1 * G_2$ é residualmente $p$-grupo finito.*

**Demonstração:** Defina $\psi : G_1 * G_2 \longrightarrow G_1 \times G_2$ por

$$\psi(a_1 b_1 \dots a_n b_n) = (a_1 \dots a_n, b_1 \dots b_n),$$

assim $\psi$ é um epimorfismo. Portanto $\frac{G_1 * G_2}{Ker(\psi)} \cong G_1 \times G_2$, onde pelo Teorema 1.48 $ker(\psi) = H * (Ker(\psi) \cap G_1^{d_1}) * (Ker(\psi) \cap G_2^{d_2})$, no qual $H$ é livre. Se $x \in (Ker(\psi) \cap G_1^{d_1})$, $x = g_1^{d_1}$ e $x \in Ker(\psi)$, logo

$$(1,1) = \psi(x) = \psi(g_1^{d_1}) = \psi(d_1^{-1} g_1 d_1) = (g_1, d_1^{-1} d_1) = (g_1, 1).$$

Portanto, $x = 1$. Analogamente, para a outra interseção, assim o $Ker(\psi)$ é livre. Pelo Teorema 1.47 e Lema 1.46, temos que $G_1 * G_2$ é residualmente $p$-grupo finito. ■

**Teorema 1.50.** *Seja $G$ o produto livre de dois grupos residualmente $p$-grupos finitos. Então $G$ é residualmente $p$-grupo finito.*

**Demonstração:** Temos $G = G_1 * G_2$. Qualquer $g \in G_1 * G_2$ tem a forma normal $g = a_1^e b_1 \dots a_n b_n$, onde $a_i \in G_1$, $b_i \in G_2$ e $e = 0$ ou 1. Temos que para cada $a_i \in G_1$ existe $N_{a_i} \lhd G_1$ tal que $G_1/N_{a_i}$ é $p$-grupo finito e $a_i \notin N_{a_i}$ Assim, fazendo $N = \bigcap N_{a_i}$ temos que $N \lhd G_1$ e $G_1/N$ é $p$-grupo finito. Analogamente para $b_i$, temos $M = \bigcap M_{b_i}$, $M \lhd G_2$ e $G_2/M$ é $p$-grupo finito. Temos, pelo Teorema 1.49, que $G_1/N * G_2/M$ é residualmente $p$-grupo finito.

Agora definimos $\pi : G_1 * G_2 \longrightarrow G_1/N * G_2/M$ o homomorfismo sobrejetor e, assim, dado $g \in G_1 * G_2$, temos $\pi(g) \in G_1/N * G_2/M$. Logo existe $K \lhd G_1/N * G_2/M$ tal que $\pi(g) \notin K$ e $\frac{G_1/N * G_2/M}{K}$ é $p$-grupo finito.

Defina $\varphi : G_1 * G_2 \to \frac{G_1/N * G_2/M}{K}$ por $\varphi(g) = \pi(g)K$, temos $\varphi$ um homomorfismo sobrejetor. Uma vez que $K \lhd G/N * G/M$ temos, pela Proposição 1.42, $\pi^{-1}(K) \lhd G_1 * G_2$.

O núcleo de $\varphi$ é

$$Ker(\varphi) = \{g \in G : \pi(g) \in K\},$$

que são exatamente os elementos de $\pi^{-1}(K)$, portanto,

$$\frac{G_1 * G_2}{\pi^{-1}(K)} \cong \frac{G_1/N * G_2/M}{K},$$

assim, $(G_1 * G_2)/\pi^{-1}(K)$ é p-grupo finito e $g \notin \pi^{-1}(K)$ pois, $\pi(g) \notin K$. Então concluímos o que queríamos. ■

## 1.4 Produto Livre com Subgrupo Amalgamado

Estudaremos, nesta seção, o produto livre com subgrupo amalgamado ou produto livre com amalgamação. Como no caso de grupos abelianos livres e produto livres, o produto livre

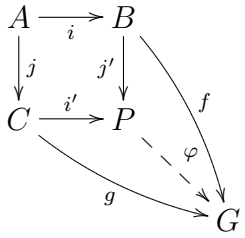
com subgrupo amalgamado é definido como uma solução para que um certo digrama comute. Uma vez estabelecidas a existência e unicidade de produtos livre com amalgamação, daremos uma descrição concreta destes grupos em termos de seus elementos e de sua apresentação.

Sejam $A, B$ e $C$ grupos, $i : A \longrightarrow B$ e $j : A \longrightarrow C$ homomorfismos (não necessariamente injetivos).

**Definição 1.51.** *Uma solução dos dados $(A, B, C, i, j)$, é uma terna (G,f,g), onde $G$ é um grupo e $f : B \longrightarrow G$ e $g : C \longrightarrow G$ são homomorfismos, para os quais o diagrama abaixo comuta.*

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle f} \\ C & \xrightarrow[g]{} & G \end{array}$$

**Definição 1.52.** *Um* **pushout** *dos dados (A,B,C,i,j), é uma solução $(P, j', i')$, tal que, para toda solução (G,f,g), existe um único homomorfismo $\varphi : P \longrightarrow G$ satisfazendo $f = \varphi j'$ e $g = \varphi i'$, ou seja, de maneira que o diagrama abaixo comuta.*




Mesmo que um *pushout* seja uma tripla $(P, j', i')$, usualmente chamamos o grupo $P$ um *pushout* dos dados.

**Teorema 1.53.**

*a) Para os dados $i : A \longrightarrow B$ e $j : A \longrightarrow C$, um pushout $(P, j', i')$ existe e é único (a menos de isomorfismo).*

*b) O pushout $P$ é isomorfo a $(B * C)/N$, onde $N$ é o subgrupo normal de $B * C$ gerado por $\{i(a)j(a^{-1}) : a \in A\}$. E mais, se $C$ tem uma apresentação $(X \mid \Delta)$ e $B$ uma apresentação $(Y \mid \Gamma)$, então $P$ tem uma apresentação*

$$P = \{X \cup Y \mid \Delta \cup \Gamma \cup \{i(a)j(a^{-1}) : a \in A\}\}$$

**Demonstração:** Provaremos $a$). Verifiquemos que $(P, j', i')$ é uma solução, onde $P = (B * C)/N$, $j'(b) = bN$, e $i'(c) = cN$. Seja $a \in A$, então

$$(j'i)(a) = j'(i(a)) = aN \text{ e } (i'j)(a) = i'(j(a)) = j(a)N.$$

Logo, vemos que $(j'i)(a) = (i'j)(a)$ para todo $a \in A$ se, somente se, $i(a)j(a^{-1}) \in N$. E pela própria definição de $N$, temos então que $j'i = i'j$ e portanto $(P, j', i')$ é de fato uma solução para os dados, ou seja, o diagrama abaixo comuta.

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle j'} \\ C & \xrightarrow[i']{} & \frac{B*C}{N} = P \end{array}$$

Agora, suponha que $(G, f, g)$ seja uma outra solução dos dados. A definição de produto livre nos dá um único homomorfismo $\psi : B * C \to G$ com $\psi|_B = f$ e $\psi|_C = g$. Logo, se $b \in B$ e $c \in C$, então $\psi(bc) = \psi(b)\psi(c) = f(b)g(c)$. E para todo $a \in A$, temos

$$\psi(i(a)j(a^{-1})) = f(i(a))g(j(a^{-1})) = 1,$$

já que $N \leq Ker(\psi)$. Portanto, $\psi$ induz um homomorfismo $\varphi : P \to G$ que satisfaz:

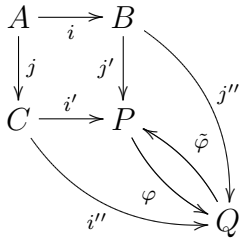
$$\varphi j'(b) = \varphi(bN) = \psi(b) = f(b)$$

e

$$\varphi i'(c) = \varphi(cN) = \psi(c) = f(c).$$

Ou seja, $\varphi j' = f$ e $\varphi i' = g$. A aplicação $\varphi$ é única, pois $P$ é gerado pelas classes laterais de $B \cup C$.

Agora suponha que exista um outro *pushout* $(Q, j'', i'')$ para os mesmos dados, então teremos o seguinte diagrama




Portanto $\varphi : P \longrightarrow Q$ é um isomorfismo e sua inversa é $\tilde{\varphi} : Q \longrightarrow P$ .

Finalmente $b$). Pelas apresentações dos grupos $B$ e $C$ e, pela relação do subgrupo $N$, está claro porque $P$ tem a apresentação citada. ■

**Exemplo 1.54.** *Sejam $G = \langle a|\varnothing\rangle$, $H = \langle b|\varnothing\rangle$, $K = \langle a^3|\varnothing\rangle$ e o monomorfismo $\phi$ de $K$ em $H$ definido por $\phi(a^3) = b^2$, tal que identifica a imagem de $a^3$ com a imagem da inclusão de $K$ em $G$ que é o próprio $a^3$, ou seja, $a^3 = b^2 = \phi(a^3) \in H$. Portanto, temos uma apresentação do produto livre com subgrupo amalgamado $K$ da forma:*

$$P = \langle a, b|a^3 = b^2\rangle$$

**Corolário 1.55.**

*a) Se $i : A \longrightarrow B, j : A \longrightarrow C$ e $C = 1$, então o pushout $P$ dos dados é $P = B/N$, onde $N$ é o subgrupo normal de $B$ gerado pela Im(i).*

*b) Se $A = 1$, então $P \cong B * C$.*

**Demonstração:** É só alterar alguns dados no Teorema 1.53. ■

Agora vamos definir o que vem a ser o produto livre com amalgamação de dois grupos $A_1$ e $A_2$.

**Definição 1.56.** *Sejam $A_1$ e $A_2$ grupos tendo subgrupos isomorfos $B_1$ e $B_2$, respectivamente. Seja $\theta : B_1 \longrightarrow B_2$ o referido isomorfismo. O produto livre com amalgamação de $A_1$ e $A_2$ sobre $\theta$ é o pushout*

$$\begin{array}{ccc} B_1 & \xrightarrow{\ i\ } & A_1 \\ {\scriptstyle j\theta}\downarrow & & \\ A_2 & & \end{array}$$

*onde $i$ e $j$ são inclusões.*

Provamos, no Teorema 1.53, que o produto livre com amalgamação existe e é único: ele é $(A_1 * A_2)/N$, onde N é o subgrupo normal de $A_1 * A_2$ gerado por $\{b\theta(b^{-1}) : b \in B_1\}$. Denotaremos o produto livre com amalgamação por

$$A_1 *_\theta A_2.$$

Um produto livre com amalgamação, como um *pushout*, é um tripla ordenada

$$(A_1 *_\theta A_2, \lambda_1, \lambda_2).$$

As aplicações $\lambda_i : A_i \longrightarrow A_1 *_\theta A_2$ são dadas como no Teorema 1.53, por $\lambda_i(a_i) = a_i N$.

A definição do produto livre com amalgamação a partir do *pushout*, nos diz pouco da sua estrutura. Assim, daremos uma descrição mais concreta do produto livre com amalgamação a partir da forma normal de seus elementos.

Mas antes, façamos uma observação: já que em $A_1 *_\theta A_2$, temos que $b\theta(b^{-1}) = 1$, então podemos identificar o elemento $b$ com sua imagem pelo isomorfismo $\theta$. Logo, no produto livre com amalgamação, temos $b = \theta(b)$ ou $\theta^{-1}(b) = b$.

Escolhamos, para cada $i = 1, 2$, uma transversal à esquerda de $B_i$ em $A_i$ sujeito somente à condição de que o representante da classe lateral $B_i$ seja 1. Para $a \in A_i$, denotamos o representante escolhido de $aB_i$ por $l(a)$, então temos que $a = l(a)b$, para algum unicamente determinado $b \in B_i$, que depende somente de $a$.

**Definição 1.57.** *Uma* **forma normal** *é um elemento de $A_1 *_\theta A_2$ da forma*

$$l(a_1)l(a_2)\dots l(a_n)b,$$

*onde $b \in B_1$, $n \geq 0$, os elementos $l(a_j)$ estão nas transversais escolhidas de $B_{i_j}$ em $A_{i_j}$, e $l(a_j)$ adjacentes estão em distintos $A_i$.*

No caso especial em que os $B_i$, são triviais, o produto livre com amalgamação é o produto livre $A_1 * A_2$ e toda palavra reduzida é uma forma normal.

**Teorema 1.58** (**Forma Normal**). *Sejam $A_1$ e $A_2$ grupos com subgrupos isomorfos $B_1$ e $B_2$ respectivamente, e seja $\theta : B_1 \longrightarrow B_2$ um isomorfismo. Então para cada elemento $wN \in A_1 *_\theta A_2$, existe uma única forma normal $F(w)$, como definido anteriormente, com $wN = F(w)N$.*

**Demonstração:** Já sabemos que $A_1 *_\theta A_2 = (A_1 * A_2)/N$, onde $N$ é o subgrupo normal de $A_1 * A_2$ gerado por $\{b\theta(b^{-1}) : b \in B_1\}$. Cada classe lateral de $N$ tem um representante $w = x_1y_1 \dots x_ny_n$ no produto livre, onde $x_i \in A_1$ e $y_i \in A_2$, e somente os elementos $x_1$ e $y_n$ podem ser iguais a 1. Vamos dar agora um algorítimo associando uma forma normal $F(w)$ a cada classe lateral $wN$ no produto livre generalizado de maneira que $F(w)N = wN$.

Seja $w = x_1y_1$. Se $y_1 = 1$, então $x_1 = l(x_1)b = F(w)$, onde $b \in B_1$. Se $x_1 = 1$, então $y_1 = l(y_1)b$, onde $b \in B_2$. Agora, da maneira como a forma normal foi definida anteriormente, nós precisamos que $b$ pertença a $B_1$. Mas, por uma observação feita anteriormente, temos que no produto livre com amalgamação os elementos $b$ e $\theta^{-1}(b)$ estão identificados. Logo, podemos simplesmente reescrever:

$$l(y_1)b = l(y_1)\theta^{-1}(b) = F(w),$$

onde $\theta^{-1}(b) \in B_1$. Se $x_1 \neq 1$ e $y_1 \neq 1$, então

$$x_1y_1 = l(x_1)by_1 = l(x_1)\theta(b)y_1 \; em \; A_1 *_\theta A_2,$$

mas $z = \theta(b)y_1 \in A_2$, e então $z = l(z)b_2$ para algum $b_2 \in B_2$. Portanto,

$$x_1y_1 = l(x_1)z = l(x_1)l(z)b_2 = l(x_1)l(z)\theta^{-1}(b_2) \; em \; A_1 *_\theta A_2,$$

onde este último elemento é uma forma normal $F(w)$ em $wN$. Este procedimento pode ser iterado, finalizando com uma classe lateral $wN \in A_1 *_\theta A_2$. Agora, provemos a unicidade desta forma normal. Para isto, vamos utilizar novamente do truque de $Van\ der\ Waerden$. Seja $M$ o conjunto de todas as formas normais de $A_1 *_\theta A_2$, pelo Teorema 1.39, temos que diferentes formas normais devem ter diferentes ortografias. Se $a \in A_i$, defina uma função $\mid a \mid : M \longrightarrow M$ por

$$\mid a \mid (l(a_1)l(a_2)\dots l(a_n)b) = F(al(a_1)l(a_2)\dots l(a_n)b).$$

Se $a$ e $l(a_1)$ estiverem em distintos $A_i$, então $al(a_1)l(a_2)\dots l(a_n)b$ tem forma $x_1y_1\dots x_ny_n$, e o algorítimo para obtenção da forma normal pode ser aplicado; se $a$ e $l(a_1)$ estiverem no mesmo $A_i$, então o algorítimo se aplica a $[al(a_1)]l(a_2)\dots l(a_n)b$.

Claramente $\mid 1 \mid$ é a função identidade sobre $M$, e considerando os diversos casos (dependendo de onde os fatores inicias estão), podemos mostrar que: se $a, a' \in A_1 \cup A_2$, então

$$\mid a \mid\mid a' \mid = \mid aa' \mid .$$

Portanto, $\mid a^{-1} \mid = \mid a \mid^{-1}$ e cada $\mid a \mid$ é uma permutação de $M$. Se $S_M$ é o grupo de todas as permutações de $M$, então $a \longmapsto \mid a \mid$ é um homomorfismo de $A_i \longrightarrow S_M$ para $i = 1, 2$. Em particular, se $b \in B_1 \leq A_1$, $\mid b \mid : M \longrightarrow M$ está definido e $\mid b \mid = \mid \theta(b) \mid$.

