UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

MÁRCIO DIAS DE LIMA

Sobre Centralizadores de Automorfismos Coprimos em Grupos Profinitos e Álgebras de Lie

Goiânia
2011

MÁRCIO DIAS DE LIMA

Sobre Centralizadores de Automorfismos Coprimos em Grupos Profinitos e Álgebras de Lie

Dissertação apresentada ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de concentração: Álgebra.

Orientadora: Prof[a]. Dr[a]. Aline de Souza Lima

Coorientador: Prof. Dr. Jhone Caldeira Silva

Goiânia
2011

Dados Internacionais de Catalogação na Publicação na (CIP)

Lima, Márcio Dias de.
L732s Sobre Centralizadores de Automorfismos Coprimos em Grupos Profinitos e Álgebras de Lie [manuscrito] / Márcio Dias de Lima.- 2011. 84 f.

Orientadora: Profª. Drª. Aline de Souza Lima; Co-orientador: Prof. Dr. Jhone Caldeira Silva.
Dissertação (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2011.
Bibliografia.

1. Álgebras de Lie 2. Anel de Lie associado a um grupo 3. Centralizadores de automorfismos Coprimos 4. Grupos localmente finito 5. Grupos profinitos. I. Título.

CDU: 512.554.3+512.542.2

MÁRCIO DIAS DE LIMA

SOBRE CENTRALIZADORES DE AUTOMORFISMOS COPRIMOS EM GRUPOS PROFINITOS E ÁLGEBRAS DE LIE

Dissertação defendida no Programa de Pós-Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Matemática, aprovada no dia 27 de junho de 2011, pela Banca Examinadora constituída pelos professores:

Aline de Souza Lima

Profa. Dra. Aline de Souza Lima
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Jhone Caldeira Silva

Prof. Dr. Jhone Caldeira Silva
Instituto de Matemática e Estatística-UFG

Aline Gomes S. Pinto

Profa. Dra. Aline Gomes da Silva Pinto
Departamento de Matemática-UnB

Ivonildes Ribeiro Martins

Profa. Dra. Ivonildes Ribeiro Martins
Instituto de Matemática e Estatística-UFG

Márcio Dias de Lima

Graduou-se em Matemática pela Universidade Federal de Goiás no campus avançado de Rialma-GO. Especializou-se em Matemática pela Universidade Federal de Goiás. Atualmente é professor na rede estadual, municipal e particular de ensino nesta mesma cidade.

A meu avô, ***JORDELINO DIAS***, que mesmo sem formação e riquezas materiais, me ensinou, pelo seu exemplo de vida, a importância de ser cristão, generoso, educado, humilde e forte a fim de conquistar meus sonhos, sem reclamar ou até mesmo desistir devido as dificuldades que a vida nos impõe. Obrigado Vovô.

Agradecimentos

A Deus, nosso grande Pai Celeste que sempre me sustentou em todos os momentos, principalmente nos mais difíceis.

Aos meus Pais, José Francisco e Wilma, que sempre me apoiaram para que eu pudesse alcançar essa vitória.

Aos meus irmãos, Assis, Rafael, Janilde, Jane, Márcia e Marcelo, que sempre torceram pela chegada desse momento.

Aos meus sobrinhos, Amanda, Raphaella, Rafaela, Ranieli, Ana Júlia, Alax, Andressa, Carlos Eduardo e Sarah, pois tenho aprendido muito com vocês.

Aos meus amigos do Mestrado, Adriane, Agenor, Alex, Allan, Alfredo, Benedito, Bruno Trindade, Bruno Rodrigues, Caíke, Danilo, Diogo, Emerson, Elaine, Edwin, Edivaldo, Flávia, Fernando, Gabriel, Gean, Victor Hugo, Kaye, Leonardo, Lidiane, Maycon, Rosane, Silvana, Silvio, Sinomar, Thárcis, Sérgio e Ubirajara, pelas incansáveis horas de estudo.

Não poderia também esquecer de duas figuras ilustres Flávio e Lucimeire, que de modo direto me ajudaram muito nessa árdua missão de ser mestre.

A todos os professores que de algum modo contribuíram para esse crescimento profissional, Walterson, Ed Carlos, Rogério, Ticiane, Levi, Armando e Jhone.

Ao professor Ronaldo, que contribuiu para que eu chegasse ao fim desse mestrado "muito obrigado professor".

A minha orientadora, Aline Lima, que desde o primeiro momento se prontificou em me ajudar nesse trabalho, mesmo com todas as minhas limitações e dificuldades

chegamos ao fim.

Aos professores, Aline Pinto, Jhone Caldeira e Ivonildes, pelas correções, sugestões e contribuições para a versão final desse trabalho.

Aos professores e funcionários do IME-UFG.

A minha esposa, Juliana Lima, que teve muita paciência e sempre esteve ao meu lado, embora não conseguisse entender o que eu estudava, e pôde descontar as broncas que eu lhe dava, enquanto ela fazia o seu mestrado. Sou muito grato e feliz por ter você em minha vida e todo nosso esforço, será motivo de orgulho para nossos filhos, que logo chegarão para fazer parte das nossas vidas e nos dar muita alegria.

A Secretaria Estadual e Municipal de Educação pelo suporte financeiro.

A todos vocês o meu sincero agradecimento, peço a Deus saúde e paz para todos nós.

Tudo é do pai, toda honra e toda glória, é dele a vitória, alcançada em minha vida.

Frederico Cruz,

.

Resumo

Lima, Márcio Dias de. **Sobre Centralizadores de Automorfismos Coprimos em Grupos Profinitos e Álgebras de Lie**. Goiânia, 2011. 87p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Sejam A um grupo abeliano elementar de ordem q^2, onde q um número primo. Neste trabalho estudamos a influência dos centralizadores de automorfismos na estrutura dos grupos profinitos, neste sentido se A age como um grupo de automorfismos coprimos sobre um grupo profinito G e que $C_G(a)$ é periódico para cada $a \in A^{\#}$, então mostraremos que G é localmente finito. Será demonstrado também o caso onde A age como um grupo de automorfismos sobre um grupo pro-p de G.

Palavras–chave

álgebras de Lie, anel de Lie associado a um grupo, centralizadores de automorfismos coprimos, grupos localmente finito, grupos profinitos.

Lista de Símbolos

$A^{\#}$	conjunto dos elementos não triviais de A
$G^{(n)}$	n-ésima derivada de G
$D_n(G)$	subgrupo de G definido por $\prod_{ip^k \geq n} \gamma_i(G)^{p^k}$
$[x,y]$	$x^{-1}y^{-1}xy$
$H \leq G$	H é um subgrupo de G
$H \trianglelefteq G$	H é um subgrupo normal de G
$H \triangleleft_{\circ} G$	H é um subgrupo normal aberto de G
$\varprojlim$	limite inverso
$\mathbb{F}_p$	corpo formado por p-elementos
$\overline{X}$	fecho do conjunto X
Hg	classe lateral de H em G
$f^{-1}(X)$	imagem inversa do conjunto X pela aplicação f
$\Phi(G)$	subgrupo de Frattini de G
$exp(G)$	expoente do grupo G
$GL_r(\mathbb{F}_p)$	grupo das matrizes $r \times r$ inversíveis com entradas em $\mathbb{F}_p$
$U_r(\mathbb{F}_p)$	grupo das matrizes triangulares $r \times r$ com entradas em $\mathbb{F}_p$
dlG	comprimento derivado de G
$\gamma_n(G)$	n-ésimo termo da série central inferior de G
$Z_n(G)$	n-ésimo termo da série central superior de G
clG	classe de nilpotência de G
G^n	subgrupo gerado pelo conjunto das n-ésimas potências dos elementos de G
$Np.i.G$	N é um subgrupo potentemente imerso em G
$N_G(H)$	normalizador de H em G
$C_G(H)$	centralizador de H em G
$\|G\|$	ordem de G
$\|G:H\|$	índice de H em G
$\langle X \rangle$	subgrupo gerado pelos elementos do conjunto X
$L(G)$	Anel de Lie associado ao grupo G
$L_p(G)$	subálgebra gerada por D_1/D_2
$\pi(G)$	conjunto de números primos não divisores de $\mid G \mid$

Sumário

Introdução

Sejam G um grupo finito e α um automorfismo de G. Denotamos o centralizador de α em G, ou subgrupo dos pontos fixos, por $C_G(\alpha) = \{x \in G | x^\alpha = x\}$. Se $C_G(\alpha) = 1$, dizemos que α é livre de pontos fixos e se a ordem de α é coprima com a ordem de G, então α é um automorfismo coprimo de G. Burnside [2] mostrou que um grupo G admitindo um automorfismo de ordem 2 livre de pontos fixos é abeliano. Este foi o primeiro resultado significante a respeito do fato da existência de automorfismos livres de pontos fixos implicar em conclusões substanciais em relação a estrutura do grupo. Burnside também analisou o caso em que o automorfismo é de ordem 3 e provou que tal grupo é necessariamente nilpotente de classe no máximo 2. Sabe-se que com o estudo de centralizadores de automorfismos de grupos finitos podemos obter várias informações importantes sobre o grupo em questão. Um dos principais exemplos dessa influência dos centralizadores de automorfismos na estrutura de grupos é devido a Higman [10] e Thompson [33] que mostraram que se G admite um automorfismo livre de pontos fixos de ordem prima p, então G é nilpotente com classe de nilpotência limitada por uma função dependendo somente de p.

Mais um exemplo da influência dos centralizadores de automorfismos de ordem coprima de um grupo G na estrutura de G é dado por Khukhro e Shumyatsky [14]: sejam p um primo, e um inteiro positivo e A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G, assuma que o expoente do $C_G(a)$ divide e para todo $a \in A^\#$, onde $A^\sharp$ é o conjunto de elementos A diferentes da identidade. Então, o expoente de G é limitado por uma função dependendo somente de e e p. Lembramos que um grupo G tem *expoente n*, se $x^n = 1$ para todo $x \in G$.

Este fenômeno, onde a estrutura dos centralizadores de automorfismos do grupo induzem a mesma estrutura no grupo, faz sentido quando a ordem é coprima com a ordem de G, pois nesse caso G é gerado por estes centralizadores. Seja G um grupo admitindo uma ação de um grupo A. Denotamos por $C_G(A)$ o conjunto formado por todos os elementos de G, fixados por A, e é claro que $C_G(A)$ é um subgrupo de G. Se A é grupo abeliano não cíclico e a ordem de A é coprima com a ordem de G, então $G = \langle C_G(a) \mid \ a \in A^\# \rangle$.

Seja F o grupo livre sobre $X = \{x_1, x_2, \ldots\}$. Uma palavra positiva em X é

qualquer elemento não-trivial de F não envolvendo os inversos dos x_i. Uma lei positiva de um grupo G é uma identidade não-trivial da forma $u \equiv v$, onde u, v são palavras positivas, fixadas sob toda substituição $X \to G$. O comprimento máximo de u e v é chamado o grau da lei $u \equiv v$.

Shumyatsky [28], mostrou que se A é um q-grupo abeliano elementar de ordem q^3 agindo sobre um q'-grupo G finito, tal que $C_G(a)$ satisfaz uma lei positiva de grau n para qualquer a em $A^{\#}$, então G satisfaz uma lei positiva de grau limitado por uma função dependendo somente de q e n. Em outro trabalho, Shumyatsky [29] mostra que se A tem ordem q^4 e $C_G(a)'$ satisfaz uma lei positiva de grau n para todo a em $A^{\#}$, então G' satisfaz uma lei positiva de grau limitado por uma função que depende somente de q e n.

Uma generalização desses resultados é apresentado por Lima e Shumyatsky [17], onde A é um q-grupo abeliano elementar de ordem q^2 agindo sobre um q'-grupo G finito, de tal forma que o subgrupo $\langle C_G(a), C_G(b)\rangle$ satisfaz uma lei positiva de grau n para a, b em $A^{\#}$. Neste caso, o grupo G satisfaz uma lei positiva de grau limitado por uma função que depende somente de q e n.

Outra pergunta que aparece com frequência na Teoria dos Grupos é como as imagens finitas de um grupo afetam sua estrutura. Hirsch, (1946), mostrou que se todo quociente de um grupo policíclico-por-finito G é nilpotente, então G é nilpotente. E Grunewald–Pickel–Segal, (1980), mostraram que existe um número finito de isomorfismos de grupos policíclico-por-finito com os mesmos quocientes de G. Questionamentos como esses motivaram as pesquisas na Teoria dos Grupos Profinitos. Um grupo profinito é um grupo topológico isomorfo a um limite inverso de grupos finitos, ou de modo equivalente, um espaço de Hausdorff, compacto e totalmente desconexo.

$$G \cong \varprojlim (G/U)_{U \lhd_o G} \subseteq \prod (G/U)_{U \lhd_o G}, \ (U \text{ subgrupo normal aberto de } G).$$

Outra importante motivação para o estudo de tais grupos é que eles respondem de forma positiva ao Problema Restrito de Burnside: um grupo profinito finitamente gerado de expoente finito é finito.

Neste trabalho, estamos interessados na influência dos centralizadores de automorfismos coprimos em grupos profinitos. Evidentemente que para isso devemos transpor esses conceitos de centralizadores de automorfismos para o contexto topológico.

No contexto de grupos profinitos, todos os conceitos usuais da Teoria de Grupos são interpretadas topologicamente. Em particular, por um automorfismo de um grupo profinito, entende-se um automorfismo contínuo. Um grupo de automorfismo A de um grupo profinito G será chamado de coprimo se A tem ordem finita e G é o limite inverso de grupos finitos cujas ordens são relativamente primos com a ordem de A.

Dado um automorfismo a de um grupo profinito G, denotamos por $C_G(a)$ o centralizador de a em G, que é o subgrupo de G formado pelos elementos fixados por a. Este subgrupo é sempre fechado.

O lema a seguir é bem conhecido no caso onde G é um grupo finito (veja [5], 6.2.2, 6.2.4).

Lema 1 *Seja A um grupo de automorfismos de um grupo profinito G.*
a) Se N é um subgrupo normal fechado A-invariante de G, então $C_{G/N}(A) = C_G(A)N/N$;
b) Se A é um grupo abeliano elementar de ordem q^2, então $G = \langle C_G(a) \mid a \in A^{\#} \rangle$.

Motivados pelo resultado apresentado por Khukhro e Shumyatsky [14], citado no segundo parágrafo deste texto, e pelo lema citado acima, questionamos a influência dos centralizadores de automorfismos na estrutura dos grupos profinitos. Será possível observar os mesmos resultados obtidos para grupos finitos?

Neste sentido, apresentaremos a prova do seguinte teorema:

Teorema 2 *Sejam q um número primo e A um grupo abeliano elementar de ordem q^2. Suponha que A age como um grupo de automorfismos coprimos sobre um grupo profinito G e que $C_G(a)$ é periódico para cada $a \in A^{\sharp}$. Então G é localmente finito.*

De fato, no sentido de demonstrar esse resultado, restringiremos ao caso em que G é um pro-p grupo, ou seja, o limite inverso de p-grupos, conforme a proposição abaixo.

Proposição 3 *Sejam q um número primo e A um grupo abeliano elementar de ordem q^2. Suponha que A age como um grupo de automorfismos coprimo sobre um grupo pro-p de G e que $C_G(a)$ é periódico para cada $a \in A^{\sharp}$. Então G é localmente finito.*

Para concluirmos esse resultado, faremos uso da conhecida série de Jenning-Lazard-Zassenhaus,

$$D_n(G) = \prod_{ip^k \geq n} \gamma_i(G)^{p^k}.$$

Obtemos por meio dessa série uma álgebra de Lie sobre $\mathbb{F}_p$ (corpo com p-elementos). Essa álgebra será denotada por $L(G) = \oplus D_i/D_{i+1}$.

As técnicas de construção, associando a um grupo um anel de Lie, foram introduzidas nos anos 30 por Zelmanov, como uma ferramenta no auxílio à resolução do Problema Restrito de Burnside.

Juntamente com a Proposição 3, outros resultados nos auxiliarão na conclusão do Teorema 2.

Em 1983, Wilson [34], demonstra que se todo subgrupo de Sylow de um grupo profinito periódico é localmente finito, então o grupo é localmente finito.

Zelmanov [38], utilizando alguns resultados de Wilson [34], realiza alguns trabalhos para provar a finitude local de grupos profinitos periódicos. Dessa forma, observe que a prova do Teorema 2, baseia-se fortemente neste resultado, bem como sobre as técnicas da teoria de Lie de Zelmanov e também sobre o resultado Herfort [9] (1979), onde o conjunto dos primos divisores das ordens dos elementos de um grupo profinito periódico é necessariamente finito.

Uma vez que não há solução para o problema de expoente para grupos profinitos periódicos conforme citado acima, apresentaremos uma prova do Teorema 2, que não se refere ao expoente, porém o esquema geral da prova do Teorema 2 é semelhante ao do resultado em Khukhro e Shymyatsky [14].

Este trabalho está dividido em quatro capítulos. No primeiro apresentamos resultados preliminares sobre a Teoria de Grupos, demonstramos algumas propriedades sobre centralizadores de automorfismos para uma melhor compreensão do leitor. No segundo capítulo, apresentamos alguns resultados sobre grupos profinitos, primeiro fazendo uma releitura sobre espaços topológicos relacionando com os conceitos de grupos. Em seguida, passamos à definição de um grupo profinito mostrando alguns exemplos e a partir daí, construímos alguns resultados conhecidos da Teoria de Grupos para a Teoria de Grupos Profinitos. No terceiro capítulo, apresentamos resultados sobre as Álgebras de Lie, produto tensorial, definimos identidade polinomial (PI) para álgebras de Lie e apresentamos resultados que nos auxiliarão posteriormente, além de apresentarmos a construção da série de Jenning-Lazard-Zassenhaus. Ao longo do três primeiros capítulos, construímos ferramentas que auxiliaram na demonstração do Teorema 2, apresentado no quarto capítulo.

CAPÍTULO 1

Preliminares

Apresentamos nesse capítulo alguns resultados que são importantes para o desenvolvimento do nosso trabalho.

1.1 Grupos

Definição 1.1 *Sejam G um grupo, x, y ∈ G. Então o comutador de x e y é:*

$$[x,y] = x^{-1}y^{-1}xy \in G.$$

Temos que $G' = [G,G] = \langle [x,y] \mid x,y \in G \rangle$ é chamado subgrupo comutador de G ou subgrupo derivado de G. Desse modo, podemos descrever uma cadeia de subgrupos da seguinte forma

$$G^{(0)} = G, G^{(1)} = [G^{(0)}, G^{(0)}], G^{(2)} = [G^{(1)}, G^{(1)}], \cdots, G^{(n)} = [G^{(n-1)}, G^{(n-1)}],$$

de tal modo que

$$G \supset G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n)} \supset \cdots.$$

Seja C um subconjunto de um grupo G. Os comutadores de peso p em elementos de C são definidos indutivamente da seguinte maneira: comutadores de peso 1, em elementos de C são exatamente os elementos de C. Agora se tivermos c_1 e c_2 comutadores de pesos p_1 e p_2 em elementos de C respectivamente, então $[c_1, c_2]$ é um comutador em elementos de C de peso $p_1 + p_2$.

Comutadores do tipo $[\ldots[[c_1,c_2]c_3]\ldots c_k]$ são chamados comutadores simples e os denotaremos por $[c_1, c_2, \ldots, c_k]$.

Podemos definir uma série de subgrupos de G, indutivamente, da forma

$$\gamma_1(G) = G, \ \gamma_2(G) = [\gamma_1(G), G] = [G,G] = G', \quad \cdots \quad , \gamma_i(G) = [\gamma_{i-1}(G), G].$$

A série $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots$ é chamada ***Série Central Inferior*** de G.

Para simplificar a escrita, omitiremos o grupo G, ou seja, escreveremos γ_i no lugar de $\gamma_i(G)$.

O centro de G é o subgrupo $Z(G) = \{z \in G \mid [z,x] = 0, \forall x \in G\}$. Por cálculos simples, verifica-se que $Z(G)$ é um subgrupo normal de G.

Podemos definir outra série de subgrupos de G, indutivamente, a partir do centro de G, como segue

$$Z_0(G) = 1, \quad Z_1(G) = Z(G)$$

e indutivamente $Z_i(G)$ como sendo o único subgrupo de G tal que

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)).$$

$Z_i(G)$ é chamado o i-ésimo centro de G. Essa série é chamada ***Série Central Superior*** de G.

O próximo resultado relaciona algumas identidades que envolvem comutadores:

Lema 1.2 *Sejam G um grupo e $a,b,c \in G$. Então:*
a) $ab = ba[a,b]$;
b) $[a,b]^{-1} = [b,a]$;
c) $[ab,c] = [a,c]^b[b,c] = [a,c][a,c,b][b,c]$;
d) $[a,bc] = [a,c][a,b]^c = [a,c][a,b][a,b,c]$;
e) $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a = 1$ *(Identidade de Witt).*

Demonstração. A demonstração dessas identidades seguem diretas da definição de comutadores, faremos somente o item e). Tome $u = aca^{-1}ba$, $v = bab^{-1}cb$ e $w = cbc^{-1}ac$. Então:

$$\begin{aligned}
[a,b^{-1},c]^b &= b^{-1}[[a,b^{-1}],c]b = b^{-1}[a,b^{-1}]^{-1}c^{-1}[a,b^{-1}]cb \\
&= b^{-1}b\underbrace{a^{-1}b^{-1}ac^{-1}a^{-1}}_{u^{-1}}\underbrace{bab^{-1}cb}_{v} \\
&= 1u^{-1}v.
\end{aligned}$$

$$\begin{aligned}
[b,c^{-1},a]^c &= c^{-1}[[b,c^{-1}],a]c = c^{-1}[b,c^{-1}]^{-1}a^{-1}[b,c^{-1}]ac \\
&= c^{-1}c\underbrace{b^{-1}c^{-1}ba^{-1}b^{-1}}_{v^{-1}}\underbrace{cbc^{-1}ac}_{w} \\
&= 1v^{-1}w,
\end{aligned}$$

e com os mesmos cálculos temos $[c,a^{-1},b]^a = w^{-1}u$, o que encerra a demonstração. □

Lema 1.3 *(Lema dos Três Subgrupos). Seja A,B,C subgrupos de um grupo G. Suponha que $[A,B,C] = [B,C,A] = 1$. Então $[C,A,B] = 1$.*

Demonstração. Considere $a \in A$, $b \in B$ e $c \in C$. Pela identidade de Witt temos que $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a = 1$ e por hipótese $[a,b^{-1},c] = [b,c^{-1},a] = 1$. Então fazendo as devidas substituições, teremos: $[1]^b[1]^c[c,a^{-1},b]^a = 1$, donde $[c,a^{-1},b] = 1$. Agora, como a é um elemento arbitrário de A, então vamos mudar a^{-1} por a e então, $[c,a,b] = 1$. Portanto $[C,A,B] = 1$. □

Lema 1.4 *Sejam A,B e C subgrupos de G e N um subgrupo normal de G. Se $[[A,B],C] \leq N$ e $[[B,C],A] \leq N$, então $[[C,A],B] \leq N$.*

Demonstração. Segue do Lema 1.3, bastando tomar *N=1*. □

Lema 1.5 *Em qualquer grupo G, temos $[\gamma_i,\gamma_j] \subseteq \gamma_{i+j}$.*

Demonstração. Por definição, temos que: $G = \gamma_1 \supset \gamma_2 \supset \cdots \gamma_{i+1} \supset \cdots$. Agora supomos sem perda de generalidade que essa série termine em $\gamma_{i+j} = 1$ e fazemos indução sobre j, como segue. Para $j = 1$, temos que: $\gamma_{i+1} = [\gamma_i, G] = [\gamma_i,\gamma_1] \subseteq \gamma_{i+1}$.

Suponha válido para $j = k$, donde $[\gamma_i,\gamma_k] \subseteq \gamma_{i+k}$. Agora vamos verificar se é válido para $j = k+1$. Observe que

$$[\gamma_i,\gamma_k,\gamma_1] = [\gamma_{i+k},\gamma_1] = \gamma_{i+k+1}.$$

$$\begin{aligned}[\gamma_1,\gamma_i,\gamma_k] &= [[\gamma_1,\gamma_i],\gamma_k],\\ &= [[\gamma_i,\gamma_1],\gamma_k],\\ &= [\gamma_{i+1},\gamma_k] = \gamma_{i+1+k}.\end{aligned}$$

Pelo Lema 1.4, temos

$$\begin{aligned}[\gamma_k,\gamma_1,\gamma_i] &= [[\gamma_k,\gamma_1],\gamma_i],\\ &= [\gamma_{k+1},\gamma_i],\\ &= [\gamma_i,\gamma_{k+1}],\\ &\subseteq \gamma_{i+k+1}.\end{aligned}$$

□

Lema 1.6 *Sejam G um grupo, k um número inteiro positivo. Então*
a) γ_k *contém todos os comutadores de peso* $\geq k$ *em G;*
b) γ_k *é gerado por um comutador simples de peso* $\geq k$ *em G;*
c) *Se* $G = \langle M \rangle$, *então* γ_k *é gerado pelos comutadores simples de peso* $\geqslant k$ *em elementos de M;*
d) $G^{(k)} \subseteq \gamma_{2^k}$.

Demonstração. Para provar o item a), vamos usar indução sobre k. Para $k = 1$, temos $\gamma_1(k) = G$. Agora para $r \geq k \geq 2$ tome um comutador c de peso r. Então $c = [c_1, c_2]$, onde c_1 e c_2 são comutadores de peso r_1 e r_2, respectivamente, e $r_1 + r_2 = r$. Por hipótese de indução, $c_1 \in \gamma_{r_1}$ e $c_2 \in \gamma_{r_2}$. Então $c = [c_1, c_2] \in [\gamma_{r_1}, \gamma_{r_2}] \subseteq \gamma_{r_1+r_2} = \gamma_r \subset \gamma_k$.