A propriedade definidora de produtos livres une estes dois homomorfismos em um único homomorfismo

$$\varphi : A_1 * A_2 \longrightarrow S_M,$$

definido por $\varphi(l(a_1)l(a_2)\dots l(a_n)b) = \mid l(a_1) \mid\mid l(a_2) \mid \dots \mid l(a_n) \mid\mid b \mid$. Para todo $b \in B_1$, $\mid b \mid = \mid \theta(b) \mid$ nos dá que $b\theta(b^{-1}) \in Ker\varphi$, e então $\varphi$ induz um homomorfismo $\Theta : A_1 *_\theta A_2 = (A_1 * A_2)/N \longrightarrow S_M$, por

$$\begin{aligned} \Theta(l(a_1)l(a_2)\dots l(a_n)bN) &= \varphi(l(a_1)l(a_2)\dots l(a_n)b) \\ &= \mid l(a_1) \mid\mid l(a_2) \mid \dots \mid l(a_n) \mid\mid b \mid . \end{aligned}$$

Agora,

$$| \, l(a_1) \, || \, l(a_2) \, | \, \ldots \, | \, l(a_n) \, || \, b \, | \, (1) = l(a_1)l(a_2)\ldots l(a_n)b,$$

isto é, $\Theta(wN) : 1 \longrightarrow F(w)$. Então se $G(w)$ for uma outra forma normal em $wN$, teremos $\Theta(wN) : 1 \longrightarrow G(w)$, e assim $G(w) = F(w)$. Portanto, para cada elemento $wN \in A_1 *_\theta A_2$, existe uma única forma normal $F(w)$ com $wN = F(w)$. ■

**Teorema 1.59.** *Sejam $A_1$ e $A_2$ grupos, sejam $B_1$ e $B_2$ subgrupos isomorfos de $A_1$ e $A_2$, respectivamente, e seja $\theta : B_1 \longrightarrow B_2$ um isomorfismo.*

*a) Os homomorfismos (do pushout) $\lambda_i : A_i \longrightarrow A_1 *_\theta A_2$ são injetivos para $i = 1, 2$;*

*b) Se $A_i' = \lambda_i(A_i)$, então $\langle A_1', A_2' \rangle = A_1 *_\theta A_2$ e $A_1' \cap A_2' = \lambda_1(B_1) = \lambda_2(B_2)$.*

**Demonstração:** A prova de $a$). Se $1 \neq a_i \in A_i$, então a forma normal $F(a_i)$ associada a $a_i$ satisfaz: $F(a_i) \neq 1$. E ainda, se $\Theta$ é a função considerada no teorema anterior, então $\Theta(a_iN) \neq 1$. Mas $\Theta(a_iN) = \varphi\lambda(a_i) \neq 1$, o que implica que $\lambda_i(a_i) \neq 1$, e então $\lambda_i$ é um homomorfismo injetor.

Agora de $b$). Já que $A_1 *_\theta A_2 = (A_1 * A_2)/N$, temos $\langle A_1', A_2' \rangle = \langle A_1N/N, A_2N/N \rangle = A_1 *_\theta A_2$. Se $u \in A_1' \cup A_2'$, então existe $a_1 \in A_1$ e $a_2 \in A_2$, tais que $a_1N = u = a_2N$. E assim, $F(a_1) = l(a_1)b$ e $F(a_2) = l(a_2)b'$. Agora, pela unicidade da forma normal, temos que $l(a_1) = l(a_2)$ e $b = b'$. Mas $l(a_1) = l(a_2)$ pode ocorrer somente quando ambos forem iguais a 1, caso em que temos a igualdade das formas normais distintas $l(a_1)l(a_2)$ e $l(a_2)l(a_1)$. Logo, $1 = l(a_1) = l(a_2)$ e $bN = a_1N = u = a_2N = b'N$, e portanto $u \in \lambda_1(B_1) = \lambda_2(B_2)$.

Para a inclusão contrária tomemos $u \in \lambda_1(B_1)$. Como $B_1 \leq A_1$, temos que $u \in \lambda_1(A_1) = A_1'$. E já que $\lambda_1(B_1) = \lambda_2(B_2)$, temos que $u \in A_2'$. Portanto, $u \in A_1' \cap A_2'$. ■

**Corolário 1.60.** *Seja $E \cong A_1 *_\theta A_2$, tendo $B$ como subgrupo amalgamadado. Se $y_1, \ldots, y_n \in E$, onde $y_j \in A_{i_j}$ e $i_j \neq i_{j+1}$ e ainda, se $y_j \notin B$, para todo $j$, então $y_1y_2 \ldots, y_n \neq 1$.*

**Demonstração:** Segue imediatamente do Teorema 1.39. ■

**Teorema 1.61 (Teorema de Torção).** *Um elemento em $A_1 *_\theta A_2$ tem ordem finita se, e somente se, ele é conjugado a um elemento de ordem finita em $A_1$ ou $A_2$.*

**Demonstração:** Suponha um elemento de ordem finita em $A_1$ e $A_2$. Sem perda de generalidade podemos supor que o elemento esteja em $A_1$. Assim, seja $g \in A_1 *_\theta A_2$ tal que

$g = a_1^h$, onde $a_1 \in A_1$ e $h \in A_1 *_\theta A_2$. Como $a_1$ tem ordem finita e a conjugação preserva ordem, temos que $g$ tem ordem finita.

Agora a recíproca. Seja $g \in A_1 *_\theta A_2$ um elemento de ordem finita. Pelo Teorema 1.39 e pela Definição 1.57, podemos escrever $g = l(a_1)l(a_2)\dots l(a_n)b$. Vamos fazer indução sobre comprimento $n$ de $g$.

Se $n = 0$, então $g = b \in B_1 \leq A_1$, assim $g = g^g$, logo, é conjugado por um elemento de $A_1$. Agora, para todo $g \in A_1 *_\theta A_2$ tal que o comprimento de $g$ é menor que $n$, a implicação vale. Seja $g = l(a_1)l(a_2)\dots l(a_n)l(a_{n+1})b$, observe que os $l(a_1)$ e $l(a_{n+1})$ estão no mesmo $A_i$. Caso contrário $g$ teria ordem infinita, pelo fato, de que em

$$g^k = l(a_1)l(a_2)\dots l(a_n)l(a_{n+1})b.l(a_1)l(a_2)\dots l(a_n)l(a_{n+1})b.\dots.l(a_1)l(a_2)\dots l(a_n)l(a_{n+1})b,$$

não pode haver cancelamentos no lado direito da equação acima.

Sem perda de generalidade podemos supor que estão em $A_1$ pois, se estivessem em $A_2$, trocaríamos $b = \theta(b)$. Assim

$$l(a_1)^{-1}gl(a_1) = l(a_2)\dots l(a_n)l(a_{n+1})bl(a_1),$$

com isso $z = l(a_{n+1})bl(a_1) \in A_1$ e portanto

$$l(a_1)^{-1}gl(a_1) = l(a_2)\dots l(a_n)l(z)\tilde{b},$$

onde $\tilde{b} \in B_1$ pela hipótese de indução $l(a_1)^{-1}gl(a_1) = \tilde{a_i}^h$, onde $\tilde{a_i} \in A_i$ e $h \in A_1 *_\theta A_2$, então $g = \tilde{a_i}^{hl(a_1)^{-1}}$ temos o que queríamos. ■

## 1.5 Grupos p-Nilpotentes

Vamos introduzir a notação $(\pi - grupo)$. A letra $\pi$ exprime um conjunto de números primos fixados, $\pi$ pode ser todos os números primos, ou uma pequena parte deles.

Seja $\pi$ um conjunto de primos fixados. O conjunto de primos que não estão contidos em $\pi$ estão em $\pi'$. Quando $\pi$ consistir de um primo $p$, usaremos a notação $p$ e $p'$ em lugar da notação correta $\pi = \{p\}$ e $\pi' = \{p'\}$, respectivamente, onde $p'$ são todos os primos distintos de $p$. Um número natural $n$ é chamado $\pi$-número, se todo fator primo de $n$ pertence a $\pi$. Por definição, 1 é um $\pi$-número para qualquer $\pi$. Qualquer número natural $n$ é representado unicamente como um produto de $\pi$-números $n_\pi$ e um $\pi'$-número $n_{\pi'}$, neste caso chamamos $n_\pi$ de $\pi$-componente de $n$.

**Definição 1.62.** *Seja $G$ um grupo. Seja $g$ um elemento de ordem finita. Dizemos que $g$ é um $\pi$-elemento se a ordem de $g$ é um $\pi$-número. Um grupo $G$ é chamado de um $\pi$-grupo se todos os elementos são $\pi$-elementos. Quando $G$ é um grupo finito, seja $\pi(G)$ o conjunto de todos os números primos que dividem a ordem de $G$.*

$$\pi(G) = \{p \mid o(G) \equiv 0 \ mod \ p\}.$$

**Definição 1.63.** *Seja $G$ um grupo de ordem $m$. Para qualquer $p \in \pi(G)$, temos $m{=}p^n m'$, onde $p$ e $m'$ são co-primos. Um subgrupo de ordem $m'$ é chamado um $p$-complemento.*

**Definição 1.64.** *Seja $p$ um primo fixado. Um grupo finito $G$ é chamado $p$-nilpotente, se $o(G) = p^n m'$ e $G$ contém um subgrupo normal $H$ tal que $o(H) = m'$, onde $p$ e $m'$ são relativamente primos, isto é, $H$ é um $p$-complemento para algum subgrupo de $G$.*

**Exemplo 1.65.** *Em $S_3$ temos $o(S_3){=}\ 6{=}\ 2.3$ e assim, para $p{=}2$, $S_3$ é 2-nilpotente, pois existe $H_3 \trianglelefteq S_3$, onde $o(H_3) = 3$. Mas $S_3$ não é 3-nilpotente pois, não tem um subgrupo normal de ordem 2.*

**Proposição 1.66.** *Seja $G$ um grupo $p$-nilpotente. Se $P$ é um $p$-subgrupo de Sylow, um $p$-complemento normal $N$ de $G$ satisfaz:*

*a) $P \cap N = 1$;*

*b) $G = PN$.*

**Demonstração:** Mostraremos $a$). Seja $x \in P \cap N$. Logo $o(x)$ divide a $o(P) = p^n$ e, como $x \in N$, $o(x)$ divide $o(N) = m'$. Portanto $o(x)$ divide o $mdc(p^n, m') = 1$, e então $o(x) = 1$ o que implica em $x$ ser o elemento neutro.

Agora $b$). Como $N \trianglelefteq G$ implica em $NP \leq G$, mas

$$| \ NP \ | = \frac{| \ N \ || \ P \ |}{| \ N \cap P \ |} = \frac{| \ N \ || \ P \ |}{1} = | \ G \ |$$

e então $G = PN$. ■

Conseqüentemente, se um grupo $G$ contém um subgrupo normal $N$ que satisfaz as condições $a$) e $b$) da proposição acima, então temos que $G/N \cong P$ e $N = O_p'(G)$, isto é, $N$ é o $p'$-subgrupo normal maximal que contém todos os $p'$-subgrupos normais de $G$ (um $p'$-subgrupo são os subgrupos que na sua ordem não há $p$). Deste modo, $G$ é $p$-nilpotente. Um $p$-complemento normal é único (se existe), e é um subgrupo característico de $G$.

**Proposição 1.67.** *Se o conjunto $N$ de todos os $p'$-elementos de $G$ formam um subgrupo e $G/N$ é $p$-grupo, então $N$ é um $p$-complemento normal e $G$ é $p$-nilpotente.*

**Demonstração:** É fácil ver que $N$ é normal e, como $\mid G/N \mid = p^m$, isso implica que, a ordem de $G$ é $o(G) = p^m \mid N \mid$, onde $mdc(p^m, \mid N \mid) = p^n$, para algum $n \in \mathbb{N}$. Assim, basta mostrar que $p^n = 1$. Como $|N| = p^n m'$, ou seja $mdc(m', p^n) = 1$, devido ao fato de $N$ conter todos $p'$-elementos, teremos que para todo $y \in N$,

$$1 = (y)^{m'p^n} = (y^{m'})^{p^n} = 1^{p^n}.$$

A ordem de $N$ é o menor número que elevando a qualquer elemento de $N$ é trivial, o que implica em $p^n = 1$, portanto $N$ é um $p$-complemento e $G$ é $p$-nilpotente. ■

**Definição 1.68.** *Um grupo infinito é $p$-nilpotente se toda imagen finita é $p$-nilpotente.*

## 1.6 Módulos

Uma das coisas que distingue o tratamento moderno de álgebra comutativa é a grande ênfase em módulos. Os problemas extras que eles trazem fornecem maior clareza e simplicidade. Nesta seção damos as definições e propriedades elementares de módulos.

### 1.6.1 Módulos e Homomorfismo de Módulos

Seja $A$ um anel (comutativo com unidade). Um $\mathbf{A-módulo}$ é um grupo abeliano $M$ (com notação aditiva) no qual $A$ tem uma ação sobre ele, mais precisamente, é um par $(M, \phi)$, onde $M$ é um grupo abeliano e $\phi$ é uma aplicação de $A \times M$ sobre $M$ tal que o par $(a, x)$ é levado em $ax$, satisfeitas as seguintes condições:

(i) $a(x + y) = ax + ay$;

(ii) $(a + b)x = ax + bx$;

(iii) $(ab)x = a(bx)$;

(iv) $1x = x$,

para todo $a, b \in A$ e $x, y \in M$ (equivalentemente, $M$ um grupo abeliano junto com um homomorfismo de anel $A \to E(M)$, onde $E(M)$ é o anéis dos endomorfismos do grupo abeliano $M$).

A notação para um módulo é uma generalização comum de vários conceitos familiares, como os seguintes exemplos mostrados:

**Exemplo 1.69.** *Todo anel $A$ é um $A$-módulo.*

**Exemplo 1.70.** *Um ideal $I$ de $A$ é um $A$-módulo, pois $IA \subseteq I$.*

**Exemplo 1.71.** *Se $A = \mathbb{Z}$, então um $\mathbb{Z}$-módulo é um grupo abeliano (definido $nx$ por $\underbrace{x + \ldots + x}_{n \text{ vezes}}$*

Sejam $M, N$ $A$-módulos. A aplicação $f : M \to N$ é um **homomorfismo de A-módulos** se satisfizer as seguintes condições:

(i) $f(x + y) = f(x) + f(y)$;

(ii) $f(ax) = af(x)$,

para todo $a \in A$ e $x, y \in M$. Assim, $f$ é um homomorfismo para grupos abelianos, o qual comuta com a ação para cada $a \in A$. Se $A$ é um corpo, um homomorfismo de $A$-módulos é a mesma coisa de uma transformação linear para um espaço vetorial.

A composição de homomorfismos de $A$-módulos é novamente um homomorfismo de $A$-módulos.

### 1.6.2 Sub-módulos e Módulos Quocientes

Um sub-módulo $M'$ de $M$ é um subgrupo de $M$ que é fechado para a multiplicação de um elemento de $A$, ou seja, $am' \in M'$, para todo $a \in A$ e $m' \in M'$. O grupo abeliano $M/M'$ herda uma estrutura de $A$-módulo sobre $M$, definida por

$$a(x + M') = ax + M'.$$

Assim $M/M'$ é um $A$-módulo quociente de $M$ por $M'$. A aplicação natural de $M$ sobre $M/M'$ é um homomorfismo de $A$-módulos. Existe uma correspondência bijetora que preserva ordem entre os sub-módulos de $M$ que contém $M'$ e os sub-módulos de $M'' = M/M'$.

Se $f : M \to N$ é um homomorfismo de $A$-módulo, o *kernel* de $f$, que é o conjunto

$$Ker(f) = \{x \in M : f(x) = 0\},$$

é um sub-módulo de $M$. A *imagem* de $f$

$$Im(f) = f(M)$$

é sub-módulo de $N$.

Se $M'$ é um sub-módulo de $M$ tal que $M' \subseteq Kerf$, então $f$ dá origem a um homomorfismo $\bar{f} : M/M' \to N$, definido por, se $\bar{x} \in M/M'$ é a imagem de $x \in M$, então $\bar{f}(\bar{x}) = f(x)$. O kernel de $\bar{f}$ é $Kerf/M'$. O homomorfismo $\bar{f}$ é dito induzido por $f$. Em particular, levando $M' = Ker(f)$, temos um isomorfismo de $A$-módulos

$$M/Kerf \cong Imf.$$

### 1.6.3 Módulos Finitamente Gerados e Condição de Cadeia

Para facilitar e obtermos teoremas importantes, precisamos impor algumas condições de finitude. A maneira mais conveniente está na forma de condições de cadeia. Ela se aplica a anéis e módulos, e nesta seção consideraremos o caso de módulo.

Um $A$-módulo é livre se é isomorfo a um $A$-módulo da forma $\bigoplus_{i\in I} M_i$, onde cada $M_i \cong A$ (como um $A$-módulo). Um $A$-módulo livre finitamente gerado é portanto isomorfo a $A \oplus \ldots \oplus A$ ($n$ somandos), com a notação $A^n$. Convencionaremos, $A^0$ é o zero módulo, denotado por 0.

**Proposição 1.72.** *$M$ é um $A$-módulo finitamente gerado se, e somente se, $M$ é isomorfo a um quociente de $A^n$, para algum $n > 0$.*

**Demonstração:** Suponha $M$ finitamente gerado. Sejam $x_1, \ldots, x_n$ geradores de $M$. Defina $\phi : A^n \to M$ por $\phi(a_1, \ldots, a_n) = a_1x_1 + \ldots + a_nx_n$. Com isso $\phi$ é um homomorfismo de $A$-módulos sobrejetor, então

$$A^n/Ker(\phi) \cong M.$$

Agora a recíproca. Temos um homomorfismo de $A$-módulos $\phi : A^n \to M$. Se $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 na coordenada $i$), então $e_i$ $(1 \leq i \leq n)$ geram $A^n$. Como $\phi$ é sobrejetora, gerador é levado em gerador assim, $\{\phi(e_i)\}$ com $1 \leq i \leq n$ gera $M$, portanto $M$ é finitamente gerado, pois os $e_i$ são finitos. ■

Seja $\Sigma$ um conjunto parcialmente ordenado pela relação $\leq$ ( isto é, $\leq$ é reflexiva e transitiva e, se $x \leq y$ e $y \leq x$, isso implica que $x = y$).

**Proposição 1.73.** *As seguintes condições em $\Sigma$ são equivalentes:*

*(i) Cada seqüência crescente $x_1 \leq x_2 \leq \ldots$ em $\Sigma$ é estacionária ( isto é, existe $n$ tal que $x_n = x_{n+1} = \ldots$);*

*(ii) Cada conjunto não vazio de $\Sigma$ tem um elemento maximal.*

**Demonstração:** Mostraremos que *(i)* implica *(ii)*. Suponha, por contradição, que exista um subconjunto diferente de vazio $T$ em $\Sigma$ que não tenha elemento máximo, assim podemos construir indutivamente uma seqüência estritamente crescente, o que é um absurdo por hipótese.

Finalmente *(ii)* implica *(i)*. O conjunto $(x_m)_{m\geq 1}$ tem um elemento maximal, seja $x_n$ este elemento. ■

Se $\Sigma$ é um conjunto de sub-módulos do módulo $M$, ordenado pela relação $\subseteq$, então *(i)* é chamada condição cadeia ascendente (abreviação a.c.c) e *(ii)* a condição maximal. Um módulo $M$ que satisfaz uma destas condições é dito **Noetheriano**.

**Definição 1.74.** *Um anel $A$ é dito Noetheriano, se satisfaz a.c.c em seus ideais.*

**Exemplo 1.75.** *O grupo $(\mathbb{Z}/n\mathbb{Z}, +) = \{\bar{0}, \ldots, \overline{n-1}\}$ satisfaz a condição a.c.c. Na verdade, isto ocorre para todo grupo abeliano finito (como $\mathbb{Z}$-módulo).*

**Exemplo 1.76.** *O anel $\mathbb{Z}$ (como $\mathbb{Z}$-módulo) satisfaz a.c.c.*

**Exemplo 1.77.** *Seja $G$ um subgrupo de $\mathbb{Q}/\mathbb{Z}$ constituído de todos os elementos de ordem $p^n$, para um primo fixado. Então $G$ tem um único subgrupo $G_n$ de ordem $p^n$ para cada $n \geq 0$, e*

$$G_0 \subset G_1 \subset \ldots \subset G_n \subset \ldots$$

*de forma que $G$ não satisfaz a.c.c.*

**Exemplo 1.78.** *O anel $\mathbb{Z}$ é Noetheriano. O anel $\mathbb{Z}/n\mathbb{Z}$, para $n \neq 0$, é Noetheriano.*

**Exemplo 1.79.** *Qualquer corpo é Noetheriano.*

**Proposição 1.80.** *$M$ é um $A$-módulo Noetheriano se, e somente se, cada sub-módulo de $M$ é finitamente gerado.*

**Demonstração:** Suponhamos $M$ um A-módulo Noetheriano. Sejam $N$ um sub-módulo e $\Sigma$ o conjunto de todos os sub-módulos de $N$ finitamente gerados. Então, $\Sigma$ não é vazio, pois $0 \in \Sigma$ e portanto existe um elemento maximal, a saber, $N_0$. Se $N_0 \neq N$, considere o sub-módulo, onde $x \in N$ e $x \notin N_0$, assim temos que $N_0 + Ax$ é finitamente gerado e contém $N_0$ estritamente absurdo, pois $N_0$ é maximal.

A recíproca. Seja $M_1 \subseteq M_2 \subseteq \ldots$ uma cadeia ascendente de sub-módulos de $M$. Então $N = \bigcup_{n=1}^{\infty} M_n$ é um sub-módulo de $M$, conseqüentemente é finitamente gerado. Assim, seja gerado por $x_1, \ldots, x_r$ e $x_i \in M_{n_i}$. Tome $n = \max_{i=1}^{r} n_i$, logo $x_i \in M$, dessa forma $M_n = N$ e portanto a cadeia é estacionária. ■

A condição de Noetheriano é justamente a condição direta de finitude para fazer muitos dos teoremas trabalhados nesta área.

**Proposição 1.81.** *Seja* $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ *uma seqüência exata de A-módulos. Então*

*i) M é Noetheriano se, e somente se, M′ e M″ são Noetheriano;*

**Demonstração:** Suponha $M$ Noetheriano. Uma cadeia ascendente de sub-módulos de $M'$ é também uma cadeia em $M$, logo, estacionária.

Seja

$$M_1/M' \subseteq M_2/M' \subseteq \ldots \tag{1.1}$$

uma cadeia ascendente de sub-módulos de $M''$, logo, temos que $M' \subseteq M_1 \subseteq M_2 \subseteq \ldots$ é uma cadeia de sub-módulo em $M$, portanto estacionária. Como temos uma correspondência biunívoca entre as duas cadeias, então 1.1 é estacionária.

Recíproca. Seja $(L_n)_{n\geq 1}$ uma cadeia ascendente de sub-módulos de $M$. Então $(\alpha^{-1}(L_n))$ é uma cadeia em $M'$ e $(\beta(L_n))$ é uma cadeia em $M''$. Para um $n$ muito grande, ambas são cadeias estacionárias, portanto a cadeia $(L_n)$ é estacionária em $M$. ■

**Corolário 1.82.** *Se* $M_i (1 \leq i \leq n)$ *são Noetherianos A-módulos, então* $\bigoplus_{i=1}^{n} M_i$ *também é.*

**Demonstração:** Aplicando indução na Proposição 1.81 para a seqüência exata

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0\,.$$

■

**Proposição 1.83.** *Seja $A$ um anel Noetheriano, $M$ um $A$-módulo finitamente gerado. Então $M$ é Noetheriano.*

**Demonstração:** Pela Proposição 1.72, temos que $M$ é um quociente de $A^n$, logo temos uma seqüência exata da forma

$$0 \longrightarrow K \longrightarrow A^n \longrightarrow M \longrightarrow 0\,,$$

onde, pelo Corolário 1.82, $A^n$ é Noetheriano.

Assim, pela Proposição 1.81 obtemos o que queríamos. ■

**Definição 1.84.** *Seja $G$ um grupo abeliano e $R$ um anel comutativo com unidade, o* **anel de grupo RG** *é definido como o conjunto de todas as somas formais $\sum_{g\in G} r_g g$, onde $r_g \in R$ e $r_g \neq 0$ para um número finito, junto com a seguintes operações:*

*i)* $(\Sigma_g r_g g) + (\sum_g r'_g g) = \sum_g \sum_g (r_g + r'_g)g$;

*ii)* $(\sum_g r_g g)(\sum_g r'_g g) = \sum_g (\sum_{yz=g} r_y r'_z)g$.

Não é difícil verificar que com estas regras $RG$ é um anel comutativo com unidade.

**Proposição 1.85** ([10, 15.3.3])**.** *Seja $G$ um grupo abeliano finitamente gerado e $R$ um anel comutativo com unidade Noetheriano. Então o anel de grupo $RG$ é também Noetheriano.*

**Proposição 1.86** ([10, 15.4.4])**.** *Se $G$ é um grupo abeliano finitamente gerado. Então todo $\mathbb{Z}G$-módulo simples $M$ é finito.*

**Teorema 1.87.** *Seja $G$ um grupo abeliano finitamente gerado e $M$ um $\mathbb{Z}G$-módulo finitamente gerado. Então $M$ é residualmente finito.*

**Demonstração:** Temos que mostrar que a intersecção $\bigcap N$ de todos os sub-módulos de índice finito de $M$ é trivial. Para isso é suficiente mostrar que para todo $m \in M - \{0\}$ existe um sub-módulo $\mathcal{M}$ de índice finito tal que $m \notin \mathcal{M}$.

Sejam $m \neq 0$, onde $m \in M$, e $\Phi = \{N \leq M : m \notin N\}$. Temos que $\Phi \neq \varnothing$, pois $\{0\} \in \Phi$. Seja

$$N_1 \subset N_2 \subset \ldots \subset N_n \subset \ldots$$

uma cadeia de sub-módulos de $\Phi$, assim temos que $\bigcup N_i \in \Phi$. Pelo Lema de Zorn, existe um elemento maximal $\mathcal{M}$ em $\Phi$. Vamos mostrar que $M/\mathcal{M}$ é finito.

Note que qualquer sub-modulado $M$ que contém $\mathcal{M}$ propriamente, obrigatoriamente contém $m$. Portanto existe um único menor sub-módulo $N$ de $M$ que contém $\mathcal{M}$ e $m$ (o sub-módulo gerado por $\{m, x | x \in \mathcal{M}\}$). Agora seja $N$ o primeiro sub-módulo que contém $m$ e $\mathcal{M}$. Com isso construa a cadeia de sub-módulos

$$\mathcal{M} \subsetneq N = N_1 \subseteq \ldots \subseteq N_n \subseteq \ldots \subseteq M$$

onde $N_{i-1}/N_i$ são simples. Pela Proposição 1.85, $\mathbb{Z}G$ é Noetheriano e portanto, pela Proposição 1.83, $M$ é Noetheriano. Assim esta cadeia estabiliza. Com isso teremos um número finito de quocientes simples, onde cada quociente é um $\mathbb{Z}Q$-módulo simples com $Q$ finitamente gerado, pela Proposição 1.86, são finitos. Então, o quociente $M/\mathcal{M}$ é finito, conseguimos um sub-módulo de $M$ que não contém $m$ e o quociente é finito. ■

# CAPÍTULO 2

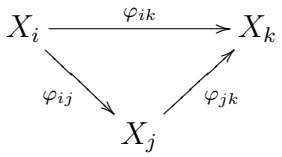
# Grupos Pro-finitos

Neste capítulo, falaremos de limite inverso e completamento pro-$\mathcal{C}$, onde $\mathcal{C}$ é uma classe de grupos abstratos. Mostraremos também um fato interessante para grupos p-nilpotentes, onde, o completamento pro-p pode ser identificado com um subgrupo do completamento pro-finito.

## 2.1 Limite Inverso

Um **conjunto dirigido I** é um conjunto não vazio parcialmente ordenado tal que, para quaisquer $i_1, i_2 \in I$, existe um elemento $j \in I$ para o qual $i_1 \preceq j$ *e* $i_2 \preceq j$.

**Definição 2.1.** *Um* **sistema inverso** (**ou projetivo**) *de espaços (grupos) topológicos sobre $I$, consiste de uma família de espaços (grupos) topológicos $\{X_i \mid i \in I\}$, e uma família de aplicações contínuas (homomorfismos contínuos) $\varphi_{ij} : X_i \longrightarrow X_j$, definidos quando $i \succeq j$, tal que $\varphi_{ii} = id_{X_i}$ e os diagramas*




*comutam para todo $i \succeq j \succeq k$, ou seja, $\varphi_{ik} = \varphi_{jk}\varphi_{ij}$.*

Denotaremos um sistema inverso por $(X_i, \varphi_{ij}, I)$, ou simplesmente $(X_i, \varphi_{ij})$.

**Exemplo 2.2.** *Seja $G$ um grupo finito e $I$ o conjunto $\{1\}$. Então $I$ é um conjunto dirigido. Defina a aplicação identidade*

$$\begin{aligned} Id_{11} \ : \ G_1 &\longrightarrow G_1 \\ g &\longmapsto g \end{aligned}$$

*para todo $g \in G$. Assim, $Id_{11} = id_{G_1}$ e o diagrama,*

$$\begin{array}{ccc} G_1 & \xrightarrow{\quad Id_{11} \quad} & G_1 \\ & {\scriptstyle Id_{11}} \searrow \quad \nearrow {\scriptstyle Id_{11}} & \\ & G_1 & \end{array}$$

*comuta, para todo $G_1 \succeq G_1 \succeq G_1$. Logo $(G_1, Id_{11})$ é um sistema inverso.*

**Exemplo 2.3.** *Sejam $(\mathbb{Z}, +)$, $I = \mathbb{N}$ e a família de subgrupos $\{\mathbb{Z}/p^i\mathbb{Z} : i \in \mathbb{N}\}$, onde $p$ é um primo fixo. Para $i \succeq j$, onde $\succeq$ é ordem natural $\geq$, defina*

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

*Assim, $\varphi_{ii} = id_{\mathbb{Z}/p^i\mathbb{Z}}$ e $\varphi_{ik} = \varphi_{jk}\varphi_{ij}$ para todo $\mathbb{Z}/p^i\mathbb{Z} \succeq \mathbb{Z}/p^k\mathbb{Z} \succeq \mathbb{Z}/p^j\mathbb{Z}$. Logo $(\mathbb{Z}/p^i\mathbb{Z}, \varphi_{ij})$ é um sistema inverso.*

**Exemplo 2.4.** *Sejam $(\mathbb{Z}, +)$, $I = \mathbb{N}$ e a família de subgrupos $\{\mathbb{Z}/i\mathbb{Z} : i \in \mathbb{N}\}$. Para $i \succeq j$, onde $\succeq$ é ordem natural $\geq$ e $j \mid i$, defina*

$$\begin{aligned} \varphi_{ij} \ : \ \mathbb{Z}/i\mathbb{Z} &\longrightarrow \mathbb{Z}/j\mathbb{Z} \\ n + i\mathbb{Z} &\longmapsto n + j\mathbb{Z} \end{aligned}$$

*Assim, $\varphi_{ii} = id_{\mathbb{Z}/i\mathbb{Z}}$ e $\varphi_{ik} = \varphi_{jk}\varphi_{ij}$ para todo $\mathbb{Z}/i\mathbb{Z} \succeq \mathbb{Z}/k\mathbb{Z} \succeq \mathbb{Z}/j\mathbb{Z}$. Logo $(\mathbb{Z}/i\mathbb{Z}, \varphi_{ij})$ é um sistema inverso.*

**Exemplo 2.5.** *Seja $G$ um grupo e $I$ a família de subgrupos normais de índice finito (ou índice potência de $p$) ordenado pela inclusão inversa ( se $U_i \succeq U_j$ se e somente se $U_i \subseteq U_j$). Note que $I$ é dirigido, pois para quaisquer $U_1, U_2 \in I$, $V = U_1 \cap U_2 \in I$. Para $U \preceq V$, defina*

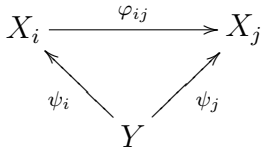
$$\begin{aligned} \varphi_{VU} \ : \ G/V &\longrightarrow G/U \\ gV &\longmapsto gU \end{aligned}$$

*para todo $g \in G$. Assim, $\varphi_{UU} = id$ e o diagrama*

$$\begin{array}{ccc} G/U & \xrightarrow{\quad \varphi_{UV} \quad} & G/W \\ & {\scriptstyle \varphi_{UW}} \searrow \quad \nearrow {\scriptstyle \varphi_{VW}} & \\ & G/V & \end{array}$$

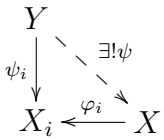
*comuta, para todo* $U \succeq V \succeq W$. *Logo* $(G_U, \varphi_{VU})$ *é um sistema inverso.*

Agora sejam $(X_i, \varphi_{ij})$ um sistema inverso e Y um espaço (grupo) topológico. Vamos chamar uma família de aplicações contínuas (homomorfismos contínuos) $\{\psi_i : Y \longrightarrow X_i \mid i \in I\}$ de aplicações **compatíveis**, se $\varphi_{ij}\psi_i = \psi_j$ sempre que $i \succeq j$, ou seja, os diagramas




comutam.