Agora para provar o item b), defina o subgrupo $N_k = \langle [g_1, g_2, \ldots, g_k] \mid g_i \in G \rangle$, onde N_k é o subgrupo gerado por todos os comutadores de peso k. Agora pelo item a), $\gamma_k \geqslant N_k$, então para provar que γ_k é gerado por um comutador simples de peso $\geqslant k$, basta mostrar que $\gamma_k \leqslant N_k$. Provaremos por indução sobre k. Para $k = 1$, temos $\gamma_1 = G = N_1$. Agora suponhamos válido para $N_{k-1} = \gamma_{k-1}$ e verifiquemos para $N_k = \gamma_k$. Como $[g_1, g_2, \ldots, g_k]^g = [g_1^g, g_2^g, \ldots, g_k^g] \in N_k, \forall g \in G$, $N_k \trianglelefteq G$. Pela definição de série central superior, concluímos que $N_{k-1}/N_k \subset Z(N_{k-1}/N_k) = Z(G/N_k)$, $[N_{k-1}, G] \subset N_k$, mas $[N_{k-1}, G] = [\gamma_{k-1}, G] = \gamma_k \subset N_k$. Portanto $N_k = \gamma_k$, ficando assim provado o item b).

Para o item c) temos o seguinte: $\gamma_k = \langle [g_1, g_2, \ldots, g_k] \mid g_i \in G \rangle$. Agora, para cada g_i podemos expressá-lo como um produto de elementos de M e seus inversos. Para isso, faremos uso das propriedades c) e d) do Lema 1.2 repetidas vezes, chegando assim ao desejado.

Falta provarmos o item d). Novamente vamos provar por indução sobre k. Para $k = 0$, temos $G^{(0)} = G = \gamma_{2^0} = \gamma_1$. Agora suponhamos válido para $k-1$, com $k > 1$ $G^{(k-1)} \subseteq \gamma_{2^{k-1}}$. Para k, temos

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] = [\gamma_{2^{k-1}}, \gamma_{2^{k-1}}] \subseteq \gamma_{2^{k-1}+2^{k-1}} = \gamma_{2^k}.$$

□

Definição 1.7 *Um grupo G é dito* ***abeliano****, se para quaisquer* $a, b \in G$ *tivermos* $ab = ba$.

Definição 1.8 *Um grupo finito G é um* ***p-grupo*** *se, e somente se, a ordem de G é uma potência de p.*

Definição 1.9 *Um grupo G é dito* ***localmente finito****, se todo subgrupo finitamente gerado de G é finito.*

Definição 1.10 *Um grupo abeliano G é dito* ***abeliano elementar****, se existe um número primo p tal que todos os elementos de G, diferentes da unidade, são de ordem p.*

É interessante notar que todo p-grupo abeliano elementar, que é finito, tem uma estrutura bem determinada.

O próximo resultado não será demonstrado e pode ser encontrado em [5].

Lema 1.11 *Seja G um p-grupo abeliano elementar finito. Então G pode ser escrito como o produto direto de um número finito de grupos cíclicos de ordem p.*

Para um grupo arbitrário G, define-se o ***expoente*** de G como o menor número natural m tal que $g^m = 1$, para todo $g \in G$.

Um grupo é dito ***periódico*** (ou um grupo de torsão) se cada elemento tem ordem finita. Todos os grupos finitos são periódicos.

Outro resultado sobre propriedades elementares de comutadores de subgrupos é o seguinte lema, cuja demonstração pode ser encontrada em [5].

Lema 1.12 *Sejam H, K e L subgrupos de um grupo G. Então, temos que*
a) $[H,K]$ *é um subgrupo normal de* $\langle H,K\rangle$*;*
b) Se H, K e L são subgrupos normais de G, então $[HK,L] = [H,L][K,L]$.

1.2 Grupos Nilpotentes

Definição 1.13 *Dizemos que um grupo G é nilpotente se ele contém uma série normal de subgrupos*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

tal que cada G_{i-1} é normal em G e cada quociente G_i/G_{i-1} está contido no centro de G/G_{i-1}, $1 \leq i \leq n$. Isto é equivalente a $[G_i, G] \leq G_{i-1}$. Uma série com estas características é chamada de série central de G.

Note que a definição acima implica que G_1 está contido no centro de G. Se $G_1 = \{1\}$, então G_2 está contido no centro, e assim sucessivamente. Como a série central acaba, resulta imediatamente que todo grupo nilpotente tem centro não trivial.

Proposição 1.14 *Seja G um grupo. As afirmações que seguem são equivalentes:*
a) G é nilpotente.
b) Existe um inteiro positivo m tal que $Z_m(G) = G$.
c) Existe un inteiro positivo n tal que $\gamma_n(G) = 1$.

Observação. Se G é nilpotente, então as séries central superior e central inferior de G têm o mesmo comprimento, que é a sua classe de nilpotência.

Definição 1.15 *Um grupo G tem a propriedade do normalizador se todo subgrupo próprio de G está estritamente contido em seu normalizador.*

Proposição 1.16 *Seja P um p-subgrupo de Sylow de um grupo G e seja H outro subgrupo de G. Se $P \subset H$, então $H = N_G(H)$. Em particular, $N_G(N_G(P)) = N_G(P)$.*

Demonstração. Seja $x \in N_G(H)$. Como $P \subset H \lhd N_G(H)$, temos que $xPx^{-1} \subset H$. Como P e xPx^{-1} são p-subgrupos de Sylow de H, existe um elemento $h \in H$ tal que $xPx^{-1} = hPh^{-1}$, donde $h^{-1}x \in N_G(H) \subset H$. Segue que $x \in H$ e portanto $N_G(H) = H$. □

Lema 1.17 *Todo p-grupo finito é nilpotente.*

Demonstração. Seja G um grupo tal que $\mid G \mid = p^m$, onde m é um inteiro positivo. Sendo $\mid G \mid > 1$, temos que $Z(G) \neq \{1\}$. Sejam $H_0 = \{1\}$ e $H_1 = Z(G)$. Se $H_k \lhd G$ já está definido, definamos $H_{k+1} \lhd G$ por $H_{k+1}/H_k = Z(G/H_k)$. Como G/H_k é um p-grupo finito, temos que se $G/H_k \neq 1$, então $H_{k+1}/H_k \neq H_k$, logo $H_k < H_{k+1} \lhd G$. Após no máximo m passos, temos

$$1 = H_0 \leq H_1 \leq \cdots \leq H_m = G,$$

onde $H_k \lhd G$ e $H_{k+1}/H_k = Z(G/H_k),\ k = 1,2,\ldots,m-1$. Portanto, G é nilpotente de classe no máximo m. □

O próximo resultado apresenta uma caracterização dos grupos nilpotentes finitos.

Teorema 1.18 *Seja G um grupo finito. Então as seguintes afirmações são equivalentes:*
a) G é nilpotente;
b) G tem a propriedade do normalizador;
c) Todo subgrupo de sylow G é normal em G;
d) G é o produto direto dos seus subgrupos de sylow;
e) Todo subgrupo de G é subnormal;
f) Todo subgrupo maximal de G é normal.

Demonstração. Utilizaremos o seguinte esquema

$$\begin{array}{ccccccc} a) & \Longrightarrow & b) & \Longrightarrow & c) & \Longrightarrow & d) \Longrightarrow a) \\ & \searrow & & & & \nearrow & \\ & & e) & \Longrightarrow & f) & \Longrightarrow & c) \end{array}$$

$a) \Rightarrow b)$ Seja H um subgrupo próprio de G. Queremos mostrar que $H \subsetneq N_G(H)$. Temos que $1 = Z_0(G) \subset H \subset Z_n(G) = G$, e como $H \leq G$, então existe um inteiro $i \geq 0$ tal que

$Z_i \subset H$ e $Z_{i+1} \nsubseteq H$. Tome $x \in Z_{i+1}\backslash H$ e $h \in H$. Como $[Z_{i+1}(G), G] \subset Z_i(G)$, temos que existe $y \in Z_i(G) \subset H$ tal que $xHx^{-1} = hy \in H$. Portanto $xHx^{-1} \subset H$ e $x \in N_G(H)$, donde $H \subsetneq N_G(H)$.

$b) \Rightarrow c)$ Sejam P um p-subgrupo de sylow de G e $H = N_G(P)$. Se $H \neq G$, por hipótese $H \subsetneq N_G(H)$, e pela Proposição 1.16, $H = N_G(H)$. Logo $H = G$, ou seja, $N_G(P) = G$, donde $P \lhd G$.

$c) \Rightarrow d)$ Sejam $P_1, P_2, \ldots, P_k$ os subgrupos de Sylow de G. Como cada $P_i \lhd G$, então $P_i \cap P_j = \{e\}$; $i, j = 1, 2, \ldots, k$. Seja $x = \alpha_1, \alpha_2, \ldots, \alpha_k$, onde $\alpha_i \in P_i$, $1 \leqslant i \leqslant k$. Temos que $P_1 \cap (P_2, \cdots, P_k) = \{e\}$ e assim temos $|P_1 \cdots P_k| = \underbrace{\frac{|P_1||P_2 \cdots P_k|}{|P_1 \cap (P_2 \cdots P_k)|}}_{\{e\}} = |P_1||P_2 \cdots P_k|$.
De modo recursivo teremos que: $|P_1 \cdots P_k| = |P_1||P_2| \cdots |P_k|$, onde $P_1^{\alpha_1} \cdots P_k^{\alpha_k} = G$.

$d) \Rightarrow a)$ G é o produto de um número finito de p-grupos. Como todos são nilpotentes, G também o é.

$a) \Rightarrow e)$ Seja H um subgrupo maximal de G. Como H é nilpotente, então safisfaz a propriedade do normalizador. Logo $H \subsetneq N_G(M)$, mas como H é maximal, então $N_G(H) = G$, o que mostra que $H \lhd G$.

$e) \Rightarrow f)$ Se todo subgrupo H de G é subnormal e H é maximal, então não existe nenhum outro subgrupo de G entre H e G, portanto $H \lhd G$.

$f) \Rightarrow c)$ Se todo subgrupo maximal de G é normal e P é um p-subgrupo de Sylow de G e $N_G(H)$ é um subgrupo próprio de G, então $N_G(H) \subset H$, que é maximal em G e com isso normal em G, então $N_G(H) = G$, o que é contradição pela Proposição 1.16 (pois $N_G(H) = H$). □

1.3 Automorfismos Coprimos

Muitos problemas na Teoria dos Grupos podem ser reduzidos a problemas sobre ações de grupos. Em particular, se trabalharmos com grupos finitos, encontraremos com frequência situações onde um grupo admite um automorfismo do qual a ordem é coprima com a ordem do grupo, ou seja $\big(\mid G \mid, \mid \varphi \mid \big) = 1$, onde φ é automorfismo de G. Tais automorfismos são chamados ***automorfismos coprimos***.

Sejam G um grupo finito, φ um automorfismo de G. Denotaremos por $C_G(\varphi)$ o conjunto dos pontos fixos de φ, isto é $C_G(\varphi) = \{x \in G \mid x^\varphi = x\}$. Dizemos que φ é livre de pontos fixos se $C_G(\varphi) = 1$. Se N é um subgrupo φ-invariante de G, ou seja $\varphi(N) \subseteq N$, então φ induz uma função $\overline{\varphi}$ do conjunto das classes laterais à esquerda de N sobre si mesmo,

$$\overline{\varphi}: \ xN \to x^\varphi N.$$

Se ocorrer $N \trianglelefteq G$, então é fácil ver que $\overline{\varphi}$ é um automorfismo do grupo quociente G/N. Abusando da notação, denotaremos o automorfismo induzido pelo mesmo símbolo φ. Este primeiro lema mostra a conexão entre $C_G(\varphi)$ e $C_{G/N}(\varphi)$.

Lema 1.19 *Seja G um grupo finito admitindo um automorfismo coprimo φ e N um subgrupo normal φ-invariante de G. Então $C_{G/N}(\varphi) = C_G(\varphi)N/N$.*

Demonstração. Seja N um subgrupo normal φ-invariante de G, então φ induz uma aplicação

$$\overline{\varphi}: xN \to x^\varphi N,$$

ou seja,

$$\begin{array}{rcl} \overline{\varphi}: G/N & \to & G/N \\ gN & \mapsto & \overline{\varphi}(gN) = \varphi(g)N. \end{array}$$

Tome $y \in C_G(\varphi)N/N$. Então $y = aN$, com $a \in C_G(\varphi)$ e

$$\begin{array}{rcl} \overline{\varphi}(aN) & = & \varphi(a)N, \ \ mas \ \varphi(a) = a \\ & = & aN, \ \text{pois } \varphi(a) = a. \end{array}$$

Portanto, $C_G(\varphi)N/N \subseteq C_{G/N}(\varphi)$.

Para a inclusão inversa, temos que mostrar que toda classe φ-invariante aN contém um elemento de $C_G(\varphi)$.

Suponha primeiro que φ tenha ordem p, onde p é um número primo. Então o tamanho de qualquer φ-órbita em G divide a ordem de φ, ou seja tem que ser 1 ou p. Suponha que aN não contenha nenhum elemento do $C_G(\varphi)$. Então aN é a união de φ-órbitas de tamanho p. Desde que a interseção de quaisquer duas órbitas é vazia, segue que p divide o número de elementos em aN. Em outras palavras, p divide $\mid aN \mid = \mid N \mid$, que é uma contradição, pois φ é um automorfismo coprimo. Assim, mostramos que aN contém um elemento de $C_G(\varphi)$.

Agora, admita que φ é de ordem $p \cdot m$, onde p é primo e proceda por indução sobre a ordem de φ. Sejam $\psi = \varphi^p$, $H = C_G(\varphi)$, $N_1 = N \cap H$.

Tomando aN como uma classe φ-invariante, aN é também ψ-invariante. Assim, pela hipótese de indução, aN contém um elemento $a_0 \in H$, donde $aN = a_0N$.

Seja $\overline{\varphi}$ o automorfismo de H induzido pela ação de φ (temos que H é φ-invariante). Evidentemente a ordem de $\overline{\varphi}$ é 1 ou p. A classe a_0N_1 é $\overline{\varphi}$-invariante e assim contém um elemento a_1 que se encontra em $C_H(\overline{\varphi})$. Segue que $a_0N_1 \subseteq a_0N = aN$ e $C_H(\overline{\varphi}) = C_G(\varphi)$. Mostramos então que $aN = a_1N$, onde a_1 é um elemento de $C_G(\varphi)$. Assim, $aN \subseteq C_G(\varphi)N/N$. □

Corolário 1.20 *Seja φ um automorfismo coprimo de um grupo G.*
a) $G = C_G(\varphi)[G,\varphi]$;
b) $[G,\varphi] = [G,\varphi,\varphi]$ onde $[G,\varphi,\varphi] = [[G,\varphi],\varphi]$;
c) Se G é abeliano então $G = C_G(\varphi) \oplus [G,\varphi]$.

Demonstração.

a) Tome $N = [G,\varphi]$ e observe que $[G,\varphi]$ é o menor subgrupo normal φ-invariante, onde φ age trivialmente sobre o grupo quociente G/N, onde $\overline{\varphi} : G/N \to G/N$. Com isso, temos que $C_{G/N}(\overline{\varphi}) = G/N$. Mas pelo Lema 1.19, temos

$$C_{G/N}(\varphi) = C_G(\varphi)N/N \;\Rightarrow\; G/N = C_G(\varphi)N/N.$$

Como $N = [G,\varphi]$, segue que $G = C_G(\varphi)[G,\varphi]$.

b) Temos

$$\begin{aligned}
[G,\varphi] &= [C_G(\varphi)[G,\varphi],\varphi], \\
&= \underbrace{[C_G(\varphi),\varphi]}_{1}{}^{[G,\varphi]}[[G,\varphi],\varphi], \\
&= 1^{[G,\varphi]}[[G,\varphi],\varphi], \\
&= [[G,\varphi],\varphi], \\
&= [G,\varphi,\varphi].
\end{aligned}$$

c) Podemos aplicar o Teorema de Maschke, uma vez que G é abeliano e φ é um autormorfismo coprimo de G. Assim, existe um subgrupo A-invariante N de G, tal que $G = C_G(\varphi) \oplus N$. Como $C_N(\varphi) = 0$, segue do item *b*) que $N = [N,\varphi]$. Portanto,

$$[G,\varphi] = [C_G(\varphi) \oplus N,\varphi] \subseteq [C_G(\varphi),\varphi] \oplus [N,\varphi] = N \;\text{ e }\; G = C_G(\varphi) \oplus [G,\varphi].$$

□

1.4 p-Grupos Potentes

Um dos objetivos desta seção é apresentar as principais propriedades de p-grupos potentes que serão requisitados no terceiro capítulo deste trabalho, no momento de definir o anel de Lie associado a um grupo G sobre $\mathbb{F}_p$. Os p-grupos potentes possuem propriedades lineares muito boas, das quais se destaca como uma ferramenta importante neste trabalho a seguinte: se um p-grupo potente G é gerado por elementos de expoente p^e, onde e é um inteiro positivo, então o expoente de G também é p^e. Esta e outras propriedades interessantes dos p-grupos potentes que citaremos nesta seção serão apresentadas sem as devidas demonstrações, mas podem ser encontradas no livro de Dixon, du Sautoy, Mann e Segal, Analytic pro-p Groups [12].

Definição 1.21 *Seja G um p-grupo finito. Para todo $i \geq 0$, definimos*

$$\Omega_i(G) = \left\langle x \in G \mid x^{p^i} = 1 \right\rangle,$$

e

$$\mho_i(G) = G^{p^i} = \left\langle x^{p^i} \mid x \in G \right\rangle.$$

Observamos que os subgrupos $\Omega_i(G)$ e $\mho_i(G)$ são característicos em G.

Já que $G/\Phi(G)$ é um p-grupo abeliano elementar, onde $\Phi(G)$ é o subgrupo de Frattini, o qual é definido como a interseção de todos os subgrupos maximais de G, assim $x^p \in \Phi(G)$, para todo $x \in G$. Assim $\mho_1(G) = G^p \leq \Phi(G)$. Consequentemente, se G é um p-grupo, $\Phi(G)$ é o menor subgrupo de G com quociente abeliano elementar.

Observamos que no caso de p-grupos finitos o expoente de G é simplesmente a ordem máxima dos elementos de G. Se $exp(G) = p^e$, então $x^{p^e} = 1$, para todo $x \in G$. Desta forma, $\Omega_e(G) = \left\langle x \in G \mid x^{p^e} = 1 \right\rangle = G$ e podemos considerar uma série ascendente

$$1 = \Omega_0(G) \leq \Omega_1(G) \leq \cdots \leq \Omega_{e-1}(G) \leq \Omega_e(G) = G,$$

que chamamos de Ω-série de G. Similarmente, temos que $\mho_e(G) = \left\langle x^{p^e} \mid x \in G \right\rangle = 1$ e definimos a seguinte série descendente

$$1 = \mho_0(G) \leq \mho_1(G) \leq \cdots \leq \mho_{e-1}(G) \leq \mho_e(G) = G,$$

que chamamos de $\mho$-série de G. A $\mho$-série é estritamente decrescente. Logo, a $\mho$-série de um p-grupo finito de expoente p^e, tem exatamente e passos.

Teorema 1.22 *Seja G um p-grupo abeliano finito. Para todo $i \geq 0$, vale as seguintes afirmações;*
a) $\Omega_i(G) = \left\{ x \in G \mid x^{p^i} = 1 \right\}$;

b) $\mho_i(G) = \{x^{p^i} \mid x \in G\}$;
c) $\mid G : \Omega_i(G) \mid = \mid \mho_i(G) \mid$ (*consequentemente* $\mid G : \mho_i(G) \mid = \mid \Omega_i(G) \mid$).

Demonstração. Considere o homomorfismo

$$\begin{aligned} \varphi : G &\to G \\ x &\mapsto x^{p^i}. \end{aligned}$$

Como G é abeliano, temos que $\Omega_i(G)$ é o núcleo de φ e $\mho_i(G)$ a imagem. Assim os ítens *a)* e *b)* são satisfeitos. Já o item *c)* segue diretamente do Primeiro Teorema do Homomorfismo. □

Uma observação importante é que nenhum dos ítens do teorema acima valem para p-grupos em geral.

Teorema 1.23 *(A Fórmula de Compilação de Phillip Hall). Sejam G um grupo e x e $y \in G$. Então, existem elementos $c_i = c_i(x,y) \in \gamma_i(\langle x,y \rangle)$, tais que*

$$x^n y^n \cong (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \dots c_n,$$

para todos $n \in \mathbb{N}$. Em outras palavras

$$x^n y^n \cong (xy)^n \left(mod \gamma_2(\langle x,y \rangle)^{\binom{n}{2}} \gamma_3(\langle x,y \rangle)^{\binom{n}{3}} \dots \gamma_2(\langle x,y \rangle)\right).$$

A Fórmula de Compilação de Phillip Hall é especialmente significativa quando G tem expoente primo p, desde que p divide $\binom{p}{i}$ para todo $i \leq i \leq p-1$. Consequentemente, podemos escrever

$$x^p y^p = (xy)^p z c_p, \text{ onde } z \in \mho_1(\langle x,y \rangle').$$

Definição 1.24 *Seja G um p-grupo finito. Dizemos que G é um p-grupo regular se*

$$x^p y^p = (xy)^p \left(mod \mho_1(\langle x,y \rangle')\right), \text{ para todos } x,y \in G.$$

Equivalentemente, se $c_p = c_p(x,y) \in \mho_1(\langle x,y \rangle')$, ou seja, se $\gamma_1(\langle x,y \rangle) \leq \mho_1(\langle x,y \rangle')$.

Definição 1.25 *Um subgrupo N de um p-grupo finito G é dito potentemente imerso em G, se $N^p \geq [N,G]$, para $p \neq 2$ (ou $N^4 \geq [N,G]$, para $p = 2$) e denotamos por $Np.i.G$.*

Algumas observações importantes podem ser feitas sobre tais subgrupos. A primeira é que $[N,N] \leq N^2$ é sempre verdade pois N/N^2 tem expoente 2, portanto é

abeliano. Outro fato importante é que se $Np.i.G$, então N é normal em G. Ainda mais, se $Np.i.G$, então $N/N^p \leq Z(G/N^p)$.

Agora, seja $\varphi : G \to G_1$ um homomorfismo qualquer do grupo G no grupo G_1. Temos que $N^\varphi \leq G_1$ e

$$[N^\varphi, G^\varphi] = [N,G]^\varphi \leq (N^p)^\varphi = (N^\varphi)^p.$$

Portanto, N^φ é potentemente imerso em G^φ. Em particular, qualquer quociente de G é potentemente imerso.

Lema 1.26 *Seja G um p-grupo finito e sejam N, M subgrupos potentemente imersos em G. Então, $[M,N], M^p$ e MN são potentemente imersos em G. Ainda, se $H \leq G$ é tal que N é normal em $G, N \leq H$ não é potentemente imerso em H, então existe um subgrupo normal J de G, tal que*

- *se p é impar,*

$$N^p[N,H,H] \leq J \leq N^p[N,H] \;\; e \;\; [N^p[N,H] : J] = p;$$

- *se $p = 2$,*

$$N^4[N,H]^2[N,H,H] \leq J \leq N^4[N,H] \;\; e \;\; [N^4[N,H] : J] = 2.$$

Definição 1.27 *Um p-grupo finito G é dito potente se, e somente se, G é potentemente imerso em si mesmo, ou seja, $G^p \geq [G,G]$ para $p \neq 2$ (ou $G^4 \geq [G,G]$ para $p = 2$).*

Outra caracterização desses grupos no caso p ímpar é a seguinte: se p é ímpar, G é potente se, e somente se, $G^p = \Phi(G) = \mho_1(G)$.

Novamente observamos que $[G,G] \leq G^2$ é sempre verdade, e se H é um subgrupo potentemente imerso em G, então H é potente.

Corolário 1.28 *Se G é um p-grupo potente, então $[G,G], G^p, \Phi(G), G^{(k)}, \gamma_k(G)$ para todo $k \in \mathbb{N}$, são potentemente imersos em G.*

Lema 1.29 *Se G é um p-grupo potente, então*
a) $G^{p^i} = \mho_i(G) = \{x^{p^i} \mid x \in G\}$, para todo $i \in \mathbb{N}$;
b) G^{p^i} formam uma série central de G. Se $exp(G) = p^e$, então G é nilpotente de classe menor ou igual a e.

Seja G um p-grupo finito e faça

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

Para simplificar a notação escrevemos $G_i = P_i(G)$.

Lema 1.30 *Seja G um p-grupo potente. Então*
a) para cada i, G_i é potentemente imerso em G e $G_{i+1} = G_i^p = \Phi(G_i)$;
b) para cada i, a aplicação $x \mapsto x^p$ induz um homomorfismo de G_i/G_{i+1} para G_{i+1}/G_{i+2}.