**Definição 2.6.** *Um* **limite inverso** *de um sistema inverso* $(X_i, \varphi_{ij})$ *é um espaço (grupos) topológico X junto com aplicações contínuas (homomorfismos contínuos) compatíveis* $\{\varphi_i : X \longrightarrow X_i \mid i \in I\}$ *que satisfaz a seguinte propriedade universal: se Y é um espaço (grupo) topológico e* $\{\psi_i : Y \longrightarrow X_i\}$ *uma família de aplicações contínuas (homomorfismos contínuos) compatíveis, então existe uma única aplicação contínua (um único homomorfismo contínuo)* $\psi : Y \longrightarrow X_i$, *tal que* $\varphi_i\psi = \psi_i$, *para todo* $i \in I$. *Deste modo requeremos que, para cada diagrama*



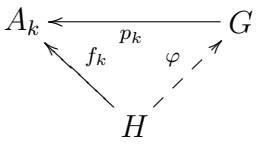

*exista uma única* $\psi$ *tal que o diagrama comuta.*

Sejam $K$ um conjunto qualquer e $\{A_k : k \in K\}$ uma família de grupos.

**Definição 2.7.** *O* **produto direto**, *denotado por* $\prod_{k\in K} A_k$, *é o grupo onde todos os elementos são "vetores"*$(a_k)$ *e têm a seguinte operação*

$$(a_k)(b_k) = (a_k b_k).$$

**Teorema 2.8.** *Sejam G um grupo,* $\{A_k : k \in K\}$ *uma família de grupos e* $\{p_k : G \to A_k : k \in K\}$ *uma família de homomorfismos. Então* $G = \prod_{k\in K} A_k$ *se, e somente se, dado algum grupo H e uma família de homomorfismos* $\{f_k : H \to A_k : k \in K\}$, *existe um único homomorfismo* $\varphi : H \to G$ *da forma que o seguinte diagrama comute para todo k:*



**Demonstração:** O argumento é análogo ao Teorema 1.3, basta definir $p_k : \prod_{k\in K} A_k \to H$ como projeção dos vetores sobre a k-ésima coordenada. ■

A proposição seguinte vai nos mostrar que o limite inverso existe e é único.

**Propriedade 2.9.** *Seja $(X_i, \varphi_{ij})$ um sistema inverso indexado por I, um conjunto dirigido.*

*a) Se $(X^{(1)}, \varphi_i^{(1)})$ e $(X^{(2)}, \varphi_i^{(2)})$ são limites inversos de um sistema inverso $(X_i, \varphi_{ij})$, então existe um isomorfismo $\overline{\varphi} : X^{(1)} \longrightarrow X^{(2)}$ de maneira que $\varphi_i^{(2)}\overline{\varphi} = \varphi_i^{(1)}$, para cada i;*

*b) Seja $C = \prod_{i\in I} X_i$ o produto direto e, para cada i, seja $\pi_i$ a aplicação projeção de C em $X_i$. Defina*

$$X = \{(x_i) \in \prod_{i\in I} X_i \mid \varphi_{ij}(x_i) = x_j \ \forall\ i, j \ com\ i \geq j\}$$

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

**Demonstração:** Mostraremos $a$). A demonstração de unicidade segue o modelo comum. Primeiramente, aplicando a propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$ para a família $\{\varphi_i^{(2)}\}$, temos

$$\begin{array}{ccc} X^{(2)} & & \\ {\scriptstyle \psi_i^{(2)}}\downarrow & \searrow^{\exists!\psi^{(1)}} & \\ X_i & \xleftarrow{\ \varphi_i\ } & X^{(1)} \end{array}$$

Com isso obtemos $\psi^{(1)} : X^{(2)} \longrightarrow X^{(1)}$ tal que $\varphi_i^{(1)}\psi^{(1)} = \varphi_i^{(2)}$. Analogamente, aplicando a propriedade universal de $(X^{(2)}, \varphi_i^{(2)})$ para a família $\{\varphi_i^{(1)}\}$, temos

$$\begin{array}{ccc} X^{(1)} & & \\ {\scriptstyle \psi_i^{(1)}}\downarrow & \searrow^{\exists!\psi^{(2)}} & \\ X_i & \xleftarrow{\ \varphi_i\ } & X^{(2)} \end{array}$$

Com isso obtemos $\psi^{(2)} : X^{(1)} \longrightarrow X^{(2)}$ tal que $\varphi_i^{(2)}\psi^{(2)} = \varphi_i^{(1)}$. Pela propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$ para a família $\{\varphi_i^{(1)}\}$, existe uma única aplicação $\theta : X^{(1)} \longrightarrow X^{(1)}$ tal que $\varphi_i^{(1)}\theta = \varphi_i^{(1)}$, o que implica em $\theta = id_{X^{(1)}}$. Mas $\psi^{(2)}\psi^{(1)} : X^{(1)} \longrightarrow X^{(1)}$ também satisfaz $\varphi_i^{(1)}\psi^{(2)}\psi^{(1)} = \varphi_i^{(1)}$. Como a aplicação é única, obtemos $\psi^{(2)}\psi^{(1)} = id_{X^{(1)}}$. Analogamente, $\psi^{(1)}\psi^{(2)} = id_{X^{(2)}}$. Logo $\psi^{(2)}$ é um isomorfismo e sua inversa é $\psi^{(1)}$.

Agora $b$) Como $\varphi_i = \pi_i \mid_X$ para cada $i$, temos que $\varphi_i$ são aplicações contínuas e a definição de $X$ assegura que $\varphi_{ij}\varphi_i = \varphi_j$ sempre que $i \succeq j$.

Agora, suponhamos que $\{\psi_i : Y \longrightarrow X_i\}$ é uma família de aplicações contínuas. Vamos mostrar que existe uma única aplicação contínua $\psi : Y \longrightarrow X$ tal que $\varphi_i\psi = \psi_i$ para cada i.

Seja $\overline{\psi} : Y \longrightarrow C$ definida por $\overline{\psi}(y) = (\psi_i(y))$. Deste modo $\pi_i\overline{\psi} = \psi_i$ para cada i, pois $\pi_i\overline{\psi}(y) = \pi(\psi_i(y)) = \psi_i(y)$. Temos também que $\overline{\psi}$ é uma aplicação contínuas, já que $\psi_i$, a composição com a projeção, é contínua para cada $i$.

Se $i \succeq j$, então

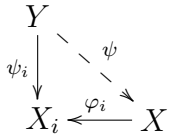
$$\pi_j\overline{\psi} = \psi_j \Rightarrow \varphi_{ij}\pi_i\overline{\psi} = \varphi_{ij}\psi_i = \psi_j.$$

Com isso

$$\varphi_{ij}\pi_i\overline{\psi}(y) = \psi_j(y) = \pi_j\overline{\psi}(y) \Rightarrow \varphi_{ij}\pi_i((\psi_i(y))) = \pi_j((\psi_i(y))) \Rightarrow \varphi_{ij}(\psi_i(y)) = \psi_j(y)$$

e assim $\overline{\psi} : Y \longrightarrow X \subseteq C$.

Agora defina $\psi : Y \longrightarrow X$ por $\psi(y) = \overline{\psi}(y)$ para cada $y \in Y$. Deste modo, $\psi$ é uma aplicação contínua e $\varphi_i\psi = \psi_i$, pois $\varphi_i = \pi_i|_X$ e $\pi_i\overline{\psi} = \psi_i$, para cada $i$. Se tivermos uma outra aplicação $\psi'$ satisfazendo $\varphi_i\psi' = \psi_i$ para cada $i$ e $y \in Y$ então, para cada entrada de $\psi'(y)$ em $X_i$ teremos $\psi_i(y)$, o mesmo ocorrendo para cada entrada de $\psi(y)$ em $X_i$. Portanto $\psi'(y) = \psi(y)$ e então existe uma única aplicação contínua tal que o diagrama




comuta. ■

O resultado acima mostra que um limite inverso de um sistema inverso $(X_i, \varphi_{ij})$ existe e é único, a menos de isomorfismo. Denotaremos por $\varprojlim (X_i, \varphi_{ij})$, $\varprojlim_{i\in I} X_i$, ou simplesmente, $\varprojlim X_i$.

**Definição 2.10.** *Um grupo $G$ é um* **grupo pro − finito** *se é um limite inverso $\varprojlim G_i$ de grupos finitos, onde cada grupo $G_i$ tem topologia discreta.*

Os grupos pro-finitos são caracterizados de várias maneiras, como podemos ver abaixo.

**Teorema 2.11** ([9, Teorema 2.1.3])**.** *Seja $G$ um grupo topológico. Então são equivalentes:*

*a) $G$ é pro-finito;*

*b) G é compacto, Hausdorff e a identidade 1 de G admite um sistema fundamental $\mathfrak{U}$ de vizinhanças abertas tais que $\bigcap_{U\in\mathfrak{U}} U = 1$ e cada U é um subgrupo normal aberto;*

*c) A identidade 1 de G admite um sistema fundamental $\mathfrak{U}$ de vizinhanças abertas tal que cada $U \in \mathfrak{U}$ é um subgrupo normal aberto de G e $G = \varprojlim_{U\in\mathfrak{U}} G/U$.*

**Lema 2.12.** *Seja $\widehat{G} = \varprojlim_{i\in I} G_i$, onde $\{G_i, \varphi_{ij}, I\}$ é um sistema inverso de grupos finitos $G_i$ e $\varphi_i : \widehat{G} \longrightarrow G_i$ o homomorfismo projetivo para $i \in I$. Então*

$$\{S_i \mid S_i = Ker(\varphi_i)\}$$

*é um sistema fundamental de vizinhanças abertas do elemento identidade 1 em $\widehat{G}$.*

**Demonstração:** Considere uma família de vizinhanças do 1 em $\Pi_{i\in I}G_i$, da forma

$$(\Pi_{i\neq i_1,\ldots,i_t}G_i) \times \{1\}_{i_1} \times \ldots \times \{1\}_{i_t},$$

para alguma coleção finita de índices, onde cada $\{1\}_{i_k}$ denota um subconjunto de $G_i$ aberto, pois $G_{i_k}$ é finito na topologia discreta. Como cada $G_i$ é discreto, esta família é um sistema fundamental de vizinhanças do elemento identidade de $(\Pi_{i\in I}G_i)$.

Agora temos que

$$\widehat{G} \cap [(\Pi_{i\neq i_1,\ldots,i_t}G_i) \times \{1\}_{i_1} \times \ldots \times \{1\}_{i_t}]$$

será um sistema fundamental de vizinhanças do elemento identidade de G.

Seja $i_o \in I$ tal que $i_0 \succeq i_1, \ldots, i_t$. Com isso obtemos

$$\widehat{G} \cap [(\Pi_{i\neq i_1,\ldots,i_t}G_i) \times \{1\}_{i_1} \times \ldots \times \{1\}_{i_t}] = \widehat{G} \cap [(\Pi_{i\neq i_0}G_i) \times \{1\}_{i_o}],$$

pelas $\varphi_{i_0 i_j}(1_{i_j}) = 1_{i_0}$, portanto o sistema fundamental de vizinhanças do 1 é

$$\widehat{G} \cap [(\Pi_{i\neq i_0}G_i) \times \{1\}_{i_o}],$$

finalmente observe que

$$\hat{G} \cap [(\Pi_{i\neq i_0}G_i) \times \{1\}_{i_o}] = Ker(\varphi_{i_0}) = S_{i_0}.$$

■

**Observação 2.13.** *Um grupo discreto é pro-finito se, e somente se, é um grupo finito. Todo subgrupo aberto de um grupo pro-finito $G$ é fechado. Além disso, um subgrupo fechado de um grupo pro-finito $G$ é aberto se, e somente se, tem índice finito. Se $H$ é subgrupo fechado de $G$, então $H$ é um grupo pro-finito com a topologia induzida, que consiste nos abertos formados da intersecção de $H$ com os abertos da topologia de $G$. Um subgrupo normal de índice finito será denota por $U \lhd_f G$.*

## 2.2 Completamento

Exemplos importantes de grupos pro-finitos vém de completamentos de grupos abstratos. Seja $\mathcal{C}$ denotando a classe de grupos finitos ou p-grupos finitos. Poderíamos definir de maneira mais geral como uma família não vazia de grupos finitos com a propriedade que, para todo $U_1, U_2 \in \mathcal{C}$, existe um grupo $V \in G$ tal que $V \leq U_1 \cap U_2$ (por exemplo, se $\mathcal{C}$ é fechada para subgrupos, quocientes e produto direto finito), mas só trataremos das mencionadas primeiro.

**Definição 2.14.** *Seja $G$ um grupo abstrato e considere $\mathcal{N} = \{N \lhd_f G : G/N \in \mathcal{C}\}$, a coleção de todos os subgrupos normais de índice finito $N$ em $G$ tais que $G/N \in \mathcal{C}$ ordenado pela inclusão inversa, com no Exercício 2.5, assim temos um sistema inverso $(G/N, \varphi_{NM})$ em $\mathcal{C}$. Então o limite inverso*

$$G_{\widehat{\mathcal{C}}} = \varprojlim_{N \in \mathcal{N}} G/N$$

*é chamado o completamento pro-$\mathcal{C}$ de $G$.*

Assim, $G_{\widehat{\mathcal{C}}}$ é um grupo pro-finito por ser o limite inverso de grupos finitos em $\mathcal{C}$. Se $\mathcal{C}$ é a família de todos os grupos finitos, então $G_{\widehat{\mathcal{C}}} = \widehat{G}$ é chamado de completamento pro-finito de $G$. Se $p$ é um primo e $\mathcal{C}$ é a classe de todos os $p$-grupos finitos, então $G_{\widehat{\mathcal{C}}}$ é chamado de completamento pro-$p$ de $G$ normalmente denotado por $G_{\widehat{p}}$.

**Exemplo 2.15.** *Seja $G$ um grupo finito e defina um sistema inverso como no Exemplo 2.2 o completamento pro-finito de $G$ é $\widehat{G} = \varprojlim_{1} G_1$, um grupo pro-finito de $G$. Observe que $\widehat{G} = G$ pois, pela Proposição 2.9*

$$\varprojlim_{1} G_1 = \{x_1 \in G_1 : Id_{11}(x_1) = x_1, \text{ se } 1 \succeq 1\} = G.$$

**Exemplo 2.16.** *Seja $G = (\mathbb{Z}, +)$ e defina um sistema inverso como no Exemplo* 2.3. *O completamento pro-p de $G$ é $\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$, o anel dos inteiros p-ádicos. De fato, pela Proposição* 2.9

$$\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \{(x_i + p^i\mathbb{Z}) \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} : \varphi_{ij}(x_i + p^i\mathbb{Z}) = x_j + p^j\mathbb{Z}, se\ i \succeq j\}.$$

*Assim, $\varphi_{ij}(x_i+p^i\mathbb{Z}) = x_j+p^j\mathbb{Z}$ para $i \succeq j$ e, por definição $\varphi_{ij}(x_i+p^i\mathbb{Z}) = x_i+p^j\mathbb{Z}$. Portanto, $x_i + p^j\mathbb{Z} = x_j + p^j\mathbb{Z} \Rightarrow x_i \equiv x_j (mod\ p^j\mathbb{Z})$. Então, podemos escrever o limite inverso da forma*

$$\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \{(x_i) \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} : x_i \equiv x_j (mod\ p^j\mathbb{Z}), i \succeq j\} = \mathbb{Z}_p.$$

**Exemplo 2.17.** *Seja $G = (\mathbb{Z}, +)$ e defina um sistema inverso como no Exemplo* 2.4 *o completamento pro-finito de $G$ é $\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$, o anel pro-finito de $G$. Observe que $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. De fato, pela Proposição* 2.9,

$$\widehat{\mathbb{Z}} = \{(x_i) \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} : \varphi_{ij}(x_i + i\mathbb{Z}) = x_j + j\mathbb{Z},\ se\ j \mid i\}.$$

*Temos que $\widehat{\mathbb{Z}}$ é pro-nilpotente, pois é o limite inverso de grupos nilpotentes e, pela [12, Proposição 2.4.3] $\widehat{\mathbb{Z}} = \prod_p S_p$, onde $S_p$ são os pro-p subgrupos de Sylow. No exemplo anterior, podemos trocar $i$ por $p^i$ e $j$ por $p^j$ pois, se vale para $i$ e $j$, vale também para $p^i$ e $p^j$, portanto*

$$\mathbb{Z}_p = \{(x_{p^i}) \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} : \varphi_{p^ip^j}(x_{p^i} + p^i\mathbb{Z}) = x_{p^j} + p^j\mathbb{Z},\ se\ p^j \mid p^i\},$$

*e temos que $\mathbb{Z} \leq \widehat{\mathbb{Z}}$.*

*Seja $S$ um subgrupo pro-p de $\widehat{\mathbb{Z}}$. Então*

$$S = \varprojlim_{i\in I\subseteq\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z} = \{(x_{p^i}) \in \prod_{p\in I} \mathbb{Z}/p^i\mathbb{Z} : \varphi_{p^ip^j}(x_{p^i} + p^i\mathbb{Z}) = x_{p^j} + p^j\mathbb{Z},\ se\ p^j \mid p^i\},$$

*o que implica $S \leq \mathbb{Z}_p$. Assim, todo subgrupo pro-p de $\widehat{\mathbb{Z}}$ está em $\mathbb{Z}_p$, logo, é maximal, sendo os subgrupos pro-p de Sylow de $\widehat{\mathbb{Z}}$, tendo o que queríamos.*

**Exemplo 2.18.** *Seja $G$ um grupo qualquer. Definimos um sistema inverso $\{G/U \mid U \lhd_f G\}$ como no Exemplo* 2.5, *e então $\widehat{G} = \varprojlim G/U$ é o completamento pro-finito de $G$. Notemos*

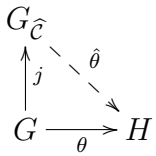
*que, pela propriedade universal, existe um homomorfismo*

$$\begin{aligned} i \ : G &\longrightarrow \widehat{G} \\ g &\longmapsto (gU). \end{aligned}$$

*Observe que i não é necessariamente injetora, pois o núcleo é* $Ker(i) = \cap U$ *e assim, se G é residualmente finito,* $Ker(i) = \cap U = \{1\}$ *e portanto temos um imersão de G em* $\widehat{G}$.

**Exemplo 2.19.** *Se no exemplo anterior todos os U têm índice* $p^n$, *onde* $n \in \mathbb{N}$, *o grupo pro-finito* $G_{\hat{p}} = \varprojlim G/U$ *é chamado de completamento pro-p de G. Se* $i : G \longrightarrow G_{\hat{p}}$ *é um monomorfismo, então G é residualmente p-grupo finito.*

Podemos caracterizar o completamento pro-$\mathcal{C}$ de um grupo $G$ abstrato, onde $\mathcal{C}$ será a classe de grupos finitos ou $p$-grupos finitos, consistindo de um grupo pro-$\mathcal{C}$ $G_{\widehat{\mathcal{C}}}$ e um homomorfismo contínuo $j : G \longrightarrow G_{\widehat{\mathcal{C}}}$, com a seguinte propriedade: sempre que $\theta : G \longrightarrow H$ for um homomorfismo contínuo de $G$ em um grupo finito $H \in \mathcal{C}$, existe um único homomorfismo contínuo $\hat{\theta} : G_{\widehat{\mathcal{C}}} \longrightarrow H$ tal que o diagrama



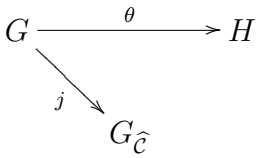

comuta.

**Proposição 2.20** ([12, Proposição 1.4.1])**.** *Sejam* $G_{\widehat{\mathcal{C}}} = \varprojlim G/U$ *e a aplicação j que leva G em* $G_{\widehat{\mathcal{C}}}$ *definida por* $g \longmapsto (gU)$. *O par* $(G_{\widehat{\mathcal{C}}}, j)$ *tem a propriedade do completamento pro-*$\mathcal{C}$ *de G.*

**Proposição 2.21** ([12, Proposição 1.4.2])**.** *Sejam G um grupo. Suponha que* $G_{\widehat{\mathcal{C}}}$ *é um grupo pro-finito e* $j : G \longrightarrow G_{\widehat{\mathcal{C}}}$ *um homomorfismo contínuo. Então, as seguintes propriedades são equivalentes:*

*(a) (*$G_{\widehat{\mathcal{C}}}$*,j) tem a propriedade definida do completamento de G com respectivo conjunto dirigido I;*

*(b) Para cada diagrama*



*com $H$ pro-finito e $\theta$ um homomorfismo contínuo, existe um único homomorfismo contínuo $\hat{\theta} : G_{\widehat{\mathcal{C}}} \longrightarrow H$ tal que o diagrama comuta.*

**Proposição 2.22** ([12, Proposição 1.4.3])**.** *Se $(G^{(1)}_{\widehat{\mathcal{C}}}, j_1)$,$(G^{(2)}_{\widehat{\mathcal{C}}}, j_2)$ são completamentos de $G$ com respectivo $I$, então existe um isomorfismo $\alpha : G^{(1)}_{\widehat{\mathcal{C}}} \longrightarrow G^{(2)}_{\widehat{\mathcal{C}}}$ tal que $\alpha j_1 = j_2$.*

**Proposição 2.23** ([12, Proposição 1.4.4])**.** *Seja $(G_{\widehat{\mathcal{C}}}, j)$ o completamento pro-$\mathcal{C}$ de $G$. Então*

*(a) $j(G)$ é denso em $G_{\widehat{\mathcal{C}}}$;*

*(b) $Ker(j) = \bigcap_{G/U \in \mathcal{C}} U$.*

Agora provaremos duas propriedades que nos ajudarão a provar os resultados posteriores. A primeira vale para qualquer quantidade finita de somandos, mas vamos fazer só para dois, para não carregar a notação. A segunda traz o fato interessante mencionado na introdução para grupos $p$-nilpotentes.

**Proposição 2.24.** *Sejam $X = \varprojlim X_i$ e $Y = \varprojlim Y_j$ onde $\{X_i \mid i \in I\}$ e $\{Y_j \mid j \in J\}$ são famílias de conjuntos finitos. Então $X \times Y = \varprojlim X_i \times Y_j$.*

**Demonstração:** Sejam $\{X_i, \varphi_{ij}\}$ o sistema inverso com conjunto dirigido $I$ para $\{X, \varphi_i\} = \varprojlim X_i$ e $\{Y_i, \psi_{ij}\}$ o sistema inverso com conjunto dirigido $I$ para $\{Y, \psi_i\} = \varprojlim Y_i$. Defina $\{X_i \times Y_j \mid (i,j) \in I \times J\}$, onde $(i,j) \succeq (k,l) \Leftrightarrow i \succeq k \text{ e } j \succeq l$. Assim temos $\{X_i \times Y_j, \Psi^{jl}_{ik}\}$, onde $\Psi^{jl}_{ik} = (\varphi_{ik}, \psi_{jl})$ é um sistema inverso com conjunto dirigido $I \times J$ pois, $\Psi^{jl}_{ik} : X_i \times Y_j \longrightarrow X_k \times Y_l$, para todo $(i,j) \succeq (k,l)$, e o digrama

$$\begin{array}{ccc} X_i \times Y_j & \xrightarrow{\Psi^{jl}_{ik}} & X_k \times Y_l \\ & {\scriptstyle \Psi^{jn}_{im}} \searrow \quad \nearrow {\scriptstyle \Psi^{nl}_{mk}} & \\ & X_m \times Y_n & \end{array}$$

comuta, para todo $(i,j) \succeq (m,n) \succeq (k,l)$, pois comuta em cada entrada e $\Psi^{jj}_{ii} = (\varphi_{ii}, \psi_{jj}) = id$. Portanto, $\varprojlim X_i \times Y_j = (X \times Y, \Psi_{ij})$ , onde $\Psi_{ij} = (\varphi_i, \psi_j)$ pois, dado $A \times B$ juntamente com aplicações compatíveis $f_{ij} = (\varphi_i, \psi_j)$, temos que existe uma única $\xi = (\varphi, \psi)$ tal que o diagrama

$$\begin{array}{ccc} A \times B & & \\ {\scriptstyle f_{ij}} \downarrow & \searrow^{\exists! \xi} & \\ X_i \times Y_j & \xleftarrow{\Psi_{ij}} & X \times Y \end{array}$$

comuta, pois existe uma única aplicação em cada entrada. Portanto, temos o que queríamos. ■

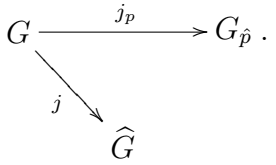
**Teorema 2.25.** *Seja $G$ um grupo $p$-nilpotente. Então o completamento pro-$p$ de $G$ pode ser identificado com um $p$-subgrupo de Sylow do completamento pro-finito.*

**Demonstração:** Um grupo $G$ é $p$-nilpotente se suas imagens finitas são $p$-nilpotentes, o que significa que toda imagem finita $G/U$ pode ser fatorada como $G/U = (P/U)(H/U)$, pela Proposição 1.66, onde $P/U$ é um $p$-subgrupo de Sylow de $G/U$ e $H/U$ é um $p$-complemento. Assim

$$\widehat{G} = \varprojlim G/U = \varprojlim (P/U)(H/U) = \varprojlim P/U \varprojlim H/U = S_pH,$$

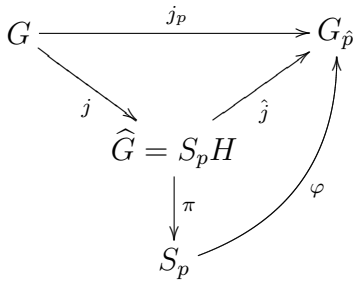
onde $S_p$ é um $p$-subgrupo de Sylow de $\widehat{G}$.

Agora considere a diagrama




Como $\widehat{G}$ é o completamento pro-finito de $G$, existe uma única aplicação $\hat{j} : \widehat{G} \longrightarrow G_{\hat{p}}$ tal que $\hat{j}j = j_p$, pela Proposição 2.21.

Seja $\pi : \widehat{G} \longrightarrow S_p$ a projeção natural ($\widehat{G}/H \cong S_p$). Assim, o nosso diagrama torna-se



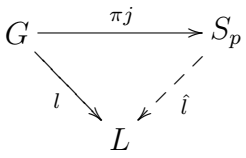

Notemos que $\widehat{G}/Ker(\hat{j}) \cong Im(\hat{j}) \subseteq G_{\hat{p}}$. Como a imagem de $\hat{j}$ é pro-$p$ grupo, então $\widehat{G}/Ker(\hat{j})$ é pro-$p$. Mas $\widehat{G}/H \cong S_p$ é o quociente pro-$p$ maximal de $\widehat{G}$. Então $Ker(\hat{j}) \supseteq H$.

Defina

$$\begin{aligned} \varphi \ : \ \widehat{G}/H &\longrightarrow G_{\hat{p}} \\ x &\longmapsto \hat{j}(x). \end{aligned}$$

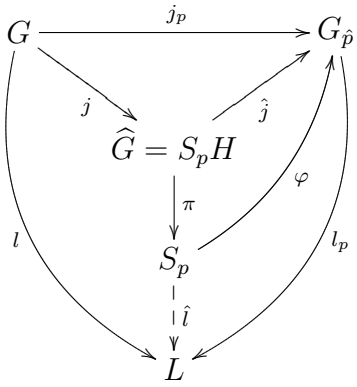
Como $Ker(\hat{j}) \supseteq H$, $\varphi$ está bem definida e $\varphi\pi = \hat{j}$.

Vamos mostrar que $(S_p, \pi j)$ satisfaz a propriedade universal do completamento pro-$p$ de $G$, ou seja, para todo diagrama




onde $L$ é pro-$p$, existe um única aplicação $\hat{l} : \ S_p \longrightarrow L$ tal que o diagrama comuta, isto é, $\hat{l}\pi j = l$.

Juntando os diagramas, obtemos




como $L$ é pro-$p$ e $G_{\hat{p}}$ é o completamento pro-$p$ de $G$, existe uma única $l_p : \ G_{\hat{p}} \longrightarrow L$ tal que $l_p j_p = l$.

Defina $\hat{l} = l_p\varphi$.

Temos que mostrar que $\hat{l}(\pi j) = l$. De fato,

$$\hat{l}(\pi j) = l_p \overbrace{\varphi\pi}^{\hat{j}} j = l_p \overbrace{\hat{j}j}^{j_p} = l_p j_p = l,$$

como queríamos.

A unicidade de $\hat{l}$. Como $j(G)$ é denso em $\widehat{G}$, temos que $\pi j(G)$ é denso em $\widehat{G}/H \cong S_p$, portanto $\hat{l}$ é única. ■

# CAPÍTULO 3

# Completamento de Grupos Livres de Torção

Neste capítulo provaremos os resultados mais importantes deste trabalho. Vamos explorar circunstâncias nas quais existe um relacionamento muito próximo entre a torção no completamento pro-finito $\widehat{G}$ de grupos metabelianos e a torção em $G$. A nossa atenção será restrita aos casos de grupos residualmente finitos pois, com isso, temos que $G$ é imerso em $\widehat{G}$, devido ao fato de sempre termos um homomorfismo entre $G$ e $\widehat{G}$ e, como $G$ é residualmente finito, temos que $\bigcap N_i = 1$, onde $N_i \trianglelefteq_f G$, como foi mencionado no Exemplo 2.18.

Lembramos que $t(G)$ é o conjunto dos elementos de torção de $G$. Se $G$ é residualmente finito, temos que $t(G) \subseteq t(\widehat{G})$. Se existir um limitante para as ordens dos elementos de torção de $G$, então existe um inteiro positivo $e$ tal que $g^e = 1$ para todo $g \in t(G)$. Com isso, temos

$$\overline{t(G)} \subseteq t(\widehat{G}). \tag{3.1}$$

De fato, temos $g \in \overline{t(G)}$ se, e somente se, para cada vizinhança $U$ de $g$, existe um elemento $g_U \in U \cap t(G)$. Assim, podemos construir uma seqüência de abertos $U_1 \supsetneq U_2 \supsetneq \ldots \supsetneq U_n \supsetneq \ldots$ tal que $g \in U_i$ e existe $g_i \in U_i \cap t(G)$ com $g_i \notin U_{i-1}$, para todo $i$. Construímos, então, uma seqüência $\{g_i\}$ de elementos de $t(G)$ que converge para $g$. Como $g_i^e = 1$, para todo $i$, segue que $g^e = 1$ e portanto $g \in t(\widehat{G})$.

**Exemplo 3.1.** *Seja $G$ um grupo abeliano finitamente gerado. Então, pelo Teorema* 1.19*,*

$$G \cong \overbrace{\mathbb{Z}^r}^{sem\ torsão} \oplus \overbrace{\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}}^{parte\ de\ torsão}.$$

*Pela Proposição* 2.24 *e Exemplo* 2.15*, obtemos*

$$\widehat{G} \cong \widehat{\mathbb{Z}}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}.$$

*Portanto $t(G) = t(\widehat{G})$.*

No exemplo acima vemos que completamento pro-finito de um grupo abeliano finitamente gerado livre de torção é também livre de torção. O mesmo acontece com grupos livres finitamente gerados, já que seu completamento pro-finito é um grupo pro-finito livre [12, Proposição 5.1.3].