Teorema 1.31 *Seja $G = \langle a_1, \ldots, a_r \rangle$ um p-grupo potente. Então, $G^p = \langle a_1^p, \ldots, a_r^p \rangle$.*

Demonstração. Seja $\theta : G/G_2 \to G_2/G_3$ o homomorfismo dado pelo lema anterior. Então, G_2/G_3 é gerado por $\{\theta(a_1G_2), \ldots, \theta(a_dG_2)\}$. Assim $G_2 = \langle a_1^p, a_2^p, \ldots, a_r^p \rangle G_3$. Como $G_3 = \Phi(G_2)$ e $G_2 = G^p$, o resultado segue pelo Lema 1.30. □

Proposição 1.32 *Se $G = \langle a_1, a_2 \ldots, a_d \rangle$ é um p-grupo potente, então $G = \langle a_1 \rangle \cdots \langle a_r \rangle$, isto é, G é o produto de seus subgrupos cíclicos $\langle a_1 \rangle$.*

O ***posto*** de um grupo G é o menor inteiro r, tal que todo subgrupo de G pode ser gerado por r elementos. Denotamos por $rk(G)$ o posto de um grupo G. Para um p-grupo finito G, denotamos por $d(G)$ a menor cardinalidade de um conjunto de geradores de G. Assim, $d(G)$ é também a dimensão de $G/\Phi(G)$ como um espaço vetorial sobre $\mathbb{F}_p$. Se G é um p-grupo potente e H um subgrupo de G, então apresentaremos no próximo teorema que $d(H) \leq d(G)$. Consequentemente, como o posto de um grupo finito G é definido por $rk(G) = sup\{d(H) \mid H \leq G\}$, se G é um p-grupo potente, então $rk(G) = d(G)$.

Teorema 1.33 *Se G é um p-grupo potente e H é um subgrupo de G, então $d(H) \leq d(G)$.*

Definição 1.34 *para um p-grupo finito G e um inteiro positivo r, $V(G,r)$ denota a interseção dos núcleos de todos os homomorfismos de G sobre $GL_r(\mathbb{F}_p)$.*

Relembramos que $GL_r(\mathbb{F}_p)$ denota o grupo das matrizes $r \times r$ inversíveis com entradas em $\mathbb{F}_p$ e $U_r(\mathbb{F}_p)$ o grupo das matrizes triangulares $r \times r$ com entradas em $\mathbb{F}_p$. Como a imagem de qualquer homomorfismo de um p-grupo G sobre $GL_r(\mathbb{F}_p)$ é um p-grupo e todo p-subgrupo de $GL_r(\mathbb{F}_p)$ é conjugado de um subgrupo do menor grupo unitriangular $U_r(\mathbb{F}_p)$, podemos definir $V(G,r)$ como a interseção dos núcleos de todos os homomorfismos de G sobre $U_r(\mathbb{F}_p)$. Apenas note que um elemento $g \in G$ pertence a $V(G,r)$ se, e somente se, g age trivialmente em toda representação linear de G sobre qualquer $\mathbb{F}_p$-espaço vetorial de dimensão no máximo r.

Para $r \in \mathbb{N}$, definimos o inteiro $\lambda(r)$ por

$$2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}.$$

Lema 1.35 *i) O grupo $U_r(\mathbb{F}_p)$ tem uma série, de comprimento $\lambda(r)$, de subgrupos normais, cujos fatores são abelianos elementares;*
ii) Se G é um p-grupo finito, então $G/V(G,r)$ tem uma série com as propriedades acima.

Proposição 1.36 *Seja G um p-grupo finito e r um inteiro positivo. Ponha $V = V(G,r)$ e seja $W = V$ se p é ímpar, $W = V^2$ se $p = 2$. Se $N \lhd G$, $d(N) \leq r$ e $N \leq W$, então N é potentemente imerso em W.*

Teorema 1.37 *Seja G um p-grupo finito de posto r. Então, G tem um subgrupo potente característico de índice no máximo $p^{r\lambda(r)}$ se p é ímpar e $p^{r+r\lambda(r)}$ se $p = 2$.*

Demonstração. Ponha $V = V(G,r)$. Pelo Lema 1.35, existe uma série de subgrupos normais de G para V, de comprimento no máximo $\lambda(r)$, com cada fator abeliano elementar. Como G tem posto r, cada fator tem ordem no máximo p^r e assim $| G : V | \leq p^{r\lambda(r)}$. Se p é ímpar, a Proposição 1.36 mostra que V é potente. Se $p = 2$, sabemos pela Proposição 1.36 que V^2 é potente, e como $| V/V^2 | \leq 2^2$, temos $| G : V^2 | \leq p^{r+r\lambda(r)}$. Isso completa a demonstração. □

Lema 1.38 *Seja G um grupo de expoente primo p e posto r. Então $| G | \leq p^s$, onde $s = s(r)$ é um número dependendo somente de r.*

Demonstração. Pelo Teorema 1.37, temos um subgrupo potente característico N de G de índice no máximo $p^{\mu(r)}$, onde $\mu(r)$ é um número dependendo somente de r. O Corolário 1.35 mostra que N é o produto de no máximo r subgrupos cíclicos. Portanto, N tem ordem no máximo p^r e o resultado segue.

□

CAPÍTULO 2

Grupos Profinitos

Neste capítulo apresentamos alguns resultados sobre topologia discreta e grupos profinitos. Definimos um grupo profinito como sendo um espaço de Hausdorff compacto totalmente desconexo ou simplesmente o limite inverso de grupos finitos. Estendemos também os conceitos sobre a teoria de Sylow para grupos profinitos, não deixando de citar, é claro, o Teorema de Lagrange. Estes e outros resultados sobre o estudo dos grupos profinitos podem ser encontrados em [21].

2.1 Espaços Topológicos

Um ***espaço topológico*** é um conjunto X juntamente com uma família de subconjuntos, chamado conjuntos abertos, satisfazendo as seguintes condições:

a) O conjunto vazio $\emptyset$ e X são ambos conjuntos abertos;
b) A intercessão de quaisquer dois conjuntos abertos é também um conjunto aberto;
c) A união de uma coleção qualquer de conjuntos abertos é também um conjunto aberto.

O conjunto de todos os conjuntos abertos de X é chamado ***topologia*** em X. Um subconjunto de X é ***fechado*** se seu complementar é aberto. Se Y é um subconjunto de X, o ***fecho*** $\overline{Y}$ de Y é a interseção de todos conjuntos fechados contendo Y; assim $\overline{Y}$ é também um conjunto fechado. Um subconjunto Y de X é chamado ***denso*** em X se $\overline{Y} = X$.

Uma ***vizinhança aberta*** de um elemento $x \in X$ é um conjunto aberto que contém x. Uma ***base*** para a topologia sobre X é uma coleção $(U_\phi \mid \phi \in \mathfrak{B})$ de conjuntos abertos, tais que todo conjunto aberto é uma união de alguns dos conjuntos U_ϕ e a base de uma vizinhança aberta de x é definida de modo similar.

Qualquer conjunto X pode ser considerado como um espaço topológico definindo a topologia em que cada subconjunto é considerado aberto; esta topologia é chamada de ***topologia discreta*** sobre X, e o espaço topológico X é chamado de ***espaço discreto***.

Se Y é um subconjunto de um espaço topológico X, então a coleção de todos subconjuntos da forma $Y \cap U$ com U aberto em X é uma topologia sobre Y. Isto é chamado

de ***subespaço topológico***, e com respeito a esta topologia Y, é chamada de subespaço de X.

Um espaço topológico X é chamado ***compacto*** se quando

$$X = \bigcup_{\alpha \in A} U_\alpha, \text{ onde } U_\alpha \text{ é aberto,}$$

então existe uma sub-família finita $U_{\alpha_1}, U_{\alpha_2}, \cdots, U_{\alpha_n}$, tal que

$$X = U_{\alpha_1} \cup U_{\alpha_2} \cup \cdots \cup U_{\alpha_n}.$$

Equivalentemente, X é compacto se, quando $(C_\alpha \mid \alpha \in A)$ é uma família de subconjuntos fechados com a propriedade que cada interseção de conjuntos finitos é não vazia e segue que a interseção de todos os conjuntos é não vazia. Pela afirmação que um subespaço Y de um espaço X é compacto, queremos dizer que Y é compacto com respeito ao subespaço topológico.

Um espaço X é chamado de ***Hausdorff***, se dados quaisquer dois elementos distintos x, y de X, existem vizinhanças abertas U, V de x, y respectivamente, tais que $U \cap V = \emptyset$. Se X é Hausdorff, então segue imediatamente que $\{x\}$ é fechado para cada elemento $x \in X$.

O espaço X é chamado ***conexo*** se não pode ser escrito como união disjunta de dois subconjuntos abertos não vazio. Por outro lado, X é ***totalmente desconexo*** se todo subespaço conexo tem no máximo um elemento. Os espaços com os quais estamos interessados são espaços de Hausdorff, compacto e totalmente desconexo.

Lema 2.1 *Seja X um espaço de Hausdorff compacto.*
a) Se C, D são subconjuntos fechados tais que $C \cap D = \emptyset$, então existem subconjuntos abertos U, V, tais que $C \subseteq U$, $D \subseteq V$ e $U \cap V = \emptyset$.
b) Sejam $x \in X$ e A a interseção de todos os subconjuntos de X contendo x, que é simultaneamente fechado e aberto. Então A é conexo.
c) Se X é totalmente desconexo, então todo conjunto aberto é uma união de conjuntos que são simultaneamente fechados e abertos.

Demonstração. Será omitida, mas pode ser encontrada em ([35], p. 02) □

Lema 2.2 *a) Cada subconjunto fechado de um espaço compacto é compacto.*
b) Cada subconjunto compacto de um espaço de Hausdorff é fechado.
c) Se $f : X \to Y$ é contínua e X é compacto, então $f(X)$ é compacto.
d) Se $f : X \to Y$ é contínua e bijetora e se X é compacto e Y é Hausdorff, então f é um homeomorfismo.

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

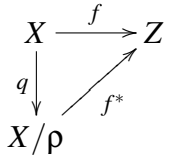
Demonstração. As demonstrações dos ítens $a)$, $b)$ e $c)$ serão omitidos e podem ser encontrados em [18]. Para provar $d)$ é suficiente mostrar que a imagem por f de cada subconjunto fechado de X é fechado. Então segue de $a)$, $b)$ e $c)$.

Agora para concluirmos, suponha por contradição que $N = \{x \in X \mid f(x) \neq g(x)\}$, seja $y \in N$, onde U e V são subconjuntos abertos de Y contendo $f(y)$ e $g(y)$. Assim $f^{-1}(U) \cap g^{-1}(V)$ é uma vizinhança aberta de x e está contida em N. Portanto N é uma união de conjuntos abertos e assim é aberto. Assim fica provado o item $e)$. □

Lema 2.3 *Seja X um espaço totalmente desconexo. Então $\{x\}$ é fechado em X, para cada $x \in X$.*

Demonstração. Seja C o fecho de $\{x\}$. Se C é a união de dois subconjuntos abertos disjuntos A, B, com $x \in A$, então A é fechado em C e assim é fechado em X, de modo que teremos $A = C$. Segue que o conjunto fechado C é conexo e que $C = \{x\}$. Portanto X é totalmente desconexo. □

Seja ρ uma relação de equivalência sobre um espaço topológico X e escrevemos X/ρ para o conjunto quociente e q para a função quociente de X em X/ρ. A topologia quociente sobre X/ρ é a topologia onde os conjuntos abertos são os subconjuntos V de X/ρ tais que $q^{-1}(V)$ é aberto em X. Assim se X/ρ é dado com a topologia quociente, então a função quociente q é contínua. É fácil verificar que q tem a seguinte propriedade: se $f : X \to Z$ é uma função contínua em um espaço Z tal que elementos equivalentes com respeito a ρ tem a mesma imagem sob f, então existe uma única função contínua $f^* : X/\rho \to Z$ tal que $f = f^* q$:



2.1.1 Produtos de Espaços Topológicos

O produto cartesiano de uma família $(X_\lambda \mid \lambda \in \Lambda)$ de conjuntos é o conjunto $C = \prod_{\lambda \in \Lambda} X_\lambda$ onde os elementos são aplicações x de Λ em $\bigcup_\lambda X_\lambda$ com a propriedade que $x(\lambda) \in X_\lambda$ para cada λ. Analisaremos os elementos de C como vetores com entradas indexadas pelos elementos de Λ. Assim um elemento de C será escrito como (x_λ). A este

elemento corresponde a função que aplica λ em x_λ. A função projeção π_λ é uma aplicação que toma um elemento de C para cada λ. O produto de uma família finita $X_1, X_2, \cdots, X_n$ de conjuntos é denotada por $X_1 \times X_2 \times \cdots \times X_n$.

Agora suponha que cada X_λ é um espaço topológico. O produto topológico sobre C tem como conjuntos abertos todas as uniões de conjuntos da forma:

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

com n finito e cada $\lambda_i \in \Lambda$ e U_i aberto em X_{λ_i}. Portanto, cada função projeção π_λ é contínua. De fato o produto topológico é a menor topologia na qual cada função projeção é contínua.

Seja Z um espaço topológico e $f : Z \to C$ uma função, dizemos que f é contínua se, e somente se, cada função $\pi_\lambda f$ é contínua. A implicação "somente se" é direta. Suponha que cada função $\pi_\lambda f$ é contínua. Se U_i é aberto em X_{λ_i}, para $i = 1, 2, \ldots, n$, então cada $(\pi_{\lambda_i} f)^{-1}(U_i)$ é aberto em Z e assim o conjunto $f^{-1}(\bigcap_{i=1}^{n} \pi_{\lambda_i}^{-1}(U_i) = \bigcap_{i=1}^{n} (\pi_{\lambda_i} f)^{-1}(U_i)$ é aberto em Z.

Teorema 2.4 *Seja $(X_\lambda \mid \lambda \in \Lambda)$ uma família de espaços topológicos e seja C seu produto cartesiano.*
a) Se cada X_λ é Hausdorff, assim é C.
b) Se cada X_λ é totalmente desconexo, assim é C.
c) Se cada X_λ é compacto, assim é C.

Demonstração. Será omitida, mas pode ser encontrada em ([35], p. 4). □

2.1.2 Grupos Topológicos

Um grupo topológico é um grupo G com a propriedade que a função multiplicação

$$\begin{aligned} m : G \times G &\to G \\ (a, b) &\mapsto ab \end{aligned}$$

e a função inversa

$$\begin{aligned} i : G &\to G \\ a &\mapsto a^{-1} \end{aligned}$$

são contínuas.

Lema 2.5 *Seja G um grupo topológico.*
a) A função $(x,y) \mapsto xy$ *de* $G \times G$ *em G é contínua e a função* $x \mapsto x^{-1}$ *de G em G é um homeomorfismo. Para cada* $g \in G$ *a função* $x \mapsto xg$ *e* $x \mapsto gx$ *de G para G são homeomorfismos.*
b) Se H é um subgrupo aberto de G (respectivamente fechado), então toda classe Hg ou gH de H em G é aberto (respectivamente fechado).
c) Todo subgrupo aberto de G é fechado e todo subgrupo fechado de índice finito é aberto. Se G é compacto, então todo subgrupo aberto de G tem índice finito.
d) Se H é um subgrupo contendo um subconjunto aberto não vazio U de G, então H é aberto em G.
e) Se H é um subgrupo de G e K é um subgrupo normal de G, então H é um grupo topológico com respeito a subgrupos topológicos, G/K *é um grupo topológico com respeito a quocientes topológicos e a função quociente q de G em* G/K *leva conjuntos abertos em conjuntos abertos.*
f) G é Hausdorff se, e somente se, $\{1\}$ *é um subconjunto fechado de G e se K é um subgrupo normal de G, então* G/K *é Hausdorff se, e somente se, K é fechado em G. Se G é totalmente desconexo, então G é Hausdorff.*
g) Se G é compacto e Hausdorff e se C, D são conjuntos fechados, então o conjunto CD é fechado.
h) Suponha que G é compacto e seja $(X_\lambda \mid \lambda \in \Lambda)$ *uma família de subconjuntos fechados com a propriedade que para todos* $\lambda_1, \lambda_2 \in \Lambda$ *existe um elemento* $\mu \in \Lambda$ *para o qual* $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$. *Se Y é um subconjunto fechado de G, então* $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y = \bigcap_{\lambda\in\Lambda} X_\lambda Y$.

Demonstração.
a) A aplicação do espaço X em $G \times G$ é contínua se, somente se o produto das aplicações projeções forem cada uma contínua. Assim se $\theta : G \to G$ e $\varphi : G \to G$ são contínuas, então a aplicação $x \mapsto (\theta(x), \varphi(x))$ de $G \to G \times G$ também será contínua. Primeiro tomemos θ constante, ou seja $x \mapsto 1$ e para φ a aplicação identidade id_G, agora compondo o resultado dessa aplicação com a aplicação contínua $c : (x,y) \mapsto xy^{-1}$ de $G \times G \to G$, concluímos que a aplicação $x \mapsto x^{-1}$ é contínua por ser igual ao seu inverso, então é um homeomorfismo. Assim a aplicação $(x,y) \mapsto (x,y^{-1})$ é contínua e o seu produto com c, $(x,y) \mapsto xy$ também é contínua. Agora tomemos θ como a aplicação id_G e φ a aplicação constante $x \mapsto g^{-1}$, fazendo o resultado do produto com a aplicação c, concluímos que a aplicação $x \mapsto xg$ é contínua e a inversa $x \mapsto xg^{-1}$ são contínuas. De modo análogo podemos tomar a aplicação $x \mapsto gx$.

b) Segue direto de a).

c) Temos $G\backslash H = \cup(H_g \mid g \notin H)$. Assim se H é aberto, então segue direto de b) que $G\backslash H$ também será, e por outro lado, o complementar de aberto é fechado, portanto H é fechado. Se H possui índice finito, então $G\backslash H$ é uma união de uma quantidade finita de classes, e assim se H é fechado, então segue direto de b) que $G\backslash H$ também é e H é aberto. Se H é aberto, então os conjuntos H_g são abertos e disjuntos e sua união é todo o grupo G. Segue da definição de compacidade que se G é compacto, então H tem índice finito em G.

d) Segue por a) que cada conjunto $U_h = \{uh \mid u \in U\}$ é aberto e, assim, $H = \cup(U_h \mid h \in H)$.

e) A afirmação sobre H é clara, pois se trata de um subgrupo de um grupo topológico. Seja V um aberto em G. Por a), kV é aberto para cada $k \in K$ e segue que $V_1 = KV$ é aberto. Assim já que $q(V) = q(V_1)$ e $q^{-1}q(V_1) = V_1$, segue que $q(V)$ é aberto em G/K. Relembremos que a aplicação $G/K \times G/K \to G/K$ definida por $(\xi, \varsigma) \mapsto \xi\varsigma^{-1}$ é contínua. Seja U aberto em G/K e seja $(Kw_1, Kw_2) \in m^{-1}(U)$. Assim, as aplicações q e $(x,y) \mapsto xy^{-1}$ são aplicações de $G \times G \to G$, então existem vizinhanças abertas W_1, W_2 de w_1, w_2, tal que $W_1W_2^{-1} \subseteq q^{-1}(U)$ e assim $q(W_1) \times q(W_2)$ é uma vizinhança aberta de (Kw_1, Kw_2) em $G/K \times G/K$ levando em $m^{-1}(U)$, como queríamos.

f) Vimos anteriormente que todo conjunto formado por um elemento no espaço de Hausdorff é fechado. Também mostramos que se o conjunto $\{1\}$ é fechado, então G é Hausdorff. Sejam a, b elementos distintos de G. Por a), o conjunto $\{ab^{-1}\}$ é fechado. Então existe um conjunto aberto U com $1 \in U$ e $ab^{-1} \notin U$. A aplicação $(x,y) \mapsto xy^{-1}$ é contínua e a imagem inversa de U é aberta. Segue que existe conjuntos abertos V, W contendo 1 tais que $VW^{-1} \subseteq U$. Com isso, $ab^{-1} \notin VW^{-1}$ e, assim, $aV \cap bW = \emptyset$. Como aV, bW são abertos, a primeira afirmação de f) segue. A segunda e a terceira afirmações são consequências imediatas da primeira, juntamente com a definição da topologia quociente e também do Lema 2.3.

g) Usaremos o Lema 2.2. Já que C, D são fechados e G é compacto, então ambos C e D são compactos, e assim é a imagem de $C \times D$ sobre a aplicação contínua $(x,y) \mapsto xy$. Esta imagem é CD e como G é Hausdorff, cada subconjunto compacto é fechado.

h) Claramente $(\cap X_\lambda)Y \subseteq \cap(X_\lambda Y)$. Se $g \notin (\cap X_\lambda)Y$, então $gY^{-1} \cap (\cap X_\lambda) = \emptyset$. Portanto, como G é compacto, gY^{-1} e o conjunto X_λ são fechados, temos $gY^{-1} \cap x_{\lambda_1} \cap \cdots \cap X_{\lambda_n} = \emptyset$, para um conjunto $\lambda_1, \ldots, \lambda_n$. Portanto $X_\mu \subseteq X_{\lambda_1} \cap \cdots \cap X_{\lambda_n}$,

para algum $\mu \in \Lambda$ e assim, temos $gY^{-1} \cap X_\mu = \emptyset$ e $g \notin X_\mu Y$.

□

Lema 2.6 *Seja G um grupo topológico compacto. Se C é um subconjunto que é fechado e aberto e que contém* 1*, então C contém um subgrupo normal aberto.*

Demonstração. Para cada $x \in C$, o conjunto $W_x = Cx^{-1}$ é uma vizinhança aberta de 1 tal que $W_x x \subseteq C$. Desde que a multiplicação seja uma aplicação contínua de $G \times G \to G$, existem conjuntos abertos L_x, R_x contendo 1, tais que a imagem de $L_x \times R_x$ está contida em W_x, isto é, tais que $L_x R_x$ esteja contido em W_x. Denotemos $S_x = L_x \cap R_x$. Assim, temos $S_x S_x \subseteq W_x$ e S_x é aberto. Como C é compacto e a união destes conjuntos abertos $C \cap S_x x$, e assim a união de uma quantidade finita destes conjuntos, digamos $C \subseteq \bigcup_{i=1}^{n} S_{x_i} x_i$. O conjunto $S = \bigcap_{i=1}^{n} S_{x_i}$ é aberto e contém 1. Temos

$$SC \subseteq \bigcup_{i=1}^{n} S S_{x_i} x_i \subseteq \bigcup_{i=1}^{n} W_{x_i} x_i \subseteq C, \tag{2-1}$$

e, assim, $S \subseteq C$.

Seja $T = S \cap S^{-1}$. Logo T é aberto, $T = T^{-1}$ e $1 \in T$. Escrevemos $T^1 = T$, para $n > 1$ e temos $T^n = TT^{n-1}$ seja $H = \bigcup_{n>0} T^n$. Segue que H é um grupo gerado por T e a união dos conjuntos da forma T_y são abertos. Por indução, usando 2-1, temos $T^n \subseteq C$, para todo $n > 0$. Segue que $H \subseteq C$. Pelo Lema 2.5 c), H tem índice finito em G e, assim, tem somente uma quantidade finita de conjugados em G. A interseção destes conjugados é portanto um subgrupo aberto normal contido em C.

□

Proposição 2.7 *Seja G um grupo topológico compacto, totalmente desconexo.*
a) Todo conjunto aberto em G é uma união de classes de subgrupos normais abertos.
b) Um subconjunto de G é fechado e aberto se, e somente se, é uma união de uma quantidade finita de classes de subgrupos normais abertos.
c) Se X é um subconjunto de G, então seu fecho $\overline{X}$ *satisfaz:*

$$\overline{X} = \bigcap \big(NX \mid N \text{ um subgrupo normal aberto de } G\big).$$

Em particular,

$$C = \bigcap \big(NC \mid N \text{ um subgrupo normal aberto de } G\big).$$

Para cada subconjunto fechado C, e a interseção dos subgrupos normais de G é um subgrupo trivial.

Demonstração.
$a)$ Note que G é um espaço de Hausdorff, pelo Lema $2.5f)$. Seja U um conjunto aberto não vazio em G. Se $x \in U$, então Ux^{-1} é um conjunto aberto contendo 1 e assim pelo Lema $2.1c)$ e o Lema 2.6, Ux^{-1} contém um subgrupo normal aberto K_x. Portanto, $U = \bigcup_{x \in U} K_x x$.
$b)$ Se P é um conjunto que é fechado e aberto, então por $a)$ P é uma união de uma família de subgrupos normais abertos e desde que P seja compacto, P é também a união de uma subfamília finita dessas classes. Consequentemente, é claro que a união de uma quantidade finita de subgrupos normais abertos são ambos abertos e fechados.
$c)$ Segue de $a)$ tomando complementares. Se $y \notin \overline{X}$, então y tem uma vizinhança aberta disjunta de X e assim há um subgrupo normal aberto N satisfazendo $Ny \cap X = \emptyset$. Portanto, $y \notin NX$.

□

Observação: Note que a definição de isomorfismo é equivalente à existência de um homomorfismo inverso (contínuo), mas não é equivalente à existência de um homomorfismo bijetor (contínuo).

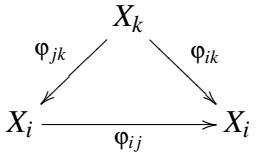
2.2 Grupos Profinitos e Completamento

Nesta seção fazemos uma discussão geral sobre limites inversos e apresentamos algumas definições e propriedades de grupos profinitos.

2.2.1 Limites Inversos

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

Definição 2.8 *Um* sistema inverso (X_i, φ_{ij}) *de espaços topológicos indexado por um conjunto dirigido, consiste de uma família* $(X_i \mid i \in I)$ *de espaços topológicos e uma família* $(\varphi_{ij} : X_j \to X_i \mid i, j \in I,\ i \leq j)$ *de funções contínuas, tal que* φ_{ii} *é a função identidade* id_{x_i} *para cada* i *e* $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$*, sempre que* $i \leq j \leq k$.

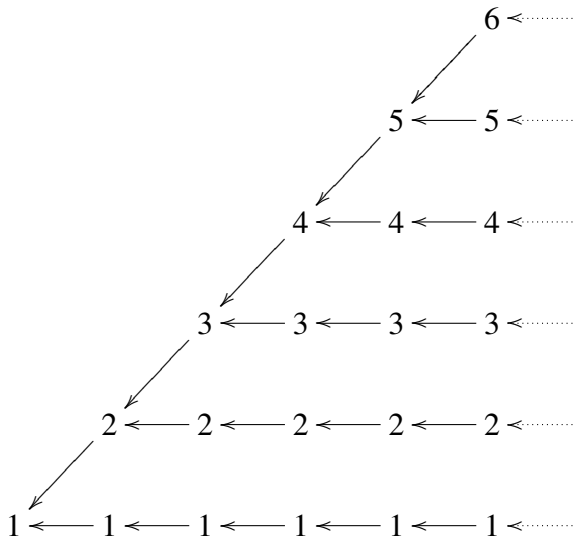


Conjuntos para os quais não seja especificado a topologia adotada serão considerados espaços topológicos com a topologia discreta.

Se cada X_i é um grupo topológico e cada φ_{ij} é uma homomorfismo contínuo, então (X_i, φ_{ij}) é chamado de ***sistema inverso de grupos topológicos***.

Exemplo.

O seguinte diagrama mostra um exemplo muito simples de um Sistema Inverso.



Neste exemplo, $I = \mathbb{N}$ e $\leq$ segue a ordem habitual. Para cada $i \in \mathbb{N}$, temos que $X_i := \{1, 2, \ldots, i\}$ e as flechas indicam as aplicações $\varphi_{i+1}i$. Por exemplo $\varphi_{43}(4) = 3$, $\varphi_{43}(i) = 3$, para $i \geq 3$ e $\varphi_{43}(i) = i$, para $i < 4$.

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

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

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

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

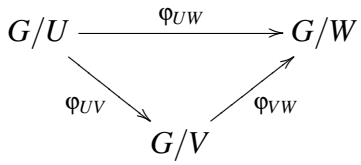
$$\begin{aligned}\varphi_{ij}:\mathbb{Z}/i\mathbb{Z} &\to \mathbb{Z}/j\mathbb{Z}\\ n+i\mathbb{Z} &\mapsto n+j\mathbb{Z}.\end{aligned}$$

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

Exemplo. Seja G um grupo e I uma família de subgrupos normais de índice finito (ou índice potência de p) ordenado pela inclusão inversa (seja $U_i\geq U_j$ 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 $U\leq V$, defina

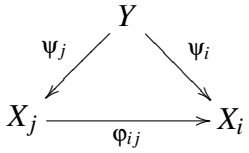
$$\begin{aligned}\varphi_{VU}:G/V &\to G/U\\ gV &\mapsto gU\end{aligned}$$

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



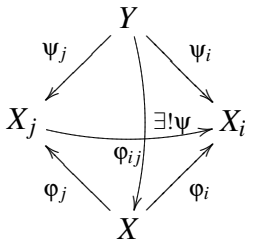
comuta, para todo $U\geq V\geq W$. Logo $(G/U,\varphi_{VU})$ é um sistema inverso.

Sejam (X_i,φ_{ij}) um sistema inverso de espaços topológicos e Y um espaço topológico. Chamamos uma família $\{\psi_i:Y\to X_i \mid i\in I\}$ de funções contínuas compatíveis se $\varphi_{ij}\psi_j=\psi_i$, sempre que $i\leq j$. Esta condição pode ser expressa esquematicamente com a exigência que o diagrama abaixo comute:



Definição 2.9 *O* limite inverso (X,φ_i) *de um sistema inverso* (X_i,φ_{ij}) *de espaços topológicos é um espaço topológico X juntamente com uma família compatível* $(\varphi_i:X\to X_i)$ *de funções contínuas com a seguinte propriedade universal: sempre que* $(\psi_i:Y\to X_i)$ *é uma família compatível de funções contínuas de um espaço Y, existe uma única função contínua* $\psi:Y\to X$*, tal que* $\varphi_i\psi=\psi_i$*, para cada i.*

Temos que existe uma única ψ, tal que o diagrama abaixo seja comutativo.



No próximo resultado, mostramos que o limite inverso existe e é único.

Proposição 2.10 *Seja (X_i, φ_{ij}) o sistema inverso, indexado por I.*
a) Se $(X^{(1)}, \varphi_i^{(1)})$ e $(X^{(2)}, \varphi_i^{(2)})$ são limites inversos do sistema inverso, então existe um isomorfismo $\overline{\varphi} : X^{(1)} \to X^{(2)}$, tal que $\varphi_i^{(2)}\overline{\varphi} = \varphi_i^{(1)}$, para cada i.
b) Escrevemos $C = \prod_{i\in I} X_i$ e para cada i escrevemos π_i para a função projeção de C para X_i e definimos:

$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c),\ para\ \ todos\ \ i, j\ \ com\ \ j \geq i\}$$

e $\varphi_i = \pi_i \mid_X$, para cada i. Então (X, φ_i) é um limite inverso de (X_i, φ_{ij}).
c) Se (X_i, φ_{ij}) é um sistema inverso de grupos topológicos X_i e homomorfismos contínuos φ_{ij}, então X é grupo topológico e as funções φ_i são homomorfismo contínuos.

Demonstração.

a) A prova da unicidade segue os argumentos de rotina. Conforme citado no capítulo anterior, a definição de isomorfismo é equivalente à existência de um homomorfismo inverso. Para mostrar que existe esse isomorfismo, faremos uso da propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$ aplicada pela família $(\varphi_i^{(2)})$ de funções compatíveis produzindo assim, uma função $\varphi^{(1)} : X^{(2)} \to X^{(1)}$, tal que $\varphi_i^{(1)}\varphi^{(1)} = \varphi_i^{(2)}$ para cada *i*. De modo similar, obtemos uma função $\varphi^{(2)} : X^{(1)} \to X^{(2)}$ tal que $\varphi_i^{(2)}\varphi^{(2)} = \varphi_i^{(1)}$ para cada *i*. Mas pela propriedade universal de $(X^{(1)}, \varphi_i^{(1)})$, existe somente uma função $\psi : X^{(1)} \to X^{(1)}$ com a propriedade que $\varphi_i^{(1)}\psi = \varphi_i^{(1)}$, para cada *i*.

No entanto, $\varphi^{(1)}\varphi^{(2)}$ e $id_{X^{(1)}}$ tem essa propriedade. Observe pelos diagramas

$$X^{(1)} \xrightarrow{\psi} X^{(1)} \xrightarrow{\varphi_i^{(1)}} X_i^{(1)}$$
$$\varphi_i^{(1)}$$

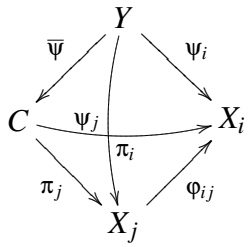
$$X^{(1)} \xrightarrow{\varphi^{(2)}} X^{(2)} \xrightarrow{\varphi^{(1)}} X^{(1)}$$
$$id_{X^{(1)}}$$

Concluímos então que $\varphi^{(1)}\varphi^{(2)} = id_{X^{(1)}}$. De modo análogo, temos $\varphi^{(2)}\varphi^{(1)} = id_{X^{(2)}}$. Segue que $\varphi^{(2)}$ é um isomorfismo.

b) Agora, suponha que $(\psi_i : Y \to X_i)$ é uma família de funções compatíveis. Mostramos que existe uma única função (contínua) $\psi : Y \to X$ tal que $\varphi_i\psi = \psi_i$, para cada i.

Seja $\overline{\psi} : Y \to C$ definida por $\overline{\psi}(y) = \psi_i(y)$. Deste modo, $\pi_i\overline{\psi} = \psi_i$ para cada i e $\overline{\psi}$ é contínua por ser composição de funções contínuas.

Se $j \geq i$, observamos pelo diagrama abaixo



que

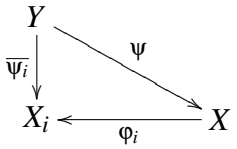
$$\pi_i\overline{\psi} = \psi_i = \varphi_{ij}\psi_j = \varphi_{ij}\pi_j\overline{\psi} = \psi_i$$

Com isso,

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

e segue que $\overline{\psi} : Y \to X \subseteq C$.

c) Definimos $\psi : Y \to X$ por $\psi(y) = \overline{\psi}(y)$, para cada $y \in Y$. Assim, ψ é contínua e $\varphi_i\psi = \psi_i$, pois $\varphi_i = \pi_i\,|_X$ e $\pi_i\overline{\psi} = \psi_i$ para cada i. Se $\psi' : Y \to X$ é uma função satisfazendo $\varphi_i\psi' = \psi_i$ para cada i e $y \in Y$, então para cada entrada em X_i de $\psi'(y)$ teremos $\psi_i(y)$ para cada i, o mesmo ocorrendo para cada entrada de $\psi(y)$ em X_i. Assim temos que $\psi'(y) = \psi(y)$. Donde existe uma única aplicação contínua tal que o diagrama abaixo comuta.



□

O resultado acima mostra que o limite inverso de um sistema inverso (X_i, φ_{ij}) existe e é único a menos de isomorfismos. Em relação ao limite inverso, denotamos por $\varprojlim(X_i, \varphi_{ij})$, ou simplesmente por $\varprojlim X_i$, suprimindo a função φ_{ij}.

Proposição 2.11 *Seja (X_i, φ_{ij}) um sistema inverso indexado por I e escrevemos $X = \varprojlim X_i$.*
a) Se cada X_i é Hausdorff, então X também o é.
b) Se cada X_i é totalmente desconexo, então X também o é.
c) Se cada X_i é Hausdorff, então $\varprojlim X_i$ é fechado no produto cartesiano $C = \prod_{i\in I} X_i$.
d) Se cada X_i é compacto e Hausdorff, então X também o é.
e) Se cada X_i é um espaço compacto de Hausdorff não vazio, então X é não vazio.

Demonstração.
$a)$ Por hipótese, X_i é Hausdorff. Tome a e b pontos distintos em $X = \prod X_i$, com coordenadas $\{a_i\}$ e $\{b_i\}$, respectivamente. Como $a \neq b$, existe i tal que $a_i \neq b_i$. Assim existem vizinhanças disjuntas A e B de a_i e b_i, respectivamente em X_i. Desta forma, existirão vizinhanças abertas disjuntas de a e b em X. Portanto X é Hausdorff.

$b)$ Segue do Teorema 2.4 pelo fato de subespaços e produtos de espaços com as propriedades citadas acima serem preservados também.

$c)$ Se $f, g : X \to Y$ são funções contínuas e Y é um espaço de Hausdorff, então pelo Lema 2.2 o conjunto $\{x \mid f(x) = g(x)\}$ é fechado em X. Segue que

$$\varprojlim X_i = \bigcap_{j>i} \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\},$$

onde π_i é a função projeção e segue que se cada X_i é Hausdorff, então $\varprojlim X_i$ é uma interseção de conjuntos fechados e, portanto, é fechado no produto cartesiano.

$d)$ Segue imediato de $c)$, $a)$ e também do teorema 2.4 $c)$ e do Lema 2.2$a)$.

$e)$ Para $j > i$, definimos o conjunto $D_{ij} = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\}$. Cada conjunto D_{ij} é fechado e C é compacto e, assim, se $\varprojlim X_i = \emptyset$, então $\bigcap_{r=1}^{n} D_{i_r j_r} = \emptyset$, para algum natural n e elementos i_r, j_r de I. Desde que I seja dirigido, podemos encontrar $k \in I$ tal que $k \geq j_r$, para cada r. Escolha $x_k \in X_k$ e defina $x_l = \varphi_{lk}(x_k)$ para $l \leq k$, defina também x_l arbitrariamente para os elementos de I. Claramente o elemento (x_i) do produto cartesiano está $\bigcap_{r=1}^{n} D_{i_r j_r}$, o que é uma contradição. □

Proposição 2.12 *Seja (X, φ_i) o limite inverso de um sistema inverso (X_i, φ_{ij}) de um espaço compacto de Hausdorff não vazio indexado por I. As seguintes afirmações valem:*
a) $\varphi_i(X) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$, para cada $i \in I$.
b) Os conjuntos $\varphi_i^{-1}(U)$ com $i \in I$ e U um aberto em X_i, formam uma base para a topologia sobre X.
c) Se Y é um subconjunto de X satisfazendo $\varphi_i(Y) = X_i$ para cada i, então Y é denso em

X.

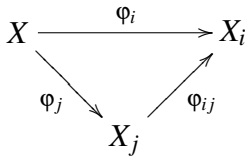
d) *Se* θ *é uma função de um espaço* Y *em* X*, então* θ *é contínua se, e somente se, cada função* $\varphi_i\theta$ *é contínua.*

e) *Se* $f : X \to A$ *é uma função contínua para um espaço discreto, então* f *fatora* X_i *para algum* i*, em outras palavras, para algum* i*, existe uma função contínua* $g : X_i \to A$ *satisfazendo* $f = g\varphi_i$.

Demonstração.

a) A primeira inclusão é direta. Observe pelo diagrama abaixo

$$\varphi_i(X) = \varphi_{ij}\varphi_j(X) \subset \varphi_{ij}(X_j), \text{ para todo } j \geq i.$$

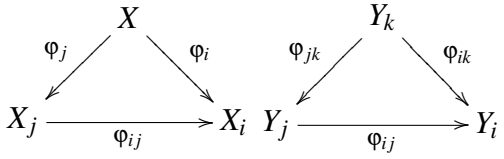


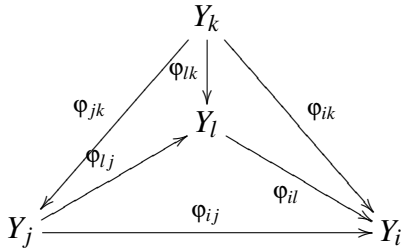
Assim, $\varphi_i(X) \subseteq \bigcap_{j\geq i} \varphi_{ij}(X_j)$. Agora, fixando i e fixando $a \in \bigcap_{j\geq i} \varphi_{ij}(X_j)$, para $j \geq i$, temos o conjunto

$$Y_j = \{y \in X_j \mid \varphi_{ij}(y) = a\}.$$

Segue que Y_j é a imagem inversa de um conjunto fechado, que é fechado em X_j e portanto é compacto. Se $i \leq j \leq k$ e $y_k \in Y_k$ são tais que $\varphi_{ij}(\varphi_{jk}(y_k)) = \varphi_{ik}(y_k) = a$ e assim $\varphi_{jk}(y_k) \in Y_j$. Portanto, $\{Y_j \mid j \geq i\}$ é um sistema inverso não vazio de um espaço de Hausdorff compacto e assim há um elemento $(b_j) \in \varprojlim_{j\geq i} Y_j$. Contudo, $\varphi_{jk}(b_k) = b_j$ se $i \leq j \leq k$ e $b_i = a$. Agora se existir um $l \in I$ e $i \not\leq l$, tome um j tal que $j \geq i, l$ e defina $b_l = \varphi_{lj}(bj)$. Isto independe de j, pois se tivermos $j' \geq i, l$ podemos tomar $k \geq j, j'$ e teremos:

$$\varphi_{lj}(b_j) = \varphi_{lj}\varphi_{jk}(b_k) = \varphi_{lj'}\varphi_{j'k}(b_k) = \varphi_{lj'}(b_{j'}).$$





Pelo diagrama acima, podemos notar que $\varphi_{jk}(b_k) = b_j$ para todo par $j,\ k$ de índices com $j \leq k$, então temos $b = (b_j)_{j\in I} \in \varprojlim_{j\geq i} Y_j \subseteq X$. Portanto $\varphi_i(b) = \pi_i(b) = a$, com isso $\bigcap_{j\geq i} \varphi_{ij}(X_j) \subseteq \varphi_i(X)$ e assim segue o resultado.

b) A união de abertos de um espaço topológico é uma base, ou equivalentemente se $a \in P$ onde P é um conjunto aberto de X, então existe um aberto Q tal que $a \in Q \subset P$. Todo conjunto aberto em X é uma união de conjuntos da forma

$$P = X \cap \pi_{i_1}^{-1}(U_1) \cap \pi_{i_2}^{-1}(U_2) \cap \cdots \cap \pi_{i_n}^{-1}(U_n),$$

onde $n \in \mathbb{N}$ e $i_1, i_2, \ldots, i_n \in I$ e U_r é aberto em X_{i_r} para cada r. O item fica provado se mostrarmos que para todo $a \in P$ existe um conjunto $\varphi_k^{-1}(U)$ com U aberto em X_k e $a \in \varphi_k^{-1}(U) \subseteq P$. Seja $a = (a_i)$, escolhendo $k \in I$ tal que $k \geq i_1, \ldots, i_n$. O conjunto $\varphi_{i_r k}^{-1}(U_r)$ é um aberto em X_k, desde que $\varphi_{i_r k}$ seja contínua e que contenha a_k tal que $\varphi_{ik}(a_k) = a_i$ para $i \leq k$. Escrevemos $U = \bigcap_{r=1}^{n} \varphi_{i_r k}^{-1}(U_r)$. Isto é uma vizinhança aberta de a_k em X_k e assim $\varphi_k^{-1}(U)$ é uma vizinhança aberta de a em X. Contudo, se $b = (b_i) \in \varphi_k^{-1}(U)$, então $b_k \in U$ e assim $b_{i_r} = \varphi_{i_r k}(b_k) \in U_k$ para $r = 1, \ldots, n$. Portanto $\varphi_k^{-1}(U) \subseteq P$, como queríamos.

c) Para cada $i \in I$ e cada subconjunto aberto não vazio U em X_i, temos que $\varphi_i(Y) \cap U \neq \emptyset$ e, assim, $Y \cap \varphi_i^{-1}(U) \neq \emptyset$. Segue de *b*) que Y é denso em X.

d) A prova é imediata pois se θ é contínua, então a composição $\varphi_i\theta$ também é contínua. Agora se a composição $\varphi_i\theta$ é contínua, então para cada i e cada conjunto aberto U em X_i, o conjunto $\theta^{-1}(\varphi_i^{-1}(U)) = (\varphi_i\theta)^{-1}(U)$ é aberto e segue de *b*) que θ é contínua.

$$Y \xrightarrow{\theta} X \underset{\varphi_i\theta}{\xrightarrow{\varphi_i}} X_i$$

e) A imagem A_0 de f é compacta e discreta, portanto é finita. Para cada $a \in A_0$, o conjunto $Y_a = f^{-1}(a)$ é compacto e aberto e assim é uma união finita de conjuntos abertos $\varphi_j^{-1}(U)$ com $j \in I$ e U aberto em X_j. Desta forma existe uma quantidade finita de conjuntos $\varphi_{j_1}^{-1}(U_1), \cdots, \varphi_{j_n}^{-1}(U_n)$ tais que cada conjunto Y_a é uma união de alguns destes conjuntos. Escolha um índice k tal que $j_r \leq k$, para $r = 1, \ldots, n$. Temos $\varphi_{j_r}^{-1}(U_r) = \varphi_k^{-1}(\varphi_{j_r k}^{-1}(U_r))$ para cada r e, assim, para cada $a \in A_0$, podemos escrever

$Y_a = \varphi_k^{-1}(V_a)$, onde V_a é um subconjunto aberto de X_k. Seja $D = X_k \setminus \bigcup_{a \in A_a} V_a$. Claramente $D \cap \varphi_k(X) = \emptyset$ e por $a)$ temos $D \cap \big(\bigcap_{l \geq k} \varphi_{kl}(X_l)\big) = \emptyset$. Portanto existe uma quantidade finita de índices $l_1, \ldots, l_s$ tais que $D \cap \varphi_{kl_1}(X_{l_1}) \cap \ldots \cap \varphi_{kl_s}(X_{l_s}) = \emptyset$. Assim, D e cada conjunto $\varphi_{kl}(X_l)$ é fechado e X_k é compacto. Escolha $i \geq l_1, \ldots, l_s$ para $k \leq l \leq i$. Temos $\varphi_{ki}(X_i) = \varphi_{kl}(\varphi_{li}(X_i)) \subseteq \varphi_{kl}(X_k)$ e concluímos que

$$D \cap \varphi_{ki}(X_i) = \emptyset \text{ e } \varphi_{ki}(X_i) \subseteq \bigcup_{a \in A_0} V_a.$$

Escreva $W_a = \varphi_{kl}^{-1}(V_a)$ para cada a, assim cada W_a é aberto em X_i, claramente $W_{a_1} \cap W_{a_2} = \emptyset$, para $a_1 \neq a_2$. Seja $x \in X_i$, então $\varphi_{ki}(x) \in U_a$ para algum a e $x \in \varphi_{ki}^{-1}(V_a) = W_a$. Portanto, $X_i = \bigcap_{a \in A_0} W_a$, onde cada conjunto W_a é também fechado. Segue que a aplicação $g : X_i \to A$ que toma W_a para a, onde $a \in A_0$ é contínua e satisfaz $f = g\varphi_i$, como queríamos. □

Proposição 2.13 *Seja X um espaço de Hausdorff, compacto e totalmente desconexo. Então X é o limite inverso do seu espaço quociente discreto.*

Demonstração. Seja I o conjunto das partições de X em uma quantidade finita de subconjuntos fechado e abertos. Para cada $i \in I$, seja X_i o espaço quociente correspondente (onde os elementos são fechados e abertos da partição i) e seja q_i a função quociente de X em X_i. Assim, o conjunto X_i é precisamente o espaço quociente de X, que é discreto na topologia quociente. Escrevemos $i \leq j$ se, e somente se, existe uma função $q_{ij} : X_j \to X_i$ satisfazendo $q_{ij}q_j = q_i$. A aplicação q_{ij} é unicamente determinada porque q_j é sobrejetivo. Temos então que I é um conjunto parcialmente ordenado. Agora se

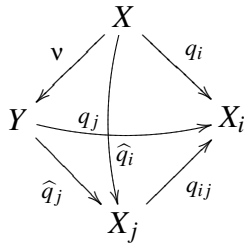
$$i = \{U_r \mid 1 \leq r \leq m\} \text{ e } j = \{V_s \mid 1 \leq s \leq n\},$$

são elementos de I, então

$$\{U_r \cap V_s \mid 1 \leq r \leq m,\ 1 \leq s \leq n\}$$

é um elemento k de I tal que $i, j \leq k$ e, assim, I é um conjunto dirigido. Como cada função q_{ij} é unicamente determinada, segue imediatamente que (X_i, q_{ij}) é um sistema inverso e que (X, q_i) é uma família de aplicações compatíveis.

Seja $Y = \varprojlim X_i$ e $\widehat{q} : Y \to X_i$ a aplicação canônica para cada i. A propriedade universal de limite inverso garante a existência de uma aplicação contínua $\nu : X \to Y$ tal que $\widehat{q}_i\nu = q_i$, para cada i.



Se x_1 e x_2 são elementos de X tais que $\nu(x_1) = \nu(x_2)$, então $q_i(x_1) = q_i(x_2)$ para cada i, de modo que nenhum conjunto aberto e fechado contenha justamente um dos x_1, x_2, então $x_1 = x_2$, logo segue que X é totalmente desconexo. Além disso, ν é injetiva, visto que $\widehat{q}_i(\nu(X)) = q_i(X) = X_i$, para cada i e segue da Proposição 2.12 $c)$ que $\nu(X)$ é denso em Y. Como ν é contínua, X é compacto e Y um espaço de Hausdorff, assim $\nu(X)$ é fechado e, portanto ν é sobrejetiva. Pelo Lema 2.2 $d)$, temos que ν é um homeomorfismo e assim segue o resultado. □

2.2.2 Caracterização dos Grupos Profinitos

Seja G um grupo topológico. Escrevemos $H \leq G$ para dizer que H é um subgrupo fechado de G e $N \lhd_\circ G$ que significa dizer que N é um subgrupo normal aberto de G. Chamamos uma família I de subgrupos normais de um grupo arbitrário G uma ***base filtrada*** se, para todos K_1, $K_2 \in I$, existir um subgrupo $K_3 \in I$ que está contido em $K_1 \cap K_2$. Começamos com dois resultados técnicos.

Proposição 2.14 *Seja (G, φ_i) o limite inverso de um sistema inverso (G_i, φ_{ij}) de grupos topológicos de um espaço de Hausdorff compacto e seja $L \lhd_\circ G$. Então ker $\varphi_i \leq L$ para algum i. Consequentemente, G/L é isomorfo (como um grupo topológico) a algum grupo quociente de um subgrupo de algum G_i, e se na adição cada função φ_i é sobrejetiva, então G/L é isomorfo ao grupo quociente de algum grupo G_i.*

Demonstração. Se L é subgrupo aberto contendo 1, temos $\varphi_i^{-1}(U) \subseteq L$ para algum i e algum conjunto aberto U de G_i contendo 1, pela Proposição 2.12. Temos por consequência que $ker\ \varphi_i \leq L$ para algum i. Assim $G/L \cong (G/ker\ \varphi_i)(L/ker\ \varphi_i)$, logo $G/ker\ \varphi_i \cong Im\ \varphi_i$, então segue que G/L é isomorfo ao quociente da $Im\ \varphi_i$. Então segue o resultado.