## 3.1 Completamento de Grupos Metabelianos Finitamente Gerados

Nesta seção vamos provar que o completamento pro-finito de grupos abeliano por abeliano, livres de torção e finitamente gerado é livre de torção. Também mostraremos uma generalização do resultado mostrado por Zoé Chatzidakis, que apresenta a inclusão reversa de (3.1) para grupos abelianos. Nas duas proposições seguintes usaremos a notação aditiva.

**Lema 3.2.** *Seja $G$ um grupo abeliano e residualmente finito e $h$ um elemento de torção de $\widehat{G}$ de ordem $n$. Para cada subgrupo $U$ de índice finito em $G$, existe um elemento $g_u$ de torção de $G$ tal que $U + g_u$ é a imagem de $h$ em $G/U$, ou seja, $h = (g_u + U)$, onde $g_u \in t(G)$.*

**Demonstração:** Escolha $g \in G$ tal que $g + U$ é a imagem de $h$ em $G/U$. Afirmamos que $ng \in nU$. Suponha, por contradição, que $ng \notin nU$. Como $G/nU$ tem expoente finito, pela Proposição 1.21, ele é soma direta de grupos cíclicos finitos. Portanto, pela Proposição 1.43, $G/nU$ é residualmente finito. Com isso temos que existe $V \lhd G$ de índice finito tal que $nU \leq V$ e $ng \notin V$. Note que $nU \leq V \cap U \leq U$ e $U \cap V$ tem índice finito em $G$. Escolha $g_1 \in G$ tal que a imagem de $h$ em $G/V \cap U$ seja $g_1 + V \cap U$. Assim $ng_1 \in V \cap U$, pois $h$ tem ordem $n$. Afirmamos que $g_1 - g \in U$. De fato, seja $W = V \cap U$. Como $W \leq U$, na relação de

ordem temos $U \preceq W$. Assim, $\varphi_{WU}(g_1 + W) = g_1 + U$ e, como $h \in \widehat{G}$, temos $\varphi_{WU}\pi_W = \pi_U$. Logo, como $\pi_W(h) = g_1 + W$ e $\pi_U(h) = g + U$, segue que

$$g_1 + U = \varphi_{WU}(g_1 + W) = g + U,$$

o que prova a afirmação. Assim, temos

$$n(g_1 - g) \in W \leq V.$$

Como $ng \in nU$, segue que $ng_1 \in V$, absurdo. Portanto, $ng \in nU$.

Como $ng \in nU$, existe $\tilde{u} \in U$ tal que $ng = n\tilde{u}$. Seja $g_u = g - \tilde{u}$. Então $g + U = g_u + U$, $g_u \in t(G)$, pois $ng_u = 0$ e $h = (g_u \ + \ U)$ como queríamos. ■

**Teorema 3.3.** *Seja $G$ um grupo abeliano e residualmente finito. Então $\overline{t(G)} \supseteq t(\widehat{G})$.*

**Demonstração:** Seja $h$ um elemento de torção de $\widehat{G}$ de ordem $n$. Para mostrar que $h \in \overline{t(G)}$ temos que mostrar que existe uma seqüência de elementos em $t(G)$ que converge para $h$. Pela Proposição 3.2, temos $h = (g_u \ + \ U)$ com $g_u \in t(G)$. Vamos mostrar que $\{g_u\}$ é seqüência desejada.

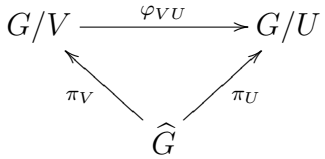
Pelo Lema 2.12, $\{h + Ker(\pi_U) | U \trianglelefteq_f G\}$, onde $\pi_U : G \to G/U$ é a projeção canônica, é um sistema fundamental de vizinhança aberta de $h$. Fixemos $U \trianglelefteq_f G$. Note que

$$g_u \in h + Ker(\pi_U)$$

pois

$$\pi_U(h) = g_u + U.$$

Temos que mostrar que $g_u \in h + Ker(\pi_U)$, para todo $U \trianglelefteq_f G$ tal que $U \preceq V$, ou seja, $V \subseteq U$.




De fato,

$$g_v + U = \varphi_{VU}(g_v + V) = \varphi_{VU}\pi_V(h) = \pi_U(h) = g_u + U.$$

Portanto $\pi_U(h) = g_u + U = g_v + U$, de onde concluímos que $g_v \in h + Ker(\pi_U)$. ■

Vamos dar um exemplo de grupo abeliano residualmente finito onde a inclusão é própria, ou seja, $\overline{t(G)} \supsetneq t(\widehat{G})$.

**Exemplo 3.4.** *Seja $G = \bigoplus_p \mathbb{Z}/p\mathbb{Z}$, onde p percorre o conjunto de todos os primos. Pela Proposição* 1.43*, G é residualmente finito e $\widehat{G} = \prod_p \mathbb{Z}/p\mathbb{Z}$. Observe que $t(G) = G$. Pela Proposição* 2.23*, G é denso em $\widehat{G}$ logo $\overline{t(G)} = \widehat{G}$. Assim $\overline{t(G)} \supsetneq t(\widehat{G})$.*

Seja $G$ um grupo finitamente gerado e abeliano por abeliano, ou seja, existe um sub-grupo normal abeliano $M$ tal que $Q = G/M$ é abeliano. A ação de $G$ sobre $M$ por conjugação

$$\begin{array}{ccc} M \times G & \longrightarrow & M \\ (m, g) & \longmapsto & m^g = g^{-1}mg \end{array}$$

dota $M$ com uma estrutura natural de $G$-módulo. Como $M$ é abeliano, a ação de $M$ sobre $M$ é trivial. Então temos uma ação de $Q = G/M$ em $M$, dada por

$$\begin{array}{ccc} M \times Q = G/M & \longrightarrow & M \\ (m, \overline{g}) & \longmapsto & m^{\overline{g}} = m^g \end{array} \tag{3.2}$$

o que está bem definida, pois $\overline{g} = \overline{h}$ se, e somente se, $gh^{-1} \in M$, o que implica $m^{gh^{-1}} = m$, assim $m^g = m^h$. Portanto, dá a $M$ uma estrutura natural de $\mathbb{Z}Q$-módulo. Além disso, a topologia pro-finita de G (que é $\{N \mid N \trianglelefteq_f G\}$) induz em $M$ a topologia pro-finita de $\mathbb{Z}Q$-módulo (que é $\{M \cap N \mid M \cap N \trianglelefteq_f M\}$).

**Lema 3.5.** *Seja $n \geq 1$ um número natural e $g \in G$ um elemento tal que $g^n \in M$. Então $M^{q^{n-1}+ \ldots + q+ 1}$ é fechado na topologia pro-finita sobre M, onde q denota a imagem de g em Q.*

**Demonstração:** Temos que $q$ é um elemento de ordem finita em $Q = G/M$, pois $g^n \in M$. Notemos que $M^{q^{n-1}+\ldots+q+1} \leq M$ é invariante pela ação de $Q$, pois para $x \in Q$ temos

$$\begin{aligned} (m^{q^{n-1}+\ldots+q+1})^x &= (m^{q^{n-1}}.m^{q^{n-2}}.\ldots.m^q.m)^x \\ &= (m^{q^{n-1}})^x.(m^{q^{n-2}})^x.\ldots.(m^q)^x.(m)^x \\ &= (m^x)^{q^{n-1}}.(m^x)^{q^{n-2}}.\ldots.(m^x)^q.(m^x)^1 \end{aligned}$$

e $m^x \in M$. Com isso temos que $M^{q^{n-1}+\ldots+q+1}$ é um $\mathbb{Z}Q$-sub-módulo de $M$. Como $Q$ é um grupo abeliano finitamente gerado e $M/M^{q^{n-1}+\ldots+q+1}$ é um $\mathbb{Z}Q$-módulo finitamente gerado, pelo Teorema 1.87, temos que $M/M^{q^{n-1}+\ldots+q+1}$ é residualmente finito. Assim a intersecção de todos os sub-módulos de índice finito que contém $M^{q^{n-1}+\ldots+q+1}$ é igual a $M^{q^{n-1}+\ldots+q+1}$. Portanto $M^{q^{n-1}+\ldots+q+1}$ é fechado na topologia profinita de $M$. ■

**Teorema 3.6.** *Se G é finitamente gerado abeliano por abeliano, então* $\overline{t(G)} = t(\widehat{G})$.

**Demonstração:** Seja $M$ o subgrupo normal abeliano tal que $Q = G/M$ é abeliano. Primeiro vamos notar que, como G é finitamente gerado, temos que Q é abeliano finitamente gerado. Logo, pelo Teorema 1.19,

$$Q \cong \overbrace{\mathbb{Z}^r}^{sem\ torsão} \oplus \overbrace{\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}}^{parte\ de\ torsão}.$$

Seja $\{g_i\}$, onde $g_i \in t(G)$, e considere $g_iM \in Q$. Temos que existe um limitante para as ordens dos elementos de torção de $Q$, que seria o mmc de $n_1, n_2, \ldots, n_k$. Assim, $g_i^{mmc} \in M$ e $g_i^{mmc} \in t(M)$, pois $g_i \in t(G)$. Mas como $M$ é abeliano finitamente gerado, temos que existe um limite para as ordens e seja $l$ esse limite. Assim $(g_i^{mmc})^l = 1$. Logo temos que existe um limitante para os elementos de $t(G)$ e então

$$\overline{t(G)} \subseteq t(\widehat{G}).$$

Agora, suponha que $h$ é um elemento de $\widehat{G}$ tal que $h^n = 1$, para algum inteiro $n \geq 1$. Temos que mostrar que $h \in \overline{t(G)}$ e para isso basta que, para cada subgrupo $K$ de índice finito em $G$, exista um elemento de torção $g_k$ de $G$ tal que $Kg_k$ seja a imagem de $h$ em $G/K$. Seja $L_k$ a imagem de $h$ em $G/K$, ou seja,

$$\begin{array}{rcl} \pi_K : \widehat{G} & \longrightarrow & G/K \\ h = (gU) & \longmapsto & L_K. \end{array}$$

Seja $g_1, g_2, \ldots$ uma seqüência de elementos de $L_K$ que converge para $h$ na topologia profinita. Note que tal seqüência existe. De fato, considere o diagrama seguinte:

$$\begin{array}{ccc} G & \hookrightarrow & \widehat{G} \\ & \searrow^{\pi} & \downarrow{\scriptstyle \tilde{\pi}_k} \\ & & G/K, \end{array}$$

onde $\tilde{\pi}_k$ é projeção na k-ésima coordenada e $\pi$ a aplicação natural. Como $\overline{G} = \widehat{G}$, temos que para $h \in \widehat{G}$, existe uma seqüência de elementos $g_i$ de $G$ que converge para $h$. Pelo Lema 2.12, $hKer(\tilde{\pi}_k)$ é uma vizinhança de $h$, portanto existe $j$ tal que $g_i \in hKer(\tilde{\pi}_k)$ para todo $i \geq j$. Assim $g_iK = \tilde{\pi}_k(h) = L_K$, o que implica em $g_i \in L_K$.

Como pelo Exemplo 3.1 $t(Q) = t(\widehat{Q})$, podemos assumir que cada $g_i$ tem a mesma imagem $q$ em $Q$, ou seja

$$\begin{array}{rcl} G & \longrightarrow & G/M \\ g_i & \longmapsto & q = g_iM. \end{array}$$

Isso significa que, dado um $g_i$, todos os outros pertencem à mesma classe $g_iM$. Assim, fixado $g_1$, temos que $g_i = g_1m_i$, para algum $m_i \in M$, e com isso temos uma seqüência $(m_i)$ de elementos de $M$ e os elementos $g_1m_1, g_1m_2, \ldots$ convergindo para $h$. Com isso $h = g_1m$, onde $m \in \widehat{M}$.

Seja $M = U_0 \geq U_1 \geq U_2 \geq \ldots$ uma base de vizinhanças de 1 na topologia profinita de $\mathbb{Z}Q$-módulo em $M$. Assim, podemos considerar uma base de vizinhanças de $m$ que são os $mU_i$. Portanto, dado $i$, existe $j$ tal que para todo $k, l \geq j$, temos $m_l,\ m_k \in mU_i$. Logo $m_k \equiv m \pmod{U_i}$ e $m_l \equiv m \pmod{U_i}$ o que implica $m_k \equiv m_l \pmod{U_i}$. Além disso, $(g_1m_i)^n$ converge para $h^n = 1$ quando $i \to \infty$, assim existe $j'$ tal que para todo $k \geq j'$, temos $(g_1m_k) \in U_i$. Contudo, podemos pegar uma subseqüência tal que, para todo $i \geq 0$ e todo $l \geq i$, temos

$$m_i \ \equiv \ m_l \pmod{U_i}$$

e

$$(g_1m_i)^n \in U_i \ \text{ para todo } i.$$

Vamos observar que

$$(g_1m_i)^n = g_1^n m_i^{q^{n-1}+ \ldots + q+ 1},$$

faremos indução sobre $n$. Para $n = 1$ é claro. Suponha agora que vale para $n-1$, assim temos

$$(g_1m_i)^{n-1} = g_1^{n-1} m_i^{q^{n-2}+ \ldots + q+ 1}.$$

Como $q = g_1M$, temos pela conjugação definida em (3.2) que $m^q = m^{g_1}$. Logo

$$\begin{aligned}
(g_1m_i)^{n-1}(g_1m_i) &= g_1^{n-1} m_i^{q^{n-2}+ \ldots + q+ 1}(g_1m_i) \\
(g_1m_i)^n &= g_1^n g_1^{-1} m_i^{q^{n-2}+ \ldots + q+ 1} g_1m_i \\
&= g_1^n (m_i^{q^{n-2}+ \ldots + q+ 1})^{g_1} m_i \\
&= g_1^n (m_i^{q^{n-2}+ \ldots + q+ 1})^{q} m_i \\
&= g_1^n m_i^{q^{n-1}+ \ldots + q+ 1}.
\end{aligned}$$

Em particular segue que $g_1^n \in U_iM^{q^{n-1}+\ldots+q+1}$ para todo $i$ e, como $M^{q^{n-1}+\ldots+q+1}$ é fechado pelo Lema 3.5, segue que $g_1^n \in M^{q^{n-1}+\ldots+q+1}$. De fato, suponha por contradição, que $g_1^n \notin M^{q^{n-1}+\ldots+q+1}$, teremos $g_1^n \in M - \{M^{q^{n-1}+\ldots+q+1}\}$ que é aberto. Considere $U_ig_1^n$ uma base de vizinhança de $g_1^n$, assim existe $k$ tal que $U_kg_1^n \subset M - \{M^{q^{n-1}+\ldots+q+1}\}$ o que implica

$U_k g_1^n \cap N = \varnothing$ absurdo, pois $g_1^n \in U_i M^{q^{n-1}+\ldots+q+1}$, assim $g_1^n = u_k m_i^{q^{n-1}+\ \ldots+\ q+\ 1}$, e com isso $u_k^{-1} g_1^n = m_i^{q^{n-1}+\ \ldots+\ q+\ 1}$.

Escolha $m_0$ tal que $g_1^n = m_0^{q^{n-1}+\ldots+q+1}$. Agora basta tomar $g_k = g_1 m_0^{-1}$, pois $K g_k = K g_1$ e temos $g_k^n = 1$. Concluímos o que queríamos. ■

## 3.2 Contra Exemplos

Nesta seção vamos dar os dois teoremas prometidos.

**Teorema 3.7.** *Para cada primo $p$, existe um grupo $H$ livre de torção e residualmente $p$-grupo finito que o seu completamento pro-$p$ contém um elemento de ordem $p$.*

**Demonstração:** Sejam $X$ e $Y$ grupos abelianos livres de posto infinito, gerados livremente por $x_1$,$x_2$,$x_3$,... e $y_1$,$y_2$,$y_3$,... respectivamente, e seja um primo $p$. Defina subgrupos $A \leq X$ e $B \leq Y$ por

$$A = \langle x_1^p x_2^{p^2} \ldots x_k^{p^k} \mid k = 1, 2, 3, \ldots \rangle \text{ e } B = \langle y_k^{p^k} \mid k = 1, 2, 3, \ldots \rangle,$$

temos $A$ e $B$ são abelianos livre pelo Teorema 1.13, gerados livremente. Assim, definindo

$$\begin{array}{rccc} \theta & : & A & \longrightarrow & B \\ & & x_1^p x_2^{p^2} \ldots x_k^{p^k} & \longmapsto & y_k^{p^k} \end{array}$$

com $k = 1, 2, 3, \ldots$ temos um isomorfismo, com isso,

$$H = \langle X, Y \mid x_1^p x_2^{p^2} \ldots x_k^{p^k} = y_k^{p^k}; k = 1, 2, 3, \ldots \rangle$$

é o produto livre de $X$ e $Y$ com $A$ e $B$ amalgamados. Em particular $H$ é livre de torção, pelo Teorema 1.61 e, mostraremos que $H$ definido acima é:

(i) residualmente $p$-grupo finito;

(ii) seu completamento pro-$p$ contém um elemento de ordem $p$.

Mostraremos (i). Note que os elementos de $A$ podem ser gerados por $x_1^p, x_2^{p^2}, \ldots, x_k^{p^k}, \ldots$, portanto $A = \langle x_1^p, x_2^{p^2}, \ldots \rangle$, como $X$ é abeliano livre, temos $X \simeq \mathbf{Dr}_{k \in \mathbb{N}^*} \langle x_k \rangle$, onde $\mathbf{Dr}$ produto direto restrito. Logo $X/A \simeq \mathbf{Dr}_{k \in \mathbb{N}^*} C_{p^k}$, pois basta definir

$$\begin{array}{rccc} \phi & : & \mathbf{Dr}_{k \in \mathbb{N}^*} \langle x_k \rangle & \longrightarrow & \mathbf{Dr}_{k \in \mathbb{N}^*} (\mathbb{Z}/p^k\mathbb{Z}) \\ & & x_k & \longmapsto & (0, 0, \ldots, 1_k, 0, 0, \ldots). \end{array}$$

Temos um epiomorfismo onde o núcleo de $\phi$ é $A$, então temos:

$$X/A \simeq \mathbf{Dr}_{k\in\mathbb{N}^*}(\mathbb{Z}/p^k\mathbb{Z}) \simeq \mathbf{Dr}_{k\in\mathbb{N}^*}C_{p^k}.$$

Analogamente temos $Y/B \simeq \mathbf{Dr}_{k\in\mathbb{N}^*}C_{p^k}$. Com isso, $X/A \simeq Y/B \simeq \mathbf{Dr}_{k\in\mathbb{N}^*}C_p^k$ que, pela Proposição 1.43, é residualmente $p$-grupo finito. Note que

$$H/A \simeq (X/A) * (Y/B),$$

pois

$$H/A = \langle X, Y \mid x_1^p x_2^{p^2} \dots x_k^{p^k} = 1, y_k^{p^k} = 1; k = 1, 2, 3, \dots\rangle$$

e

$$X/A = \langle X \mid x_1^p x_2^{p^2} \dots x_k^{p^k} = 1; k = 1, 2, 3, \dots\rangle,\ Y/B = \langle Y \mid y_k^{p^k} = 1; k = 1, 2, 3, \dots\rangle.$$

Pelo Teorema 1.50, $H/A$ é residualmente $p$-grupo finito.

Agora é suficiente mostrar que, para cada $1 \neq a \in A$, existe $N \lhd H$, tal que $a \notin N$ e $H/N$ é $p$-grupo finito. Temos que $A \cap H' = 1$, pois nenhum elemento do comutador será formado só por elementos $x_i \in X$, assim $x_i^{p^i} \notin H'$ para todo $i$.

Considere agora a abelianização de $H$

$$H_{ab} = H/H' = \langle X, Y \mid [X, Y] = 1, x_1^p x_2^{p^2} \dots x_k^{p^k} = y_k^{p^k}; k = 1, 2, 3, \dots\rangle.$$

Vamos mostrar que $\bigcap_{i=1}^{\infty} H_{ab}^{p^i} = \{1\}$, onde $H_{ab}^{p^i} = \{\ h^{p^i} | h \in H_{ab}\}$. Para isso, vamos identificar $X$ e $Y$ com suas cópias naturais em $H_{ab}$. Observe que

$$H_{ab}/X = \langle Y \mid y_k^{p^k} = 1; k = 1, 2, 3, \dots\rangle = Y/B \simeq \mathbf{Dr}_{k\in\mathbb{N}^*}C_{p^k}.$$

Assim,

$$(H_{ab}/X)^{p^i} \simeq C_p \times C_{p^2} \times \dots \times C_{p^{i-1}} \times \{1\} \times C_{p^{i+1}} \times C_{p^{i+2}} \dots.$$

Portanto $\bigcap_{i=1}^{\infty}(H_{ab}/X)^{p^i} = 1$ e então $\bigcap_{i=1}^{\infty} H_{ab}^{p^i} \leq X$.

Agora, para cada $i \in N^*$ temos que $H_{ab}^{p^i} \cap X = X^{p^i}Y^{p^i} \cap X$, pois os elementos de $H_{ab}$ comutam. Olhando para $Y^{p^i} \cap X$ vemos, pelas relações de $H_{ab}$, que $Y^{p^i} \cap X = \langle y_j^{p^i}, y_l^{p^l} \mid 1 \leq j \leq i, l > i\rangle$, pois para $j = i$ e $l > i$, temos $x_1^p x_2^{p^2} \dots x_i^{p^i} = y_i^{p^i}$ e $x_1^p x_2^{p^2} \dots x_i^{p^i} \dots x_l^{p^l} = y_l^{p^l}$ e para $1 \leq j < i$ podemos escrever $y_j^{p^i} = (y_j^{p^j})^{p^{i-j}} = (x^p \dots x_j^{p^j})^{p^{i-j}}$. Escrevendo esses geradores em termos de $x_1, x_2, x_3, \dots$, vemos que $X^{p^i}(Y^{p^i} \cap X) = \langle X^{p^i}, x_1^p x_2^{p^2} \dots x_i^{p^i}\rangle$. De fato,

$$X^{p^i} = \langle x_1^{p^i}, x_2^{p^i}, \dots\rangle \text{ e } Y^{p^i} \cap X = \langle y_1^{p^i}, y_2^{p^i}, \dots, y_i^{p^i}, y_{i+1}^{p^{i+1}}, \dots\rangle,$$

e com isso temos $y_1^{p^i} = (y_1^p)^{p^{i-1}} = x_1^{p^i}$, $y_2^{p^i} = (y_2^{p^2})^{p^{i-2}} = (x_1^p x_2^{p^2})^{p^{i-2}} = (x_1^{p^i})^{p^{-1}} x_2^{p^i}$, e assim até $i-1$, para $i$ e $l > i$, temos $y_i^{p^i} = x_1^p x_2^{p^2} \dots x_i^{p^i}$ e $y_l^{p^l} = x_1^p x_2^{p^2} \dots x_i^{p^i} x_{i+1}^{p^{i+1}} \dots x_l^{p^l}$, onde $x_{i+n}^{p^{i+n}} = (x_{i+n}^{p^i})^{p^n} \in X^{p^i}$.

Assim, temos que $H_{ab}^{p^i} \cap X = \langle X^{p^i}, x_1^p x_2^{p^2} \dots x_i^{p^i} \rangle$ e portanto

$$\bigcap_{i=1}^{\infty} H_{ab}^{p^i} = \bigcap_{i=1}^{\infty} (H_{ab}^{p^i} \cap X) = \bigcap_{i=1}^{\infty} (\langle X^{p^i}, x_1^p x_2^{p^2} \dots x_i^{p^i} \rangle) = \{1\},$$

observe que para $i = n$, onde $n$ é um inteiro positivo, temos que o elemento $x_1^p x_2^{p^2} \dots x_n^{p^n}$ estará em todos os conjuntos gerados para $i \leq n$, mas como $i$ vai para infinito não teremos nenhum elemento finito que esteja em todos, somente o trivial.

Note que, para cada $i$, $H_{ab}/H_{ab}^{p^i}$ é grupo abeliano de expoente finito. Logo, pelas Proposições 1.21 e 1.43, $H_{ab}/H_{ab}^{p^i}$ é residualmente $p$-grupo finito. Então $H_{ab} = H_{ab}/\bigcap_{i=1}^{\infty} H_{ab}^{p^i}$ é também residualmente $p$-grupo finito.

Portanto, $H$ é residualmente $p$-grupo finito, pois

$$H = H/A \cap H' \cong H/A \times H/H',$$

assim concluímos $(i)$.

Agora $(ii)$. Seja $\mathcal{N} = \{N \lhd H \mid H/N \text{ é } p\text{-grupo finito } \}$ e seja $\prod(H/N)$, denotando o produto direto dos grupos $H/N$, com $N \in \mathcal{N}$. Definimos um elemento $(g_N N) \in \prod(H/N)$ por

$$g_H = 1$$

e

$$g_N = x_1 x_2^p x_3^{p^2} \dots x_k^{p^{k-1}},$$

se $H/N$ tem expoente $p^k > 1$, ou seja, $H^{p^k} \leq N$ e $H^{p^{k-1}} \not\leq N$. Identificamos o completamento pro-$p$ de $H$ como limite inverso dos $H/N$, onde $N$ percorre $\mathcal{N}$. Temos também que $\varprojlim_{N \in \mathcal{N}} H/N \leq \prod(H/N)$. Vamos mostrar agora que $(g_N N) \in \varprojlim_{N \in \mathcal{N}} H/N$.

Suponha $N \succeq M$, onde $N, M \in \mathcal{N}$ e $H/N$, $H/M$ tendo expoentes $p^k$ e $p^r$ respectivamente. Com isso $\mid H/N \mid \geq \mid H/M \mid$, o que implica que $k \geq r$ e assim podemos escrever

$$g_N M = x_1 x_2^p x_3^{p^2} \dots x_k^{p^{k-1}} M = x_1 x_2^p x_3^{p^2} \dots x_r^{p^{r-1}} \underbrace{x_{r+1}^{p^r} \dots x_k^{p^{k-1}}}_{(*)} M.$$

Como $(*) \in H^{p^r}$, pois $x_{r+1} x_{r+2}^p \dots x_k^{k-1-r} \in H$, temos

$$g_N M = x_1 x_2^p x_3^{p^2} \dots x_r^{p^{r-1}} M = g_M M,$$

pois $H^{p^r} \leq M$. Logo, como $N$ e $M$ são arbitrários, vale para todos $N,\ M \in \mathcal{N}$ tais que $N \succeq\ M$. Assim $(g_N N) \in \varprojlim H/N$. Além disso, $(g_N N)$ tem ordem $p$, pois

$$(g_N)^p = x_1^p x_2^{p^2} \dots x_k^{p^k} = y_k^{p^k},$$

como $y_k^{p^k} \in H^{p^k} \leq N$, temos $(g_N)^p \in N$.

Assim concluímos que completamento pro-$p$ contém um elemento de ordem $p$. ■

**Teorema 3.8.** *Para cada primo $p$, existe um grupo $G$ (de posto enumerável) metabeliano, livre de torção e residualmente finito tal que seu completamento pro-finito contém um elemento de ordem $p$.*

**Demonstração:** Seja $p$ denotando um primo fixado. Vamos construir o grupo $G$ referido no teorema como o produto central de dois produtos "wreath" $X$ e $Y$. Conseqüentemente, vamos construir primeiro os grupos $X$ e $Y$, e estabelecer algumas propriedades.

*O grupo X*

Para cada $i \in \mathbb{N}$, denotando por $A_i$ o grupo abeliano livre, de posto $p$ gerado por $a_{i,1}, a_{i,2}, \dots, a_{i,p}$. Seja $A$ o produto direto restrito dos $A_i$, denotado por $A = \mathbf{Dr}_{i\in\mathbb{N}} A_i$. Definamos uma ação de $\langle x \rangle \cong C_\infty$ em $A$ por $a_{i,j}^x = a_{i,j+1},\ \forall\ i \in \mathbb{N}$, onde $j$ e $j+1$ são reduzidos módulo $p$. Seja $X = A \rtimes \langle x \rangle$ e, observe que $A_i$ comuta com todos os elementos de $A$, pois é abeliano, e $A_i$ é invariante pela ação de $\langle x \rangle$. Assim $A_i \lhd X,\ \forall\ i \in \mathbb{N}$. Além disso, $X$ é livre de torção, metabeliano ($\{1\} \lhd A \lhd X$) e o centro $\mathbf{Z}(X)$ de $X$ é abeliano livre, gerado livremente por $x^p$ e pelos os elementos $a_{i,1}a_{i,2}\dots a_{i,p}$, onde $i = 1, 2, 3, \dots$. De fato,

$$a_{i,j}x^p = x^p x^{-p} a_{i,j} x^p = x^p a_{i,j+p} = x^p a_{i,j},$$

e os elementos $a_{i,1}a_{i,2}\dots a_{i,p}$ são os únicos que comutam com os elementos de $\langle x \rangle$, pois

$$(\ a_{i,1}a_{i,2}\dots a_{i,p})^{x^t} =\ a_{i,t+1}a_{i,t+2}\dots a_{i,t+p},\ assim\ a_{i,1}a_{i,2}\dots a_{i,p}x^t = x^t a_{i,t+1}a_{i,t+2}\dots a_{i,t+p}$$

e, quando fazemos a redução módulo $p$ nos $t+l$ onde $l = 1, 2, \dots, p$, estes voltarão a ser os números $1, 2, \dots, p$ em ordem diferente da anterior, mas como $A_i$ é abeliano teremos que

$$a_{i,1}a_{i,2}\dots a_{i,p}x^t = x^t a_{i,1}a_{i,2}\dots a_{i,p}.$$

Portanto,

$$\mathbf{Z}(X) = \langle x^p, a_{i,1}a_{i,2}\dots a_{i,p};\ i = 1, 2, \dots \rangle.$$

Também observamos que os elementos

$$(xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})^p,$$

onde $k = 1, 2, \dots$, geram livremente um subgrupo $R$ de $\mathbf{Z}(X)$. Temos que este elemento pode ser escrito na forma

$$(xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})^p = x^p(a_{1,1}^{p}a_{1,2}^{p}\dots a_{1,p}^{p})\dots(a_{k,1}^{p^k}a_{k,2}^{p^k}\dots a_{k,p}^{p^k}),$$

pois

$$\begin{aligned}
(xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})^p &= \underbrace{(xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})(xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})\dots(xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})}_{p\ vezes}\\
&= (xa_{1,1}^{p}\dots a_{k,1}^{p^k})(x^{-1}x)(xa_{1,1}^{p}\dots a_{k,1}^{p^k})\dots(xa_{1,1}^{p}\dots a_{k,1}^{p^k})\\
&= a_{1,p}^{p}\dots a_{k,p}^{p^k}x^2a_{1,1}^{p}\dots a_{k,1}^{p^k}(x^{-2}x^2)xa_{1,1}^{p}\dots a_{k,1}^{p^k}\dots xa_{1,1}^{p}\dots a_{k,1}^{p^k}\\
&= a_{1,p}^{p}\dots a_{k,p}^{p^k}a_{1,p-1}^{p}a_{2,p-1}^{p^2}\dots a_{k,p-1}^{p^k}x^3a_{1,1}^{p}\dots a_{k,1}^{p^k}(x^{-3}x^3)x\dots xa_{1,1}^{p}\dots a_{k,1}^{p^k}\\
&\vdots\\
&= a_{1,p}^{p}a_{2,p}^{p^2}\dots a_{k,p}^{p^k}a_{1,p-1}^{p}a_{2,p-1}^{p^2}\dots a_{k,p-1}^{p^k}\dots a_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k}x^p\\
&= x^p(a_{1,1}^{p}a_{1,2}^{p}\dots a_{1,p}^{p})\dots(a_{k,1}^{p^k}a_{k,2}^{p^k}\dots a_{k,p}^{p^k})
\end{aligned}$$

*O grupo $Y$*

Para cada $i \in \mathbb{N}$, denotando por $B_i$ o grupo abeliano livre, de posto $p^i$, gerado por $b_{i,1},\ b_{i,2},\dots,\ b_{i,p^i}$. Seja $B$ o produto direto restrito dos $B_i$, denotado por $B = \mathbf{Dr}_{i\in\mathbb{N}}B_i$. Definamos uma ação de $\langle y\rangle \cong C_\infty$ em $B$ por $b_{i,j}^{y} = b_{i,j+1},\ \forall\ i \in \mathbb{N}$, onde $j$ e $j+1$ são reduzidos módulo $p^i$. Seja $Y = B \rtimes \langle y\rangle$ e observe que $B_i$ comuta com todos os elementos de $B$, pois é abeliano, e é invariante pela ação de $\langle y\rangle$ pela ação. Assim $B_i \lhd Y,\ \forall\ i \in \mathbb{N}$. Além disso, $Y$ é livre de torção, metabeliano ($\{1\} \lhd B \lhd Y$) e o centro

$$\mathbf{Z}(Y) = \langle b_{i,1}b_{i,2}\dots b_{i,p^i}; i = 1, 2, 3, \dots\rangle$$

de $Y$ é abeliano livre gerado livremente, por $b_{i,1}b_{i,2}\dots b_{i,p^i}$.