□

Proposição 2.15 *Sejam G um grupo topológico e I uma base filtrada de subgrupos normais fechados de G. Para K, $L \in I$, definimos $K \leq' L$ se, e somente se, $L \leq K$. Assim, I é dirigido com respeito à ordem $\leq'$ e o homomorfismo*

sobrejetor $q_{KL} : G/L \to G/K$, *definido por* $K \leq' L$, *torna o grupo* G/K *um sistema inverso. Escrevemos* $(\widehat{G}, \varphi_K) = \varprojlim G/K$. *Existe um homomorfismo contínuo* $\theta : G \to \widehat{G}$ *com kernel* $\bigcap_{K \in I} K$ *e com imagem um subgrupo denso de* $\widehat{G}$ *tal que* $\varphi_k\theta$ *é a aplicação quociente de* G *em* G/K, *para cada* $K \in I$. *Se* G *é compacto, então* θ *é sobrejetivo; se* G *é compacto e* $\bigcap_{K \in I} K = 1$, *então* θ *é um isomorfismo de grupos topológicos (isto é, um isomorfismo de grupos e um homeomorfismo).*

Demonstração. A demonstração será omitida, mas pode ser encontrada em ([35], p. 17) □

Corolário 2.16 *Seja* G *um grupo topológico, então as afirmações que seguem são equivalentes:*
a) G *é profinito.*
b) G *é isomorfo (como um grupo topológico) a um subgrupo fechado do produto cartesiano de grupos finitos.*
c) G *é compacto e* $\bigcap(N \mid N \lhd_\circ G) = 1$.
d) G *é compacto e totalmente desconexo.*

Demonstração. *a*) $\Rightarrow$ *b*) É uma aplicação imediata da Proposição 2.11 *c*).
b) $\Rightarrow$ *c*) Seja G isomorfo ao subgrupo fechado $\widehat{G}$ de $C = \prod(G_i)$, onde cada G_i é um grupo finito, e para cada i, escrevemos K_i para o *kernel* da aplicação projeção de C para G_i. Pelo Teorema 2.4, C é compacto e, assim o mesmo vale para $\widehat{G}$, Lema 2.2*c*). Para cada i, escrevemos $N_i = K_i \cap \widehat{G}$. Como $K_i \lhd_o C$, temos $N_i \lhd_o \widehat{G}$ e, assim, $\cap K_i = 1$ segue que $\cap N_i = 1$.
c) $\Rightarrow$ *a*) Sejam $N_1, N_2 \lhd_\circ G$ e considere a aplicação de G em um grupo finito $G/N_1 \times G/N_2$ definido por $g \mapsto (N_1 g, N_2 g)$. Essa aplicação é um homomorfismo contínuo, cujo *kernel* é $N_1 \cap N_2$. Portanto, pela Proposição 2.15, temos que $G \cong \varprojlim_{N \in I} G/N$.
a) $\Rightarrow$ *d*) Pela Proposição 2.11, o grupo G é compacto e totalmente desconexo. Agora, para concluirmos, basta aplicar a Proposição 2.14.
d) $\Rightarrow$ *c*) É uma aplicação imediata da Proposição 2.7. □

Seja $\mathcal{C}$ uma classe de grupos finitos. Chamamos um grupo F de um ***$\mathcal{C}$-grupo*** se $F \in \mathcal{C}$ e chamamos G de um ***grupo pro-$\mathcal{C}$*** se este é um limite inverso de $\mathcal{C}$-grupos. Note que $\mathcal{C}$-grupos são pro-$\mathcal{C}$ grupos. Dizemos que $\mathcal{C}$ é fechado para subgrupos (respectivamente para quocientes) se todo subgrupo (respectivamente grupo quociente) de um $\mathcal{C}$-grupo é um $\mathcal{C}$-grupo e dizemos que $\mathcal{C}$ é fechado para produto direto se $F_1 \times F_2 \in C$, sempre que $F_1 \in \mathcal{C}$ e $F_2 \in \mathcal{C}$.

Algumas classes importantes de grupos são: grupos finitos, p-grupos finitos onde p é um primo fixado, grupos cíclicos finitos e grupos nilpotentes finitos. Um limite inverso

de p-grupos finitos é chamado ***grupo pro-p***, um limite inverso de grupos cíclicos finitos é chamado ***grupo procíclico*** e assim por diante.

Teorema 2.17 *Seja G um grupo profinito. Se I é uma base filtrada de subgrupos normais fechados de G tal que $\bigcap(N \mid N \in I) = 1$, então:*

$$G \cong \lim_{\leftarrow N \in I} G/N.$$

Além disso,

$$H \cong \lim_{\leftarrow N \in I} H/(H \cap N),$$

para cada subgrupo fechado H de G e

$$G/K \cong \lim_{\leftarrow N \in I} G/KN,$$

para cada subgrupo normal fechado K de G.

Demonstração. As duas primeiras afirmações seguem da Proposição 2.15. Agora a família $J = (KN \mid N \in I)$ é uma base filtrada de subgrupos normais abertos de G contendo K e pelo Lema 2.5 h), temos

$$\cap(M \mid M \in J) = K \cap (N \mid N \in I) = K.$$

Portanto, a terceira afirmação decorre da Proposição 2.15. □

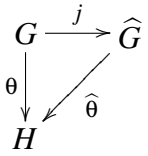
Lema 2.18 *Seja $f : G \to A$ uma função de um grupo profinito em um espaço discreto. Então f é contínua se, e somente se, existe um subgrupo normal aberto N tal que f fatora inteiramente G/N.*

Demonstração. Será omitida, mas pode ser encontrada em ([35], p. 20). □

2.2.3 Completamento

Sejam G um grupo abstrato e I uma base filtrada não vazia de subgrupos normais de índice finito. Chamamos um subconjunto de G ***aberto*** se, e somente se, G é uma união de classes Kg de subgrupos $K \in I$. Então G torna-se um grupo topológico (observe que uma interseção $K_1g_1 \cap K_2g_2$ de classes de dois subgrupos K_1, K_2 ou é vazia ou uma classe de $K_1 \cap K_2$). O completamento de G com respeito a I consiste de um grupo profinito $\widehat{G}$ e um homomorfismo contínuo $j : G \to \widehat{G}$ com a seguinte propriedade: sempre que $\theta : G \to H$

é um homomorfismo contínuo em um grupo finito H, existe um único homomorfismo contínuo $\widehat{\theta} : \widehat{G} \mapsto H$ tal que $\theta = \widehat{\theta} j$. Observe o diagrama abaixo:

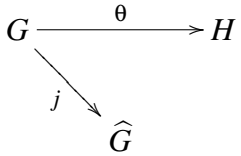


Proposição 2.19 *Seja* $\widehat{G} = \lim_{\leftarrow k \in I} G/K$ *e seja* j *uma aplicação* $g \mapsto (Kg)$ *de* G *para* $\widehat{G}$. *O par* $(\widehat{G}, j)$ *tem a propriedade da completamento de* G *com respeito a* I.

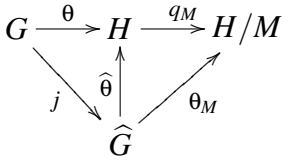
Demonstração. Primeiro note que j é contínua, pela Proposição 2.15. Seja $\theta : G \to H$ dado. Como θ é contínua, *ker* θ é aberto, assim *ker* θ contém algum $L \in I$. Defina $\widehat{\theta} : \widehat{G} \to H$ sendo o produto da aplicação de $\widehat{G}$ em G/L tomando cada elemento de sua coordenada em G/L e o homomorfismo induzido $Lg \mapsto \theta(g)$ de G/L para H. Assim, $\widehat{\theta}$ é contínua e é claro que $\theta = \widehat{\theta} j$. Se $\varphi : \widehat{G} \to H$ é um homomorfismo contínuo satisfazendo $\theta = \varphi j$, então $\widehat{\theta}$ e φ agem sobre $j(G)$, que é denso em $\widehat{G}$ pela Proposição 2.15 e, assim, $\varphi = \widehat{\theta}$, pelo Lema 2.2 e). □

Podemos mostrar que o completamento de G com respeito a I é unicamente determinado. Reformularemos a definição de completamento em termos da propriedade universal, como segue.

Proposição 2.20 *Sejam* G *e* I *como acima e suponha que* $\widehat{G}$ *é um grupo profinito e* $j : G \to \widehat{G}$ *um homomorfismo contínuo. Os ítens que seguem são equivalentes:*
a) $(\widehat{G}, j)$ *satisfaz a propriedade do completamento de* G *com respeito a* I.
b) *Para todo grupo profinito* H *e um homomorfismo contínuo* $\theta\, \theta : G \to H$, *então existe um único homomorfismo contínuo* $\widehat{\theta} : \widehat{G} \to H$ *que completa a comutatividade do triângulo:*



Demonstração. Para essa equivalência, precisamos mostrar apenas $a) \Rightarrow b)$. Sejam θ um homomorfismo contínuo e q_M a aplicação quociente de $H \to H/M$ para cada $M \lhd_o H$. Considere o diagrama abaixo para cada M:



Aplicando a definição de completamento para o grupo H/M, juntamente com a aplicação $q_M\theta$, produzem uma única função θ_M tal que o outro triângulo comuta. Se $M_1 \leqslant M_2$ e $q_{M_1M_2}$ é um homomorfismo $M_1h \mapsto M_2h$ de $H/M_1 \to H/M_2$, então temos $q_{M_2} = q_{M_2M_1}q_{M_1}$ e assim

$$q_{M_2M_1}\theta_{M_1}j = q_{M_2M_1}q_{M_1}\theta = q_{M_2}\theta = \theta_{M_2}j.$$

Assim, pela unicidade de θ_{M_2}, temos $q_{M_2M_1}\theta_{M_1} = \theta_{M_2}$. Como $H \cong \varprojlim H/M$, segue da definição de limite inverso que existe uma aplicação $\widehat{\theta}$ fazendo com que o lado direito do triângulo comute para cada M. Contudo, o produto de $\widehat{\theta}j$ e θ com cada q_M são iguais. Para $g \in G$, temos $q_M(\widehat{\theta}j)(g) = q_M\theta(g)$. Logo $\widehat{\theta}j(g)(\theta(g))^{-1} \in ker\ q_M = M$. Uma vez que vale para cada M e $\cap M = 1$, concluímos que $\widehat{\theta}j = \theta$ e $\widehat{\theta}$ tem a propriedade considerada. Suponha que $\tau\widehat{G} \to H$ satisfaz $\tau j = \theta$. Então $(q_M\tau)j = q_M\theta$. Assim temos $q_M\tau = \theta_M$ pela unicidade de θ_M. Para $u \in \widehat{G}$, temos $q_M(\tau(u)) = q_M(\widehat{\theta}(u))$ tal que $\widehat{\theta}(u)(\tau(u))^{-1} \in ker\ q_M = M$. Uma vez válido para cada M, concluímos que $\tau = \theta$. □

Proposição 2.21 *Se $(\widehat{G_1}, j_1)$, $(\widehat{G_2}, j_2)$ são completamentos de G com respeito a I, então existe um isomorfismo $\alpha : \widehat{G_1} \to \widehat{G_2}$, tal que $\alpha j_1 = j_2$.*

Demonstração. Será omitida, mas pode ser encontrada em ([35], p. 25). □

Proposição 2.22 *Seja $(\widehat{G}, j)$ a completamento de G com respeito a I. Então:*
a) $j(G)$ é denso em $\widehat{G}$ e;
b) $ker\ j = \bigcap_{K \in I} K$.

Demonstração. Será omitida, mas pode ser encontrada em ([35], p. 26). □

2.3 Teoria de Sylow

Muitos dos conceitos e resultados da teoria de Sylow de grupos finitos podem ser transferidos diretamente para grupos profinitos. Os resultados da Teoria dos Grupos Finitos serão assumidos, suas demonstrações podem ser encontradas em ([3], [4] e [23]). Nesta seção todos os subgrupos com os quais iremos trabalhar são subgrupos fechados e quando não forem serão explicitamente indicados.

2.3.1 Índices de Subgrupos e Teorema de Lagrange

Um número de ***Steinitz*** (ou número ***supernatural***) é um produto formal $a = \prod p^{n(p)}$, onde p varia sobre um conjunto de números primos, e cada $n(p) \in \mathbb{N} \cup \{\infty\}$. Sejam $a,\ b$ dois números supernaturais. Segue que $ab = \prod p^{a_p + b_p}$. Definimos também o $mdc(a,\ b) = \prod p^{min(a_p,\ b_p)}$ e o $mmc(a,\ b) = \prod p^{max(a_p,\ b_p)}$ e dizemos que $a \mid b$ (a divide b) se $a_p \leq b_p$, para todo p.

Se G é um grupo profinito e H um subgrupo de G, definimos o índice de H em G como o número supernatural $[G : H] = mmc_{U \lhd_\circ G}[G/U : HU/U]$.

A ordem de G é o número $\mid G \mid = [G : 1] = mmc_{U \lhd_\circ G}[G/U]$.

Mediante essas informações, podemos provar a versão do Teorema de Lagrange para grupos profinitos.

Proposição 2.23 *Sejam $H,\ K$ subgrupos de G tais que $K \leq H \leq G$. Então $\mid G : K \mid = \mid G : H \mid \mid H : K \mid$.*

Demonstração.
Se $U \lhd_\circ G$, então $[G : UK] = [G : UH][UH : UK] = [G : UH][H : (U \cap H)K]$ e $U \cap H \lhd_\circ H$. Assim $[G : K]$ divide $[G : H][H : K]$. Reciprocamente, se $N_1 \lhd_\circ G$ e $N_2 \lhd_\circ H$, então $N_2 \geq H \cap M$ para algum $M \lhd_\circ G$. Seja $N = M \cap N_1$. Logo $N \lhd_\circ G$ e $[G : N_1H][H : N_2K]$ divide $[G : NH][H : (N \cap H)K]$, que é igual a $[G : NK]$. Assim, $[G : H][H : K]$ divide $[G : K]$. □

Lema 2.24 *Se $\{H_i, \mid i \in I\}$ é uma família de subgrupos tal que para todos $i, j \in I$ existe um índice $k \in I$ com $H_k \leq H_i \cap H_j$, então*

$$\mid G : \bigcap H_i \mid = mmc([G : H_i] \mid i \in I).$$

Demonstração. Observe que pela Proposição 2.23 o lado direito divide o lado esquerdo. Agora, se U é um subgrupo aberto contendo $\bigcap H_i$, então $\bigcap (H_i \cap (G \backslash U)) = \emptyset$. Então o conjunto $H_i \cap (G \backslash U)$ são todos fechados, e assim por compacidade

$$\bigcap_{\lambda=1}^{r} (H_{i_\lambda} \cap (G \backslash U)) = \emptyset,$$

para algum conjunto finito $\{i_i, i_2, \ldots, i_r\}$. Logo $\bigcap_{\lambda=1}^{r} H_{i_\lambda} \leq U$. Escolhendo $k \in I$ tal que $H_k \leq H_{i_\lambda}$, para $\lambda = 1, 2, \ldots, r$. Temos $H_k \leq U$ e $\mid G : U \mid$ divide $\mid G : H_k \mid$. Portanto, o resultado segue. □

2.3.2 Teoremas de Sylow

Definição 2.25 *Sejam G um grupo profinito e p um primo. Um p-subgrupo de Sylow de G é um subgrupo P tal que $\mid P \mid$ é uma (possivelmente infinita) potência de p e $|G:P|$ é coprimo com p.*

Assim, p-subgrupos de Sylow são *subgrupos pro-p maximais* de G. O ***normalizador*** $N_G(H)$ de um subgrupo H de um grupo abstrato G é definido por $N_G(H) = \{g \in G \mid g^{-1}Hg = H\}$, e é um subgrupo de G. Se G é profinito e H é fechado, então $N_G(H)$ é fechado.

Os resultados que seguem estendem os Teoremas de Sylow, conforme Teorema 1.18 de grupos finitos, para grupos profinitos.

Proposição 2.26 *Sejam G um grupo profinito, K um subgrupo normal e P um p-subgrupo de Sylow de G. Então*
a) $K \cap P$ é um p-Sylow subgrupo de K;
b) KP/K é um p-Sylow subgrupo de G/K;
c) $G = N_G(Q)K$ para cada p-Sylow subgrupo Q de K;
d) $H = N_G(H)$, sempre H é um subgrupo que contem $N_G(Q)$ para algum p-Sylow subgrupo Q de K.

Demonstração. Será omitida, mas pode ser encontrada em ([35], p. 37). □

O lema a seguir é bem conhecido no caso onde o grupo G é finito (ver [5], 6.2.2, 6.2.4 para a prova).

Lema 2.27 *Seja A um grupo de automorfismos coprimos de um grupo profinito G.*
a) Se N é um subgrupo normal fechado A-invariante de G, então $C_{G/N}(A) = C_G(A)N/N$.
b) Se H é um subgrupo pro-p A-invariante de G, então H está contido em um subgrupo pro-p A-invariante de Sylow de G.
c) Se A é um grupo abeliano elementar de ordem q^2, então $G = \langle C_G(a) \mid \ a \in A^\sharp \rangle$.

Demonstração. Comentaremos a demonstração do item a), os ítens b) e c) ficam como exercício.

a) Como por hipótese N é fechado, então G/N tem índice finito, portanto segue de modo análogo ao caso de grupos finitos, conforme o Lema 1.19.

□

2.3.3 Subgrupos de Hall

Seja π um conjunto de números primos. Um grupo finito F é chamado ***π-grupo*** se todo primo divisor da $\mid F \mid$ pertence a π.

Um grupo profinito é chamado grupo ***pro-π*** se ele é um limite inverso de π-grupos finitos.

Segue do Teorema de Lagrange que a classe de π-grupos finitos não é fechada somente para subgrupos e quocientes, mas também para extensões, isto é, um grupo F necessariamente pertence a classe de π-grupos finitos se tem um subgrupo normal E tal que ambos E e F/E pertencem à classe de π-grupos finitos.

Um ***subgrupo de Hall*** de um grupo profinito G é um subgrupo H tal que $\mid H \mid$ e $\mid G : H \mid$ são coprimos. Mais precisamente, se π é um conjunto de primos, um subgrupo H de G é chamado um ***π-subgrupo de Hall*** se $\mid H \mid$ é divisível somente pelos primos em π e $\mid G : H \mid$ é divisível somente pelos primos que não estão em π. Temos que um π-subgrupo de Hall de um grupo profinito são subgrupos pro-π maximais, mas subgrupos pro-π maximais não são necessariamente um π-subgrupo de Hall, mesmo quando G finito.

Seja p um número primo. Um ***$\{p\}$-subgrupo de Hall*** de um grupo profinito G é simplesmente um p-subgrupo de Sylow. Um $\{p\}'$-subgrupo de Hall, onde $\{p\}'$ é o complementar de $\{p\}$ em um conjunto de números primos, é chamado um ***p-complemento*** de G.

2.3.4 Grupos Pronilpotentes

No intuito de dar uma caracterização aos grupos pronilpotentes (limite inverso de grupos nilpotentes finitos), similar a caracterização realizada na Seção 1.2, necessitamos descrever um isomorfismo entre produtos cartesianos e grupos profinitos.

Lema 2.28 *Seja $\{H_i \mid i \in I\}$ uma família de subgrupos normais de um grupo profinito G. Suponha que G é o fecho do subgrupo abstrato gerado pela $\bigcup_{i\in I} H_i$. Para cada i, seja K_i o fecho do subgrupo abstrato gerado pela $\bigcup_{j\neq i} H_j$. Se $\bigcap_{i\in I} K_i = 1$, então $G \cong \prod_{i\in I} H_i$.*

Demonstração. Para cada i, temos $K_i \lhd G$ e além disso $K_i \cap H_i = 1$ e K_iH_i é um subgrupo fechado contendo $\bigcup_{j\in I} H_j$. Assim, $G = K_iH_i$. Portanto $G/K_i \cong H_i$, para cada i. Definimos

$$\begin{array}{rcl} \varphi : G & \to & \prod G/K_i \\ g & \mapsto & (K_i g) \end{array}$$

e obtemos que $ker\varphi = \cap K_i = 1$ e φ é contínua, desde que a composta com cada função projeção seja contínua. Vamos provar que $\varphi(G)$ é denso no produto cartesiano. Uma vez

que G é também compacto, portanto fechado, segue que φ é sobrejetora e portanto é um isomorfismo de grupos profinitos, pelo Lema 2.2 d). Agora $\varphi(H_j)$ consiste de todos os elementos (c_i) do $\prod G/K_i$ tais que c_i é trivial para todos $i \neq j$. Assim, $\varphi(G)$ contém

$$D = \{(c_i) \mid c_i = 1, \text{ para uma quantidade finita de índices } i\},$$

no entanto cada conjunto aberto não vazio no $\prod G/K_i$, contendo um conjunto da forma

$$U = \pi_{i_1}^{-1}(U_1) \cap \pi_{i_2}^{-1}(U_2) \cap \ldots \pi_{i_n}^{-1}(U_n),$$

onde π_{i_α} denota a função projeção para G/K_{i_α} e U_α é um subconjunto não vazio de G/K_{i_α}, para $\alpha = 1, 2, \ldots, r$, temos que $U \cap D$ é não vazio. Assim $\varphi(G)$ é denso no produto cartesiano, como queríamos. □

Proposição 2.29 *Seja G um grupo profinito. As afirmações que seguem são equivalentes.*
a) G é pronilpotente;
b) Cada subgrupo de Sylow de G é normal em G;
c) G é (isomorfo ao) o produto cartesiano de seus subgrupos de Sylow;
d) $N_G(U) \neq U$ para cada subgrupo normal próprio U de G.

Demonstração.

$a) \Rightarrow d)$ Sejam U um subgrupo próprio em G e N a interseção dos conjugados de U. Assim $N \leq U$ e $N \lhd_\circ G$; além disso G/N é nilpotente pela Proposição 2.14. Portanto, $N_G(U) \neq U$ a partir da implicação $a) \Rightarrow d)$ do Teorema 1.18.

$d) \Rightarrow b)$ Seja P um subgrupo de Sylow e U um subgrupo normal aberto contendo $N_G(P)$. Pela Proposição 2.26 d), temos $U = N_G(U)$ e segue que $U = G$, pelo item $d)$. Como $N_G(P)$ é a interseção de subgrupos abertos o contendo, concluímos que $N_G(P) = G$ e que P é normal em G.

$b) \Rightarrow c)$ Sejam I um conjunto de números primos divisores de $| G |$ e $\{P_i \mid i \in I\}$ o conjunto dos subgrupos de Sylow de G. Para cada i, seja K_i o fecho do grupo abstrato gerado pela $\bigcup_{j \neq i} P_j$. Note que $| K_i |$ é coprimo com i. De fato, se o primo p divide K_i, então p divide K_i/M para algum subgrupo $M \lhd_\circ K_i$. Somente uma quantidade finita de grupos MP_j/M não são triviais e K_i/M é o produto destes grupos. Concluímos que p divide P_j para algum $j \neq i$ e que $p \neq i$.

Segue que $K_i \cap P_i = 1$ para cada i e que $\cap K_i = 1$. Todo grupo profinito é o fecho do grupo abstrato gerado por todos os subgrupos de Sylow, uma vez que este fecho tem claramente índice 1. Portanto, aplicando o Lema 2.28 segue o resultado.

$c) \Rightarrow a)$ Como p-grupos finitos são nilpotentes, grupos pro-p são pronilpotentes e pelo corolário 2.16 qualquer produto cartesiano de grupos

pronilpotentes é pronilpotente. □

2.3.5 Automorfismos Livres de Pontos Fixos

Agora, finalizamos os resultados sobre grupos profinitos analisando o Teorema de Thompson que afirma que para cada primo p existe um natural c_p com a seguinte propriedade: se G é um grupo finito tendo um automorfismo α de ordem p tal que $\{g \in G \mid \alpha(g) = g\} = 1$, então G é nilpotente de classe no máximo c_p. O teorema não se sustenta quando G é profinito. A diferença surge porque no caso finito a hipótese implica $\mid G \mid \equiv 1 \mod p$ (uma vez que os elementos que não são identidades são permutados em órbitas de tamanho p por α), de modo que $\mid G \mid$ é primo com p, de modo que isso não ocorre para grupos profinitos.

Lema 2.30 *Sejam G um grupo profinito e α um automorfismo contínuo de G cuja ordem é uma potência finita de um primo p. Suponha que K é um subgrupo normal α-invariante de G. Se $\mid K \mid$ é coprimo com p e cada classe $Kx \neq K$ é levada nela mesma por φ, então existe um elemento $y \in Kx$ que é fixado por α.*

Demonstração. Seja

$$S = \{N \mid N \lhd_\circ G, N = \alpha(N)\}.$$

Fixe $N \in S$. Agora Kx é uma união de n classes $(N \cap K)hx$ onde $n = \mid K : N \cap K \mid$ e n é coprimo com p. Como $\alpha(Kx) = Kx$ e $\alpha(N \cap K) = N \cap K$, as n classes $(N \cap K)hx$ são permutáveis por α e, assim, já que cada órbita tem tamanho 1 ou uma potência de p, podemos ter uma órbita $\{(N \cap K)hx\}$ de tamanho 1. Assim, para cada N o conjunto

$$R(N) = \{y \in Kx \mid \alpha(y) \in (N \cap K)y\}$$

é não vazio e, sendo uma união de quantidade finita de classes de $N \cap K$, isto é: fechado. Se $M,\ N \in S$ e $M \leq N$, então claramente $R(M) \subseteq R(N)$. Por compacidade, segue que existe um elemento $y \in \cap R(N)$. Portanto se $L \lhd_\circ G$, então $\bigcap_{i=0}^{q-1} \alpha^i(L) \in S$, onde q é a ordem de α e, assim, $\bigcap_{N \in S} (N) = 1$. Desta forma:

$$\alpha(y) \in \bigcap_{N \in S} (N \cap K)y = ((\bigcap_{N \in S} (N)) \cap K)y = \{y\},$$

o que completa a demonstração do lema. □

Relembramos da Seção 1.2 que um grupo G é nilpotente se $Z_c(G) = G$ para algum c, onde $Z_c(G)$ é o c-ésimo termo da série central. O menor valor de c tal que isso acontece é chamado classe de nilpotência de G. Podemos também verificar que se G é nilpotente de classe no máximo c, então cada subgrupo de G também o é, e ainda que se $\{G_i \mid i \in I\}$ é uma família de grupos nilpotentes de classe no máximo c, então $\prod_{i\in I} G_i$ é nilpotente de classe no máximo c. Assim pela Proposição 2.10 o limite inverso de grupos nilpotentes finitos de classe no máximo c é nilpotente de classe no máximo c.

Teorema 2.31 *Seja G um grupo profinito de ordem coprima com um primo p. Suponha que exista um automorfismo contínuo α de G de ordem p tal que $\{g \in G \mid \alpha(g) = g\} = 1$. Então G é nilpotente de classe no máximo c_p.*

Demonstração. Pelo Lema 2.30, os subgrupos normais $N \lhd_\circ G$ tais que $N^\alpha = N$ tem interseção 1 e, assim, é suficiente mostrar que G/N é nilpotente de classe no máximo c_p para cada N. Se não o Teorema de Thompson para grupos finitos, aplicado para um automorfismo de G/N induzido por α dá uma classe $Nx \neq N$ tal que $(Nx)^\alpha = Nx$ temos então pelo Lema 2.30, que existe $y \in Nx$, fixado por α, o que contradiz a hipótese de que $\{g \in G \mid \alpha(g) = g\} = 1$. □

CAPÍTULO 3

Álgebras e Anéis de Lie

3.1 Anéis de Lie

Definição 3.1 *Um anel L com a operação de multiplicação denotada por $[\ ,\ ]$ é chamado um anel de Lie se satisfaz os seguintes axiomas:*
1) $[x,x]=0, \quad \forall \quad x\in L$*;*
2) $[x,y,z]+[y,z,x]+[z,x,y]=0 \quad \forall \quad x,y,z\in L$ *(Identidade de Jacobi).*

Observe que a propriedade antissimétrica é verificada pelo item 1*):*

$$[x+y,x+y]=0\Rightarrow [x,x]+[x,y]+[y,x]+[y,y]=0\Rightarrow [x,y]=-[y,x].$$

Se X é um subconjunto de L, denotaremos por $\langle X\rangle$ o subanel gerado por X e ${}_+\langle X\rangle$ o subgrupo que X gerado como grupo aditivo de L. Sejam X e Y subconjuntos de L. Definimos

$$X+Y=\{x+y \mid \quad x\in X \ \text{ e } \ y\in Y\},$$
$$[X,Y]=_+\langle\{[x,y] \mid \quad x\in X \ \text{ e } \ y\in Y\}\rangle.$$

Um subconjunto I de L é chamado um ***ideal*** de L, se $[L,I]\subseteq I$, ou de modo equivalente, $[I,L]\subseteq I$. Usando a propriedade de antissimetria, obtemos que as noções de ideais à esquerda, à direita e bilateral coincidem em álgebras de Lie. Logo, se X e Y são ideais de L, então $X+Y$ e $[X,Y]$ também o são.

O ***centralizador*** $C_L(X)$ do conjunto $X\subseteq L$ é um subanel de L, definido por

$$C_L(X)=\{y\in L \mid [X,y]=0\}.$$

O ***normalizador*** em L de um anel X é um subanel de L, definido por

$$N_L(X)=\{y\in L \mid [X,y]\subseteq X\}.$$

De modo análogo ao que foi feito para grupos, obtemos a série central superior, a série central inferior e a série derivada de uma álgebra de Lie. Façamos

$$Z_0(L) = 0,\ \ Z_1(L) = Z(L),\ \ Z_{i+1}(L) = \{x \in L \mid [L,x] \subseteq Z_i(L)\},\ \ i = 1,2,\ldots$$

A série

$$Z_0(L) \subseteq Z_1(L) \subseteq \cdots \subseteq Z_i(L) \subseteq \cdots ,$$

é chamada a *série central superior* de L. Façamos

$$L^{(0)} = L,\ \ L^{(1)} = L' = [L,L],\ \ L^{(i+1)} = [L^{(i)},L^{(i)}],\ \ \ i = 0,1,2,\ldots$$

e

$$\gamma_1(L) = L,\ \gamma_{i+1}(L) = [\gamma_i(L),L],\ \ i = 1,2,\ldots$$

As séries

$$L^{(0)} \supseteq L^{(1)} \supseteq \cdots \supseteq L^{(i+1)} \supseteq \cdots ,$$

e

$$\gamma_1(L) \supseteq \gamma_2(L) \supseteq \cdots \supseteq \gamma_i(L) \supseteq \cdots$$

são chamadas *série derivada* de L e *série central inferior* de L, respectivamente.

Um comutador $[\ldots[[a_1,a_2],a_3],\ldots,a_k]$ será denotado por $[a_1,a_2,\ldots,a_k]$ e é chamado de ***comutador simples*** em L. As definições de solubilidade e nilpotência são similares para Anéis de Lie, como feito para grupos.

Um anel de Lie L é dito ***solúvel*** se existe um número natural k tal que $L^{(k)} = 0$. O menor k tal que $L^{(k)} = 0$ é chamado de ***comprimento derivado*** de L e é denotado por dlL.

Um anel de Lie L é chamado ***nilpotente*** se existe um número natural k tal que $\gamma_{k+1}(L) = 0$. O menor número k tal que $\gamma_{k+1}(L) = 0$ é chamado ***classe de nilpotência*** de L e é denotado por clL.

Os dois teoremas que seguem são apresentados sem as devidas demonstrações, pois são completamente análogas à de grupos e podem ser encontradas em [30].

Teorema 3.2 *Sejam L um anel e k um número natural. Então:*
a) O ideal $\gamma_k(L)$ contém todos os comutadores de peso $\geq k$ em elementos de L;
b) O grupo aditivo de $\gamma_k(L)$ é gerado pelos comutadores de peso $\geq k$;
c) Se $L = \langle M \rangle$, então o grupo aditivo $\gamma_k(L)$ é gerado por comutadores simples de

peso $\geq k$ em elementos de M;
d) $L^{(k)} \subseteq \gamma_{2^k}(L)$. Em particular, se L é nilpotente de classe no máximo $2^k - 1$, então L é solúvel e o comprimento derivado é no máximo k.

Teorema 3.3 *Em qualquer anel de Lie L são equivalentes as seguintes afirmações*
a) $\gamma_{k+1}(L) = 0$;
b) $[x_1, x_2, \ldots, x_{k+1}] = 0$, para todos $x_1, x_2, \ldots, x_{k+1} \in L$;
c) $Z_k(L) = L$;
d) $\gamma_i(L) \subseteq Z_{k-i+1}(L)$, para cada $i = 1, 2, \ldots, k+1$.

3.1.1 Álgebras de Lie

Definição 3.4 *Seja R um anel (não necessariamente comutativo nem com 1). Um R-módulo à esquerda ou um R-módulo sobre R é um conjunto M junto com*

a) uma operação binária + sobre M sobre a qual M é um grupo abeliano
b) uma ação de R sobre M (isto é, uma função $R \times M \to M$) denotado por rm, para todo $r \in R$ e para todo $m \in M$, satisfazendo para todos $r, s \in R$, $m, n \in M$:

1) $(r+s)m = rm + sm$;
2) $(rs)m = r(sm)$;
3) $r(m+n) = rm + rn$.

Se o anel R tem o elemento unidade 1 impomos o axioma adicional:

(d) $1m = m$.

Se L é um anel de Lie no qual o grupo aditivo é um R-módulo, então L é chamado *álgebra de Lie* sobre R, com a condição que

(e) $r[a,b] = [ra,b] = [a,rb]$, para todos $r \in R$ e a e $b \in L$.

Em particular, todo anel de Lie pode ser visto como uma álgebra de Lie sobre $\mathbb{Z}$.

Quando R é um corpo, a definição de R-módulo é justamente a definição de espaço vetorial sobre R. Assim,

módulos sobre um corpo F são espaços vetoriais sobre F.

Definição 3.5 *Sejam R um anel e M um R-módulo. Um R-submódulo de M é um subgrupo N de M o qual é fechado para a ação dos elementos do anel, isto é, $rn \in N$, para todos $r \in R$ e $n \in N$.*

Nos casos onde R é um corpo, submódulos são subespaços.

Exemplo. ($\mathbb{Z}$-módulos) Sejam $R = \mathbb{Z}$, A qualquer grupo abeliano (finito ou infinito) e escreva a operação de A como +. Podemos fazer de A um $\mathbb{Z}$-módulo como segue: para quaisquer $z \in \mathbb{Z}$ e $a \in A$, defina

$$na = \begin{cases} a+a+\cdots+a \quad (n \text{ vezes}), & \text{se } n > 0 \\ 0, & \text{se } n = 0 \\ -a-a-\cdots-a \quad (-n \text{ vezes}), & \text{se } n < 0. \end{cases}$$

(Aqui 0 é a **identidade** do grupo aditivo A). Esta ação de $\mathbb{Z}$ sobre A faz de A um $\mathbb{Z}$-módulo, e os axiomas de módulo mostram que esta é a única ação possível de $\mathbb{Z}$ sobre A fazendo dele um $\mathbb{Z}$-módulo com unidade. Por conseguinte, todo grupo abeliano é um $\mathbb{Z}$-módulo. Inversamente, se M é qualquer $\mathbb{Z}$-módulo, então M é, a princípio, um grupo abeliano. O mesmo vale para $\mathbb{Z}$-submódulos e subgrupos de grupos abelianos.

3.1.2 Produto Tensorial de Módulos

Nesta seção apresentamos o produto tensorial de dois R-módulos M e N onde R é um anel (não necessariamente comutativo) contendo 1. O produto tensorial é em geral uma construção que nos permite formar um novo módulo no qual podemos tomar "produtos" mn de elementos $m \in M$ e $n \in N$. Consideraremos considerar uma motivação interessante para se construir esse produto tensorial, que é a "extensão de escalares".

Vamos supor primeiramente o caso mais trivial. Suponha que o anel R é um subanel do anel S e que N é um S-módulo à esquerda. Então, naturalmente N pode ser considerado como um R-módulo à esquerda, pois os elementos de R, sendo elementos de S, agem sobre N por hipótese. Observando os axiomas de módulos, temos neste caso que

$$(sr)n = s(rn), \qquad \text{para todos} \quad s \in S, r \in R \quad \text{e} \quad n \in N. \tag{3-1}$$

De modo mais geral, se $f : R \to S$ é um homomorfismo (de anéis) do anel R no anel S (por exemplo, a aplicação identidade de S restrita a R se R for um subanel de S) então é fácil ver que N pode ser considerado como um R-módulo com $rn = f(r)n$, para $r \in R$ e $n \in N$. Nesta situação, S pode ser considerado como uma extensão do anel R e o R-módulo resultante é dito como obtido a partir de N pela *restrição dos escalares* de S para R.

Agora inversamente do que foi feito no parágrafo anterior, suponha que R é um subanel de S. Vamos começar com um R-módulo N e busquemos obter a partir deste uma estrutura de um S-módulo sobre N ("estendendo os escalares" a partir de R até S). Isto em geral é impossível, mesmo na situação mais simples: o anel R é ele próprio um R-módulo, mas geralmente não é um S-módulo para um anel S maior. Por exemplo, $\mathbb{Z}$ é um

$\mathbb{Z}$-módulo, mas ele não pode ser considerado como um $\mathbb{Q}$-módulo (se isto fosse possível, então $\frac{1}{2} \circ 1 = z$ deveria ser um elemento de $\mathbb{Z}$ com $z+z=1$, sendo portanto impossível). Mas observe que mesmo $\mathbb{Z}$ não sendo um $\mathbb{Q}$-módulo, $\mathbb{Z}$ está contido no $\mathbb{Q}$-módulo $\mathbb{Q}$. Neste caso podemos então dizer que existe uma injeção, também chamada de imersão, do $\mathbb{Z}$-módulo $\mathbb{Z}$ no $\mathbb{Q}$-módulo $\mathbb{Q}$. A partir desta discussão, se torna interessante saber se um R-módulo N pode ser imerso como um R-submódulo de algum S-módulo, ou de maneira mais geral, saber quais homomorfismos de módulos existem de N no S-módulo.

Para ilustrar o que foi dito no parágrafo anterior, apresentamos o seguinte exemplo. Suponha que N é o grupo abeliano finito $\mathbb{Z}/2\mathbb{Z}$ e considere os possíveis homomorfismos do $\mathbb{Z}$-módulo N em algum $\mathbb{Q}$-módulo. Observe que em N todo elemento tem ordem finita, enquanto todo elemento não nulo do $\mathbb{Q}$-módulo tem ordem infinita (aditivamente). Logo todo elemento de N deve ser levado em 0 por tal homomorfismo. Sendo assim, não existe nenhum homomorfismo não nulo de N em algum $\mathbb{Q}$-módulo, muito menos imersões de N identificando N como um submódulo de um $\mathbb{Q}$-módulo.

Vimos até aqui que dois R-módulos podem ter comportamentos diferentes quando tentamos "estender os escalares". O que vamos fazer daqui para frente é construir para um R-módulo geral N um S-módulo que é o melhor possível na tentativa de incluir N. Veremos que estes módulos determinam os possíveis homomorfismos de R-módulos N nos S-módulos. Vamos começar a construção retornando aos axiomas de módulos a fim de examinar se podemos definir produtos da forma sn, com $s \in S$ e $n \in N$.

Iniciemos então com o grupo abeliano N junto com uma função $S \times N$ em N, onde a imagem de um par (s,n) é denotado por sn. Então podemos considerar o $\mathbb{Z}$-módulo livre sobre o conjunto $S \times N$, isto é, a coleção de todas somas comutativas finitas de elementos da forma (s_i, n_i) onde $s_i \in S$ e $n_i \in N$. Isto nos dá um grupo abeliano onde não há relações entre quaisquer pares distintos, isto é, nenhuma relação entre os "produtos formais" sn. A fim de satisfazer os axiomas de S-módulo e a relação de compatibilidade com a ação de R sobre N em (3-1), devemos tomar o quociente deste grupo abeliano pelo subgrupo H gerado por todos os elementos da forma

$$\begin{aligned} (s_1+s_2,n)-(s_1,n)-(s_2,n), \\ (s,n_1+n_2)-(s,n_1)-(s,n_2) \quad \text{e} \\ (sr,n)-(s,rn), \end{aligned}$$

onde rn refere-se à estrutura de R-módulo já definida sobre N.

O resultado do grupo quociente é denotado por $S \bigotimes_R N$ e é chamado o ***produto tensorial*** de S e N sobre R e seus elementos são chamados ***tensores*** e podem ser escritos como uma soma finita de tensores da forma $s \otimes n$. Se $s \otimes n$ denota a classe contendo (s,n)

em $S \bigotimes_R N$, então pela definição do quociente temos as seguintes relações:

$$\begin{aligned} (s_1 + s_2) \otimes n &= s_1 \otimes n + s_2 \otimes n \\ s \otimes (n_1 + n_2) &= s \otimes n_1 + s \otimes n_2 \\ sr \otimes n &= s \otimes rn. \end{aligned}$$

Não é difícil mostrar que o produto tensorial é um S-módulo à esquerda sobre a ação definida por

$$s\left(\sum_{finito} s_i \otimes n_i\right) = \sum_{finito} (ss_i) \otimes n_i.$$

$S \bigotimes_R N$ é chamado o ***S-módulo*** (à esquerda) obtido pela extensão de escalares a partir do R-módulo (à esquerda) N.

Existe uma aplicação natural $\iota : N \to S \bigotimes_R N$ definida por $n \mapsto 1 \otimes n$. Não é uma tarefa difícil provar que esta aplicação é um homomorfismo. O que devemos perceber é que em geral ι não é injetiva, o que significa que, $S \bigotimes_R N$ nem sempre precisa conter uma cópia isomorfa de N.

Exemplo.

Sejam $R = \mathbb{Z}$, $S = \mathbb{Q}$ e seja A um grupo abeliano finito de ordem n. Neste caso, o $\mathbb{Q}$-módulo $\mathbb{Q} \otimes_{\mathbb{Z}} A$ obtido pela extensão dos escalares a partir do $\mathbb{Z}$-módulo A é 0. Para ver isto, observe primeiro que em qualquer produto tensorial $1 \otimes 0 = 1 \otimes (0+0) = 1 \otimes 0 + 1 \otimes 0$, donde

$$1 \otimes 0 = 0.$$

Agora, para qualquer tensor $q \otimes a$, podemos escrever o número racional q como $(q/n)n$. Mas como $na = 0$ em A, temos

$$q \otimes a = \left(\frac{q}{n} \cdot n\right) \otimes a = \frac{q}{n} \otimes (na) = (q/n)(1 \otimes 0) = 0.$$

Donde segue que $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$. Em particular, a função $\iota : a \to S \bigotimes_R A$ é a aplicação nula. Em particular, se A é não trivial, o $\mathbb{Z}$-módulo original não está contido no $\mathbb{Z}$-módulo obtido pela extensão dos escalares.

Definição 3.6 *Seja G um grupo abeliano. Um anel de Lie L tem uma G-graduação ou é G-graduado, se para cada elemento $g \in G$ corresponde um subgrupo L_g do grupo aditivo de L tal que*

$a)\ L = \sum_{g_i \in G} L_{g_i}\ ;$
$b)\ [L_{g_i}, L_{g_j}] = L_{g_i g_j},\ para\ \ todos\ \ g_1, g_2 \in G.$

Qualquer elemento de L_g chama-se ***homogêneo***. Observe que a condição $a)$ da definição acima nos diz que todo elemento de L é uma soma finita de elementos homogêneos que são unicamente determinados. Se

$$x = x_0 + x_1 + x_2 + \cdots + x_l$$

é a decomposição de um elemento $x \in L$, então os elementos x_i chamam-se ***componentes homogêneas*** de x.
Exemplo. Se L é uma $\mathbb{C}$-álgebra de Lie e φ é um automorfismo de L de ordem finita n, então o grupo aditivo de L decompõe-se como um $\mathbb{C}$-espaço vetorial na soma direta dos auto-espaços da transformação linear φ:

$$L = L_0 \oplus L_1 \oplus \cdots \oplus L_{n-1},$$

onde $L_i = \{l \in L \big| l^\varphi = \omega^i l\}, \quad i = 0, 1, \ldots, n-1$, e ω é uma n-ésima raiz primitiva da unidade. Temos também que $[L_a, L_b] \subseteq L_{a+b}$, onde $a, b, a+b$ são resíduos módulo n, pois seja $x \in L_{a+b}$ então $x^\varphi = \omega^{a+b} x$. Sejam $m \in L_a$ e $n \in L_b$. Assim $m^\varphi = \omega^a m$ e $n^\varphi = \omega^b n$. Logo

$$[m,n]^\varphi = [m^\varphi, n^\varphi] = [\omega^a m, \omega^b n] = \omega^{a+b}[m,n] \Longrightarrow [L_a, L_b] \subseteq L_{a+b},$$

e com esta decomposição temos uma $\mathbb{Z}/n\mathbb{Z}$-graduação de L.

Observe que se e é o elemento identidade de G, então L_e é um subanel de L, pois da definição acima temos $[L_e, L_e] \subseteq L_e$. Outro fato não difícil de notar é que se temos uma G-graduação para o anel de Lie L, conseguimos a partir desta uma G-graduação para os termos da série derivada do anel de Lie L, da seguinte forma:

$$L_g^{(i)} = L^{(i)} \cap L_g \qquad \text{e} \qquad L_g^{(i+1)} = \sum_{h_1 . h_2 = g} [L_{h_1}^{(i)}, L_{h_2}^{(i)}].$$

Se ω é uma n-ésima raiz primitiva da unidade, então podemos construir o anel

$$\mathbb{Z}[\omega] = \mathbb{Z}\omega \oplus \mathbb{Z}\omega^2 \oplus \cdots \oplus \mathbb{Z}\omega^{\phi(n)-1},$$

onde $\phi(n)$ é a função de Euler.

Como já foi dito anteriormente, todo anel de Lie L pode ser considerado como uma álgebra de Lie sobre $\mathbb{Z}$. Daí, como $\mathbb{Z}[\omega]$ e L são $\mathbb{Z}$-módulos, podemos definir o

produto tensorial $L \otimes \mathbb{Z}[\omega]$, onde este naturalmente se torna um anel de Lie sobre $\mathbb{Z}[\omega]$ com as operações

$$b(a_1 \otimes b_1) = a_1 \otimes bb_1;$$

$$[a_1 \otimes b_1, a_2 \otimes b_2] = [a_1, a_2] \otimes b_1 b_2.$$

Em se tratando de um anel de Lie (álgebra de Lie) e o anel $\mathbb{Z}[\omega]$ (de dimensão finita sobre $\mathbb{Z}$) temos que o anel de Lie L pode ser imerso em $L \otimes \mathbb{Z}[\omega]$ pela aplicação $l \mapsto l \otimes 1$, pois neste caso a única maneira de $l \otimes 1$ ser zero é quando $l = 0$, o que mostra que o núcleo só tem o elemento trivial, sendo portanto uma aplicação injetiva.

Cada automorfismo φ de ordem n de um anel de Lie L é dito *semissimples* se, com anel base $\mathbb{Z}$ se estendido para o anel $\mathbb{Z}[\omega]$ como descrito acima, o grupo aditivo $L = L \otimes \mathbb{Z}[\omega]$ se decompõe em uma soma direta dos autoespaços da transformação linear φ:

$$L = \bigoplus_{i=0}^{n-1} L_i,$$

onde $L_i = \{l \in L | l^{\varphi} = \omega^i l\}$ é um subgrupo aditivo chamado de φ-componente correspondente ao autovalor ω^i. Ao contrário da definição usual, neste contexto usamos o termo "autovalor" ainda que $L_i = 0$.

Outro exemplo similar ao caso de $L \otimes \mathbb{Z}[\omega]$ é se L é uma álgebra de Lie sobre $\mathbb{F}_p[\omega]$. Podemos considerar a álgebra de Lie $\overline{L} = L \otimes \mathbb{F}_p[\omega]$ e L também está imersa em $\overline{L}$.

3.1.3 Derivações

Para descrevermos sobre derivações precisamos relembrar alguns fatos básicos envolvendo anéis.

Definição 3.7 *Sejam A e B anéis e $f : A \to B$ uma função. Dizemos que f é um homomorfismo de anéis, se valer:*
a) $f(a+b) = f(a) + f(b)$, para todos $a,\ b \in A$;
b) $f(a \cdot b) = f(a) \cdot f(b)$, para todos $a,\ b \in A$.

Observe que as operações $+$ e $\cdot$ à esquerda da igualdade acima são as operações de A, enquanto que as operações $+$ e $\cdot$ à direita da igualdade são as operações de B.

Se A e B são anéis e $f : A \to B$ é um homomorfismo injetor, dizemos que f é um monomorfismo. Se f é um homomorfismo sobrejetor, dizemos que f é um epimorfismo. Se f é um homomorfismo bijetor, dizemos que f é um isomorfismo. Neste último caso, dizemos que os anéis são isomorfos e denotaremos por $A \cong B$. Quanto temos um homomorfismo $f : A \to A$, chamaremos f de endomorfismo.

Álgebra Linear Geral. Seja V um espaço vetorial de dimensão finita sobre um corpo F , digamos $dimV = n$. Denotamos por ***EndV*** o conjunto de todas as transformações lineares de V em V . Como um espaço vetorial sobre F, $EndV$ possui dimensão n^2 e $EndV$ é uma álgebra associativa em relação à operação do produto usual. Definamos uma nova operação $[x,y] = xy - yx$, o comutador de x e y. Com esta operação, $EndV$ se torna uma álgebra de Lie sobre F. Para distinguir esta nova estrutura algébrica da álgebra associativa formada pelas transformações lineares em V com o produto usual, vamos escrever ***gl(V)*** para $EndV$ visto como álgebra de Lie e a chamaremos de *álgebra Linear Geral*, este nome é devido ao fato de estar relacionada com o *Grupo Linear Geral* $GL(V)$, que consiste de todos os endomorfismos inversíveis sobre V.

Definição 3.8 *Seja L uma álgebra de Lie sobre K. A função $D : L \to L$ é chamada derivação de L se:* $[a,b]^D = [a^D, b] + [a, b^D]$.

O conjunto de todas as derivações L será denotado por $D(L)$. Se D_1, $D_2 \in D(L)$ e $\alpha, \beta \in K$, então a combinação $\alpha D_1 + \beta D_2$ é derivação de L.

Podemos verificar também que $[D_1, D_2] = D_1D_2 - D_2D_1 \in D(L)$, pois:

$$\begin{aligned}
[a,b]^{[D_1,D_2]} &= [a,b]^{D_1D_2 - D_2D_1} \\
&= [a,b]^{D_1D_2} - [a,b]^{D_2D_1} \\
&= \left([a^{D_1},b] + [a,b^{D_1}]\right)^{D_2} - \left([a^{D_2},b] + [a,b^{D_2}]\right)^{D_1} \\
&= [a^{D_1D_2},b] + [a,b^{D_1D_2}] - [a^{D_2D_1},b] - [a,b^{D_2D_1}] \\
&= [a^{D_1D_2 - D_2D_1},b] + [a,b^{D_1D_2 - D_2D_1}] \\
&= [a^{[D_1,D_2]} + [a,b^{[D_1,D_2]}].
\end{aligned}$$

Agora seja I um ideal de uma álgebra L. Para todo $b \in L$, definimos a função

$$\begin{aligned}
\overline{b} : I &\to I \\
a &\mapsto a^{\overline{b}} = [a,b].
\end{aligned}$$

Essa função é uma derivação, pois se verifica a Definição 3.8, conforme segue:

$$[a,b]^{\overline{b}} = [[a,b],b] = -[[b,b],a] - [[b,a],b] = [[a,b],b] + [a,[b,b]] = [a^{\overline{b}},b] + [a,b^{\overline{b}}].$$

Exemplo. Seja L uma álgebra de Lie. Se $x \in L$, a aplicação que leva $y \in L$ em $[x,y]$ é um endomorfismo de L, o qual denotaremos por **adx**. Escrevemos $adx(y) = [x,y]$. Claramente, adx é uma derivação, basta utilizar a Identidade de Jacobi e obteremos a seguinte igualdade

$$[x,[y,z]] = [[x,y],z] + [y,[x,z]], \quad para\ todo\ x,\ y,\ z \in L,$$

ou seja,

$$adx([y,z]) = [adx(y),z] + [y,adx(z)].$$

Portanto, $adx \in D(L)$.

Lema 3.9 *A aplicação $ad : L \to gl(L)$, definida por $ad(x) = adx$ é um homomorfismo.*

A aplicação $L \to D(L)$ que leva x em adx é conhecida como a ***representação adjunta*** de L.

Definição 3.10 *Um elemento $a \in L$ é chamado* ad-nilpotente *se existe $n \in \mathbb{N}$ tal que $[x,_n a] = 0$, para todo $x \in L$. Se n é o menor número natural com esta propriedade, dizemos que a é ad-nilpotente de **índice n**.*

Observação: Se L é nilpotente, então todos os seus elementos são ad-nilpotentes.

Agora considere o homomorfismo

$$\begin{aligned} \varphi : L &\to D(I) \\ b &\mapsto b^{\varphi} = \overline{b}, \end{aligned}$$

Observe que seu núcleo coincide com o centralizador $C_L(I)$, pois $Ker(\varphi) = \{b \in L \mid b^{\varphi} = 0\}$ e $C_L(I) = \{b \in L \mid [I,b] = 0\}$.

Definiremos o ***produto semi direto*** de duas álgebras: dadas A e B duas álgebras sobre um anel K e um homomorfismo $\delta : B \to D(A)$ considere $A \leftthreetimes B = \{(a,b) \mid a \in A \text{ e } b \in B\}$ com as operações definidas por:

- Multiplicação:
  $[(a_1,b_1),(a_2,b_2)] = ([a_1,a_2] - a_2^{\delta(b_1)} + a_1^{\delta(b_2)}, [b_1,b_2])$;
- Adição:
  $(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$;
- Multiplicação por escalar:
  $\alpha(a_1,b_1) = (\alpha a_1, \alpha b_1)$, para todos $a_1,a_2 \in A$ e $b_1,b_2 \in B$

3.2 Identidades Polinomiais para Álgebras de Lie

Lembramos que um elemento $a \in L$ é ad-nilpotente se existe um número natural n tal que $[x,_n a] = 0$, para todo $x \in L$. Se n é o menor inteiro que satisfaz essa propriedade dizemos que a é ad-nilpotente de índice n. Denote por F a álgebra de Lie sobre R com geradores livres enumeráveis $x_1,x_2,x_3,\cdots$ Seja $f = f(x_1,x_2,\ldots,x_n)$ um elemento de F diferente de zero. A álgebra de Lie L satisfaz a identidade $f \equiv 0$ se $f(a_1,a_2,\ldots,a_n) = 0$

para quaisquer $a_1, a_2, \ldots, a_n \in L$. Neste caso, L satisfaz uma ***identidade polinomial*** e dizemos que L é ***PI***. Um resultado bem conhecido de Zelmanov diz que se uma PI-álgebra de Lie L é finitamente gerada onde qualquer comutador em seus geradores é ad-nilpotente, então L é nilpotente ([37], III (0,4)). Usando esse resultado e alguns argumentos rotineiros, podemos deduzir o próximo teorema.

Teorema 3.11 *Seja L uma álgebra de Lie sobre um corpo R gerada por $a_1, a_2, \ldots, a_m$. Assuma que L satisfaz uma identidade $f \equiv 0$ e que cada comutador nos geradores $a_1, a_2, \ldots, a_m$ é ad-nilpotente de índice no máximo n. Então, L é nilpotente de classe $\{f, n, m, R\}$-limitada.*

Demonstração. Considere a R-álgebra livre m-gerada F_m com geradores $f_1, f_2, \ldots, f_m$ e seja T o ideal de F_m gerado por todos os valores de f nos elementos de F_m e por todos os elementos da forma $[g,_n c]$, onde $g \in F_m$ e c é um comutador arbitrário nos f_i. Então, o quociente F/T satisfaz as hipóteses do resultado de Zel'manov citado no parágrafo anterior e portanto é nilpotente de classe $u = u(m, n, f, R)$. Temos que L é uma imagem de F/T pelo homomorfismo induzido pela aplicação $f_i \to a_1$. Portanto, L é nilpotente de classe no máximo u. □

Um importante critério para uma álgebra de Lie ser PI é o seguinte:

Teorema 3.12 *(Bahturin-Linchenko-Zaicev). Seja L uma álgebra de Lie sobre um corpo R. Assuma que um grupo finito A age sobre L por automorfismos tal que $C_L(A)$, a subálgebra formada pelos elementos fixos, é PI. Assuma ainda que a característica é zero ou coprima com a ordem de A. Então, L é PI.*

Esse teorema foi primeiro demonstrado para o caso onde A é solúvel por Bahturin e Zaicev [1] e mais tarde estendido para o caso geral por Linchenko [19].

3.3 Associando um Anel de Lie a um Grupo

Existem algumas maneiras de obter um anel de Lie associado a um grupo G. Nesta seção apresentamos uma forma de construir um anel de Lie a partir de um dado grupo G, utilizando a conhecida série de Jennings-Lazard-Zassenhaus e obtendo um anel de Lie sobre o corpo com p elementos $\mathbb{F}_p$, onde p é um número primo.

3.3.1 A Série de Jennings-Lazard-Zassenhaus e a Álgebra de Lie Correspondente

Lema 3.13 *Sejam G um grupo e $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots$ a série central inferior de G. Temos que:*

a) Se x,y são elementos de G, então para $n \geq 1$,

$$(xy)^{p^n} \equiv x^{p^n} y^{p^n} mod \gamma_2(G)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(G)^{p^{n-r}}.$$

b) Se x, y são elementos de G e H é um subgrupo de G tal que x e $[x,y]$ pertencem a H, então para $n \geq 1$,

$$[x^{p^n}, y] \equiv [x,y]^{p^n} mod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}.$$

Demonstração. Seja $R = \gamma_2(G)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(G)^{p^{n-r}}$. Pela Fórmula de Compilação de Phillip Hall ([16], p.25), existe um elemento $c_i \in \gamma_i(G)$, com $i = 2, \ldots, p^n$, de tal forma que $x^{p^n} y^{p^n} = (xy)^{p^n} c_2^{\binom{p^n}{2}} \ldots c_{p^n}$. Se $(i,p) = 1$, então $\binom{p^n}{i}$ é divisível por p^n, e para $i > 1$, $c_i^{\binom{p^n}{i}} \in \gamma_2(G)^{p^n} \leq R$. Agora, se $i = p^r j$, com $r \geq 1$ e $(p,j) = 1$, então $c_i^{\binom{p^n}{i}}$ é divisível por p^{n-r} e $i \geq p^r$. Assim, $c_i^{\binom{p^n}{i}} \in \gamma_{p^r}(G)^{p^{n-r}} \leq R$. Portanto, $x^{p^n} y^{p^n} \equiv (xy)^{p^n} \mod R$ e o item a) segue.

Consequentemente,

$$(x[x,y])^{p^n} \equiv x^{p^n} [x,y]^{p^n} mod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}.$$

Mas, $(x[x,y])^{p^n} = (x^y)^{p^n} = (x^{p^n})^y = x^{p^n}[x^{p^n}, y]$ e o resultado segue. □

Lema 3.14 *Se $n \geq 0$, então $[\gamma_i(G)^{p^n}, \gamma_j(G)] \leq \prod_{r=0}^{n} \gamma_{j+ip^r}(G)^{p^{n-r}}$.*

Demonstração. Seja $R = \gamma_{j+ip^r}(G)^{p^{n-r}}$. Como R é normal em G, é suficiente mostrar que $[x^{p^n}, y] \in R$ para quaisquer $x \in \gamma_i(G)$, $y \in \gamma_j(G)$. Pelo item (ii) do Lema 3.13,

$$[x^{p^n}, y] \equiv [x,y]^{p^n} \mod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}},$$

onde $H = \langle x, [x,y] \rangle$. Então $\gamma_2(H)$ é o fecho normal de $[x,y,x]$ em H. Assim, temos que $\gamma_2(H) \leq \gamma_{2i+j}(G)$. Como $H \leq \gamma_i(G)$, segue que $\gamma_m(H) \leq \gamma_{mi+j}(G)$, para todo $m \geq 2$. Logo $\gamma_{p^r}(H)^{p^{n-r}} \leq \gamma_{p^r i+j}(G)^{p^{n-r}} \leq R$, para $r = 1, \ldots, n$. Também temos que $\gamma_2(H)^{p^n} \leq \gamma_{i+j}(G)^{p^n} \leq R$ e $[x,y]^{p^n} \in \gamma_{i+1}(G)^{p^n} \leq R$. Portanto, $[x^{p^n}, y] \in R$, como queríamos. □

Definição 3.15 *Para qualquer número natural n e um primo p, faça*

$$D_n(G) = \prod_{ip^k \geq n} \gamma_i(G)^{p^k}.$$

Temos que $D_n(G)$ é um subgrupo característico de G e obtemos a seguinte série:

$$G = D_1(G) \geq D_2(G) \geq \cdots D_n(G) \geq \cdots.$$

Note que é possível que $D_{n-1}(G) = D_n(G) \leq D_{n+1}(G)$. Se G for um grupo abeliano, então $D_n(G) = G^{p^k}$, onde k é o menor inteiro tal que $p^k \geq n$. Assim, $D_n(G) = G^{p^k}$ se $p^{k-1} < n < p^k$. Se G for um p-grupo finito então, $D_n(G) = \Phi(G)$ é o subgrupo de Frattini de G. Agora, se G e um grupo de expoente p, então $D_n(G) = \gamma_n(G)$, para todo n.

A série $D_n(G)$ é central em G e para mostrar isso precisamos dos seguintes lemas.

Lema 3.16 *Suponha que $i, j \geq 1$ e $h \geq 0$. Seja $R = \prod_{r=0}^{h} \gamma_{i+jp^r}(G)^{p^{h-r}}$. Se $x \in \gamma_i(G)$ e $n \geq 2$, então $\gamma_n\big(\langle x, R\rangle\big) \leq \prod_{r=0}^{h} \gamma_{in+jp^r}(G)^{p^{h-r}}$.*

Demonstração. Usamos indução sobre n. Para $n = 2$, temos $\gamma_2\big(\langle x,R\rangle\big) = [R, \langle x,R\rangle]$. Como $\langle x,R\rangle \leq \gamma_i(G)$, segue que $\gamma_2\big(\langle x,R\rangle\big) = \big[R, \gamma_i(G)\big]$. Para $n \geq 2$, temos $\gamma_n\big(\langle x,R\rangle\big) \leq \big[\gamma_{n-1}\big(\langle x,R\rangle\big), \gamma_i(G)\big]$. Usando a definição de R para $n = 2$ e a hipótese de indução para $n > 2$, segue que para $n \geq 2$,

$$\gamma_n\big(\langle x,R\rangle\big) \leq \big[\prod_{r=0}^{h} \gamma_{in-1+jp^r}(G)^{p^{h-r}}, \gamma_i(G)\big].$$

Aplicando os Lemas 3.14 e 1.12, temos que

$$\begin{aligned}
\gamma_n\big(\langle x,R\rangle\big) &\leq \prod_{r=0}^{h} \big[\gamma_{in-1+jp^r}(G)^{p^{h-r}}, \gamma_i(G)\big] \\
&\leq \prod_{r=0}^{h} \prod_{s=0}^{h-r} \big[\gamma_{i+p^s(in-1+jp^r)}(G)^{p^{h-r-s}}, \gamma_i(G)\big] \\
&\leq \prod_{r+s\leq h} \gamma_{in+jp^{r+s}}(G)^{p^{h-r-s}},
\end{aligned}$$

pois $i + p^s in - p^s i \geq in$. E assim se verifica o Lema. □

Lema 3.17 *Sejam $i, j \geq 1$ e $h, k \geq 0$. Então $[\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \leq D_{ip^k+jp^h}(G)$.*

Demonstração. Suponha que $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$. Sejam $z = [x, y^{p^h}]$ e $H = \langle x, z \rangle$. Pelo Lema 3.13 b), temos:

$$[x^{p^k}, y^{p^h}] \equiv [x, y^{p^h}]^{p^k} = z^{p^k} \mod \gamma_2(H)^{p^k} \prod_{m=1}^{k} \gamma_{p^m}(H)^{p^{k-m}}.$$

Para $n = 1, \ldots, p^k$, defina $H_n = \prod_{r=0}^{h} \gamma_{in+jp^r}(G)^{p^{h-r}}$. Pelo Lema 3.14, $z \in H_1$. Assim $H \leq \langle x, H_1 \rangle$ e pelo Lema 3.16, $\gamma_n(H) \leq H_n$. Portanto,

$$[x^{p^k}, y^{p^h}] \in \prod_{m=0}^{n} H_{p^m}^{p^{k-m}}.$$

Faça $R = D_{ip^k+jp^h}(G)$. Se $m+h-r \geq k$, então, pela definição de D_i, $\gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq R$. Assim, se $s = \max(m+h-k+1, 0)$, então,

$$H_{p^n} \leq R \prod_{r=s}^{h} \gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq R_{\gamma_{ip^m+jp^s}}(G).$$

Logo,

$$H_{p^m}^{p^{k-m}} \leq R_{\gamma_{ip^m+jp^s}}(G)^{p^{k-m}} = R,$$

pois $ip^k + jp^{s+k-m} \geq ip^k + jp^h$. Logo $[x^{p^k}, y^{p^h}] \in R$ e $(x^{p^k})R$ comuta com $(y^{p^h})R$. Portanto, cada elemento de $\gamma_i(G)^{p^k}R/R$ comuta com cada elemento de $\gamma_j(G)^{p^h}R/R$ e $[\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \leq R$. □

Teorema 3.18 *Sejam $\{D_i\}$ a série definida em 3.15 e p um número primo. Então:*
a) $[D_m(G), D_n(G)] \leq D_{m+n}(G)$;
b) $D_n(G)^p \leq D_{p^n}(G)$;
c) *Para $n > 1$, $D_n(G) = [D_{n-1}(G), G]D_m(G)^p$, onde m é o menor número natural tal que $pm \geq n$.*

Demonstração. O item a) segue imediatamente da definição de $\{D_i\}$ e do Lema 3.17. Logo restam os dois últimos itens.

Pelo item a) temos que $\gamma_p(D_n(G)) \leq \gamma_{pn}(G)$, assim $D_n(G)/D_{pn}(G)$ é regular. Mas $D_n(G)/D_{pn}(G)$ é gerado por elementos de ordem p pois se $ip^k \geq n$ e $x \in \gamma_i(G)$, então $(x^{p^k})^p \in D_{ip^{k+1}} \leq D_{pn}(G)$. Portanto, pelo Lema 1.26, temos $(D_n(G)/D_{pn}(G))^p = 1$ e ainda $D_n(G)^p \leq D_{pn}(G)$. E o item b) está provado.

Pelos itens a) e b), $[D_{n-1}(G), G]D_m(G)^p \leq D_n(G)$. Suponha que $ip^k \geq n$. Se $k = 0$, então

$$\gamma_i(G)^{p^k} = \gamma_i(G) \leq \gamma_n(G) = [\gamma_{n-1}(G), G].$$

Se $k > 0$, então $ip^{k-1} \geq m$, pela definição de m e

$$\gamma_i(G)^{p^k} \leq (\gamma_i(G)^{p^{k-1}})^p \leq D_{ip^{k-1}}(G)^p \leq D_m(G)^p.$$

Portanto, $\gamma_i(G)^{p^k} \leq [D_{n-1}(G), G]D_m(G)^p$ em qualquer caso e a afirmação segue da definição de $\{D_i\}$. □

Corolário 3.19 *Suponha que $G = R_1 \geq R_2 \geq \cdots$ é uma série do grupo G tal que $R_n \trianglelefteq G$, $[R_n, G] \leq R_{n+1}$ e $R_n^p \leq R_{np}$ para todo $n \geq 1$. Então $R_n \geq D_n(G)$ para todo $n \geq 1$.*

Demonstração. Segue do Teorema 3.18 item c) por indução sobre n. □

Com isso, demonstramos que a série $D_n(G)$ é central em G. A série $D_n(G)$ é chamada Série de ***Jennings-Lazard-Zassenhaus***.

Definição 3.20 *Seja p um número primo arbitrário mas fixo. Seja G um grupo. Uma série de subgrupos*

$$G = G_1 \geq G_2 \geq \cdots \qquad (*)$$

é uma N-série se satisfaz $[G_i, G_j] \leq G_{i+j}$ para todos i, j. Toda N-série é central (i.e. é $G_i/G_{i+1} \leq Z(G/G_{i+1})$ para todo i). Uma N-série é uma N_p-série se $G_i^p \leq G_{pi}$ para todo i.

Podemos associar um anel de Lie $L^*(G)$ a qualquer N_p-série (*) de um grupo G da seguinte forma:

Dado uma N_p-série (*), seja $L^*(G) = \oplus L_i^*$, onde $L_i^* = G_i/G_{i+1}$, escrito aditivamente. A comutação em G induz uma operação binária [,] em L. Para elementos homogêneos $xG_{i+1} \in L_i^*$ e $yG_{j+1} \in L_j^*$ a operação e definida por

$$[xG_{i+1}, yG_{j+1}] = [x, y]G_{i+j+1} \in L_{i+j}^*,$$

e estendida para elementos arbitrários de $L^*(G)$ por linearidade. Vamos verificar que essa operação está bem definida e que $L^*(G)$ com as operações $+$ e [,] e um anel de Lie sobre $\mathbb{F}_p$.

Proposição 3.21 *Com respeito às operações de $+$ e [,], o conjunto $L^*(G)$ é um anel de Lie.*

Demonstração. Primeiro vamos mostrar que [,] está bem definido, ou seja, independe da escolha dos seus elementos.

Suponha que $a^{'}G_{i+1} = aG_{i+1}$ e $b^{'}G_{i+1} = bG_{i+1}$, onde $a,\ a^{'},\ b,\ b^{'} \in G$, assuma também que $g_1 \in G_{i+1}$ e $g_2 \in G_{j+1}$ tal que $a^{'} = ag_1$ e $b^{'} = bg_2$,

$$[a^{'},b^{'}] = [ag_1,b^{'}] = [a,b^{'}][a,b^{'},g_1][g_1,b],$$

mas

$$[a,b^{'},g_1] \subseteq G_{i+j+1} \ \ e \ \ [g_1,b] \subseteq G_{i+j+1},$$

então

$$[a^{'},b^{'}] = [a,b^{'}]G_{i+j+1}.$$

Porém,

$$[a,b^{'}] = [a,bg_2] = [a,g_2][a,b][a,b,g_2]$$

logo, de modo análogo, teremos

$$[a,g_2] \subseteq G_{i+j+1} \ \ e \ \ [a,b,g_2] \subseteq G_{i+j+1}.$$

Então,

$$[a^{'},b^{'}] = [a,b^{'}]\ G_{i+j+1} \ = \ [a,b]G_{i+j+1}.$$

Portanto,

$$[a^{'},b^{'}]\ G_{i+j+1} \ = \ [a,b]G_{i+j+1}.$$

Agora resta mostrar que as operações satisfazem os axiomas de Lie. $a)$ $[a^{'},a^{'}] = 0$, pois:

$$\begin{aligned}
[a^{'},a^{'}] &= [aG_{i+1},aG_{i+1}] \\
&= [a,a]G_{2i+1} \\
&= 0.
\end{aligned}$$

$b)$ $[\overline{a},\overline{b},\overline{c}] + [\overline{b},\overline{c},\overline{a}] + [\overline{c},\overline{a},\overline{b}] = 0$, pois

$$\begin{aligned}
[\overline{a},\overline{b},\overline{c}] + [\overline{b},\overline{c},\overline{a}] + [\overline{c},\overline{a},\overline{b}] &= [aG_{i+1},bG_{j+1},cG_{k+1}] + [bG_{j+1},cG_{k+1},aG_{i+1}] \\
&\quad + [cG_{k+1},aG_{i+1},bG_{j+1}] \\
&= [a,b,c]G_{i+j+k+1} + [b,c,a]G_{i+j+k+1} + [c,a,b]G_{i+j+k+1} \\
&= [a,b,c][b,c,a][c,a,b]G_{i+j+k+1} \\
&= [a,b^{-1},c]^{-b}[b,c^{-1},a]^{-c}[c,a^{-1},b]^{-a}G_{i+j+k+1} \\
&= [c,b^{-1},b]^{-a}[b,c^{-1},a]^{-c}[a,b^{-1},c]^{-b}G_{i+j+k+1} \\
&= \left([a,b^{-1},c]^{b}[b,c^{-1},a]^{c}[c,a^{-1},b]^{a}\right)^{-1}G_{i+j+k+1}.
\end{aligned}$$

Pelo Lema 1.2 e),

$$[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a = 1.$$

Segue que

$$[\overline{a},\overline{b},\overline{c}] + [\overline{b},\overline{c},\overline{a}] + [\overline{c},\overline{a},\overline{b}] = 0.$$

Portanto, $L^*(G)$ é um anel de Lie. □

Para qualquer $x \in G_i/G_{i+1}$, denotamos x^* como o elemento xG_{i+1} de $L^*(G)$.

Lema 3.22 *(Lazard [15]). Se $(*)$ é uma N_p-série então $(adx^*)^p = ad(x^p)^*$ para qualquer $x \in G$. Consequentemente, se x tem ordem finita t, então x^* é ad-nilpotente de índice no máximo t.*

Seja Fr o grupo livre com geradores livres $x_1, x_2, \ldots, x_s$ em Fr. Dizemos que o grupo G satisfaz a identidade $w \equiv 1$ se $w(g_1, g_2, \ldots, g_s) = 1$ para quaisquer elementos $g_1, g_2, \ldots, g_s$ em G. A seguinte proposição pode ser extraída da demonstração do Teorema 1 no artigo de Wilson e Zelmanov [36].

Proposição 3.23 *Seja G um grupo satisfazendo uma identidade $w \equiv 1$. Então existe um polinômio de Lie f sobre $\mathbb{F}_p$ multilinear, diferente de zero, dependendo somente de p e w, tal que para qualquer N_p-série $(*)$ de G a álgebra $L^*(G)$ satisfaz a identidade $f \equiv 0$*

De fato, Wilson e Zelmanov [36], descreveram um algoritmo efetivo para escrever f explicitamente para qualquer p e w. Mas não vamos precisar desse algoritmo nesse trabalho.

Um grupo G pode ter muitas N_p-séries, em particular podemos observar pelo Teorema 3.18 que a série Jennings-Lazard-Zassenhaus $\{D_i\}$, definida anteriormente, é uma N_p-série. Associamos a G a álgebra de Lie $DL(G)$ sobre $\mathbb{F}_p$ correspondente a série de Jennings-Lazard-Zassenhaus, ou seja, $DL(G) = \oplus L_i$ com $L_i = D_j/D_{j+1}$, onde $D_i = D_i(G)$.

Se A age sobre o grupo G, A induz um grupo de automorfismo de todo quociente D_j/D_{j+1}. Essa ação estende-se para a soma direta $\oplus D_j/D_{j+1}$. Assim, A pode ser visto como um grupo agindo sobre a subálgebra $L_p(G) = \langle L_1 \rangle$ de $DL(G)$ gerada por L_1, como automorfismo de álgebras de Lie.

Proposição 3.24 *Seja G um grupo gerado pelos elementos $a_1, a_2, \ldots, a_m$ e assuma que $L_p(G)$ é nilpotente de classe no máximo c. Seja $\rho_1, \rho_2, \ldots, \rho_s$, a lista de todos os comutadores simples nos geradores $a_1, a_2, \ldots, a_m$ de peso $\leq c$. Então, para qualquer inteiro não negativo i, o grupo G pode ser escrito como um produto:*

$$G = \langle \rho_1 \rangle \langle \rho_2 \rangle \cdots \langle \rho_s \rangle D_{i+1},$$

dos subgrupos cíclicos gerados por $\rho_1, \rho_2, \ldots, \rho_s$ *e* D_{i+1}.

Demonstração. Primeiramente observamos que para qualquer inteiro i o subgrupo D_i é gerado por D_{i+1} e elementos da forma $[b_1, \ldots, b_j]^{p^k}$, onde $jp^k \geq i$ e $b_1, \ldots, b_j \in \{a_1, a_2, \ldots, a_m\}$. Essa observação pode ser demonstrada usando o Lema 3.13 e a Identidade de Witt. Para demonstrar a proposição usamos indução sobre i. O caso $i = 0$ é trivial. Assuma que $i \geq 1$ e

$$G = \langle \rho_1 \rangle \langle \rho_2 \rangle \cdots \langle \rho_s \rangle D_i.$$

Então qualquer elemento $x \in G$ pode ser escrito na forma:

$$x = \rho_1^{\alpha_1} \rho_2^{\alpha_2} \ldots \rho_s^{\alpha_s} y,$$

onde $y \in D_i$. Sem perda de generalidade podemos assumir que $D_{i+1} = 1$. Pela observação feita no primeiro parágrafo podemos escrever:

$$y = (\sigma_1^{p^{k_1}})^{\beta_1} (\sigma_2^{p^{k_2}})^{\beta_2} \ldots (\sigma_t^{p^{k_t}})^{\beta_t},$$

onde cada σ_n é da forma $[b_1, \ldots, b_j]$, com $jp^{k_n} \geq i$ e $b_1, \ldots, b_j \in \{a_1, a_2, \ldots, a_m\}$.

Denote $a_l D_2 \in L_p(G)$ por $\overline{a}_l$, $l = 1, \ldots, m$. Por hipótese $L_p(G)$ é nilpotente de classe c, logo $[\overline{b_1}, \ldots, \overline{b_{c+1}}] = 0$, para quaisquer $b_1, \ldots, b_{c+1} \in \{a_1, a_2, \ldots, a_m\}$. Isso implica que $[b_1, \ldots, b_{c+1}] \in D_{c+2}$ para quaisquer $b_1, \ldots, b_{c+1} \in \{a_1, a_2, \ldots, a_m\}$ e $\gamma_{c+1} \leq D_{c+2}$. Então como $\{D_i\}$ é uma N_p-série, para qualquer $d \geq c+1$ temos $\gamma_d \leq D_{d+1}$.

Agora, se σ_n é da forma $[b_1, \ldots, b_j]$ com $j \geq c+1$, então

$$\sigma_n^{p^{k_n}} \in \gamma_j^{p^{k_n}} \leq D_{j+1}^{p^{k_n}} \leq D_{(j+1)p^{k_n}} \leq D_{i+1} = 1.$$

Portanto, podemos assumir que cada σ_n é da forma $[b_1, \ldots, b_j]$ com $j \leq c$, e nesse caso σ_n pertence a lista $\rho_1, \rho_2, \ldots, \rho_s$.

Novamente, pelo fato de $\{D_i\}$ ser uma N_p-série, temos que $\sigma_n^{p^{k_n}} \in Z(G)$. Agora, comparando a maneira que escrevemos x e y, obtemos que:

$$x \in \langle \rho_1 \rangle \langle \rho_2 \rangle \ldots \langle \rho_s \rangle,$$

como queríamos. □

Lema 3.25 *Suponha que G é um p-grupo finito d-gerado tal que a álgebra de Lie* $L_p(G)$ *é nilpotente de classe c. Então, G tem um subgrupo potente característico de índice* $\{p, c, d\}$*-limitado.*

Demonstração. Sejam $\rho_1, \rho_2, \ldots, \rho_s$ todos os comutadores simples de peso $\geq c$ nos geradores de G. Aqui s é um número $\{c,d\}$-limitado. Como G é um p-grupo finito e a classe de nilpotência de $L_p(G)$ é c, pela proposição anterior, temos que todo elemento $g \in G$ pode ser escrito da forma $g = \rho_1^{k1} \cdot \rho_2^{k2} \cdot \cdots \rho_s^{ks}$. Portanto, $\mid G/G^{p^m} \mid \leq p^{sm}$ para qualquer número natural m. Seja V a interseção dos núcleos de todos os homomorfismos de P em $GL_s(\mathbb{F}_p)$. Faça $W = V$ se $p \neq 2$, ou $W = V^2$ se $p = 2$. O expoente do p-subgrupo de Sylow de $GL_s(\mathbb{F}_p)$ é um número $\{p,s\}$-limitado. Então $G^{p^a} \leq W$ para algum número $\{p,s\}$-limitado a que também é $\{p,c,d\}$-limitado, pois s é $\{c,d\}$-limitado. Existe um número $u \geq a$ $\{p,c,d\}$-limitado tal que $\mid G^{p^u}/G^{p^{u+r}} \mid \leq p^s$. Por outro lado, a desigualdade $\mid G/G^{p^m} \mid \leq p^{sm}$ será falsa para algum m. Então $G^{p^u} \leq G^{p^a} \leq W$ e G^{p^u} é um grupo potente. O índice de G^{p^u} é no máximo p^{us} e portanto é $\{p,c,d\}$-limitado. □

O seguinte resultado foi obtido por Riley [22] e pode ser deduzido utilizando o Lema 3.25 em conjunto com o Teorema 1.33.

Lema 3.26 *Suponha que G é um p-grupo finito d-gerado tal que a álgebra de Lie $L_p(G)$ é nilpotente de classe c. Então o posto de G é $\{p,c,d\}$-limitado.*

Seja H um subgrupo de um grupo G. Denotamos por $L(G,H)$ o subconjunto de $DL(G)$ gerado pelos elementos homogêneos da forma hD_{j+1}, onde $h \in D_j \cap H$. Temos que $L(G,H)$ é uma subálgebra de $DL(G)$. Além disso, $L(G,H)$ é isomorfo à álgebra de Lie associada com a N_p-série $\{H_i\}$ de H com $H_i = D_i \cap H$. Da mesma forma, temos ainda que $L_p(G,H) = L_p(G) \cap L(G,H)$. Pelo Lema 1.19, se G é um grupo finito e se A é de ordem coprima com G, então $L_p(G, C_G(A)) = C_{L_p(G)}(A))$.

O lema seguinte é retirado de [14].

Lema 3.27 *Suponha que L é uma álgebra de Lie, H uma subálgebra de L gerada por r elementos $h_1, h_2, \ldots, h_r$ tal que todos os comutadores em h_i são ad-nilpotentes em L. Se H é nilpotente, então para algum número v, temos: $[L, \underbrace{H, H, \ldots, H}_{v}] = 0$.*

Lema 3.28 *Suponha que qualquer comutador de Lie em elementos homogêneos $x_1, x_2, \ldots, x_r$ de $DL(G)$ é ad-nilpotente de índice no máximo t. Seja $K = \langle x_1, x_2, \ldots, x_r \rangle$ e assuma que $K \leq L(G,H)$ para algum subgrupo H de G satisfazendo a identidade $w \equiv 1$. Então para algum número u, $\{r,t,w,p\}$-limitado, temos que $[DL(G), \underbrace{K, \ldots, K}_{u}] = 0$.*

Demonstração. Em vista do Lema 3.27 é suficiente mostrar que K tem classe de nilpotência $\{r,t,w,p\}$-limitada. Sabemos pela Proposição 3.23 que K satisfaz certa identidade polinomial multilinear dependendo somente de w. Assim, o Teorema 3.11

mostra que K tem classe de nilpotência $\{r,t,w,p\}$-limitada. □

Existe uma outra maneira de associar um anel de Lie para um grupo, que inclusive de um modo geral é mais simples do que a que apresentamos acima, utilizando quocientes da série central inferior de G e pode ser encontrada em ([30], p.27). Optamos em apresentar apenas a técnica acima, pois é a que utilizaremos no nosso trabalho.

Agora seja L uma álgebra de Lie sobre um corpo k. Além da Definição 3.10, podemos dizer que um elemento $a \in L$ é chamado de ad-nilpotente se o correspondente operador adjunto $ad\ a$ de L é nilpotente. Seja $X \subseteq L$ qualquer subconjunto de L. Para um comutador em elementos de X, dizemos que qualquer elemento de L pode ser obtido por meio de repetição da operação de comutação envolvendo elementos de X com um sistema arbitrário de colchetes. Denote por F a álgebra de Lie livre sobre k de enumeráveis geradores livres $x_1, x_2, \ldots$ e seja $f = f(x_1, x_2, \ldots, x_n)$ um elemento não-nulo de F.

Os dois teoremas que seguem são demonstrados em ([9] e [34]) respectivamente, e serão fundamentais para o desenvolvimento desse trabalho.

Teorema 3.29 *Um grupo periódico compacto G não pode ter p_i-subgrupos de Sylow não triviais para uma quantidade infinita de diferentes primos p_i.*

Teorema 3.30 *Seja G um grupo periódico, compacto e Hausdorff. Então G possui uma série finita*

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G.$$

de subgrupos característicos fechados, em que cada fator G_i/G_{i-1} é
a) um grupo pro-p para algum primo p, ou
b) isomorfo ao produto cartesiano de grupos finitos simples.

Um grupo analítico p-ádico é uma variedade analítica p-ádica que é também um grupo, onde as operações são dadas por funções analíticas. Os grupos analíticos p-ádicos foram estudado primeiramente por Lazard em 1965 e recentemente (1987) por Lubotzky e Mann.

Dizemos que um grupo pro-p é ***potente***, se H/H^p é abeliano, onde H^p denota o subgrupo fechado gerado pela p-ésima potência de H (se p = 2, H^2 deve ser substituído por H^4.

De fato, Lazard mostrou que um grupo pro-p G é p-ádico analítico se, e somente se, é finitamente gerado (como um grupo topológico) e possue um subgrupo aberto potente H (necessariamente de índice finito). De acordo por Lubotzky e Mann é equivalente a G ter rank finito, onde o rank de um pro-p grupo é o menor inteiro r (possivelmente infinito), tal que todo subgrupo fechado (equivalentemente aberto) de G pode ser gerado por r elementos.

Teorema 3.31 *Seja G um grupo pro-p finitamente gerado. Se $L_p(G)$ é nilpotente, então G é um grupo analítico p-ádico.*

Demonstração. Esse resultado pode ser encontrado em [15]. □

Sejam $x \in G$ e $i = i(x)$ o maior inteiro tal que $x \in D_i$. Denotemos por $\widetilde{x}$ o elemento $xD_{i+1} \in L(G)$. Temos uma condição suficiente para $\widetilde{x}$ ser ad-nilpotente.

Seja H um subgrupo de G e $g_1, g_2, \ldots, g_n \in G$. Seja $w = w(x_1, x_2, \ldots, x_n)$ sendo um elemento não-trivial do grupo livre de geradores livres $x_1, x_2, \ldots, x_n$. Seguindo [36], dizemos que a lei $w \equiv 1$ é satisfeita sobre as classes $g_1H, g_2H, \ldots, g_nH$, se $w(g_1h_1, g_2h_2, \ldots, g_nh_n) = 1$, para todo $h_1, h_2, \ldots, h_n \in H$. Em [36] Wilson e Zelmanov provaram o seguinte teorema.

Teorema 3.32 *Se G tem um subgrupo aberto H e elementos $a_1, a_2, \ldots, a_n$ tais que a lei $w \equiv 1$ é satisfeita sobre as classes $a_1H, a_2H, \ldots, a_nH$, então a álgebra de Lie $L_p(G)$ é PI.*

CAPÍTULO 4

Automorfismos Coprimos de Grupos Profinitos

O nosso objetivo até o momento foi encontrar ferramentas que pudessem ser utilizadas no desenvolvimento deste trabalho relacionando Grupos Profinitos e Automorfismos Coprimos, a fim de provarmos o seguinte teorema devido a Shumyatsky [27]:

Teorema 2 *Sejam q um número primo, A um grupo abeliano elementar de ordem q^2. Suponha que A age como um grupo de automorfismos coprimos de um grupo profinito G. Assuma que $C_G(a)$ é periódico para cada $a \in A^\sharp$. Então G é localmente finito.*

Com esse objetivo, apresentamos os seguintes lemas:

Lema 4.1 *Seja G um grupo profinito periódico. Então existe um subgrupo aberto $H \leq G$ e uma classe gH tal que, para algum $n \in \mathbb{N}$, a lei $x^n \equiv 1$ é satisfeita sobre a classe gH.*

Demonstração. Para cada $i \in \mathbb{N}$, denotemos X_i como o conjunto de todos os elementos de G de ordem i. Então, cada conjunto X_i é fechado e G é a união dos X_i. Segue do Teorema de Categoria de Baire ([13], p. 200) que alguns conjuntos X_i não têm interior vazio e, portanto, contém uma classe gH do tipo exigido. □

Uma observação importante é que o Lema 2.27 a) tem implicações importantes no contexto das álgebras de Lie associadas. Seja G um grupo pro-p com um automorfismo coprimo a. Obviamente a induz um automorfismo ao quociente D_j/D_{j+1}. Esta ação estende-se à soma direta $\oplus D_j/D_{j+1}$. Assim, a pode ser visto como um automorfismo agindo em $L(G)$ $\big($e sobre $L_p(G)\big)$. Seja $C_j = D_j \cap C_G(a)$. Então o Lema 2.27 a) mostra que

$$C_{L(G)}(a) = \oplus C_j D_{j+1}/D_{j+1}.$$

Assim, as propriedades de $C_{L(G)}(a)$ estão muito relacionadas com os de $C_G(a)$. Em particular, modificando a prova do Teorema 3.32 pode-se mostrar que se $C_G(a)$ tem uma certa classe de identidade, então $C_{L(G)}(a)$ é PI (ver também [26], Proposição 2.7). Combinando isso com o Lema 4.1, Shumyatsky [**?**] pôde estabelecer o seguinte resultado.

Lema 4.2 *Seja a um automorfismo coprimo de um pro-p grupo G. Se o $C_G(a)$ é periódico, então $C_G(a)$ é PI.*

No intuito de demonstrarmos o Teorema 2, reduziremos ao caso pro-p.

Proposição 3 *Sejam q um número primo, A um grupo abeliano elementar de ordem q^2. Suponha que A age como um grupo de automorfismos coprimos sobre um grupo pro-p de G e que $C_G(a)$ é periódico para cada $a \in A^\sharp$. Então G é localmente finito.*

Demonstração. Podemos assumir que G é finitamente gerado, digamos por m elementos, pois todo subconjunto finito de G está contido em um subgrupo fechado finitamente gerado A-invariante. Então, será suficiente mostrar que G é finito.

Sejam $A_1, A_2, \ldots, A_{q+1}$ os subgrupos cíclicos distintos de A. Sejam $D_j = D_j(G)$, $L = L_p(G)$, $L_j = L \cap D_j/D_{j+1}$, de modo que $L = \oplus L_j$. Seja $L_{ij} = C_{L_j}(A_i)$. Então, pelo Lema 2.27 c), para qualquer j, temos:

$$L_j = \sum_{1 \leq i \leq q+1} L_{ij}.$$

Pelo Lema 2.27 a), para qualquer $l \in L_{ij}$, existe $x \in D_j \cap C_G(A_i)$ tal que $l = xD_{j+1}$. Como por hipótese x é de ordem finita, do Lema 3.22, segue que l é ad-nilpotente. Assim,

$$qualquer\ \ elemento\ \ em\ \ L_{ij}\ \ é\ \ ad-nilpotente. \tag{4-1}$$

Como G é gerado por m elementos, o $\mathbb{F}_p$-espaço L_1 é gerado por m elementos. Em particular, L é gerado por no máximo m elementos ad-nilpotentes, de cada L_{i1} para algum i. Mas não podemos afirmar que todo comutador de Lie destes geradores estão novamente em algum L_{ij} e, portanto, não podemos afirmar que esses comutadores podem ser ad-nilpotente.

Para superar esta dificuldade, estendemos o corpo base $\mathbb{F}_p$ por uma raiz primitiva da unidade ω, formando $\overline{L} = L \otimes \mathbb{F}_p[\omega]$. A idéia é mostrar que $\overline{L}$ é nilpotente, o que implica L nilpotente, pois é natural identificarmos L com a $\mathbb{F}_p$-subálgebra $L \otimes 1$ de $\overline{L}$. Note que se um elemento $x \in L$ é ad-nilpotente, então o elemento semelhantemente $x \otimes 1$ é ad-nilpotente em $\overline{L}$.

Coloque $\overline{L_j} = L_j \otimes \mathbb{F}_p[\omega]$. Então $\overline{L} = \langle \overline{L_1} \rangle$, uma vez que $L = \langle L_1 \rangle$ e $\overline{L}$ é a soma direta das componentes homogêneas $\overline{L_j}$. Desde que o $\mathbb{F}_p$-espaço L_1 é gerado por m elementos, assim $\mathbb{F}_p[\omega]$-espaço $\overline{L_1}$ também o é.

O grupo A age naturalmente em $\overline{L}$ e temos $\overline{L_{ij}} = C_{\overline{L_j}}(A_i)$, onde $\overline{L_{ij}} = L_{ij} \otimes \mathbb{F}_p[\omega]$.

Mostraremos que

$$qualquer\ \ elemento\ \ y\ \in\ \overline{L_{ij}}\ \ é\ \ ad-nilpotente. \tag{4-2}$$

Seja $y \in \overline{L_{ij}} = L_{ij} \otimes \mathbb{F}_p[\omega]$. Podemos escrever

$$y = x_0 + \omega x_1 + \omega^2 x_2 + \cdots + \omega^{q-2} x_{q-2},$$

para algum $x_s \in L_{ij}$, $0 \leqslant s \leqslant q-2$, onde cada somando $\omega^s x_s$ é ad-nilpotente por (4-1). Seja $H = \langle x_0, \omega x_1, \ldots, \omega^{q-2} x_{q-2} \rangle$. Note que $H \subseteq C_{\overline{L}}(A_i)$, uma vez que $\omega^s x_s \in C_{\overline{L}}(A_i)$, para todo s. Um comutador de peso k em $\omega^s x_s$ tem a forma $\omega^t x$ para algum $x \in L_{in}$, onde $n = kj$. Por (4-1) temos que x é ad-nilpotente e, portanto, $\omega^t x$ também o é.

Além disso, o Lema 4.2 nos diz que $C_L(A_i)$ é PI. Como $C_{\overline{L}}(A_i) = C_L(A_i) \otimes \mathbb{F}_p[\omega]$. Temos então que $H \subseteq C_{\overline{L}}(A_i)$, onde H é PI. Assim, pelo Teorema 3.11, H é nilpotente. Deduzimos do Lema 3.27 que $[L, \underbrace{H, H, \ldots, H}_{v}] = 0$, para algum número v. Isto estabelece (4-2).

Como A é abeliano, e o corpo base é agora um corpo de decomposição de A, todo L_j decompõe-se em soma direta de auto espaços comuns de A. Em particular, $\overline{L_1}$ é gerado por autovetores comuns de A, e que exige no máximo m deles para abranger $\overline{L_1}$. Daí $\overline{L}$ é gerado por m autovetores comuns A de $\overline{L_1}$. Todo autoespaço comum está contido no centralizador $C_{\overline{L}}(A_i)$ para algum $1 \leq i \leq q+1$, uma vez que A é não-cíclico. Note que qualquer comutador de autovetores comuns é novamente um autovetor comum. A principal vantagem de estender nosso corpo base agora se torna clara: se $l_1, l_2, \ldots, l_m \in \overline{L_1}$ são autovetores comuns de A gerando $\overline{L}$, então qualquer comutador destes geradores pertence a algum $\overline{L_{ij}}$ e portanto, por (4-2), é ad-nilpotente. Sabemos que $C_{\overline{L}}(A_i)$ também é PI. Assim, pelo Teorema 3.12, $\overline{L}$ também é PI. Agora, o Teorema 3.11 mostra que $\overline{L}$ (daí L) é nilpotente.

Assim, pelo Teorema 3.31, G é um grupo analítico p-ádico . Neste caso, G possui um subgrupo potente aberto característico P ([12], Capítulo 3). O subgrupo P é novamente finitamente gerado e assim os elementos de ordem finita de P formam um subgrupo finito ([12], Teorema 4.20). Sabemos pelo Lema 2.27 c) que $P = \langle C_P(a) \mid a \in A^{\#} \rangle$. Por hipótese, os centralizadores $C_G(a)$ são periódicos e concluímos que P é finito. E segue o resultado. □

Finalmente passamos à demonstração do Teorema 2

Teorema 2 *Sejam q um número primo, A um grupo abeliano elementar de ordem q^2. Suponha que A age como um grupo de automorfismos coprimos de um grupo profinito G*

e que $C_G(a)$ é periódico para cada $a \in A^{\#}$. Então G é localmente finito.

Demonstração. Seja $\pi = \pi(G)$ o conjunto dos números primos p, tais que G possua um p-subgrupo de Sylow não trivial e escolha $p \in \pi$. Pelo Lema 2.27 b), G possui um p-subgrupo de Sylow A-invariante P. Aplicando agora o Lema 2.27 c), concluímos que $p \in \pi(C_G(a))$ para todo $a \in A^{\#}$. Portanto, π é a união de $\pi(C_G(a))$, onde a percorre todo $A^{\#}$. De acordo com o Teorema 3.29, Herfort mostrou que o conjunto de primos divisores da ordem dos elementos de um grupo profinito periódico tal que G possua um p-subgrupo de Sylow não trivial é finito. Por isso, cada conjunto $\pi(C_G(a))$ é finito e assim π também será. Suponha $\pi = \{p_1, p_2, \ldots, p_n\}$. Seja x um elemento arbitrário de G e seja $\langle x \rangle$ o subgrupo procíclico gerado por x. Escreva $\langle x \rangle = S_1 \cdot S_2 \cdot \cdots \cdot S_n$, onde S_i denota um p_i-subgrupo de Sylow de $\langle x \rangle$. Para cada $i \leq n$, escolha um p_i-subgrupo de Sylow A-invariante P_i de G. Pela Proposição 3 cada P_i é localmente finito. Notamos que cada S_i é isomorfo a um subgrupo procíclico de P_i, logo cada S_i é finito e portanto $\langle x \rangle$ é finito. Assim, x tem ordem finita. Como escolhemos x em G arbitrariamente, podemos concluir que G é periódico. No Teorema 3.30, Wilson mostrou que se todos os subgrupos de Sylow de um grupo profinito periódico são localmente finitos, então o grupo é localmente finito. Daqui temos que G é localmente finito. Portanto a prova está completa. □

Referências Bibliográficas

[1] BAHTURIN, Y. A; ZAICEV, M. V. **Identities of Graded Algebras**. J. Algebra 205 , 1-12, 1998.

[2] BURNSIDE, W. **Theory of Groups**. 2nd edition, New York, 1955.

[3] DUMMIT, D. S; FOOTE, R. M. **Abstract algebra**. University of Vermont, 1999.

[4] GARCIA, A; LEQUAIN, Y. **Elementos de Álgebra**. IMPA, Rio de Janeiro, 2008.

[5] GORENSTEIN, D. **Finite Groups**. Evanston, London: Harper & Row, New York, 1968.

[6] GORESTEIN, D. **An Introduction to Their Classification**. Plenun Press, New York, 1982.

[7] HALL, P. **A Contribution to the theory of groups of prime power order**. Proc. London Math. Soc..36, 29-95, 1933.

[8] HALL, P. **Some sufficient conditions for a group to be nilpotent**. Illinois J. Math., 2, 787-801, 1958.

[9] HERFORT, W. **Compact Torsion Groups and Finite Exponent**. Arch Math 33. 404-410, 1979.

[10] HIGMAN, G. **Groups and Lie Rings Having Automorphisms Without Non-Trivial Fixed Points**. J. London Math. Soc., 32, 321-334, 1957.

[11] HUPPERT, B; BLACKBURN, N. **Finite Groups II**. Springer, Berlin, 1982.

[12] J. D. DIXON, M P. F. DU SAUTOY, A. M; SEGAL, D. **Analytic Pro-p Groups**. Cambridge University Press, Cambridge, 1991.

[13] KELLEY, J. L. **General Topology**. Van Nostrand, Toronto, 1995.

[14] KHUKHRO, E. I; SHUMYATSKY, P. **Bounding the Exponent of a Finite Group with Automorphisms**. J. Algebra 212. 363-374, 1999.

[15] LAZARD, M. **Groupes Analytiques p-Adiques**. Publications Mathématiques 26 IHES, Paris. 57-66, 1965.

[16] LIMA, A. S. **Sobre Centralizadores de Automorfismos Coprimos em Grupos Profinitos**. Tese de Doutorado, Universidade de Brasília-DF., 2009.

[17] LIMA, A. S; SHUMYATSKY, P. **On groups satisfying a positive law in fixed points**. J. Algebra 322, pp. 245–253, 2009.

[18] LIMA, E. L. **Elementos de Topologia Geral**. 2.ed. Livros Técnicos e Científicos Editora S/A, Rio de Janeiro, 1976.

[19] LINCHENKO, V. **Identities of Lie Algebras with Action of Hopf Algebras**. Comm. Algebra 25. 3179-3187, 1997.

[20] LIPSCHUTZ, S. **Topologia Geral**. McGraw-Hill do Brasil, São Paulo, 1973.

[21] RIBES, L; ZALESSKII, P. **Profinite Groups**. Springer-Berlim, 2000.

[22] RILEY, D. M. **Analytic Pro-p Groups and their Graded Groups Rings**. J. Pure Appl. Algebra 90. 69-76, 1993.

[23] ROTMAN, J. J. **An Introduction to the Theory of Groups**. 4.ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[24] SAN MARTIN, L. A. B. **Álgebras de Lie**. Campinas, Editora da Unicamp, São Paulo, 1999.

[25] SHUMYATSKY, P. **Centralizers in Groups with Finiteness Conditions**. J. Group Theory 1. 275-282, 1998.

[26] SHUMYATSKY, P. **Aplication of Lie Ring Methods to Group Theory**. Nonassociative Algebra and Its Applications, (Eds R. Costa et al.) Marcel Dekker, New York. 373-395, 2000.

[27] SHUMYATSKY, P. **Coprime Automorphisms of Profinite Groups**. Quart. J. Math., 53, 371-376, 2002.

[28] SHUMYATSKY, P. **Positive Laws in Fixed Points**. Trans. Amer. Math. Soc. 356 (5) 2081-2091, 2004.

[29] SHUMYATSKY, P. **Positive Laws in Derived Subgroups of Fixed Points**. Q. J. Math., 2008.

[30] SHUMYATSKY, P. **On finite Nilpotent Groups Having Fixed Point Free Automorphisms**. Department of Mathematics University of Brasília, Brasília-DF, 1996.

[31] SILVA, J. C. **Álgebras de Lie de Derivações Livres de Constanstes**. Dissertação de Mestrado UNB, 2004.

[32] SILVA, J. C. **Variedades de Grupos e Generalizações Verbais para o Problema Restrito de Burniside**. Tese de Doutorado, Universidade de Brasília-DF., 2009.

[33] THOMPSON, J. G. **Finite Groups With Fixed-Point-Free Automorphisms of Prime Order**. Proc. Nat. Acad. Sci. USA, 45, 578-581, 1959.

[34] WILSON, J. S. **On the Structure of Compact Torsion Groups**. Monatshefte fur Mathematik 96. 57-66, 1983.

[35] WILSON, J. S. **Profinite Groups**. Claredon Press, Oxford, 1998.

[36] WILSON, J. S; ZELMANOV, E. **Identities for Lie Algebras of Pro-p Groups**. J. Pure Appl. Algebra 81. 103-109, 1992.

[37] ZELMANOV, E. **Nil Rings and Periodic Groups**. Lecture Notes in Mathematics, Korean Mathematical Society, Seoul, 1992.

[38] ZELMANOV, E. **On Periodic Compact Groups**. Israel J. Math 77. 83-95, 1992.