Temos que $Y/\mathbf{Z}(Y)$ também é livre de torção. De fato, suponha, por contradição, que exista $y \in Y/\mathbf{Z}(Y)$ tal que $y^k\mathbf{Z}(Y) = \mathbf{Z}(Y)$ para algum inteiro positivo $k$, onde $y \notin \mathbf{Z}(Y)$. Portanto $y^k \in \mathbf{Z}(Y)$ absurdo, pois como $y$ não é gerado somente por elementos de $\mathbf{Z}(Y)$, temos $y^k \notin \mathbf{Z}(Y)$ pelo fato de não haver cancelamentos em $Y$.

*O grupo $G$*

Construiremos $G$ como o produto central de $X$ e $Y$, identificando $\mathbf{Z}(Y)$ com o subgrupo $R$ de $\mathbf{Z}(X)$ via o isomorfismo

$$\begin{array}{rccc} \theta & : & R & \longrightarrow & \mathbf{Z}(Y) \\ & & (xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})^p & \longmapsto & b_{k,1}b_{k,2}\dots b_{k,p^k}, \end{array}$$

onde $k = 1, 2, \dots$. Assim temos a seguinte apresentação:

$$G = \langle\ X,\ Y\ \mid\ [X,Y] = 1, (xa_{1,1}^{p}a_{2,1}^{p^2}\dots a_{k,1}^{p^k})^p = b_{k,1}b_{k,2}\dots b_{k,p^k}; k = 1, 2, \dots\rangle.$$

Podemos ver que $G$ é enumerável e metabeliano. O último segue vem da equação (A.2) no Apêndice, onde temos $G'' \leq [[X,X],[X,X]][[Y,Y],[Y,Y]]$, como $X$ e $Y$ são metabelianos $G'' \leq 1$. Além disso, $G$ é livre de torção, pois $G/X = XY/X \simeq Y/X \cap Y = Y/\mathbf{Z}(Y)$ é livre de torção e, como $X$ é livre de torção, temos o que queremos.

Vamos observar, para uso posterior que, se $W$ é um subgrupo finitamente gerado de $G$, então existe um $k \in \mathbb{N}$ tal que $y^{p^k}$ centraliza $W$, ou seja $y^{p^k} \in C_G(W)$ e $y^{p^k}$ comuta com todos elementos de $W$. Isto segue do fato que, para uma quantidade finita de $B_i$, basta tomar $k$ igual ao produto dos seus sub-índices dos $B_i$. Assim, teremos que $y^{p^k}$ comuta com qualquer elemento de $X$ e com os elementos dos $B_i$ que geraram $W$. De fato, pois $b_{i,j}^{y^{p^k}} = b_{i,j+p^k}$, assim na redução módulo $p^i$ onde $i$ são os índices dos $B_i$, teremos

$$b_{i,j}y^{p^k} = y^{p^k}b_{i,j}.$$

Sabemos, pelo Teorema 2.25, que se o completamento pro-$p$ de um grupo $p$-nilpotente contém um elemento de ordem $p$, o completamento pro-finito também o tem. Agora nosso teorema segue se provarmos que

(i) G é p-nilpotente;

(ii) G é residualmente finito;

(iii) O completamento pro-$p$ de G contém um elemento de ordem $p$.

Mostraremos (i). Para isso vamos considerar a Definição 1.68.

Seja $\overline{G}$ alguma imagem finita de $G$ e $\bar{g}$ denotando a imagem de $g \in G$ em $\overline{G}$, via o homomorfismo natural $\pi :\ G \longrightarrow\ \overline{G}$. Como $x^p \in \mathbf{Z}(G)$ temos que $\overline{x}^p \in \mathbf{Z}(\overline{G})$. Existe um subgrupo $W$ finitamente gerado de $G$ que é levado sobrejetivamente em $\overline{G}$ via $\pi$, ou seja, tal que $\pi(W) = \overline{G}$. Esta existência, segue do fato de $\overline{G}$ ser finito, então tem um número finito

de geradores. Tomando a imagem inversa desses geradores e consideramos $W$ o subgrupo gerado por essas imagens inversas.

Recordamos que existe $k \in \mathbb{N}$ tal que $y^{p^k}$ centraliza $W$. Assim temos $\overline{y}^{p^k} \in \mathbf{Z}(\overline{G})$, pois comuta com todos os elementos de $\overline{G}$. Portanto

$$\overline{M} = \langle \overline{x}^p, \overline{y}^{p^k}, \overline{A}, \overline{B} \rangle$$

é um subgrupo abeliano normal. O fato de $\overline{M}$ ser abeliano é claro, e normal pois os geradores de $\overline{M}$ são invariantes via conjugação. Note também que $\overline{G}/\overline{M}$ é $p$-grupo finito, pois $\overline{G} = \langle \overline{X}, \overline{Y}, \overline{A}, \overline{B} \rangle$. Então, pela Proposição 1.67, temos que G é p-nilpotente.

Agora $(ii)$. Para isso é suficiente mostrar que $G$ é residualmente finitamente gerado. De fato, com isso temos que dado $g \in G$, $\exists \ \ N_g \lhd G$ tal que $G/N_g$ é finitamente gerado e $g \notin N_g$. Então $\overline{1} \neq \overline{g} \in G/N_g$. Como o quociente de grupo metabeliano é metabeliano temos, pelo Teorema de Hall [5], que $G/N_g$ é residualmente finito. Assim, existe um subgrupo normal $V$ de $G$, que contém $N_g$, tal que $g \notin V$ e $G/V$ é finito. Portanto temos o que $G$ é residualmente finito.

Agora vamos mostrar que $G$ é residualmente finitamente gerado. Suponha que $1 \neq g \in G$. Assim temos que $g \in \langle x, y, A_1, A_2, \ldots, A_r, B_1, B_2, \ldots, B_r \rangle$, para algum $r \in \mathbb{N}$. Seja $N = \langle \ A_{r+2}, A_{r+3}, \ldots, B_{r+1}, B_{r+2}, \ldots \ \rangle$. Temos que $N \lhd G$ e $g \notin N$. Com isso e o fato de que $G/N$ é finitamente gerado, concluímos o item (ii).

Finalmente (iii). A prova é bem similar à do Teorema 3.7. Sejam $\mathcal{N} = \{N \lhd G \mid G/N$ é $p$-grupo finito $\}$, $G^{p^k} = \langle g^{p^k} \mid g \in G \rangle$ e $\prod(G/N)$ o produto direto dos grupos $G/N$, com $N \in \mathcal{N}$. Definimos um elemento $(g_N N) \in \prod(G/N)$, por

$$g_G = 1$$

e

$$g_N = x a_{1,1}^p a_{2,1}^{p^2} \ldots a_{k,1}^{p^k}, \text{ se } G/N \text{ tem expoente } p^k > 1.$$

Temos que $(g_N N) \in \varprojlim_{N \in \mathcal{N}} G/N$. Portanto, $(g_N N)$ tem ordem $p$, pois pela definição da ação de $\langle y \rangle$ em $B$ temos

$$\begin{aligned}
(g_N)^p &= (x a_{1,1}^p a_{2,1}^{p^2} \ldots a_{k,1}^{p^k})^p \\
&= b_{k,1} b_{k,2} \ldots b_{k,p^k} \\
&= b_{k,1} y^{-1} b_{k,1} y y^{-2} b_{k,1} y^2 \ldots y^{-(p^k-1)} b_{k,1} y^{(p^k-1)} \\
&= b_{k,1} y^{-1} b_{k,1} y^{-1} \ldots b_{k,1} y^{p^k} y^{-1} \\
&= (b_{k,1} y^{-1})^{p^k} y^{p^k}.
\end{aligned}$$

Então como

$$g_N^p = (b_{k,1}y^{-1})^{p^k} y^{p^k} \in G^{p^k} \leq N,$$

temos $(g_N N)^p = \mathrm{N}$.

Assim concluímos que completamento pro-$p$ contém um elemento de ordem $p$. Então, pelo fato já mencionado, o completamento pro-finito tem um elemento não trivial de ordem $p$. ■

# APÊNDICE A

## A.1 Lema de Zorn

Seja $X$ um conjunto não vazio. Uma relação binária $\leq$ em $X$ é uma **ordem parcial** satisfazendo:

(i) $x \leq x$;

(ii) $x \leq y$ e $y \leq x$, o que implica em $x = y$;

(iii) $x \leq y$ e $y \leq z$ o que implica em $x \leq z$,

para todos $x, y, z \in X$.

O melhor exemplo de um conjunto parcialmente ordenado é os subconjuntos de um conjunto $Y$, onde $\leq$ significa $\subset$.

Uma ordem parcial é uma **ordem simples** (ou ordem total) se para cada $x, y \in X$, temos $x \leq y$ ou $y \leq x$.

Se $X$ é um conjunto parcialmente ordenado, uma **cadeia** é um subconjunto simplesmente ordenado. Por exemplo, os números racionais dão forma a uma cadeia nos números reais.

Se $S$ é um subconjunto não vazio de $X$, um **limite superior** de $S$ é um elemento $x_0 \in X$ ( não necessariamente em $S$) tal que $s \leq x_0$ para todo $s \in S$. Finalmente, o **elemento máximo** em $X$ é um elemento $y_0$, se $x \in X$ e $y_0 \leq x$, então $y_0 = x$.

Há conjuntos parcialmente ordenados que possuem muitos elementos maximais, o contrário também ocorre. Por exemplo, o conjunto dos números reais $\mathbb{R}$ considerado como um conjunto parcialmente ordenado por $\leq$ não possui elemento maximal.

**Lema A.1** (**Lema de Zorn**). *Se $X$ é um conjunto parcialmente ordenado em que cada cadeia tem um limite superior, então existe um elemento maximal em $X$.*

## A.2 Algumas Definições

**Definição A.2.** *Seja $G$ um grupo.Um subgrupo $A$ é dito um* **somando direto** *se existir $B$, um subgrupo de $G$, tal que $G = A \oplus B$.*

**Definição A.3.** *Seja $K$ um subgrupo de $G$ (não necessariamente normal). Então o subgrupo $Q$ é um* **complemento** *de $K$ em $G$ se $K \cap Q = 1$ e $KQ = G$.*

Um subgrupo normal $K$ de $G$ não necessariamente tem um complemento mas, se tiver, o complemento é único a menos de isomorfismos. Em $S_3$, por exemplo, cada subgrupo de ordem 2 pode ser um complemento para $A_3$. Por outro lado, são únicos a menos de isomorfismos, pois

$$G/K = KQ/K \cong Q/(K \cap Q) = Q/1 \cong Q.$$

Se $K$ e $Q$ são normais, $K \cap Q = 1$ e $G = KQ$ isso implica que $G$ é o produto direto de $K$ e $Q$.

**Definição A.4.** *Um grupo $G$ é um produto semi-direto de $K$ por $Q$, denotado por $G = K \rtimes Q$, se $K \trianglelefteq G$ e $K$ tem um complemento $Q_1 \cong Q$.*

Note que não assumimos que $Q_1$ é um subgrupo normal de G.

**Definição A.5.** *Se $\Omega$ é um conjunto e $G$ um grupo, então $\Omega$ um $G-$conjunto se existi uma ação de $G$ sobre $\Omega$.*

Seja $\Omega$ um $Q-conjunto$, e $\{D_w : w \in \Omega\}$ uma família de cópias isomorfas de $D$, indexadas por $\Omega$.

**Definição A.6.** *Sejam $D$ e $Q$ grupos, $\Omega$ e $K = \mathbf{Dr}_{w\in\Omega} D_w$, onde $D_w \cong D$ para todo $w \in \Omega$. Então o* **produto wreath** *(ou entrelaçado) de $D$ por $Q$, denotado por $D \wr Q$ (ou por $D$ wr $Q$), é o produto semi-direto de $K$ por $Q$, onde $Q$ age sobre $K$ por $q.(d_w) = (d_{qw})$ para $q \in Q$ e $(d_w) \in K$. O subgrupo normal $K$ de $D \wr Q$ é chamado de* **base** *do produto "wreath".*

Admitíamos a possibilidade de $\Omega$ ser infinito, no qual usaremos $K = \mathbf{Dr_{w\in\Omega} D_w}$, onde **Dr** é produto cartesiano.

**Exemplo A.7.** *Se* $Q = \{1, a, a^2\}$*, temos* $K = D_1 \times D_a \times D_{a^2}$*, e então* $D_1^a = D_a, D_a^a = D_{a^2}, D_{a^2}^a = D_1$*. Portanto temos uma ação de* $Q$ *sobre* $K$*, então o produto "wreath"de* $D$ *com* $Q$ *é o produto semi-direto* $K \rtimes Q$*.*

**Definição A.8.** *Um grupo* $G$ *é dito um* **produto central** *de subgrupos normais* $G_1, \ldots, G_n$ *se* $G = G_1 G_2 \ldots G_n$*,* $[G_i, G_j] = 1$ *para* $i \neq j$ *e* $G_i \cap \prod_{i \neq j} G_j = \mathbf{Z}(G)$ *para todo* $i$*, onde* $\mathbf{Z}(G)$ *é centro de* $G$*. Como* $\mathbf{Z}(G_i) \leq \mathbf{Z}(G)$ *e dado* $g \in \mathbf{Z}(G)$ *comuta com todos elementos de* $G_i$*, segue que* $\mathbf{Z}(G_i) = \mathbf{Z}(G)$

Observamos que se $G$ é produto central gerado por dois grupos $X$ e $Y$, temos:

$$G' \leq [X, X][Y, Y], \tag{A.1}$$

pois $[X, Y] = 1$, da mesma forma:

$$G'' \leq [[X, X], [X, X]][[Y, Y], [Y, Y]] = X''Y'' \tag{A.2}$$

# BIBLIOGRAFIA


[1] M.F. Atiyah, *Introduction to Cammutative Algebra* , Addison-Wesley, London, (1969).

[2] W.W. Crawley-Boevey, P.H. Kropholler e P.A. Linnell, *Torsion-free soluble groups, completions and the zero divisor conjecture*, J. Pure Appl. Algebra 54 (1988), 181–196.

[3] M.J. Evans, *Torsion in pro-finite completions of torsion-free groups* , J. Pure Appl. Algebra 65 (1990), 101–104.

[4] K.W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc. (3) 7 (1957), 29–62.

[5] P. Hall, *On the finiteness of certain soluble groups*, Proc. London Math. Soc. (3) 9 (1959), 595–622.

[6] P.H. Kropholler, J.S. Wilson, *Torsion in pro-finite completions*, J. Pure Appl. Algebra 88 (1993), 143–154.

[7] A. Lubotzky , *Torsion in pro-finite completions of torsion-free groups*, Quart. J. Math. Oxford (2), 44 (1993), 327–332.

[8] M. Quick, *Subspace Topologies in Central Extensions*, J. Algebra 246 (2001) n° 2, 491–513.

[9] L. Ribes, P. Zalesskii, *Profinite groups* , Springer-Verlag, Berlin, (2000).

[10] D.J.S. Robinson, *A Course in the Theory of Groups* , 2th edn., Springer-Verlag, New York, (1995).

[11] J.J. Rotman, *An Introduction to the Theory of Groups* , 4th edn., Springer-Verlag, New York, (1994).

[12] J.S. Wilson, *Profinite groups* ,Clarendon Press, New York, (1998).

# Livros Grátis

( http://www.livrosgratis.com.br )

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo