Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Variedades de p-Grupos sem Base Finita

por

Jorge Augusto Gonçalo de Brito

Brasília
2008

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Variedades de p-Grupos sem Base Finita

por

Jorge Augusto Gonçalo de Brito*

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

MESTRE EM MATEMÁTICA

Brasília, 29 de fevereiro de 2008.

Comissão Examinadora:

Prof. Dr. Alexei Krassilnikov - UnB (Orientador)

Prof. Dr. Pavel Shumyatsky - UnB

Prof. Dr. Plamen E. Koshlukov - Unicamp

*O autor foi bolsista CNPq durante a elaboração deste trabalho.

Agradecimentos

-Agradeço primeiramente a Deus por mais essa conquista e pela oportunidade diária de aprendizado que é a dádiva da vida.

-Aos meus pais (Juvenal e Francisca) e às minhas irmãs pelo apoio e incentivo.

-Ao professor Dr. Alexei Krassilnikov, pela orientação, paciência e por sua suma importância nessa minha busca pela construção do conhecimento.

-Ao CNPq pelo suporte financeiro.

-Aos professores Dr. Pavel Shumyatsky, Dr. Plamen E. Koshlukov e Dr. Rudolf R. Maier por participarem da banca examinadora.

-Aos professores e funcionários do Dmat que me acompanharam e ajudaram durante essa caminhada de dois anos.

-Aos meus professores da UFG/CAJ em Jataí que colaboraram em minha formação inicial como professor de matemática.

-Aos meus amigos de Jataí pelo incentivo e apoio que me deram para seguir este difícil caminho.

- Por fim agradeço a todos os amigos e a todos que torceram por mim. Peço desculpas e a compreensão destes, pois, embora alguns realmente merecessem, optei por não explicitar seus nomes. Obrigado a todos.

"Preocupe-se mais com a sua consciência do que com sua reputação. Porque sua consciência é o que você é, e a sua reputação é o que os outros pensam de você. E o que os outros pensam, é problema deles."

—

Resumo

Seja $F = F(X)$ o grupo livre com base $X = \{x_1, x_2, \ldots\}$. Para cada $v = v(x_1, \ldots, x_n) \in F$, a expressão $v \equiv 1$ é dita uma *identidade* ou uma *lei* em um grupo G se $v(g_1, \ldots, g_n) = 1$ para todos $g_1, \ldots, g_n \in G$. A classe de grupos satisfazendo todas as identidades de um conjunto V é chamada *variedade de grupos*. Denotaremos esta variedade por $\mathbf{V}$ e chamaremos o conjunto V de *base de identidades* desta variedade. Um problema que ganhou importância no estudo de variedades de grupos é o seguinte: uma dada variedade de grupos $\mathbf{V}$ tem base finita de identidades?

Nesta dissertação estudaremos este problema para certas variedades, ela está dividida em quatro capítulos. Faremos dois capítulos iniciais de preliminares, sobre grupos e variedades de grupos. Já nos capítulos finais falaremos sobre duas variedades de grupos que não possuem base finita de identidades. A primeira destas é uma variedade solúvel de expoente p^2. A segunda variedade consiste de todos os grupos que são extensões de um grupo de expoente p^2 por um grupo de expoente p. A questão da inexistência de base finita para esta variedade generaliza, de forma natural, um problema bem conhecido proposto por Hanna Neumann [14]. Nos basearemos no trabalho de Gupta e Krassilnikov [5] e no trabalho de Kleiman [10].

Palavras-chave: Variedades de grupos, identidades em grupos, base finita de identidades.

Abstract

Let $F = F(X)$ be the free group with a basis $X = \{x_1, x_2, \ldots\}$. For any $v = v(x_1, \ldots, x_n) \in F$, the expression $v \equiv 1$ is said to be an *identity* or a *law* of a group G if $v(g_1, \ldots, g_n) = 1$ for all $g_1, \ldots, g_n \in G$. The class of groups satisfying all the identities of a set V is called a *variety of groups*. We denote this variety by $\mathbf{V}$ and we call the set V a *basis of identities* of this variety. One of the important problems in the study of varieties of groups is the following: a given variety of groups $\mathbf{V}$ is finitely based?

In this dissertation we study the problem above for certain varieties. The dissertation is divided in four chapters. The two initial chapters contain preliminaries on groups and varieties of groups. In the final chapters we will talk about two varieties of groups that have no finite basis of identities. The first variety is a soluble variety of exponent p^2. The second variety consists of all groups that are extensions of a group of exponent p^2 by a group of exponent p. The question of inexistence of finite basis for the latter variety generalizes, in a natural way, a well-known problem proposed by Hanna Neumann [14]. This dissertation is based on the work of Gupta and Krassilnikov [5] and on the work of Kleiman [10].

Keywords: Varieties of groups, identities in groups, finite basis of identities.

Sumário

Introdução

A teoria de identidades de grupos e variedades de grupos é uma importante sub-área da álgebra contemporânea. Ela ganhou importância em 1937, quando B. H. Neumann fez a seguinte pergunta:

Toda variedade de grupos pode ser definida por um conjunto finito de identidades?

A pergunta que parece muito natural ficou sem resposta até 1970, quando Olshanskii [15] provou a existência de variedades de grupos sem base finita. No mesmo ano Adyan [1] e Vaughan-Lee [20] exibiram explicitamente sistemas de identidades que não são equivalentes a nenhum conjunto finito de identidades.

Para entender o que é uma variedade de grupos primeiramente definamos uma identidade em um grupo. Sejam $F(X)$ o grupo livre com base $X = \{x_1, x_2, \ldots\}$ e $u = u(x_1, \ldots, x_n)$ um elemento de $F(X)$. Dizemos que a expressão $u \equiv 1$, ou simplesmente o elemento u, é uma *identidade* em um grupo G, se $u(g_1, \ldots, g_n) = 1$ para todos $g_1, \ldots, g_n \in G$. A classe de grupos satisfazendo todas as identidades de um conjunto V é chamada *variedade de grupos*. Denotaremos esta variedade por $\mathbf{V}$. Nesta situação o conjunto V, que define a variedade $\mathbf{V}$, é dito uma *base de identidades* para esta variedade.

Por exemplo, a classe de todos os grupos satisfazendo a identidade $[x, y] \equiv 1$, é a variedade $\mathbf{A}$ dos grupos abelianos. Já a classe de todos os grupos de expoente dividindo n, isto é, dos grupos que satisfazem a identidade $x^n \equiv 1$, é chamada de variedade de Burnside de expoente n, e denotada por $\mathbf{B}_n$. Outros exemplos de variedades são a variedade $\mathbf{N}_c$ dos grupos nilpotentes de classe menor que ou igual a c, a variedade $\mathbf{A}_n$ dos grupos abelianos de expoente dividindo n e a variedade $\mathbf{N}_{c,n}$ dos grupos nilpotentes de classe no máximo c e expoente dividindo n.

Sejam $\mathbf{U}$ e $\mathbf{V}$ duas variedades de grupos. Definimos a variedade produto, denotada $\mathbf{UV}$, como a classe de todos grupos G, tais que existe $N \triangleleft G$, com $N \in \mathbf{U}$ e $G/N \in \mathbf{V}$. É fácil verificar

que este produto é associativo. Um exemplo de variedade produto é a variedade dos grupos solúveis de comprimento derivado no máximo n, que é a variedade $\mathbf{A}^n = \underbrace{\mathbf{A}\ldots\mathbf{A}}_{n}$, produto de n variedades de grupos abelianos.

Dizemos que uma variedade tem base finita se ela pode ser definida por um conjunto finito de identidades. É fácil verificar que as variedades $\mathbf{B}_2\mathbf{B}_s$ e $\mathbf{B}_3\mathbf{B}_s$ tem base finita. Estas variedades têm bases de identidades, respectivamente,

$$\{x^{2s}, [x^s, y^s]\} \text{ e } \{(x^s y^s z^s)^3, [x^s, y^s, z^s, t^s]\},$$

vide Hanna Neumann [14]. Além disso $\{(x^s y^s)^r\}$ é uma base para a variedade $\mathbf{B}_r\mathbf{B}_s$, desde que r e s sejam coprimos. No mesmo livro Hanna Neumann [14] fez a seguinte pergunta: A variedade $\mathbf{B}_4\mathbf{B}_2$ tem base finita?

Este problema foi resolvido em 1973 quando R. M. Bryant [3] e Ju. G. Kleiman [10] provaram independentemente e simultaneamente que esta variedade não tem base finita. A generalização natural deste fato, isto é, o fato que a variedade $\mathbf{B}_{p^2}\mathbf{B}_p$ não tem base finita, para todo primo p, foi provada por Ju. G. Kleiman [10] e será assunto do capítulo 4 desta dissertação.

Desta forma temos um exemplo de uma variedade de expoente p^3 que não tem base finita. Por outro lado, em 1991, Olshanskii [16] provou que, para todo primo p suficientemente grande ($p > 10^{10}$), existe uma subvariedade de $\mathbf{B}_p\mathbf{B}_p$ sem base finita. Esta subvariedade não é solúvel e tem expoente p^2. Esta questão ficou em aberto para primos "pequenos".

Em 1993 M. F. Neumann perguntou se para todo primo impar existe uma variedade de expoente p^2 sem base finita. Em 1996 Gupta e Krassilnikov [5] deram resposta positiva à esta pergunta . Na verdade provaram algo ainda mais forte, que para todo primo impar existe uma subvariedade metanilpotente de $\mathbf{B}_p\mathbf{B}_p$ sem base finita. Uma variedade é dita metanilpotente se cada grupo G desta variedade possui um subgrupo normal N, tal que N e G/N são nilpotentes. Este resultado será o assunto do capítulo 3 desta dissertação.

Ainda sobre subvariedade de variedades de Burnside, Kozhevinikov [11] provou que, para todo primo "suficientemente grande", existe uma subvariedade de $\mathbf{B}_p$ que não tem base finita. Para primos "pequenos", maiores que 3, esta questão está em aberto.

Existem muitos resultados positivos sobre a questão da existência de uma base finita para variedades de grupos. Por exemplo, em 1952 Lyndon [12] provou que variedades nilpotentes possuem base finita. Outro fato conhecido é que variedades metabelianas têm base finita, provado

em 1967 por Cohen [4]. No entanto são conhecidos alguns exemplos de variedades solúveis de classe 4 sem base finita, como a que estudaremos no capítulo 3. Por outro lado, a existência de variedades solúveis de classe 3 sem base finita é uma questão que ainda está em aberto.

Tendo em vista estas considerações históricas, objetivamos estudar neste trabalho variedades de grupos que não possuem base finita. Estudaremos variedades de expoente p^2 e p^3. Nos basearemos no trabalho de Gupta e Krassilnikov [5] e no trabalho de Kleiman [10]. Esta dissertação se divide em quatro capítulos.

No primeiro capítulo falaremos sobre alguns tópicos básicos da teoria de grupos, como grupos nilpotentes, grupos solúveis e produto entrelaçado de grupos. Já no segundo capítulo discorremos sobre grupos livres e variedades de grupos. Essa é a teoria principal sobre a qual se apóia este trabalho. Serão tratados assuntos como subgrupos verbais, grupos relativamente livres, produto de variedades entre outros. Nestes dois primeiros capítulos vários resultados ficarão sem demonstração, isso porque nosso objetivo nestes capítulos é formar uma base teórica para os capítulos finais, onde trataremos dos assuntos principais desta dissertação.

A variedade $\mathbf{AA} \cap \mathbf{B}_n$ dos grupos metabelianos de expoente n será denotada por $\mathbf{M}_n$. Assim no terceiro capítulo provaremos que a variedade $\mathbf{M}_p\mathbf{N}_{2,p}$ contém uma subvariedade $\mathbf{B}$ sem base finita. Essa subvariedade é a interseção de $\mathbf{M}_p\mathbf{N}_{2,p}$ com a variedade definida pelo conjunto de identidades

$$\{w_k = [[x,y,z],[x,y,z]^{u_k},...,[x,y,z]^{u_k^{p-1}}]; k \in \mathbb{N}\},$$

onde $u_k = [x_1,x_2]...[x_{2k-1},x_{2k}]$. Isto mostra a existência de uma variedade solúvel de classe 4 e expoente p^2, sem base finita. Por outro lado, como um grupo metabeliano de expoente p é nilpotente (Meier-Wunderli [13]), esta variedade é metanilpotente.

No último capítulo provaremos que o sistema de identidades

$$\{x_1^{p^3}, (x_1^p x_2^p)^{p^2}, \ldots, (x_1^p x_2^p \ldots x_n^p)^{p^2}, \ldots\}$$

não é equivalente à nenhum sistema finito de identidades. Como veremos, este conjunto é uma base de identidades para a variedade $\mathbf{B}_{p^2}\mathbf{B}_p$. Assim, o que provaremos na verdade é que esta variedade não possui base finita. Para isto construiremos um grupo contido na variedade $(\mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_p)(\mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_{p+1})$ satisfazendo todas as identidades $u_n^{p^2}, n = 1,2,\ldots k-1$, mas que não satisfaz $u_k^{p^2}$, onde $u_n = x_1^p x_2^p \ldots x_n^p$. A importância deste exemplo está na simplicidade de exibir o sistema de identidades.

Capítulo 1

Alguns Tópicos da Teoria de Grupos

Neste capítulo exporemos alguns resultados gerais sobre a teoria de grupos. Discorreremos sobre grupos nilpotentes, grupos solúveis e produto entrelaçado. Na seção de grupos nilpotentes falaremos sobre álgebras associativas livres, onde exibiremos um método importante de obtenção de grupos nilpotentes. Nessa breve exposição definiremos cada um desses objetos e enunciaremos os principais resultados, os quais serão de suma importância nos dois últimos capítulos. Procuraremos demonstrar a maior parte possível destes resultados, no entanto nossa intenção é apenas dar base para os capítulos posteriores.

1.1 Grupos Nilpotentes

Uma importante classe de grupos, entre outros fatores por sua proximidade com grupos abelianos, é a classe dos grupos nilpotentes, a qual definiremos agora.

Definição 1.1. Um grupo G é chamado *nilpotente* se possui uma série de subgrupos

$$G = G_1 \geq G_2 \geq \ldots \geq G_{c+1} = \{1\},$$

tal que $G_i \lhd G$, $G_i/G_{i+1} \subset Z(G/G_{i+1})$, para todo $i = 1, \ldots, c$. Tal série de subgrupos é chamada *série central* de G. O menor de todos os comprimentos c das séries centrais de G é chamado de *classe de nilpotência* do grupo G.

Definamos o comutador $[x,y]$ dos elementos x,y, o conjugado x^y de x por y e o comutador simples de comprimento n $[x_1,\ldots,x_n]$ como

1. $[x,y] = x^{-1}y^{-1}xy$;
2. $x^y = y^{-1}xy$;
3. $[x_1,\ldots,x_n] = [[x_1,\ldots,x_{n-1}],x_n], n \geq 3$.

Para uso posterior estabeleceremos algumas identidades de comutadores.

Proposição 1.2. *Sejam G um grupo e $a,b,c \in G$. Então:*

1. $ab = ba[a,b]$;
2. $[a,b] = [b,a]^{-1}$;
3. $[ab,c] = [a,c]^b[b,c] = [a,c][a,c,b][b,c]$;
4. $[c,ab] = [c,b][c,a]^b = [c,b][c,a][c,a,b]$;
5. *(identidade de Witt)* $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a = 1$ *as vezes escrita na forma* $[a,b,c^b][b,c,a^c][c,a,b^a] = 1$.

Para uma demonstração veja [17, p. 123] e [2, p. 215].

Sejam G um grupo e $X_1, X_2 \subset G$. Definimos o subgrupo $[X_1,X_2] < G$ por

$$[X_1,X_2] = \langle \{[x_1,x_2]; x_1 \in X_1, x_2 \in X_2\} \rangle.$$

Aqui $\langle A \rangle$ denota o subgrupo gerado pelo conjunto A. Com esta definição é fácil ver que na definição de grupos nilpotentes a condição $G_i/G_{i+1} \subset Z(G/G_{i+1})$, pode ser substituída por $[G_i,G] \leq G_{i+1}$.

Definamos uma série, chamada de *série central inferior* de G, por:

$$\begin{aligned} \gamma_1(G) &= G, \\ \gamma_2(G) &= [G,G] = G', \\ \gamma_k(G) &= [\gamma_{k-1}(G),G]. \end{aligned}$$

Temos que $\gamma_i(G)/\gamma_{i+1}(G) \subset Z(G/\gamma_{i+1}(G))$, ou seja, esta série realmente é central. Seguem alguns resultados importantes sobre esta série.

Proposição 1.3. *Sejam G um grupo arbitrário e M um conjunto gerador de G. Então:*

1. $\gamma_i(G) = \langle [g_1, g_2, \ldots, g_i]; g_l \in G, l = 1, 2, \ldots, i \rangle$;
2. $\gamma_i(G) = \langle [x_1, x_2, \ldots, x_i]; x_l \in M, l = 1, 2, \ldots, i \rangle^G$;
3. $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$;
4. *Se* $a \in \gamma_i(G)$ *e* $b \in G$ *então* $[a, b^n] = [a, b]^n \pmod{\gamma_{i+2}(G)}$.

No item 2 $\langle A \rangle^G$ *denota o subgrupo de G gerado pelo conjunto* $\{a^g \mid a \in A \text{ e } g \in G\}$. *Este subgrupo é chamado de fecho normal de A.*

Demonstração:

(1) Seja $N_i = \langle [g_1, g_2, \ldots, g_i]; g_l \in G \rangle$. Provaremos que $N_i = \gamma_i(G)$. O resultado é claro para $i = 1$. Também é claro que $N_i \leq \gamma_i(G)$. Assim podemos fazer o quociente $\gamma_i(G)/N_i$. Pela definição de $\gamma_i(G)$ um elemento deste quociente tem a forma $cN_i = [c_1, g_1]^{\varepsilon_1} \ldots [c_k, g_k]^{\varepsilon_k} N_i$, onde $\varepsilon_l \in \{1, -1\}, c_l \in \gamma_{i-1}(G)$. Por hipótese de indução c_l é um produto de comutadores de comprimento $i - 1$. Usando os itens (2), (3) e (4) da proposição 1.2 segue que $cN_i = N_i$. Portanto, $N_i = \gamma_i(G)$.

(2) Façamos $M_i = \langle [x_1, x_2, \ldots, x_i]; x_l \in M, l = 1, 2, \ldots, i \rangle^G$. Usando N_i definido no item anterior podemos ver que $M_i \leq N_i$. Consideremos o quociente N_i/M_i. Novamente usando a proposição 1.2 obtemos $M_i = N_i = \gamma_i(G)$.

(3) Segue diretamente da identidade de Witt.

(4) Para $n = 0$ ou $n = 1$ a afirmação é obvia. Suponhamos que a mesma seja válida para $n - 1$. Pelo item (3) de 1.2 $[a, b^n] = [a, b^{n-1}][a, b][a, b, b^{n-1}]$, por hipótese de indução segue $[a, b^n] = [a, b]^n [a, b, b^{n-1}]$. Como $a \in \gamma_i(G)$ pelo item (1) segue o resultado desejado. □

Enunciaremos a proposição a seguir separadamente pela sua importância, no entanto ela segue diretamente do item 2 da proposição anterior.

Proposição 1.4. *Seja G um grupo arbitrário. Seja M um conjunto gerador de G. Então* $\gamma_i(G)$ *é gerado por* $\gamma_{i+1}(G)$ *e todos os comutadores simples de peso i,* $[x_{j_1}, x_{j_2}, \ldots, x_{j_i}]$, *com* $x_{j_k} \in M$.

Definamos também outra série central, a chamada *série central superior,* da seguinte forma:

$$\begin{aligned} Z_0(G) &= \{1\}, \\ Z_1(G) &= Z(G), \\ Z_i(G)/Z_{i-1}(G) &= Z(G/Z_{i-1}(G)). \end{aligned}$$

Esta série é central pela forma que foi construída. O motivo destas séries serem chamadas de série inferior e série superior ficará claro na

Proposição 1.5. *Seja $G = G_1 \geq G_2 \geq \ldots \geq G_{c+1} = \{1\}$, uma série central. Então:*

1. *$\gamma_i(G) \leq G_i$, para todo i, desta forma $\gamma_{c+1}(G) = \{1\}$;*
2. *$G_i \leq Z_{c-i+1}(G)$, para todo i, desta forma $Z_c(G) = G$;*
3. *A classe de nilpotência c de G é igual ao comprimento da série central inferior, que também é igual ao comprimento da série central superior.*

Para uma demonstração veja [17, p. 125].

Proposição 1.6. *Sejam G um grupo, $a, b_1, \ldots, b_l \in G$ e $z_l \in Z_l(G)$. Então*

$$[az_l, b_1, \ldots, b_l] = [a, b_1, \ldots, b_l].$$

Demonstração: Usaremos indução sobre l. O resultado é fácil para $l = 1$. Supondo válido para $l-1$ segue:

$$\begin{aligned} [[az_l, b_1], \ldots, b_l] &= [[a, b_1]^{z_l}[z_l, b_1], b_2, \ldots, b_l] \\ &= [[a, b_1][a, b_1, z_l]z_{l-1}, b_2, \ldots, b_l] \\ &= [[a, b_1]z_{l-1}^{(1)}, b_2, \ldots, b_l]. \end{aligned}$$

Por hipótese de indução, temos

$$[[a, b_1]z_{l-1}^{(1)}, b_2, \ldots, b_l] = [[a, b_1], b_2, \ldots, b_l].$$

onde $z_{l-1}, z_{l-1}^{(1)} \in Z_{l-1}(G)$. Isto prova a proposição. □

Proposição 1.7. *Sejam G um grupo nilpotente de classe c e $g_1, g_2, \ldots, g_c, h \in G$. Então*

$$[g_1, g_2, \ldots, g_{i-1}, g_i h, g_{i+1} \ldots, g_c] = [g_1, g_2, \ldots, g_i, \ldots, g_c][g_1, g_2, \ldots, h, \ldots, g_c].$$

Demonstração: Provaremos para $i = 2$, os outros casos podem ser feitos de forma análoga. Pela proposição 1.2 temos

$$[g_1, g_2 h, g_3, \ldots, g_c] = [[g_1, h][g_1, g_2][g_1, g_2, h], g_3, \ldots, g_c]$$

Pelas proposições 1.6 e 1.2, temos

$$\begin{aligned}[g_1, g_2h, g_3, \ldots, g_c] &= [[g_1, h][g_1, g_2], g_3, \ldots, g_c] \\ &= [[g_1, h, g_3][g_1, h, g_3]z_4, g_4, \ldots, g_c],\end{aligned}$$

onde $z_4 \in \gamma_4(G) \leq Z_{c-3}(G)$. Assim, novamente pela proposição anterior, temos

$$[g_1, g_2h, g_3, \ldots, g_c] = [[g_1, h, g_3][g_1, h, g_3], g_4, \ldots, g_c].$$

Continuando assim, depois de alguns passos, obtemos

$$\begin{aligned}[g_1, g_2h, g_3, \ldots, g_c] &= [[g_1, h, g_3, \ldots, g_{c-1}][g_1, g_2, g_3, \ldots, g_{c-1}], g_c] \\ &= [g_1, h, g_3, \ldots, g_{c-1}, g_c][g_1, g_2, g_3, \ldots, g_{c-1}, g_c]z_{c+1},\end{aligned}$$

onde $z_{c+1} \in \gamma_{c+1}(G) \leq Z_0(G) = \{1\}$. Isto conclui a demonstração. □

Seguem alguns resultados importantes sobre grupos nilpotentes.

Proposição 1.8. *A classe dos grupos nilpotentes é fechada para subgrupos, quocientes e produtos diretos finitos.*

Demonstração: Basta observar que se um grupo G possui uma cadeia central $G = G_1 \geq G_2 \geq \ldots \geq G_{c+1} = \{1\}$, então, para cada subgrupo $H < G$, a interseção de H com esta cadeia $H = G_1 \cap H \geq G_2 \cap H \geq \ldots \geq G_{c+1} \cap H = \{1\}$, é uma cadeia central para H. De fato, $[G_i, G] \leq G_{i+1}$ implica diretamente $[G_i \cap H, G \cap H] \leq G_{i+1} \cap H$. De forma análoga, a imagem de uma cadeia central é uma cadeia central para um quociente. Para produtos diretos o resultado segue do fato:

O i-ésimo termo da série central inferior do produto direto é igual ao produto direto dos i-ésimos termos das respectivas séries centrais.

Este fato é de direta verificação. □

Note que um produto direto de uma quantidade infinita de grupos nilpotentes pode não ser nilpotente. De fato, seja $G_i, i \in \mathbb{N}$, uma família de grupos nilpotentes, onde G_i é nilpotente de classe i. Logo o produto direto $G = \prod_{i=1}^{\infty} G_i$ não é nilpotente.

Proposição 1.9. *Todo p-grupo finito é nilpotente.*

A demonstração desta proposição pode ser feita facilmente usando indução e o conhecido fato de que um p-grupo finito tem centro não trivial.

Proposição 1.10. *Seja G um grupo finito. As seguintes condições são equivalentes:*

1. *G é nilpotente.*
2. *G é o produto direto de seus subgrupos de Sylow.*
3. *Todo subgrupo* maximal *de G é normal.*

Para uma demonstração veja [8, p. 116].

Álgebras Associativas Livres e Grupos Nilpotentes

Nesta subseção exibiremos um método importante para obtenção de grupos nilpotentes. Este método consiste em fazer o quociente de uma álgebra associativa livre por um ideal adequado, como veremos a seguir. Primeiramente façamos algumas definições.

Definição 1.11. Uma *álgebra R* sobre um corpo K é definida como um espaço vetorial sobre K com uma multiplicação $\cdot : R \times R \longrightarrow R$ com as seguintes propriedades:

1. A terna $(R, +, \cdot)$ é um anel, isto é, valem as leis distributivas:

$$(x+y)\cdot z = x\cdot z + y\cdot z, \text{ para todos } x,y,z \in R,$$
$$x\cdot(y+z) = x\cdot y + x\cdot z, \text{ para todos } x,y,z \in R.$$

2. Para todos $x, y \in A$ e $\alpha \in K$, temos

$$\alpha(xy) = (\alpha x)y = x(\alpha y).$$

A álgebra R é dita associativa, comutativa ou com unidade conforme o anel $(R, +, \cdot)$ for, respectivamente, associativo, comutativo ou com unidade.

Assim como para grupos e anéis um homomorfismo de álgebras é uma função que preserva as operações das respectivas álgebras, isto é:

Definição 1.12. Sejam R_1 e R_2 duas álgebras sobre um corpo K. Uma aplicação $f : R_1 \to R_2$ chama-se um homomorfismo se:

1. f é uma transformação linear do K-espaço vetorial R_1 para o K-espaço vetorial R_2.
2. $f(x \cdot y) = f(x) \cdot f(y)$, para todos $x, y \in R$.

Definição 1.13. Sejam K um corpo e X um conjunto, $X \neq \phi$. A K-álgebra $K\langle X \rangle$ definida como o K-espaço vetorial com base $\{x_{i_1} \dots x_{i_n}; x_i \in X, n = 0, 1, \dots\}$ com uma multiplicação tal que

$$(x_{i_1} \dots x_{i_m})(x_{j_1} \dots x_{j_n}) = x_{i_1} \dots x_{i_m} x_{j_1} \dots x_{j_n}; x_{i_k}, x_{j_l} \in X$$

chama-se *K-álgebra associativa livre*.

Agora exibiremos uma propriedade para álgebras associativas chamada *propriedade universal*.

Proposição 1.14. *Seja R uma K-álgebra associativa. Então qualquer aplicação $\varphi : X \to R$ pode ser estendida à um único homomorfismo $f : K\langle X \rangle \to R$. Em outras palavras, existe um único homomorfismo $f : K\langle X \rangle \to R$ tal que $f(x) = \varphi(x)$, para todos $x \in X$.*

Demonstração: Definamos uma função $f : K\langle X \rangle \to R$ como segue. Seja

$$\bar{X} = \{x_{i_1} \dots x_{i_n};\ x_i \in X, n = 0, 1, \dots\}.$$

Primeiramente,

$$\text{se } m \in \bar{X}, \text{ então } f(m) = f(x_{i_1} \dots x_{i_n}) = \varphi(x_{i_1}) \dots \varphi(x_{i_n}).$$

Seja $p = \alpha_1 m_1 + \dots + \alpha_r m_r \in K\langle X \rangle$, onde $m_j \in \bar{X}$. Assim podemos definir

$$f(p) = \alpha_1 f(m_1) + \dots + \alpha_r f(m_r).$$

Pela definição de f temos que $f(x) = \varphi(x)$, para todos $x \in X$. Por outro lado é fácil verificar que f é um homomorfismo. □

Descrevamos agora o método de obtenção de grupos nilpotentes através de uma álgebra associativa livre com unidade. Seja R uma tal K-álgebra com conjunto de geradores livres $A = \{a_1, a_2, \dots, a_n\}$. Consideremos os ideais Δ e Δ^m de R, onde Δ é o ideal bilateral gerado

por $\{a_1, a_2, \ldots, a_n\}$, isto é, Δ contém todos os elementos com termo constante nulo. Sejam $\bar{R} = R/\Delta^m$ e $\bar{\Delta} = \Delta/\Delta^m$ a imagem de Δ neste quociente. Definamos ainda

$$G = 1 + \bar{\Delta} = \{1 + x; x \in \bar{\Delta}\}$$

É fácil verificar que o subconjunto $G \subset \bar{R}$ é um grupo multiplicativo. Por outro lado, consideremos a cadeia

$$\{1\} = G_{n-1} < G_{n-2} < \ldots < G_0 = G,$$

onde $G_i = 1 + \bar{\Delta}^{i+1}, i = 0, 1, \ldots, n-1$. É possível provar que esta cadeia é uma cadeia central para G, o que implica que G é nilpotente de classe no máximo $n-1$.

Comutadores Básicos e Processo de Coleção

Definiremos nesta seção um subconjunto importante do conjunto de comutadores, chamados comutadores básicos.

Seja G um grupo gerado por $X = \{x_1, x_2, \ldots\}$. Ordenemos os elementos de X da seguinte forma: $x_1 < x_2 < x_3 < \ldots$.

Podemos considerar os elementos de X como comutadores de comprimento 1. Desta forma podemos definir recursivamente os comutadores em X, que são os elementos do tipo:

$$[c_{i_1}, \ldots, c_{i_n}], n \geq 2,$$

onde cada c_{i_l} é um comutador em X. O comprimento deste comutador é definido como a soma dos comprimentos dos comutadores c_{i_l}, $l = 1, \ldots, n$.

Assim fixemos uma ordenação para os comutadores em X, de tal forma que um comutador é maior quanto maior for seu comprimento. Nestas condições o conjunto C de comutadores básicos em X é definido pelas seguintes condições:

1. $x_i \in C, i \in I$.
2. Se $c_1, c_2 \in C$ então $c = [c_1, c_2] \in C$ desde que:
   a) $c_1 \geq c_2$ e
   b) se $c_1 = [c_1', c_2']$, então $c_2 \geq c_2'$.

Um resultado que mostra a grande importância dos comutadores básicos é o

Teorema 1.15. *Sejam $G = \langle x_i; i \in I \rangle$ e $C^{(n)}$ o conjunto de comutadores básicos de comprimento n em X. Então $\gamma_n(G)/\gamma_{n+1}(G)$ é gerado por $\{c\gamma_{n+1}(G); c \in C^{(n)}\}$.*

Sobre o processo de coleção enunciaremos a seguir um importante resultado, quando se aplica este processo à uma *n*-ésima potência.

Teorema 1.16. *Sejam G um grupo e $a_1, a_2, \ldots, a_r \in G$. Então a n-ésima potência $(a_1 a_2 \ldots a_r)^n$ pode ser escrita na forma*

$$(a_1 a_2 \ldots a_r)^n = a_1^n a_2^n \ldots a_r^n c_{r+1}^{e_{r+1}} \ldots c_i^{e_i} R_1 \ldots R_t,$$

onde $c_{r+1}, \ldots, c_i, R_1, \ldots R_t$ são comutadores básicos sobre $a_1, a_2, \ldots, a_r$, tais que:

1. $c_1 \leq c_2 \leq \ldots \leq c_i$;
2. $c_i \leq R_j, j = 1, 2, \ldots, t$.

Além disso, temos que os expoentes e_j são dados por

$$e_j = b_1 n^{(1)} + b_2 n^{(2)} + \ldots + b_l n^{(l)},$$

onde l é o comprimento de comutador c_j, os elementos b_i são inteiros não-negativos dependem apenas do comutador c_j e não dependem de n. Aqui $n^{(k)} = \frac{n(n-1)\ldots(n-k+1)}{k!}, k = 1, 2, \ldots, l$.

Para uma demonstração veja [7, p. 182].

1.2 Grupos Solúveis

Outra importante classe de grupos é a dos grupos solúveis, definidos a seguir.

Definição 1.17. Um grupo G é chamado *solúvel* se possui uma série de subgrupos

$$G = G_0 > G_1 > \ldots > G_n = \{1\},$$

tal que $G_{i+1} \lhd G_i$ e G_i/G_{i+1} é abeliano. Uma tal série é chamada *série subnormal abeliana* de G. O menor de todos os comprimentos n de tais séries é chamado *comprimento de solubilidade* ou *comprimento derivado* do grupo G.

Para estudar grupos solúveis é fundamental entender a chamada *série derivada* de G, definida por:

$$\begin{aligned} G^{(0)} &= G, \\ G^{(1)} &= G' = [G,G], \\ G^{(n)} &= [G^{(n-1)}, G^{(n-1)}]. \end{aligned}$$

A importância desta série se deve à

Proposição 1.18. *Se $G = G_0 > G_1 > \ldots > G_n = \{1\}$ é uma série subnormal abeliana, então $G^{(i)} < G_i, i = 1, \ldots, n$.*

Demonstração: Usaremos indução sobre i. Como G/N é abeliano se, e somente se, $G' < N$, o resultado vale para $i = 1$. Supondo válida para i, temos

$$G_i/G_{i+1} \text{ é abeliano, isto implica } G_{i+1} > G_i' = [G_i, G_i] > [G^{(i)}, G^{(i)}] = G^{(i+1)}.$$

□

Desta proposição segue que um grupo é solúvel se, e somente se, a série derivada estabiliza, isto é, existe n tal que $G^{(n)} = G^{(n+1)}$. Além disso o comprimento de solubilidade de G é igual ao comprimento da série derivada de G.

Grupos Metabelianos

Um grupo solúvel de comprimento derivado 2 é chamado de *metabeliano*.

Teorema 1.19 (Meier-Wunderli)**.** *Um grupo metabeliano de expoente p é nilpotente de classe no máximo p.*

Para um demonstração veja [13].

Teorema 1.20. *Para um grupo metabeliano G e $a_1, a_2, \ldots, a_n \in G$, temos as seguintes identidades:*

1. $[a_1, a_2, \ldots, a_n][a_2, a_1, \ldots, a_n] = 1$;

2. $[a_1, a_2, \ldots, a_i, a_{i+1}, \ldots, a_n] = [a_1, a_2, \ldots, a_{i+1}, a_i, \ldots, a_n], i \geq 2$;

3. $[a_1,a_2,a_3,\ldots,a_n][a_2,a_3,a_1,\ldots,a_n][a_3,a_1,a_2,\ldots,a_n]=1$;

4. $[a_1,a_2,\ldots,a_n][a_2,a_3,\ldots,a_n,a_1]\ldots[a_n,a_1,\ldots,a_{n-1}]=1$.

Demonstração: Usaremos indução sobre n nas identidades 1, 3 e 4.

1. Para $n=2$ é válida para qualquer grupo. Por hipótese de indução temos

$$[a_1,a_2,a_3,\ldots,a_{n-1}][a_2,a_1,a_3,\ldots,a_{n-1}]=1, \text{segue que}$$

$$[[a_1,a_2,a_3,\ldots,a_{n-1}][a_2,a_1,a_3,\ldots,a_{n-1}],a_n]=1, \text{pela proposição 1.2 temos}$$

$$[a_1,a_2,a_3,\ldots,a_n]^{[a_2,a_1,a_3,\ldots,a_{n-1}]}[a_2,a_1,a_3,\ldots,a_n]=1.$$

Portanto, como G é metabeliano, obtemos

$$[a_1,a_2,a_3,\ldots,a_n][a_2,a_1,a_3,\ldots,a_n]=1.$$

2. Provemos que $[a_1,a_2,a_3,a_4]=[a_1,a_2,a_4,a_3]$. O caso geral se faz de forma completamente análoga.

Façamos $c=[a_1,a_2]$, segue

$$[a_1,a_2,a_3,a_4]=[c,a_3,a_4]=[c^{-1}c^{a_3},a_4]=c(c^{-1})^{a_3}(c^{-1}c^{a_3})^{a_4}=c(c^{-1})^{a_3}(c^{-1})^{a_4}c^{a_3a_4}.$$

Analogamente,

$$[a_1,a_2,a_4,a_3]=c(c^{-1})^{a_4}(c^{-1})^{a_3}c^{a_4a_3}.$$

Desta forma, basta verificar que $c^{a_4a_3}=c^{a_3a_4}$. Isto segue de $a_3a_4=[a_3,a_4]^{-1}a_4a_3$ e de G ser metabeliano, o que conclui a demonstração deste item.

3. Utilizaremos a identidade de Witt, assim, para $n=3$, temos

$$[a_1,a_2,a_3^{a_2}][a_2,a_3,a_1^{a_3}][a_3,a_1,a_2^{a_1}]=1,$$

segue que

$$[a_1,a_2,a_3[a_3,a_2]][a_2,a_3,a_1[a_1,a_3]][a_3,a_1,a_2[a_2,a_1]]=1$$

Pelo item (4) da proposição 1.2 segue

$$[a_1,a_2,[a_3,a_2]][a_1,a_2,a_3][a_1,a_2,a_3,[a_3,a_2]][a_2,a_3,[a_1,a_3]][a_2,a_3,a_1][a_2,a_3,a_1,[a_1,a_3]]$$
$$\times[a_3,a_1,[a_2,a_1]][a_3,a_1,a_2][a_3,a_1,a_2,[a_2,a_1]] = 1$$

Logo,

$$[a_1,a_2,a_3][a_2,a_3,a_1][a_3,a_1,a_2] = 1$$

Supondo válida para $n-1$, provemos para n

$$[a_1,a_2,a_3,\ldots,a_{n-1}][a_2,a_3,a_1,\ldots,a_{n-1}] = [a_3,a_1,a_2,\ldots,a_{n-1}]^{-1},$$

logo,

$$[[a_1,a_2,a_3,\ldots,a_{n-1}][a_2,a_3,a_1,\ldots,a_{n-1}],a_n] = [[a_3,a_1,a_2,\ldots,a_{n-1}]^{-1},a_n].$$

Pela proposição 1.2 e pelo item (1), segue

$$[[a_1,a_2,a_3,\ldots,a_{n-1}],a_n]^c[[a_2,a_3,a_1,\ldots,a_{n-1}],a_n] = [[a_1,a_3,a_2,\ldots,a_{n-1}],a_n],$$

onde $c = [a_2,a_3,a_1,\ldots,a_{n-1}]$, como G é metabeliano essa conjugação por c desaparece, obtendo finalmente

$$[a_1,a_2,a_3,\ldots,a_n][a_2,a_3,a_1,\ldots,a_n][a_3,a_1,a_2,\ldots,a_n] = 1.$$

4. Para $n = 3$ segue do item anterior. Supondo válida para $n-1$ temos

$$[a_1,a_2,\ldots,a_{n-1}][a_2,a_3,\ldots,a_{n-1},a_1]\ldots[a_{n-1},a_1,\ldots,a_{n-2}] = 1,$$

assim,

$$[[a_1,a_2,\ldots,a_{n-1}][a_2,a_3,\ldots,a_{n-1},a_1]\ldots[a_{n-1},a_1,\ldots,a_{n-2}],a_n] = 1,$$

logo,

$$[a_1,a_2,\ldots,a_{n-1},a_n][a_2,a_3,\ldots,a_{n-1},a_1,a_n]\ldots[a_{n-1},a_1,\ldots,a_{n-2},a_n] = 1.$$

Agora por (3), temos

$$[a_{n-1},a_1,a_n,a_2,\ldots,a_{n-2}][a_1,a_n,a_{n-1},a_2,\ldots,a_{n-2},][a_n,a_{n-1},a_1,a_2,\ldots,a_{n-2},a_n] = 1,$$

segue que

$$[a_{n-1}, a_1, a_n, a_2, \ldots, a_{n-2}] = [a_n, a_1, a_{n-1}, a_2, \ldots, a_{n-2},][a_{n-1}, a_n, a_1, a_2, \ldots, a_{n-2}, a_n]$$

Utilizando esta igualdade e o item (2), da expressão acima obtemos por fim

$$[a_1, a_2, \ldots, a_n][a_2, a_3, \ldots, a_n, a_1] \ldots [a_n, a_1, \ldots, a_{n-1}] = 1.$$

□

1.3 Produto Entrelaçado

Primeiramente definamos o produto direto.

Seja $\{A_i; i \in I\}$ uma família de grupos. Definimos o *produto direto* dos grupos desta família, denotado por $\prod_{i \in I} A_i$, como o conjunto das funções de I para A assumindo apenas finitos valores não triviais, isto é,

$$\{f : I \longrightarrow A; \{i;\ f(i) \neq 1\} \text{ é finito}\}.$$

A operação deste grupo é o produto usual de funções.

Nos interessará o caso em que I é finito ou enumerável. Os elementos do produto direto podem ser vistos como seqüências finitas.

Agora definamos produto semidireto de dois grupos.

Sejam N e H dois grupos e $\varphi : H \rightarrow \text{Aut}(N)$ um homomorfismo. O grupo $H \ltimes N$ é chamado o produto semidireto de N e H com respeito à φ e é definido como o conjunto $H \times N$ (produto cartesiano de conjuntos) com a operação $*$ definida por

$$(h_1, n_1) * (h_2, n_2) = (h_1 h_2, \varphi(h_2)(n_1) n_2).$$

As vezes este grupo é denotado por $N \rtimes H$. É fácil verificar que existem N_1 um subgrupo normal de $H \ltimes N$ e H_1 é um subgrupo de $H \ltimes N$, tais que $H \ltimes N = H_1 N_1$ e $N_1 \cap H_1 = \{1\}$.

Na situação oposta, consideremos um grupo G tal que existem N um subgrupo normal de G e H um subgrupo de G, com as seguintes propriedades:

1. $G = NH$;
2. $N \cap H = \{1\}$.

Nestas condições, para cada elemento $h \in H$ podemos associar o automorfismo natural $\phi_h : N \to N$, definido por $\phi(n) = n^h$. Esta associação define um homomorfismo φ de H para Aut$N$. Além disso, não é difícil verificar que $G \cong N \rtimes H$, com respeito à φ.

Por fim definamos o produto entrelaçado. Sejam A e B dois grupos. Definamos o grupo $A^{(B)}$ com produto direto de copias de A indexadas por elementos do grupo B, mais precisamente,

$$A^{(B)} = \prod_{b \in B} A_b, \text{ onde } A_b \cong A.$$

O grupo B atua em $A^{(B)}$ de forma natural

$$f^b(x) = f(xb^{-1})$$

ou, equivalentemente,

$$f^b(xb) = f(x),$$

onde $x, b \in B$.

Assim, existe um homomorfismo de B para Aut$A^{(B)}$. Desta forma, definimos o produto entrelaçado de A por B, denotado por Awr$B$, como o produto semidireto de $A^{(B)}$ por B com esta ação.

Segue diretamente desta definição que o produto entrelaçado W de A por B é finito se, e somente se, A e B são finitos. Em caso positivo temos $|W| = |A|^{|B|}|B|$.

Capítulo 2

Grupos Livres e Variedades de Grupos

Neste segundo capítulo falaremos sobre a principal teoria a qual se apóia este trabalho, a teoria sobre variedades de grupos. Para isto primeiramente falaremos sobre grupos livres, tópico fundamental para estudo de variedades.

2.1 Grupos Livres e Apresentações de Grupos

Definição 2.1. Sejam F um grupo e $X \subset F$. O grupo F, também denotado por $F(X)$, chama-se *grupo livre* com *base* X (ou conjunto de *geradores livres* X) se para cada grupo G, qualquer aplicação $\varphi : X \to G$ pode ser estendida à um único homomorfismo $f : F \to G$. Em outras palavras, existe um único homomorfismo $f : F \to G$ tal que $f(x) = \varphi(x)$, para todos $x \in X$. A cardinalidade do conjunto X é chamada de *posto* do grupo livre $F(X)$.

Esta definição de grupo livre através de uma propriedade, chamada propriedade universal, é muito útil em várias aplicações. No entanto ela tem a deficiência de não garantir a existência de tais grupos. A prova desta existência se faz pela construção de um grupo livre para cada conjunto gerador X. Contudo não faremos essa construção aqui, ela pode ser encontrada em [17, p. 44].

Agora enunciaremos um importante teorema sobre grupos livres. Este teorema diz, em outras palavras, que a classe dos grupos livres é fechada para subgrupos.

Teorema 2.2 (Nielsen-Schreier)**.** *Se H é um subgrupo de um grupo livre $F(X)$, então H é livre.*

Suponhamos ainda que F tem posto finito n. Então H é finitamente gerado se, e somente se, $j = [F : H] < \infty$. Em caso afirmativo o posto de H é $1 + (n-1)j$.

Para uma demonstração veja [17, p. 162].

Segue diretamente da definição e da existência de grupos livres, que todo grupo é isomorfo à um quociente de um grupo livre. Desta forma para cada grupo G existem um grupo livre $F(X)$ e um subgrupo normal $N < F(X)$ tal que $G \cong F(X)/N$.

Definição 2.3. Seja G um grupo isomorfo à $F(X)/N$, onde $F(X)$ é um grupo livre com base X e $N = \langle R \rangle^F$ é um subgrupo normal de $F(X)$ (N é o fecho normal de um subconjunto R). O par ordenado $(X|R)$ chama-se uma *apresentação* de G. Os elementos do conjunto X são ditos *geradores* e os elementos do conjunto R são ditos *relações* do grupo G. Escrevemos $G = \langle X|R \rangle$.

Pelo comentário acima, segue que todo grupo G possui alguma apresentação.

Teorema 2.4 (von Dyck)**.** *Sejam $G = \langle X \mid R \rangle$ e $H = \langle Y \mid R' \rangle$ dois grupos, tais que X e Y têm a mesma cardinalidade. Seja ainda $\bar{}: X \longrightarrow Y$ uma bijeção. Suponhamos que H satisfaz todas as relações $r \in R$, isto é,*

$$\text{se } r(x_1, \ldots, x_l) = 1 \ (x_1, \ldots, x_l \in X), \text{ então } r(\bar{x}_1, \ldots, \bar{x}_l) = 1.$$

Então existe um epimorfismo $\varphi : G \longrightarrow H$, ou seja, H é isomorfo à um quociente de G.

Demonstração: Sejam F um grupo livre com base X (isto é, um conjunto de mesma cardinalidade, o qual identificamos com X) e $N = \langle R \rangle^F$ o fecho normal de R. Assim, temos que $G \cong F/N$. Definamos o homomorfismo

$$\phi : F \longrightarrow H \text{ tal que } \phi(x) = \bar{x}, x \in X.$$

Este homomorfismo ϕ é sobrejetivo, pois a imagem contém o conjunto gerador Y. Como H satisfaz todas as relações $r \in R$ temos que $\phi(N) = 1$, logo $N \leq ker\phi$. Segue que:

$$H \cong F/ker\phi \cong (F/N)/(ker\phi/N) \cong G/(ker\phi/N).$$

□

2.2 Variedades de Grupos e Subgrupos Verbais

Seja $F(X)$ um grupo livre, com conjunto de geradores livres $X = \{x_i; i = 1,2,\ldots\}$, G um grupo e $u(x_1,\ldots,x_k)$ um elemento no grupo livre $F(X)$. Nestas condições u pode ser visto como uma função $u : \underbrace{G \times G \times \ldots \times G}_{k} \longrightarrow G$.

A imagem de uma k-upla $(g_1,\ldots,g_k)$ por esta função é dita um valor de u em G. Para um subconjunto V de $F(X)$ os valores assumidos por seus elementos em G é, em geral, um subconjunto não trivial de G. O subgrupo gerado por todos estes valores será chamado de *subgrupo verbal de G relativo à V* e denotado por $V(G)$. Isto é,

$$V(G) = \langle v(g_1,\ldots,g_{n(v)}) | v \in V, g_i \in G \rangle.$$

Segue facilmente das definições que todo subgrupo verbal é completamente invariante.

Dizemos que o elemento u é uma *identidade* ou *lei* em G, se todos os valores de u em G são triviais. Usaremos u ou $u \equiv 1$ para denotar uma identidade.

Definição 2.5. A classe **V** , de todos os grupos satisfazendo um dado conjunto de identidades V, será chamada uma *variedade de grupos.* O conjunto V é dito uma *base de identidades* para a variedade **V**.

O conjunto V de todas as identidades em um grupo G é um subgrupo de um grupo livre $F(X)$. De fato, sejam $u(x_1,\ldots,x_k), v(x_1,\ldots,x_k) \in F(X)$ identidades em um grupo G. Como $u(g_1,\ldots,g_k) = v(g_1,\ldots,g_k) = 1$, segue que

$$uv^{-1}(g_1,\ldots,g_k) = u(g_1,\ldots,g_k)v(g_1,\ldots,g_k)^{-1} = 1,$$

para todos $g_1,\ldots,g_k \in G$, portanto uv^{-1} é uma identidade em G. Além disso é fácil verificar que este subgrupo é totalmente invariante.

Proposição 2.6. *Sejam* **V** *uma variedade de grupos e V uma base de identidades para* **V**. *Um grupo G está em* **V** *se, e somente se, G é um quociente de $F/V(F)$, para algum grupo livre F. O grupo $F/V(F)$ é dito o grupo livre na variedade* **V**.

Demonstração: Se G é um quociente de $F/V(F)$. Claramente G satisfaz todas as identidades de **V**. Portanto, temos que $G \in \mathbf{V}$. Inversamente, suponhamos que $G \in \mathbf{V}$ e mostremos que G é

um quociente de $F/V(F)$. Sejam M um conjunto gerador de G e $F(X)$ um grupo livre com base X, onde X é um conjunto com a mesma cardinalidade que M. Seja $\alpha : X \longrightarrow M$ uma bijeção. Como F é livre, temos que α pode ser estendida a um epimorfismo $\varphi : F \longrightarrow G$. Como $V(F)$ é completamente invariante, temos

$$\varphi(V(F)) = V(\varphi(F)) = V(G) = 1,$$

pois $G \in \mathbf{V}$.

Logo, obtemos que $V(F) \subset \ker\varphi$ se, e somente se, $V(G) = 1$. Portanto

$$G \cong F/\ker\varphi \cong (F/V(F))/(\ker\varphi/V(F)).$$

Isto demonstra a proposição. □

Com esta proposição estamos preparados para demonstrar um importante teorema sobre variedades de grupos. Este teorema dá outra visão deste objeto o qual definimos por variedades de grupos.

Teorema 2.7 (Birkhoff)**.** *Uma classe de grupos* $\mathbf{C}$ *é fechada para subgrupos, quocientes e produtos cartesianos se, e somente se,* $\mathbf{C}$ *é uma variedade de grupos.*

Demonstração: É claro que uma variedade é fechada para subgrupos, quocientes e produtos cartesianos. Inversamente, suponhamos que uma classe de grupos $\mathbf{C}$ é fechada para subgrupos, quocientes e produtos cartesianos. Sejam V o conjunto das identidades satisfeitas por todos os grupos de $\mathbf{C}$. Definamos $\mathbf{V}$ como a variedade com base V. É claro que $\mathbf{C} \subset \mathbf{V}$. Queremos provar que $\mathbf{V} \subset \mathbf{C}$. Como $\mathbf{C}$ é fechada para quocientes, é suficiente provar que cada grupo livre de $\mathbf{V}$ pertence à $\mathbf{C}$. Pela proposição anterior um grupo livre nesta variedade é da forma

$$\bar{F} = F(X)/V(F(X)).$$

Para cada $w \notin V$ existe um grupo $G_w \in \mathbf{C}$ tal que w não é uma identidade em G_w. Desta forma, existe um homomorfismo

$$\varphi_w : \bar{F} \longrightarrow G_w, \text{ com } \varphi_w(wV(F)) \neq 1.$$

O produto cartesiano $G = \prod_{w\in\bar{F}} G_w$ pertence à $\mathbf{C}$, pois esta classe é fechada para produtos cartesianos. Seja $\varphi : \bar{F} \longrightarrow G$ o homomorfismo cuja imagem de um elemento x na w-ésima posição

é $\varphi_w(x)$. Pela forma que definimos φ temos que $\ker\varphi = V(F)$, ou seja, φ é um monomorfismo. Portanto $\bar{F} \cong \varphi(\bar{F}) < G$. Como **C** é fechada para subgrupos o teorema está demonstrado. □

Seja U um subconjunto de $F(X)$. Uma identidade w é conseqüência de U, se w é identidade em um grupo G, sempre que todo elemento de U é uma identidade de G. Dois conjuntos U e V são equivalente se toda palavra de U é conseqüência de V e vice versa.

Teorema 2.8. *Toda palavra w é equivalente à um par de palavras, onde uma é da forma* $x^m, m \geq 0$ *e a outra é uma palavra comutador.*

Demonstração: Seja $w = w(x_1, \ldots, x_n)$ uma palavra em um alfabeto X. É fácil ver que podemos escrever w na forma

$$w = x_1^{m_1} \ldots x_n^{m_n} c,$$

onde c é uma palavra comutador, isto é, $c \in [F(X), F(X)]$. Se todos expoentes m_i são nulos, $w = c$ e não temos nada a provar. Sejam $m_{i_1}, \ldots, m_{i_r}$ os expoentes não nulos. Se w é uma lei em um grupo G substituindo $x_1, \ldots, x_{i_1-1}, x_{i_1+1}, \ldots, x_n$ por 1, temos que $x^{m_{i_1}}$ é uma lei em G. Analogamente $x^{m_{i_j}}$ é uma lei em G para cada $j = 1, 2, \ldots, r$. Segue que x^m é uma lei em G, onde $m = mdc(m_{i_1}, \ldots, m_{i_r})$. Por outro lado, como o conjunto de identidades de um grupo é um subgrupo de um grupo livre de posto apropriado, segue que $c = x_n^{-m_n} \ldots x_1^{-m_1} w$ é conseqüência de w. Reciprocamente, se x^m e c são identidades em um grupo, é claro que w também o é . Portanto w é equivalente à $\{x^m, c\}$. □

Grupos Relativamente Livres

Definição 2.9. Um grupo G é chamado *relativamente livre* se possui um conjunto de geradores, chamados *geradores livres*, tal que toda aplicação deste conjunto no grupo G pode ser estendida à um endomorfismo.

Como dissemos acima um subgrupo verbal é completamente invariante. A recíproca deste fato em geral não é verdadeira. No entanto ela vale para grupos relativamente livres, como veremos na proposição seguinte.

Proposição 2.10. *Sejam G um grupo relativamente livre. Então todo subgrupo completamente invariante de G é um subgrupo verbal de G.*

Demonstração: Sejam U um subgrupo completamente invariante de G e X é um conjunto de geradores livres de G. Sejam ainda $u = u(x_1, x_2, \ldots, x_r) \in U$, com $x_i \in X$ e $g_1, \ldots, g_r \in G$. Pela

definição de grupos relativamente livres, existe um homomorfismo

$$\varphi : G \longrightarrow G, \text{ tal que } \varphi(x_i) = g_i, i = 1, \ldots, r.$$

Segue que $\varphi(u) = u(g_1, \ldots, g_r) \in U$, pois U é completamente invariante. Assim, para todo $u \in U$, todos os valores de u em G pertencem à U, o que demonstra a proposição. □

Exemplos triviais de grupos relativamente livre são os grupos livres. Outros exemplos de tais grupos são obtidos através da

Proposição 2.11. *Um grupo G é relativamente livre se, e somente se, $G \cong F/R$, onde R é um subgrupo verbal de um grupo livre F.*

Demonstração: Ver [14, p. 9]. □

A proposição seguinte relaciona grupos relativamente livres com grupos livres em variedades.

Proposição 2.12. *Um grupo G é relativamente livre se, e somente se, G é o grupo livre de posto apropriado de alguma variedade* $\mathbf{V}$.

Demonstração: Vamos inicialmente supor que G é relativamente livre. Pela proposição anterior temos que $G \cong F/V$, onde $V = V(F)$ é um subgrupo verbal do grupo livre F. Assim, G é o grupo livre da variedade definida pelo conjunto de identidades V.

Por outro lado, suponhamos que G é o grupo livre na variedade $\mathbf{V}$. Por definição $G \cong F/V(F)$, onde F é um grupo livre e $V(F)$ é o subgrupo verbal correspondente a $\mathbf{V}$. Assim, pela proposição anterior, segue que G é relativamente livre. □

Com estas proposições podemos definir grupos abelianos livres como sendo os grupos livres na variedade dos grupos abelianos. Desta forma todo grupo abeliano é um quociente de um grupo abeliano livre. Temos ainda o

Teorema 2.13.

1. *Se um grupo A é abeliano livre com base X então A é a soma direta dos subgrupos cíclicos infinitos $\langle x \rangle$, $x \in X$.*
2. *A soma direta $A = \sum_{x \in X} C_x$, onde cada C_x é um grupo cíclico infinito, é abeliano livre com base X.*

A cardinalidade do conjunto X será chamada posto *de A.*

Para uma demonstração veja [17, p. 61].

Teorema 2.14. *Sejam G é um grupo relativamente livre e M um conjunto de geradores livres para G. Então o grupo quociente G/G' é abeliano relativamente livre, livremente gerado pelo conjunto MG'/G'. Além disso, G/G' tem mesmo expoente (zero ou $m > 0$) que G.*

Demonstração: Seja F o grupo livre com base X, um conjunto de mesma cardinalidade de M. Façamos $U = \ker\varphi$, onde φ é o epimorfismo canônico $\varphi : F \longrightarrow G$. Nestas condições $G/G' \cong F/F'U$. De fato, como $\varphi(F') = G'$, podemos definir o epimorfismo

$$\varphi' : F/F' \longrightarrow G/G',$$

tal que

$$\varphi'(xF') = \varphi(x)G'.$$

Além disso, é claro que $\ker\varphi' \geq UF'$.

Reciprocamente provemos assim que $UF' \geq \ker\varphi'$. Seja $xF' \in \ker\varphi'$, temos

$$\varphi'(xF') = 1, \text{ logo } \varphi(x) \in G', \text{ isto implica que } \varphi(x) = [g_1, g_2]^{n_1} \dots [g_{2k-1}, g_{2k}]^{n_k}.$$

Seja $f = [y_1, y_2]^{n_1} \dots [y_{2k-1}, y_{2k}]^{n_k}$, onde $y_i \in F$ e $\varphi(y_i) = g_i$, $i = 1, 2, \dots 2k$. Desta forma, temos

$$\varphi(f) = \varphi(x), \text{ logo } \varphi(xf^{-1}) = 1, \text{ assim } x \in UF'.$$

Segue que $\ker\varphi' = UF'$. Como U e F' são verbais segue que $F'U$ é verbal, portanto $G/G' \cong F/F'U$ é abeliano relativamente livre. Por outro lado, tendo em vista o teorema 2.8, segue que:

G tem expoente zero se, e somente se, $UF' = F'$ se, e somente se,

$U \subset F'$ se, e somente se, $G/G' \cong F/F'U = F/F'$ se, e somente se,

G/G' tem expoente zero.

Por fim, novamente usando o teorema 2.8, temos

G tem expoente $m > 0$ se, e somente se, x^m é uma identidade em G se, e somente se, $x^m \in U$.

□

Variedades com Base Finita

Dizemos que uma variedade possui base finita se o conjunto identidades desta variedade é equivalente à um conjunto finito de identidades. Um problema que ficou algumas décadas sem solução é o problema da existência de variedades de grupos sem base finita. Este problema foi proposto por B. H. Neumann em 1937. Nos capítulos posteriores daremos exemplos de variedades de grupos sem base finita. Contudo isto não pode ocorrer para variedades abelianas, como veremos na seguinte proposição.

Proposição 2.15. *Toda subvariedade da variedade de grupos abelianos possui base finita.*

Demonstração: Seja **V** uma subvariedade da variedade de grupos abelianos. Definamos m como o menor inteiro não negativo tal que x^m é uma identidade em **V**. Isto é, m é o expoente de **V**, podendo inclusive ser nulo.

Provaremos que $\{[x_1,x_2],x^m\}$ é uma base de identidades para **V**. Todavia isto segue facilmente do teorema 2.6. Com efeito, por este teorema uma identidade w em **V** é equivalente à um par de identidades na forma x^n, $n \geq 0$ e uma palavra comutador c. Pela nossa definição de m segue que x^n é conseqüência de x^m. Por outro lado uma palavra comutador c é conseqüência de $[x_1,x_2]$, o que prova o teorema. □

O mesmo resultado vale para grupos nilpotentes de classe no máximo c e para grupos metabelianos.

Teorema 2.16. *Toda subvariedade da variedade de grupos nilpotentes de classe no máximo c possui base finita.*

Para uma demonstração veja [14, p. 89].

Teorema 2.17. *Toda subvariedade da variedade dos grupos metabelianos possui base finita.*

Para uma demonstração veja [4].

Para encerrar esta subseção consideraremos um teorema importante para este trabalho, haja vista que utilizá-lo-emos para demonstrar os principais teoremas nos capítulos posteriores.

Teorema 2.18. *Seja* **V** *uma variedade de grupos. Então* **V** *possui uma base finita de identidades* $v_1 \equiv 1, v_2 \equiv 1, \ldots, v_k \equiv 1$ *se, e somente se, toda base* β *de* **V** *possuir um subconjunto finito equivalente a* β.

Demonstração: Primeiramente, é claro que se toda base β de **V** é equivalente a um subconjunto finito de β, então **V** possui uma base finita.

Reciprocamente, seja $\{v_1, v_2, \ldots, v_k\}$ uma base finita de **V**. Seja $\beta = \{w_j \mid j = 1,2,\ldots\}$ uma base qualquer de **V**. Notemos que cada v_i, pertence a um subgrupo gerado por um número finito de elementos $w_{i_1}, w_{i_2}, \ldots, w_{i_{l_i}}$, para algum $l_i \geq 1$. Assim, temos que cada $v_i \equiv 1$, $i = 1,2,\ldots,k$ é conseqüência de um número finito de identidades $w_{i_1} \equiv 1, w_{i_2} \equiv 1, \ldots, w_{i_{l_i}} \equiv 1$, para algum $l_i \geq 1$. Assim, a base finita é conseqüência de um número finito de identidades w_j, $j = 1,2,\ldots,s$ e também qualquer outra identidade em **V**. Logo, a base de identidades $\beta = \{w_1, w_2, \ldots\}$ é conseqüência de seu subconjunto finito $\{w_j \mid j = 1,2,\ldots,s\}$. Portanto β é equivalente a subconjunto finito. □

Produto de Variedades

Chamaremos o grupo C de uma extensão de A por B se C possui um subgrupo normal isomorfo à A, tal que o quociente por este subgrupo é isomorfo à B.

Sejam **U** e **V** duas variedades de grupos. Consideremos a classe **UV** de todos os grupos que são extensões de um grupo de **U** por um grupo de **V**.

Proposição 2.19. *A classe de grupos* **UV**, *definida acima, é uma variedade de grupos.*

Demonstração: Sejam U e V os conjuntos de todas as identidades de **U** e **V** respectivamente e

$$W = \{w = u(v_1, v_2, \ldots, v_k) \in F(X); u = u(x_1, x_2, \ldots, x_k) \in U, \text{ e } v_1, v_2, \ldots, v_k \in V\},$$

onde $F(X)$ é um grupo livre. Mais precisamente, provaremos que **UV** é a variedade definida pelo conjunto de identidades W.

Seja **W** a variedade de grupos definida pelo conjunto de identidades W. Queremos mostrar que um grupo $G \in \mathbf{W}$ se, e somente se, $G \in \mathbf{UV}$.

Suponhamos inicialmente que $G \in \mathbf{UV}$. Assim, pela definição de **UV**, temos que existe $N \lhd G$ tal que, $N \in \mathbf{U}$ e $G/N \in \mathbf{V}$. Segue que $U(N) = \{1\}$ e $V(G/N) = \{1\}$. A segunda igualdade

implica em $V(G) \subset N$, conseqüentemente $U(V(G)) \subset U(N) = \{1\}$. Portanto

$$W(G) = U(V(G)) = \{1\},$$

ou seja, $G \in \mathbf{W}$.

Inversamente, se $G \in \mathbf{W}$ então $U(V(G)) = \{1\}$. Observemos que se $N = V(G)$, temos que $U(N) = \{1\}$, isto é, $N \in \mathbf{U}$. Mas temos também que $N \lhd G$, e assim, $V(G/N) = V(G/V(G)) = \{1\}$, ou seja, $G/N \in \mathbf{V}$.

Assim, concluímos que $G \in \mathbf{UV}$. Desta forma, temos que $\mathbf{W} = \mathbf{UV}$, e portanto $\mathbf{UV}$ é a variedade de grupos definida pelo conjunto de identidades $W = U(V(F(X)))$. □

A variedade de grupos $\mathbf{UV}$ é chamada de *variedade produto* de $\mathbf{U}$ por $\mathbf{V}$.

Capítulo 3

Uma Variedade Metanilpotente de Expoente p^2 sem Base Finita

Neste capítulo exibiremos, para todo primo $p \geq 3$, uma subvariedade $\mathbf{B}$ da variedade $\mathbf{M}_p\mathbf{N}_{2,p}$ a qual não tem base finita. Desta forma daremos um exemplo de uma variedade solúvel de expoente p^2 que não tem base finita de identidades. Como vimos no capítulo 2 isto não pode ocorrer para variedades abelianas e variedades nilpotentes de classe c, onde toda subvariedade tem base finita. Além disso, por Meier-Wunderli [13], a variedade $\mathbf{M}_p$ dos grupos metabelianos de expoente dividindo p, é nilpotente de classe p. Logo $\mathbf{M}_p\mathbf{N}_{2,p}$ é metanilpotente e tem expoente p^2. Recordemos que uma variedade é metanilpotente se cada grupo G desta variedade possui um subgrupo normal N tal que N e G/N são nilpotentes. Assim $\mathbf{B}$ também é metanilpotente de expoente p^2.

Mais precisamente provaremos o

Teorema 3.1. *Para todo primo p, $p \geq 3$, existe uma subvariedade $\boldsymbol{B}$ de $\boldsymbol{M}_p\boldsymbol{N}_{2,p}$ a qual não tem base finita.*

Seja p um primo arbitrário, $p \geq 3$. No grupo livre no conjunto $\{x,y,z,x_1,x_2,\ldots\}$ de geradores livres, sejam

$$u_k = [x_1,x_2]\ldots[x_{2k-1},x_{2k}]$$

e

$$w_k = [[x,y,z],[x,y,z]^{u_k},\ldots,[x,y,z]^{{u_k}^{p-1}}],$$

$k \in \mathbb{N}$. Sejam ainda $\mathbf{W}$ a variedade definida pelas identidades $w_k \equiv 1, k \in \mathbb{N}$ e V um conjunto

de identidades que define $\mathbf{M}_p\mathbf{N}_{2,p}$. Para provar o teorema 3.1 construiremos, para cada $n \in \mathbb{N}$, um grupo C_n na variedade $\mathbf{M}_p\mathbf{N}_{2,p}$ o qual satisfaz as identidades $w_1 \equiv 1, \ldots, w_n \equiv 1$; mas não a identidade $w_{n+1} \equiv 1$. De fato, isto demonstra o seguinte teorema, o qual implica o teorema 3.1.

Teorema 3.2. *A variedade $\boldsymbol{B} = \boldsymbol{W} \cap \boldsymbol{M}_p\boldsymbol{N}_{2,p}$ não tem base finita.*

Lema 3.3. *Existe um grupo metabeliano $\bar{M}$ de expoente p com geradores $y_k, k = 0, 1, \ldots, p-1$, satisfazendo as seguintes condições:*

j) $[y_{k_1}, y_{k_2}, \ldots, y_{k_p}] = 1$ *se* $k_r = k_s$ *para algum par* $(r,s); 1 \leq r < s \leq p$;

jj) Para cada $2 \leq l \leq p-1$, *temos*

$$[y_0, y_l, y_1, \ldots, \bar{y}_l, \ldots, y_{p-1}] = [y_0, y_1, \ldots, y_{p-1}]^l \tag{3.1}$$

onde $[y_0, y_l, y_1, \ldots, \bar{y}_l, \ldots, y_{p-1}] = [y_0, y_l, y_1, \ldots, y_{l-1}, y_{l+1}, \ldots, y_{p-1}]$. *Além disso,* $\gamma_p(\bar{M})$ *é um p-grupo cíclico gerado por* $[y_0, y_1, \ldots, y_{p-1}]$;

jjj) Para todo k, $0 \leq k \leq p-1$, *existe um automorfismo* ϕ *de* $\bar{M}$ *tal que* $\phi(y_l) = y_{l+k}, (l = 0, 1, \ldots, p-1)$ *onde os índices devem ser lidos módulo p.*

Deste lema segue facilmente o

Lema 3.4. *Existe um grupo metabeliano M de expoente p com geradores $y_k^{(i)}$ $(i \in \mathbb{N}, k = 0, 1, \ldots, p-1)$ satisfazendo as seguintes condições:*

i) $[y_{k_1}^{(i_1)}, y_{k_2}^{(i_2)}] = 1$, *se* $i_1 \neq i_2$;

ii) $[y_{k_1}^{(i)}, y_{k_2}^{(i)}, \ldots, y_{k_p}^{(i)}] = 1$, *se* $k_r = k_s$ *para algum par* $(r,s); 1 \leq r < s \leq p$;

iii) O conjunto $\{[y_0^{(i)}, y_1^{(i)}, \ldots, y_{p-1}^{(i)}], i \in \mathbb{N}\}$ *é uma base de* $\gamma_p(M)$. *Além disso,*

$$[y_0^{(i)}, y_1^{(i)}, \ldots, y_{l-1}^{(i)}, y_{l+1}^{(i)}, \ldots, y_{p-1}^{(i)}] = [y_0^{(i)}, y_1^{(i)}, \ldots, y_{p-1}^{(i)}]^l;$$

iv) Para toda permutação τ *de* $\mathbb{N}$ *e para toda seqüência* $\{k^{(i)} \mid 0 \leq k^{(i)} \leq p-1, i \in \mathbb{N}\}$ *existe um automorfismo* ϕ *de M tal que* $\varphi(y_k^{(i)}) = y_{k+k^{(i)}}^{(\tau(i))}, (i \in \mathbb{N},\ k = 0, 1, \ldots, p-1)$, *escrevemos que se* $k \geq p$, *então* $y_k^{(i)} = y_l^{(i)}$, *onde* $0 \leq l \leq p-1$ *e* $k \equiv l \pmod{p}$.

Demonstração: Sejam $\bar{M}$ como no lema anterior e, para cada $i \in \mathbb{N}$, $\bar{M}_i$ um grupo isomorfo à $\bar{M}$, com isomorfismo $\phi_i : \bar{M} \to \bar{M}_i, \phi_i(y_l) = y_l^{(i)}$, $l = 0, 1, \ldots, p-1$. Desta forma podemos definir $M = \prod_{i \in \mathbb{N}} \bar{M}_i$ (produto direto).

A condição (i) é satisfeita por M ser um produto direto; (ii) e (iii) seguem de (j) e (jj) respectivamente. Para provar (iv) sejam $(k^{(i)})_{i\in\mathbb{N}}$ e τ uma permutação de $\mathbb{N}$. Por (jjj), para cada par $(i,\tau(i))$ existem isomorfismos

$$\varphi_i : \bar{M}_i \to \bar{M}_{\tau(i)} \text{ e } \psi_i : \bar{M}_i \to \bar{M}_i,$$

tais que

$$\varphi_i(y_k^{(i)}) = y_k^{(\tau(i))} \text{ e } \psi_i(y_k^{(i)}) = y_{k+k^{(i)}}^{(i)}.$$

Assim a composta

$$(\varphi_i\psi_i) : \bar{M}_i \to \bar{M}_{\tau(i)} \text{ é tal que } (\varphi_i\psi_i)(y_k^{(i)}) = y_{k+k^{(i)}}^{\tau(i)}.$$

Desta forma basta definir ϕ agindo em $\bar{M}_i$ tal como $\varphi_i\psi_i$. □

Demonstração do lema 3.3: Sejam $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ e $R = \mathbb{Z}_p\langle a_0, a_1, \ldots, a_{p-1}\rangle$ a álgebra livre associativa sobre $\mathbb{Z}_p$ (com unidade) nas variáveis $a_0, a_1, \ldots, a_{p-1}$. Definamos os ideais J_1, J_2, J_3, J_4 de R como segue:

$$J_1 = ideal\langle\{a_{i_1}\ldots a_{i_{p+1}} \mid 0 \le i_1, \ldots, i_{p+1} \le p-1\}\rangle;$$

$$J_2 = ideal\langle\{a_{i_1}\ldots a_{i_l} \mid l \le p, i_r = i_s \text{ para algum } r \ne s\}\rangle;$$

$$J_3 = ideal\langle\{a_ia_ja_k - a_ia_ka_j \mid 0 \le i,j,k \le p-1\}\rangle$$

e

$$J_4 = ideal\langle\{a_la_0a_1\ldots\bar{a}_l\ldots a_{p-1} - la_1a_0a_2\ldots a_{p-1} + (l-1)a_0a_1a_2\ldots a_{p-1};$$
$$l = 2,3,\ldots,p-1\}\rangle.$$

Seja $J = J_1 + J_2 + J_3 + J_4$. Definamos agora $\bar{M}$ como o subgrupo das unidades do anel quociente R/J gerado por $y_i = 1 + a_i + J$, $i = 0,1,\ldots,p-1$. Observe que, como

$$(1+a_i)^p + J_2 = 1 + pa_i + \frac{p(p-1)}{2}a_i^2 + \ldots + pa_i^{p-1} + a_i^p + J_2 = 1 + J_2,$$

os elementos y_i realmente são invertíveis.

Observemos que para um arbitrário $g \in \bar{M}$, podemos escrever $g = 1+h+J$, onde $h = \alpha_0a_0 + \ldots + \alpha_{p-1}a_{p-1} + h'$ e h' é uma combinação linear de monômios nas variáveis $a_0, \ldots, a_{p-1}$ de

grau 2 ou mais. Desta forma,

$$g^p = (1+h)^p + J = 1 + ph + \frac{p(p-1)}{2}h^2 + \ldots + ph^{p-1} + h^p + J = 1 + h^p + J.$$

Como h' é uma combinação linear de monômios de grau 2 ou mais, temos que

$$a_{i_1} \ldots a_{i_l} h' a_{i_{l+1}} \ldots a_{i_{p-1}} \in J_1,$$

$l = 0, 1, \ldots, p-1$. Assim

$$\begin{aligned} g^p &= 1 + (\alpha_0 a_0 + \ldots + \alpha_{p-1} a_{p-1} + h')^p + J \\ &= 1 + (\alpha_0 a_0 + \ldots + \alpha_{p-1} a_{p-1})^p + J \\ &= 1 + \sum_{\delta \in S_p} \alpha_{\delta(0)} a_{\delta(0)} \ldots \alpha_{\delta(p-1)} a_{\delta(p-1)} + J \\ &= 1 + \alpha_0 \ldots \alpha_{p-1} \sum_{\delta \in S_p} a_{\delta(0)} \ldots a_{\delta(p-1)} + J. \end{aligned}$$

Por outro lado, como $J > J_3$, temos

$$a_{\delta(0)} \ldots a_{\delta(p-1)} = a_{\delta(0)} a_0 a_1 \ldots \bar{a}_{\delta(0)} \ldots a_{p-1} \pmod{J},$$

onde $a_l a_0 \ldots \bar{a}_l \ldots a_{p-1} = a_l a_0 a_1 \ldots a_{l-1} a_{l+1} \ldots a_{p-1}$.

Assim,

$$\sum_{\delta \in S_p} a_{\delta(0)} \ldots a_{\delta(p-1)} + J = \sum_{\delta \in S_p} a_{\delta(0)} a_0 a_1 \ldots \bar{a}_{\delta(0)} \ldots a_{p-1} + J = (p-1)!S + J,$$

onde $S = \sum_{l=0}^{p-1} a_l a_0 \ldots \bar{a}_l \ldots a_{p-1}$. Isto já implica que $\bar{M}$ tem expoente dividindo p^2.

Como $J > J_4$, temos

$$a_l a_0 \ldots \bar{a}_l \ldots a_{p-1} = l a_1 a_0 a_2 \ldots a_{p-1} - (l-1) a_0 a_1 \ldots a_{p-1} \pmod{J}.$$

Desta forma,

$$S = \frac{p(p-1)}{2} a_1 a_0 \dots a_{p-1} - \frac{p(p-3)}{2} a_0 a_1 \dots a_{p-1} \pmod{J}.$$

Como R é de característica p, segue que $S = 0$. Assim para todo $g \in \bar{M}, g = 1+h+J$, temos

$$g^p = 1 + \alpha_0 \dots \alpha_{p-1}(p-1)!S + J = 1 + J.$$

Assim $\bar{M}$ definido acima tem expoente p.

Definamos os comutadores aditivos indutivamente por

$$(u,v) = uv - vu$$

e

$$(u_1, u_2, \dots, u_n) = ((u_1, u_2, \dots, u_{n-1}), u_n) \text{ para } n \geq 3.$$

Agora provemos que $\bar{M}$ é metabeliano. Primeiramente definamos Δ como o ideal de R gerado pelos elementos $a_0, \dots, a_{p-1}$. Assim, como $J > J_3$, temos

$$f(h_1 h_2 - h_2 h_1) = 0 \pmod{J},$$

para $h_1, h_2 \in R$, e $f \in \Delta$.

Observe que $(h_i, h_j) \in \Delta$, para quaisquer $h_i, h_j \in R$. Desta forma,

$$\begin{aligned} ((h_1,h_2),(h_3,h_4)) &= (h_1,h_2)(h_3,h_4) - (h_3,h_4)(h_1,h_2) \\ &= (h_1,h_2)(h_3h_4 - h_4h_3) - (h_3,h_4)(h_1h_2 - h_2h_1) \\ &= 0 \pmod{J}, \end{aligned}$$

para todos $h_1, h_2, h_3, h_4 \in R$.

Isto implica que $\bar{M}$ é metabeliano, vide [19, 9]. Agora provaremos as condições (j), (jj) e (jjj).

Lema 3.5. *Sejam $g_1 = 1 + h_1, g_2 = 1 + h_2 \in \bar{M}$. Então*

$$[g_1, g_2] = 1 + (h_1, h_2) + \bar{h} + J,$$

onde $\bar{h}$ é uma combinação linear de monômios de grau 3 ou mais.

Demonstração:

$$\begin{aligned}
[g_1,g_2] &= g_1^{-1}g_2^{-1}g_1g_2+J \\
&= (1+h_1)^{-1}(1+h_2)^{-1}(1+h_1)(1+h_2)+J \\
&= (1+h_1)^{p-1}(1+h_2)^{p-1}(1+h_1)(1+h_2)+J \\
&= (1-h_1+h_1^2+\ldots+h_1^{p-1})(1-h_2+h_2^2+\ldots+h_2^{p-1})(1+h_1+h_2+h_1h_2)+J \\
&= (1-h_1-h_2+h_1h_2+h_1^2+h_2^2-h_1h_2^2+\ldots+h_1^{p-1}h_2^{p-1})(1+h_1+h_2+h_1h_2) \\
&\quad +J \\
&= 1-h_1-h_2+h_1+h_2+h_1^2-h_1h_2-h_2h_1-h_2^2+h_1h_2+h_1^2+h_2^2 \\
&\quad +h_1h_2-h_1h_2^2+\ldots+h_1^{p-1}h_2^{p-1}h_1h_2+J \\
&= 1+h_1h_2-h_1h_2-h_1h_2^2+\ldots+h_1^{p-1}h_2^{p-1}h_1h_2+J \\
&= 1+(h_1,h_2)+\bar{h}+J.
\end{aligned}$$

□

Observe que, como $J > J_2$, fazendo $h_i = a_{k_i}$ na demonstração do lema 3.5, temos

$$[y_{k_1},y_{k_2}] = 1+(a_{k_1},a_{k_2})+J.$$

De fato, o elemento $\bar{h}$ neste caso, sendo uma combinação linear de monômios de grau 3 ou mais em duas variáveis, pertence a J_2.

Esta é a base indutiva para a afirmação

$$[y_{k_1},\ldots,y_{k_l}] = 1+(a_{k_1},\ldots,a_{k_l})+J, l \geq 3. \tag{3.2}$$

Supondo válida para $l-1$, temos

$$\begin{aligned}
[[y_{k_1},\ldots,y_{k_{l-1}}],y_{k_l}] &= [y_{k_1},\ldots,y_{k_{l-1}}]^{-1}y_l^{-1}[y_{k_1},\ldots,y_{k_{l-1}}]y_{k_l} \\
&= (1+(a_{k_1},\ldots,a_{k_{l-1}}))^{(p-1)}(1+a_{k_l})^{(p-1)}(1+(a_{k_1},\ldots,a_{k_{l-1}})) \\
&\quad \times(1+a_{k_l})+J \\
&= (1-(a_{k_1},\ldots,a_{k_{l-1}}))(1-a_{k_l})(1+(a_{k_1},\ldots,a_{k_{l-1}}))(1+a_{k_l})+J \\
&= 1+(a_{k_1},\ldots,a_{k_{l-1}})a_{k_l}-a_{k_l}(a_{k_1},\ldots,a_{k_{l-1}})+J \\
&= 1+(a_{k_1},\ldots,a_{k_l})+J.
\end{aligned}$$

Por outro lado, pela definição de J_3, temos

$$(h_1,h_2,\ldots,h_l)=(h_1,h_2)h_3\ldots h_l, l\geq 3 \pmod{J}. \tag{3.3}$$

Assim, de (3.2) e (3.3), segue que

$$[y_{k_1},\ldots,y_{k_p}]=1+(a_{k_1},a_{k_2})a_{k_3}\ldots a_{k_p}+J. \tag{3.4}$$

Logo, pela definição de J_2, $\bar{M}$ satisfaz a condição (j). Observe também que, como $J>J_1$, esta igualdade também implica que $\gamma_{p+1}(\bar{M})=1$, isto é, $\bar{M}$ é nilpotente de classe no máximo p. Como $\bar{M}$ é metabeliano de expoente p, poderíamos chegar à mesma conclusão usando o resultado de Meier-Wunderli.

Para provar que (jj) é satisfeita por $\bar{M}$, verificaremos primeiramente (3.1).

$$[y_0,y_l,y_1,\ldots,\bar{y}_l,\ldots,y_{p-1}]=1+(a_0,a_l,a_1\ldots,\bar{a}_l,\ldots,a_{p-1})+J.$$

Segue de (3.3) e de $J > J_4$, que

$$\begin{aligned} & 1+(a_0,a_l,a_1\ldots,\bar{a}_l,\ldots,a_{p-1})+J \\ = \;& 1+(a_0,a_l)a_l\ldots\bar{a}_l\ldots a_{p-1}+J \\ = \;& 1+a_0a_la_1\ldots\bar{a}_l\ldots a_{p-1}-a_la_0a_1\ldots\bar{a}_l\ldots a_{p-1}+J \\ = \;& 1+a_0a_la_1\ldots a_{p-1}-la_1a_0a_2\ldots a_{p-1}+(l-1)a_0a_1\ldots a_{p-1}+J \end{aligned}$$

Pela definição de J_3, temos

$$\begin{aligned} & 1+a_0a_la_1\ldots a_{p-1}-la_1a_0a_2\ldots a_{p-1}+(l-1)a_0a_1\ldots a_{p-1}+J \\ = \;& 1+l(a_0a_1-a_1a_0)a_2\ldots a_{p-1}+J \\ = \;& 1+l(a_0,a_1,\ldots,a_{p-1})+J \\ = \;& (1+(a_0,a_1,\ldots,a_{p-1}))^l+J \\ = \;& [y_0,y_1,\ldots,y_{p-1}]^l, \end{aligned}$$

ou seja,

$$[y_0,y_l,y_1,\ldots,\bar{y}_l,\ldots,y_{p-1}]=[y_0,y_1,\ldots,y_{p-1}]^l.$$

Assim, para provar que $\bar{M}$ satisfaz (jj) basta provar que $[y_0,y_1,\ldots,y_{p-1}]\neq 1$. Como

$$[y_0,y_1,\ldots,y_{p-1}]=1+(a_0,a_1,\ldots,a_{p-1})+J=1+(a_0a_1\ldots a_{p-1}-a_1a_0\ldots a_{p-1})+J,$$

é equivalente provar que

$$a_0a_1\ldots a_{p-1}\neq a_1a_0\ldots a_{p-1} \pmod{J}.$$

Provaremos que os elementos $a_0a_1\ldots a_{p-1}$ e $a_1a_0\ldots a_{p-1}$ formam uma base, sobre $\mathbb{Z}_p$, do ideal Δ^p/J de R/J.

Primeiro observemos que módulo $J_1 + J_2$ o conjunto

$$A = \{a_{i_1} \dots a_{i_k} \mid 1 \leq k \leq p, 0 \leq i_1, \dots, i_k \leq p-1, i_r \neq i_s, se\ r \neq s\}$$

forma uma $\mathbb{Z}$-base para Δ. Com efeito, Δ contém todos os elementos de R que tem termo constante igual a 0, isto é, o conjunto

$$\{a_{i_1} \dots a_{i_k}; 0 \leq i_1, \dots, i_k \leq p-1, k \in \mathbb{N}\}$$

é uma base linear para Δ. Assim a imagem desta base, que é o conjunto A, gera Δ módulo $J_1 + J_2$. Por outro lado A é linearmente independente em R e uma combinação linear de elementos em A claramente não pertence à $J_1 + J_2$. Segue que A também é linearmente independente módulo $J_1 + J_2$.

Podemos também ver que o conjunto

$$\begin{aligned} B \;=\; & \{a_l a_{i_1} \dots a_{i_k} - a_l a_{j_1} \dots a_{j_k}; 1 \leq k \leq p-1, i_1 < i_2 < \dots < i_k, \\ & \{i_1, i_2, \dots, i_k\} = \{j_1, j_2, \dots, j_k\}, l \neq i_s \text{ para todo } s\}, \end{aligned}$$

forma uma base para J_3 módulo $J_1 + J_2$. É claro que estes elementos estão contidos em J_3 e todo elemento de J_3 é uma combinação linear de elementos da forma

$$a_{m_1} \dots a_{m_r} a_i a_j a_k a_{n_{r+1}} \dots . a_{n_s} - a_{m_1} \dots a_{m_r} a_i a_k a_j a_{n_{r+1}} \dots . a_{n_s}.$$

Por outro lado, um elemento nesta forma é a diferença dos elementos

$$a_{m_1} a_{i_1} \dots a_{i_{s+2}} - a_{m_1} \dots a_{m_r} a_i a_j a_k a_{n_{r+1}} \dots a_{n_s}$$

e

$$a_{m_1} a_{i_1} \dots a_{i_{s+2}} - a_l \dots a_{m_r} a_i a_k a_j a_{n_{r+1}} \dots a_{n_s}$$

onde $i_1 < i_2 < \dots < i_{s+2}, \{i_1, i_2, \dots, i_{s+2}\} = \{m_2, \dots, m_r, i, j, k, n_{r+1}, \dots, n_s\}, l \neq i_k$, os quais pertencem a B. Assim B gera J_3 módulo $J_1 + J_2$. Por outro lado B é linearmente independente em R e uma combinação linear de elementos em B claramente não pertence à $J_1 + J_2$. Assim temos que B também é linearmente independente módulo $J_1 + J_2$.

Destas duas observações segue que a imagem do conjunto

$$\{a_l a_{i_1} \dots a_{i_k} \mid 0 \leq k \leq p-1, i_1 < i_2 < \dots < i_k, l \neq i_s \text{ para todo } s\} \tag{3.5}$$

é uma base de Δ módulo $J_1+J_2+J_3$. Em particular os elementos $a_l a_0 a_1 \ldots \bar{a}_l \ldots a_{p-1}$ $(l = 0,1,\ldots,p-1)$ formam uma base de Δ^p módulo $J_1+J_2+J_3$. Pela definição de J_4 segue que $\{a_0a_1\ldots a_{p-1}+J, a_1a_0a_2\ldots a_{p-1}+J\}$ é uma base do ideal Δ^p/J e que $(a_0,a_1,\ldots,a_{p-1}) = a_0a_1\ldots a_{p-1} - a_1a_0\ldots a_{p-1}$ não é trivial módulo J. Portanto a condição (jj) está satisfeita.

Por fim provemos que $\bar{M}$ satisfaz (jjj). Observemos que, como R é uma álgebra associativa livre, pela proposição 1.14, para cada aplicação $f : \{a_0,\ldots,a_{p-1}\} \to R$ existe um automorfismo χ de R tal que $\chi(a_i) = f(a_i), i = 0,1,\ldots,p-1$.

Provaremos que J é fechado por todos os automorfismos de R tal que $\chi(a_l) = a_{l+k}, k \in \mathbb{N}$ (entendendo que para $i > p-1$, $a_i = a_j$ onde $0 \leq j \leq p-1$ e $i \equiv j \pmod p$). Desta forma χ restrito aos invertíveis de R/J será um automorfismo do grupo $u(R/J)$ que preserva $\bar{M}$.

Como J_1, J_2, J_3 são obviamente fechados por automorfismo de R induzidos por permutações do conjunto $\{a_0,\ldots,a_{p-1}\}$, verifiquemos que $\chi(J_4) \subseteq J$.

Consideremos

$$\begin{aligned} S_l &= \chi(a_l a_0 \ldots \bar{a}_l \ldots a_{p-1} - l a_1 a_0 a_2 \ldots a_{p-1} + (l-1) a_0 a_1 \ldots a_{p-1}) \\ &= a_{k+l} a_k \ldots \bar{a}_{k+l} \ldots a_{k+p-1} - l a_{k+1} a_k a_{k+2} \ldots a_{k+p-1} + (l-1) a_k a_{k+1} \ldots a_{k+p-1}. \end{aligned}$$

Pela definição de J_3, temos

$$S_l = a_{k+l} a_0 \ldots \bar{a}_{k+l} \ldots a_{p-1} - l a_{k+1} a_0 a_1 \ldots \bar{a}_{k+l} \ldots a_{p-1} + (l-1) a_k a_0 \ldots \bar{a}_k \ldots a_{p-1} \pmod J.$$

Pela definição de J_4, temos

$$\begin{aligned} S_l &= (k+l) a_1 a_0 \ldots . a_{p-1} - (k+l-1) a_0 a_1 \ldots a_{p-1} - l[(k+1) a_1 a_0 a_2 \ldots a_{p-1} - k a_0 a_1 \\ &\quad \ldots a_{p-1}] + (l-1)[k a_1 a_0 a_2 \ldots a_{p-1} - (k-1) a_0 a_1 \ldots a_{p-1}] = 0 \pmod J. \end{aligned}$$

Logo $\chi(J) \subseteq J$ e a condição (jjj) é satisfeita por $\bar{M}$, o que prova o lema. □

Agora construiremos para cada $n \in \mathbb{N}$ um grupo $C_n \in \mathbf{M}_p\mathbf{N}_{2,p}$ o qual satisfaz todas as identidades $w_1, w_2, \ldots, w_n$ mas não a identidade w_{n+1}. Observe que para todo $n \in \mathbb{N}$, $w_k \equiv 1$, $k \leq n$ é conseqüência de $w_n \equiv 1$. Assim é suficiente verificar que C_n satisfaz $w_n \equiv 1$ e não satisfaz $w_{n+1} \equiv 1$.

Sejam G o grupo livre na variedade $\mathbf{N}_{2,p}$, livremente gerado por $\{x_1, x_2, \ldots\}$, e $d = [x_1,x_2]\ldots[x_{2n+1},x_{2n+2}] \in G'$.

Proposição 3.6. $Z(G) = G'$.

Demonstração: $G' \leq Z(G)$, pois G é nilpotente de classe 2. Provemos que $Z(G) \leq G'$. Seja $f \notin G'$. Temos que $G/G' = \langle x_1G' \rangle \times \langle x_2G' \rangle \times \ldots$. Assim, $f = x_1^{n_1} \ldots x_k^{n_k} c$, $c \in G'$ e $n_i \neq 0$ para algum $i \in \{1,2,\ldots,k\}$. Fixemos este i e tomemos $j \neq i$, segue que

$$[f,x_j] = [x_1^{n_1},x_j] \ldots [x_k^{n_k},x_j] = [x_1,x_j]^{n_1} \ldots [x_k,x_j]^{n_k}.$$

Note que não aparecem conjugados, pois G é nilpotente de classe 2. Como os elementos $[x_l,x_j], l = 0,1,\ldots,j-1,j+1,\ldots,k$, são linearmente independentes e $[x_j,x_i] \neq 1$ segue que $[f,x_j] \neq 1$ o que implica $f \notin Z(G)$. Portanto $Z(G) = G'$. □

Proposição 3.7. *O elemento d não pode ser escrito como produto de n ou menos comutadores.*

Demonstração: Suponhamos que d possa ser escrito como produto de n comutadores, isto é, $d = [y_1,y_2] \ldots [y_{2n-1},y_{2n}]$. Seja $c = [g_1,g_2] \ldots [g_{2n+1},g_{2n+2}] \in G'$ um produto de n comutadores. Considerando o endomorfismo φ de G tal que $\varphi(x_i) = g_i, i = 1,2,\ldots,2n+2$, segue que c pode ser escrito como produto de n comutadores. Supondo que G é k gerado, ou seja, $G = \langle x_1,x_2,\ldots,x_k \rangle$, temos $\frac{k(k-1)}{2}$ comutadores do tipo $[x_i,x_j], i > j$. Estes são comutadores básicos de comprimento 2. Logo a ordem de G' é $p^{\frac{k(k-1)}{2}}$, pois G' é p-grupo abeliano elementar gerado por estes comutadores.

Tendo em vista a proposição anterior, consideremos agora $\left|\frac{G}{G'}\right| = \left|\frac{G}{Z(G)}\right| = p^k$ e seja $A = \{g_1,g_2,\ldots,g_{p^k}\}$ um transversal de $Z(G)$ em G. Dados $a,b \in G, a = a_1z_1, b = b_1z_2$ tal que $a_1,b_1 \in A$ e $z_1,z_2 \in Z(G)$, temos: $[a,b] = [a_1,b_1]$. Desta forma a quantidade de comutadores de comprimento 2 é menor que p^{2k}. Como G' é abeliano e, pelo que supomos, todo elemento pode ser escrito como produto de no máximo n comutadores, segue que $|G'| < (p^{2k})^n = p^{2kn}$. Mas para k suficientemente grande temos

$$\left|G'\right| = p^{\frac{k(k-1)}{2}} > p^{2kn} > \left|G'\right|,$$

que é um absurdo. Portanto, vemos que d não pode ser escrito como um produto de n comutadores. □

Sejam D o subgrupo cíclico e normal de G gerado por d e $\{g^{(i)} \mid i \in \mathbb{N}\}$ um transversal de D em G tal que $g^{(1)} = 1$ (estamos usando o fato de que um grupo livre com base enumerável é enumerável). Para todo $g \in G$, com $g = g^{(i)}d^k$, façamos $y^g = y_k^{(i)}$. Assim podemos considerar

que $\{y^g \mid g \in G\}$ é um conjunto gerador para M como descrito no lema 3.4. Façamos ainda $y^1 = y$, onde 1 é o elemento neutro de G.

Primeiro verificaremos que para todo $g' \in G$ a permutação $\varphi : y^g \longmapsto y^{gg'}$ do conjunto $\{y^g \mid g \in G\}$ pode ser estendida a um automorfismo de M.

Definamos, para cada $g' \in G$, a permutação τ de $\mathbb{N}$ e a seqüência $k(i)$ assumindo valores em $\{0,1,\ldots,p-1\}$, tais que $g^{(i)}g' = g^{(\tau(i))}d^{k(i)}$. Então para todo $i \in \mathbb{N}$ e $k \in \{0,1,\ldots,p-1\}$, temos

$$\varphi(y_k^{(i)}) = \varphi(y^{g^{(i)}d^k}) = y^{g^{(i)}d^k g'} = y^{g^{(i)}g'd^k} = y^{g^{\tau(i)}d^{k+k(i)}} = y_{d^{k+k(i)}}^{(\tau(i))}.$$

Desta forma, para cada $g' \in G$, construímos a permutação τ e a seqüência $k(i)$, de forma que pela condição (iv) do lema 3.4 existe o desejado automorfismo de M.

Observemos que

$$(y^g)^{g'g''} = y^{gg'g''} = ((y^g)^{g'})^{g''},$$

para todos $g, g', g'' \in G$. Isto implica que G age em M, isto é, existe um homomorfismo de G para $\mathrm{Aut}(M)$. É fácil verificar que este homomorfismo é injetivo.

Seja $Y = [y, y^d, \ldots, y^{d^{p-1}}]$, segue que

$$[y_0^{(i)}, y_1^{(i)}, \ldots, y_{p-1}^{(i)}] = [y^{g^{(i)}}, y^{g^{(i)}d}, \ldots, y^{g^{(i)}d^{p-1}}] = [y, y^d, \ldots, y^{d^{p-1}}]^{g^{(i)}} = Y^{g^{(i)}}.$$

Estes últimos formam uma base para $\gamma_p(M)$, condição (iii) do teorema 3.4.

Por outro lado, como M é metabeliano, pelo teorema 1.20 segue que para todo $1 \leq l \leq p-1$,

$$\begin{aligned}
Y^{d^l} &= [y^{d^l}, y^{d^{l+1}}, \ldots, y^{d^{l+p-1}}] = [y_l^{(1)}, y_{l+1}^{(1)}, \ldots, y_{(l+p-1)}^{(1)}] \\
&= [y_l^{(1)}, y_{l+1}^{(1)}, y_0^{(1)}, \ldots, y_{l-1}^{(1)}, y_{l+2}^{(1)}, \ldots, y_{p-1}^{(1)}] \\
&= [y_{l+1}^{(1)}, y_0^{(1)}, y_l^{(1)}, \ldots, y_{p-1}^{(1)}]^{-1}[y_0^{(1)}, y_l^{(1)}, y_{l+1}^{(1)}, \ldots, y_{p-1}^{(1)}]^{-1} \\
&= [y_0^{(1)}, y_{l+1}^{(1)}, y_l^{(1)}, \ldots, y_{p-1}^{(1)}][y_0^{(1)}, y_l^{(1)}, y_{l+1}^{(1)}, \ldots, y_{p-1}^{(1)}]^{-1} \\
&= [y_0^{(1)}, y_1^{(1)}, \ldots, y_{p-1}^{(1)}]^{l+1}[y_0^{(1)}, y_1^{(1)}, \ldots, y_{p-1}^{(1)}]^{-l} \\
&= [y_0^{(1)}, y_1^{(1)}, \ldots, y_{p-1}^{(1)}] = [y, y^d, \ldots, y^{d^{p-1}}].
\end{aligned}$$

Logo,

$$Y^{d^l} = Y. \tag{3.6}$$

Definamos N como o subgrupo de $\gamma_p(M)$ gerado pelo conjunto

$$\{Y^{g_i c}(Y^{g_i})^{-1}; i \in \mathbb{N} \text{ e } c \in G'\}.$$

Observe que N é um subgrupo normal, pois está no centro de M. Segue de (3.6) que

$$Y^{gc}(Y^g)^{-1} \in N, \text{ para todos } g \in G, c \in G'.$$

De fato, se $g = g^{(i)}d^l$ $(i \in \mathbb{N},\ l = 0,1,\ldots,p-1)$, então

$$Y^{gc}(Y^g)^{-1} = Y^{g^{(i)}d^l c}(Y^{g^{(i)}d^l})^{-1} = (Y^{d^l})^{g^{(i)}c}((Y^{d^l})^{g^{(i)}})^{-1} = Y^{g^{(i)}c}(Y^{g^{(i)}})^{-1} \in N.$$

Assim, para todo $h \in G$, temos

$$\{Y^{g^{(i)}c}(Y^{g^{(i)}})^{-1}\}^h = Y^{g^{(i)}hc}(Y^{g^{(i)}h})^{-1} \in N,\ c \in G',\ i \in \mathbb{N}.$$

Isto implica que para todo $h \in G$, $N^h = N$ e G atua no grupo quociente $B = M/N$ como segue

$$(fN)^g = f^g N \text{ para todos } f \in M, g \in G.$$

Assim, existe um homomorfismo de G para Aut$B$.

Como para todos $c \in G',\ g \in G$, $Y^{cg} = Y^g \pmod N$ e $\gamma_p(M)$ é gerado por $Y^{g^{(i)}},\ i \in \mathbb{N}$, segue que

$$b^{gc} = b^g \pmod N,$$

para todo $b \in \gamma_p(M)$.

Com isto já estamos preparados para demonstrar o teorema principal deste capítulo.

Demonstração do teorema 3.2: Definamos o grupo C_n, mencionado acima, como sendo o produto semidireto de B por G com esta ação. Assim $C_n \in \mathbf{M}_p\mathbf{N}_{2,p}$ por construção. Para verificar que C_n satisfaz a identidade $w_n \equiv 1$, utilizaremos o item (4) do teorema 1.20, que é a seguinte identidade de comutadores para grupos metabelianos

$$[x_1,x_2,\ldots,x_n][x_2,x_3,\ldots,x_n,x_1]\ldots[x_n,x_1,\ldots,x_{n-1}] = 1 \tag{3.7}$$

Seja w um valor arbitrário de w_n em C_n,

$$w = [[f_1, f_2, f_3], [f_1, f_2, f_3]^u, \ldots, [f_1, f_2, f_3]^{u^{p-1}}],$$

onde $f_1, f_2, f_3 \in C_n,\ u = [h_1, h_2] \ldots [h_{2n-1}, h_{2n}],\ h_1, h_2, \ldots, h_{2n} \in C_n$. Como G é nilpotente de classe 2, temos que

$$[f_1, f_2, f_3] \in B, \text{ dai } [f_1, f_2, f_3] = \prod_{i=1}^{r} y^{a_i} N, a_i \in G.$$

Por outro lado

$$u = \bar{u} b N,$$

onde $\bar{u} = [g^{(1)}, g^{(2)}], \ldots, [g^{(2n-1)}, g^{(2n)}]; g^{(1)}, g^{(2)}, \ldots, g^{(2n)} \in G,\ b \in M$. Observe que $u^l = (\bar{u}b)^l = \bar{u}^l b_l,\ b_l \in M$ e, pela proposição 1.7,

$$[m_1^{b_1}, m_2^{b_2}, \ldots, m_p^{b_p}] = [m_1[m_1, b_1], m_2[m_2, b_2], \ldots, m_p[m_p, b_p]] = [m_1, m_2, \ldots, m_p],$$

onde $m_i, b_j \in M$. Desta forma,

$$\begin{aligned} w &= [\prod_{i=1}^{r} y^{a_i}, (\prod_{i=1}^{r} y^{a_i r})^{\bar{u}}, \ldots, (\prod_{i=1}^{r} y^{a_i})^{\bar{u}^{p-1}}] N \\ &= \prod [y^{a_{i_1}}, (y^{a_{i_2}})^{\bar{u}}, \ldots, (y^{a_{i_p}})^{\bar{u}^{p-1}}] N, \text{ onde } (i_1, \ldots, i_p) \in \{1, \ldots, r\}^p. \end{aligned}$$

Assim,

$$w = \prod_{i=1}^{r} [y^{a_i}, (y^{a_i})^{\bar{u}}, \ldots, (y^{a_i})^{\bar{u}^{p-1}}] \prod [y^{a_{i_1}}, (y^{a_{i_2}})^{\bar{u}}, \ldots, (y^{a_{i_p}})^{\bar{u}^{p-1}}] N,$$

onde $i_s \neq i_t$ para algum par (s,t).

Observe que $\prod [y^{a_{i_1}}, (y^{a_{i_2}})^{\bar{u}}, \ldots, (y^{a_{i_p}})^{\bar{u}^{p-1}}] N$, $i_s \neq i_t$ para algum par (s,t) é um produto de elementos da forma

$$[y^{a_{i_1}}, y^{a_{i_2}\bar{u}}, \ldots, y^{a_{i_p}\bar{u}^{p-1}}][y^{a_{i_2}}, y^{a_{i_3}\bar{u}}, \ldots, y^{a_{i_1}\bar{u}^{p-1}}] \ldots [y^{a_{i_p}}, y^{a_{i_1}\bar{u}}, \ldots, y^{a_{i_{p-1}}\bar{u}^{p-1}}] N$$

$$= [y^{a_{i_1}}, y^{a_{i_2}\bar{u}}, \ldots, y^{a_{i_p}\bar{u}^{p-1}}][y^{a_{i_2}\bar{u}}, y^{a_{i_3}\bar{u}^2}, \ldots, y^{a_{i_1}}]^{\bar{u}^{-1}} \ldots [y^{a_{i_p}\bar{u}^{p-1}}, y^{a_{i_1}}, \ldots, y^{a_{i_{p-1}}\bar{u}^{p-2}}]^{\bar{u}^1} N$$

$$= [y^{a_{i_1}}, y^{a_{i_2}\bar{u}}, \ldots, y^{a_{i_p}\bar{u}^{p-1}}][y^{a_{i_2}\bar{u}}, y^{a_{i_3}\bar{u}^2}, \ldots, y^{a_{i_1}}] \ldots [y^{a_{i_p}\bar{u}^{p-1}}, y^{a_{i_1}}, \ldots, y^{a_{i_{p-1}}\bar{u}^{p-2}}] N.$$

Por (4.3) essa última expressão é trivial, logo

$$w = \prod_{i=1}^{r} [y, y^{\bar{u}}, \ldots, y^{\bar{u}^{p-1}}]^{a_i} N.$$

No entanto $\bar{u}$ é um produto de n comutadores, assim, pela proposição 3.7, $\bar{u}$ não pode ser da forma $d^l = [x_1, x_2]^l \ldots [x_{2n+1}, x_{2n+2}]^l, 1 \leq l \leq p-1$. Segue que $\bar{u} = g^{(j)} d^k$ ou, equivalentemente, $y^{\bar{u}} = y_k^{(j)}$ para algum $j \neq 1$. Dai, pelo lema 3.4 ,

$$[y, y^{\bar{u}}] = [y_0^{(1)}, y_k^{(j)}] = 1 \text{ e } w = 1 \pmod{N},$$

ou seja, w_n é uma identidade em C_n.

Para ver que C_n não satisfaz a identidade $w_{n+1} \equiv 1$ provemos que o valor

$$v = [[y, x_1, x_2], [y, x_1, x_2]^d, \ldots, [y, x_1, x_2]^{d^{p-1}}],$$

de w_{n+1} em C_n, não é trivial.

Como

$$[y, x_1, x_2] = [y^{-1} y^{x_1}, x_2] = y^{-x_1} y y^{-x_2} y^{x_1 x_2},$$

fazendo os mesmos cálculos que fizemos para w obtemos:

$$\begin{aligned} v &= [y^{-x_1}, y^{-x_1 d}, \ldots, y^{-x_1 d^{p-1}}] \cdot [y, y^d, \ldots, y^{d^{p-1}}] \cdot [y^{-x_2}, y^{-x_2 d}, \ldots, y^{-x_2 d^{p-1}}] \\ &\times [y^{x_1 x_2}, y^{x_1 x_2 d}, \ldots, y^{x_1 x_2 d^{p-1}}] = Y^{-x_1} Y Y^{-x_2} Y^{x_1 x_2} \pmod{N}. \end{aligned}$$

Suponhamos, por absurdo, que $v = 1 \pmod{N}$. Assim

$$Y^{-x_1} Y Y^{-x_2} Y^{x_1 x_2} \in N$$

isto implica que

$$Y Y^{x_1 x_2} N = Y^{x_1} Y^{x_2} N.$$

Como $\gamma_p(B)$ é um p-grupo abeliano elementar segue que

$$Y = Y^{x_1} \text{ ou } Y = Y^{x_2} \pmod{N}.$$

Logo $x_1 \in N$ ou $x_2 \in N$, o que é uma contradição pois $x_1, x_2, x_3, \ldots$ são geradores livres.

Em suma, construímos para cada $n \in \mathbb{N}$, um grupo C_n contido na variedade $\mathbf{M}_p\mathbf{N}_{2,p}$, tal que $w_k \equiv 1, k = 1,2,\ldots,n$, são identidades em C_n, mas $w_{n+1} \equiv 1$ não é. Portanto, pelo teorema 2.18, a variedade **B** não possui base finita.

□

Capítulo 4

Um Produto de Variedades de Burnside sem Base Finita

Neste capítulo exibiremos um produto de variedades de Burnside que não tem base finita. A importância deste exemplo está, como veremos na proposição 4.2, na simplicidade de sua base, a qual não ocorre para a variedade apresentada no capítulo anterior. Mais precisamente provaremos o

Teorema 4.1 ([10])**.** *A variedade $\boldsymbol{B}_{p^2}\boldsymbol{B}_p$ não tem base finita.*

Primeiramente obtenhamos uma base de identidades para esta variedade.

Proposição 4.2. *O conjunto $\{(x_1^p x_2^p \dots x_n^p)^{p^2}; n = 1,2,\dots\}$ é uma base de identidades para a variedade $\boldsymbol{B}_{p^2}\boldsymbol{B}_p$.*

Demonstração: Sejam $u_n = x_1^p x_2^p \dots x_n^p$ e $\mathbf{V}$ a variedade gerada pelo conjunto de identidades $\{u_n^{p^2}\ ; n = 1,2,\dots\}$. É claro que $\mathbf{B}_{p^2}\mathbf{B}_p \subset \mathbf{V}$. Por outro lado, sejam $G \in \mathbf{V}$ e $N < G$ o subgrupo verbal correspondente a palavra x^p. Assim G/N tem expoente p, o que implica que $G/N \in \mathbf{B}_p$. Por outro lado, um elemento de N é um valor de u_n em G, para algum $n \in \mathbb{N}$. Logo $N \in \mathbf{B}_{p^2}$. Desta forma $G \in \mathbf{B}_{p^2}\mathbf{B}_p$ e $\mathbf{V} \subset \mathbf{B}_{p^2}\mathbf{B}_p$. □

Para demonstrar o teorema construiremos, para cada $l \in \mathbb{N}$ e algum $k > l$, um grupo C e um subgrupo $R < C$, tais que R contém todos os valores dos elementos $u_1^{p^2}, \dots, u_{k-1}^{p^2}$ em C, mas não contém alguns valores de $u_k^{p^2}$. O grupo C será o produto semidireto de um grupo B por um grupo A, onde $B \in \mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_p$ e $A \in \mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_{p+1}$. Desta forma, sendo $V < C$ o

subgrupo verbal correspondente ao elemento $u_{k-1}^{p^2}$, este elemento é uma identidade em C/V, mas, como veremos, $u_k^{p^2}$ não é. Logo, pelo teorema 2.18, a variedade $\mathbf{B}_{p^2}\mathbf{B}_p$ não tem base finita de identidades.

Seja A_m o grupo livre na variedade $\mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_{p+1}$, livremente gerado por $X = \{x_1, x_2, \ldots, x_m\}$. Consideremos $\{t_1, t_2, \ldots, t_{a_m}\}$ um transversal de $\gamma_{p+1}(A_m)$ em A_m. Para cada $g \in A_m$, existe $t_g \in \{t_1, \ldots, t_{a_m}\}$ e $z \in \gamma_{p+1}(A_m)$, tais que $g = t_g \cdot z$. Como $\gamma_{p+1}(A_m)$ está contido no centro de A_m e tem expoente p, segue que $g^p = t_g^p \cdot z^p = t_g^p$. Desta forma o número de p-ésimas potências em A_m é no máximo $a_m = \left|A_m/\gamma_{p+1}(A_m)\right|$.

Consideremos a cadeia

$$A_m = \gamma_1(A_m) \geq \gamma_2(A_m) \geq \ldots \geq \gamma_p(A_m) \geq \gamma_{p+1}(A_m).$$

Para $j = 2, 3, \ldots, p$, temos que $\gamma_j(A_m)/\gamma_{j+1}(A_m)$ é um p-grupo abeliano elementar, gerado por $[x_{i_1}, \ldots, x_{i_j}]\gamma_{j+1}$, $x_{i_l} \in X$, $l = 1, \ldots, j$. Assim $\left|\gamma_j(A_m)/\gamma_{j+1}(A_m)\right| \leq p^{m^j}$.

Para $j = 1$ temos que $A_m/\gamma_2(A_m)$ é abeliano de expoente p^2, dai $|A_m/\gamma_2(A_m)| \leq (p^2)^m$. Segue que

$$\left|A_m/\gamma_{p+1}(A_m)\right| \leq p^{2m}.p^{m^2}.p^{m^3}.\ldots.p^{m^p} = p^{2m+m^2+\ldots+m^p}.$$

Desta forma $a_m = \left|A_m/\gamma_{p+1}(A_m)\right| \leq p^{q_m}$, onde q_m é um polinômio de grau p em m. Por outro lado temos o

Proposição 4.3. *$\left|\gamma_{p+1}(A_m)\right| \geq p^{q'_m}$, onde q'_m é um polinômio de grau $p+1$ em m.*

Recordemos que um p-grupo abeliano elementar G é um espaço vetorial sobre o corpo de p-elementos $\mathbb{Z}_p$. Nesse sentido dizemos que os elementos $g_1, \ldots, g_n \in G$ são linearmente independentes se

$$\langle g_1, \ldots, g_n\rangle \cong \langle g_1\rangle \times \ldots \times \langle g_n\rangle.$$

Para provar a proposição anterior primeiramente consideraremos o

Lema 4.4. *Seja G_t o grupo livre na variedade $\mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_c$, livremente gerado por $Z = \{z_1, z_2, z_3, \ldots, z_t\}$. O p-grupo abeliano elementar $\gamma_c(G_t)$ pode ser visto como espaço vetorial sobre o corpo $\mathbb{Z}_p$. Nesse sentido, o conjunto de comutadores básicos na forma*

$$[z_{i_1}, z_{i_2}, \ldots, z_{i_c}], \tag{4.1}$$

tais que os índices $i_1, i_2, \ldots, i_c$ são distintos (isto é, $i_1 > i_2$ e $i_2 < i_3 < \ldots < i_c$), é linearmente independente.

Demonstração: Seja $\Gamma = \{c_1, \ldots, c_q\}$ um conjunto de comutadores básicos na forma (4.1), onde $c_1 = [z_{j_1}, z_{j_2}, \ldots, z_{j_c}]$. Suponhamos, por contradição, que este conjunto não é linearmente independente. Para isto podemos supor que esses comutadores contêm os mesmos elementos z_i, isto é, todos são formados pelos elementos $z_{j_1}, z_{j_2}, \ldots, z_{j_c}$. De fato, caso contrário, como G_t é relativamente livre, podemos considerar o endomorfismo ψ de G_t tal que

1. $\psi(z_i) = z_i$, se $i \in \{j_1, j_2, \ldots, j_c\}$,
2. $\psi(z) = 1$, se $z \in Z - \{j_1, j_2, \ldots, j_c\}$.

Na imagem de Γ por este homomorfismo restam apenas comutadores contendo elementos do conjunto $\{z_{j_1}, z_{j_2}, \ldots, z_{j_c}\}$. Como supomos que Γ é linearmente dependente, segue que imagem de Γ por ψ também é.

Desta forma podemos assumir que $t = c$.

Para provar esta independência linear exibiremos um quociente de G_t no qual esses elementos são linearmente independentes.

Sejam $S_c = \langle s_1 \rangle_p \times \ldots \times \langle s_c \rangle_p$ e $R_c = \langle r_1 \rangle_p \times \ldots \langle r_c \rangle_p$ p-grupos abelianos elementares c gerados. Seja ainda $W = S_c$ wr $R_c = D \rtimes R_c$, onde $D = \prod_{r \in R_c} S_r$ e $S_r \cong S_c$, para cada r. Façamos $h_i = s_i r_i, i = 1, 2, \ldots, c$ e $H = \langle h_i; i = 1, 2, \ldots, c \rangle < W$. Assim $H \in \mathbf{A}_p\mathbf{A}_p$ pois W pertence a esta variedade.

Escreveremos os elementos de D na forma $s_1^{p_1(r_1,\ldots,r_c)} \ldots s_c^{p_c(r_1,\ldots,r_c)}$, onde $p_i(r_1, \ldots, r_c)$ é um polinômio nas variáveis $r_1, \ldots, r_c$ e $s_i^{\bar{r}_1 + \bar{r}_2}$ representa o elemento $s_i^{\bar{r}_1} s_i^{\bar{r}_2}$; $\bar{r}_1, \bar{r}_2 \in R_c$.

Seja N o subgrupo normal de W gerado pelo fecho normal do conjunto

$$\{s_i^{(r_{i_1}-1)(r_{i_2}-1)\ldots(r_{i_c}-1)}; i_k = 1, 2, \ldots p\}.$$

Provaremos que o grupo $\bar{H} = H/H \cap N$ é nilpotente de classe c, o que implicará que $\bar{H}$ é um

quociente de G_c. Segue:

$$\begin{aligned}[h_1,h_2] &= [s_1r_1, s_2r_2] \\ &= r_1^{-1}s_1^{-1}r_2^{-1}s_2^{-1}s_1r_1s_2r_2 \\ &= s_1^{r_1(r_2-1)}s_2^{-r_2(r_1-1)}.\end{aligned}$$

Assim

$$[h_1,h_2,h_3] = [s_1^{r_1(r_2-1)}s_2^{-r_2(r_1-1)}, r_3] = s_1^{r_1(r_2-1)(r_3-1)}s_2^{-r_2(r_1-1)(r_3-1)}.$$

Indutivamente obtemos

$$[h_1,h_2,\ldots,h_n] = s_1^{r_1(r_2-1)(r_3-1)\ldots(r_n-1)}s_2^{-r_2(r_1-1)(r_3-1)\ldots(r_n-1)}.$$

Analogamente,

$$[h_{i_1},h_{i_2},\ldots,h_{i_n}] = s_{i_1}^{r_{i_1}(r_{i_2}-1)(r_{i_3}-1)\ldots(r_{i_n}-1)}s_{i_2}^{-r_{i_2}(r_{i_1}-1)(r_{i_3}-1)\ldots(r_{i_n}-1)}.$$

Segue que

$$[h_{i_1},h_{i_2},\ldots,h_{i_{c+1}}] = s_{i_1}^{r_{i_1}(r_{i_2}-1)(r_{i_3}-1)\ldots(r_{i_{c+1}}-1)}s_{i_2}^{-r_{i_2}(r_{i_1}-1)(r_{i_3}-1)\ldots(r_{i_{c+1}}-1)} = 1 \pmod N.$$

Logo $\gamma_{c+1}(\bar{H}) = \{1\}$, ou seja, $\bar{H}$ é nilpotente de classe no máximo c.

Desta forma existe um epimorfismo $\varphi : G_c \longrightarrow \bar{H}$, tal que $\varphi(z_i) = \bar{h}_i, i = 1,\ldots,c$.

É suficiente provar que os elementos $\varphi(c_i), i = 1,2,\ldots,q$, são linearmente independentes. Assim provaremos esta independência linear para comutadores do tipo

$$[\bar{h}_{i_1},\bar{h}_{i_2},\ldots,\bar{h}_{i_c}].$$

Temos

$$\begin{aligned}[h_{i_1},h_{i_2},\ldots,h_{i_c}] &= s_{i_1}^{r_{i_1}(r_{i_2}-1)(r_{i_3}-1)\ldots(r_{i_c}-1)}s_{i_2}^{-r_{i_2}(r_{i_1}-1)(r_{i_3}-1)\ldots(r_{i_c}-1)} \\ &= s_{i_1}^{(r_{i_2}-1)(r_{i_3}-1)\ldots(r_{i_c}-1)}s_{i_2}^{-(r_{i_1}-1)(r_{i_3}-1)\ldots(r_{i_c}-1)} \pmod N.\end{aligned}$$

Como estamos considerando comutadores básicos, devemos ter $i_1 > i_2$, e ainda $i_2 < i_3 < \ldots < i_c$.

Assim i_2 é o menor dos índices, isto é, $i_2 = 1$. Segue que

$$\begin{aligned}[h_{i_1}, h_{i_2}, \ldots, h_{i_c}] &= [h_{i_1}, h_1, \ldots, h_{i_1-1}, h_{i_1+1}, \ldots, h_c] \\ &= s_{i_1}^{(r_1-1)\ldots(r_{i_1-1}-1)(r_{i_1+1}-1)\ldots(r_c-1)} s_1^{-(r_2-1)\ldots(r_c-1)} \pmod{N}.\end{aligned}$$

Um comutador deste tipo fica determinado por i_1, isto é, se $i_1 = i_1^{'}$ então $[h_{i_1}, h_1, \ldots, h_{i_c}] = [h_{i_1^{'}}, h_1, \ldots, h_{i_c^{'}}]$. Além disso, não é difícil verificar que os elementos

$$s^{(r_1-1)\ldots(r_{i_1-1}-1)(r_{i_1+1}-1)\ldots(r_c-1)}, i = 1, 2, \ldots, c,$$

não pertencem a N. Desta forma temos $c-1$ comutadores. Em cada um destes comutadores aparece um elemento s_i diferente. Portanto, como cada conjunto da forma $\{s_{j_1}^{r^{(1)}}, \ldots, s_{j_c}^{r^{(c)}}; r^{(i)} \in R_c \text{ e } j_i \neq j_k, \text{ se } i \neq k\}$, é linearmente independente, segue os comutadores acima também o são. Isso prova que os comutadores que contêm os mesmos elementos são linearmente independentes.

□

Demonstração da Proposição 4.3: Sejam $[x_{i_1}, x_{i_2}, \ldots, x_{i_{p+1}}]$; $x_i \in X$, comutadores básicos de comprimento $p+1$. Como $\gamma_{p+1}(A_m)$ é gerado por comutadores básicos de comprimento $p+1$, provaremos que a quantidade destes comutadores linearmente independentes, que depende de m, é maior que algum polinômio de grau $p+1$ em m. Para isto consideraremos apenas comutadores desse tipo tais que os elementos $x_{i_1}, x_{i_2}, \ldots, x_{i_{p+1}}$ são distintos. Pelo lema 4.4 estes comutadores são linearmente independentes.

Inicialmente consideremos comutadores desse tipo com $i_2 = 1$. Como i_1 deve ser maior que i_2, temos $m-1$ opções para i_1. Pelo teorema 1.20 comutadores gerados por uma permutação de uma $(p-1)$-upla $(i_3, \ldots, i_{p+1})$ são iguais. Desta forma tomemos apenas um comutador para cada conjunto $\{i_3, \ldots, i_{p+1}\}$, onde $i_k \in \{2, 3, \ldots, m\}$ e $i_k \neq i_1$, $k = 3, 4, \ldots, p+1$. A quantidade destes conjuntos é

$$\frac{(m-2)!}{(p-1)!(m-p-1)!} = \frac{(m-2)(m-3)\ldots(m-p)}{(p-1)!}.$$

Assim para $i_2 = 1$ a quantidade destes comutadores básicos é maior que

$$\frac{(m-1)(m-2)(m-3)\ldots(m-p)}{(p-1)!} \geq \frac{(m-p)^p}{(p-1)!}.$$

De forma análoga, obtemos que para $i_2 = 2$ a quantidade destes comutadores básicos é maior que

$$\frac{(m-2)(m-3)(m-4)\ldots(m-p-1)}{(p-1)!} \geq \frac{(m-p-1)^p}{(p-1)!}.$$

Tomando $i_2 = 3,4,\ldots,m-p$, obtemos que a quantidade de comutadores básicos, de comprimento $p+1$ no grupo A_m, é maior que:

$$\begin{aligned} \tfrac{(m-p)^p}{(p-1)!} + \tfrac{(m-p-1)^p}{(p-1)!} + \ldots + \tfrac{1^p}{(p-1)!} &= \tfrac{1}{(p-1)!}((m-p)^p + (m-p-1)^p + \ldots + 1^p) \\ &= \tfrac{1}{(p-1)!}(n^p + (n-1)^p + \ldots + 1^p). \end{aligned}$$

Observe que para n par

$$1 + 2^p + \ldots + n^p = (1+n^p) + (2^p + (n-1)^p) + \ldots + ((\frac{n}{2})^p + (\frac{n+2}{2})^p).$$

Como cada uma das $\frac{n}{2}$ parcelas é maior do que $(\frac{n}{2})^p$, temos

$$n \cdot n^p \geq 1 + 2^p + \ldots + n^p \geq \frac{n}{2} \cdot (\frac{n}{2})^p = (\frac{n}{2})^{p+1}.$$

Fazendo de forma análoga para n impar obtemos que a expressão acima é um polinômio de grau $p+1$ em $n = m-p$, o que implica que é um polinômio de grau $p+1$ em m.

□

Decorre da proposição 4.3 que para cada l existe m tal que

$$a_m^l \leq p^{lq_m} < p^{q'_m} \leq \left|\gamma_{p+1}(A_m)\right|.$$

Isto significa que existe $d \in \gamma_{p+1}(A_m)$ o qual não é um valor de u_l em A_m. Por outro lado, aplicando o conhecido resultado de Meier-Wunderli (teorema 1.19), no grupo $A_m/x^p(A_m)$, temos que $\gamma_{p+1}(A_m) \subset x^p(A_m)$. Assim d é um valor de u_k, para algum $k > l$. Considerando o menor de tais k, podemos assumir que d não é um valor de u_{k-1}. Podemos escrever $d = g_1^p \ldots g_k^p$, onde $g_i \in A_m$. Seja $D = \langle d \rangle$ e $A = A_m$.

Seja B o grupo livre na variedade $\mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_p$ de posto igual a ordem de A e livremente gerado pelos elementos $\{b_a;\ a \in A\}$. O grupo A atua em B de forma natural: $(b_{a_1})^{a_2} = b_{a_1 a_2}$, é fácil ver que A é isomorfo a um subgrupo de Aut$B$. Seja C o produto semidireto de B por A, com esta ação. Mostraremos neste capítulo que o grupo que queremos construir é um quociente

do grupo C.

Observação 4.5. O subgrupo $\gamma_p(B)$ é um p-grupo abeliano elementar no centro de B gerado pelos elementos $[b_{a_1},\ldots,b_{a_p}]$, onde $a_i \in A$, $i = 1,\ldots,p$.

Os elementos $[b_{a_1},\ldots,b_{a_p}]$ serão denotados daqui em diante por $[[a_1,\ldots,a_p]]$.

A seguir construiremos um subgrupo R de $\gamma_p(B)$ com a propriedade de conter todos os valores em C da palavra $u_{k-1}^{p^2}$ mas não todos os valores de $u_k^{p^2}$. Isto implica que o subgrupo V correspondendo à palavra $u_{k-1}^{p^2}$ está contido em R mas o subgrupo W correspondendo à palavra $u_k^{p^2}$ não está. Disto temos que $V \subsetneq W$, assim o grupo quociente C/V satisfaz a identidade $u_{k-1}^{p^2}$ mas não satisfaz a identidade $u_k^{p^2}$. Observe que, como $u_{k'}$ é conseqüência de u_k desde que $k' < k$, o quociente C/V satisfaz todas as identidades $u_1^{p^2},\ldots,u_{k-1}^{p^2}$.

Agora vejamos o que acontece com um elemento de B quando é elevado à p-ésima potência.

Lema 4.6. *Se $x,y \in B$ se encontram na mesma classe lateral de B', então $x^p = y^p$.*

Demonstração: Primeiramente definamos:

$$c^{-b_o} = (c^{-1})^{b_0};$$

$$c^{b_1+b_2} = c^{b_1}c^{b_2};$$

$$c^{(b_0+b_1)(b_2+b_3)} = c^{b_0b_2+b_0b_3+b_1b_2+b_2b_3};$$

$c \in B', b_i \in B, i = 1,2,3,4$.

Temos que $x = yc$ para algum $c \in B'$. Dai

$$x^p = (yc)^p = ycyc\ldots yc = y^2c^ycyc\ldots yc = \ldots = y^pc^{y^{p-1}+y^{p-2}+\ldots+y+1}.$$

A demonstração do lema segue de dois fatos:

i) $c^{(y-1)^{p-1}} = c^{y^{p-1}-(p-1)y^{p-2}+\frac{(p-1)(p-2)}{2}y^{p-3}-\ldots-(p-1)y+1} = c^{y^{p-1}+y^{p-2}+\ldots+y+1}$,

onde $c \in B', y \in B$.

ii) $c^{(y-1)^n} = [c,\underbrace{y,y,\ldots,y}_{n}]$.

Mostraremos *ii*) por indução sobre n. O resultado é obvio para $n = 0$. Supondo válido para $n-1$ segue

$$\begin{aligned}
[c,\underbrace{y,\ y,\ \ldots,\ y}_{n}] &= [[c,\underbrace{y,\ y,\ \ldots,\ y}_{n-1}],y] \\
&= [c^{(y-1)^{n-1}},y] \\
&= c^{-(y-1)^{n-1}}y^{-1}c^{(y-1)^{n-1}}y \\
&= c^{-(y-1)^{n-1}}c^{(y-1)^{n-1}y} = c^{(y-1)^n}.
\end{aligned}$$

Portanto, $x^p = y^p[c,\underbrace{y,\ldots,y}_{p-1}] = y^p$. □

Seja S o subgrupo de B gerado pelo conjunto $\left\{b_a^p;\ a \in A\right\}$.

Corolário 4.7. *S está contido no centro de B.*

Demonstração:

$$\begin{aligned}
[b_{a_1},b_{a_2}^p] &= [b_{a_1},b_{a_2}][b_{a_1},b_{a_2}^{p-1}]^{b_{a_2}} \\
&= [b_{a_1},b_{a_2}]([b_{a_1},b_{a_2}][b_{a_1},b_{a_2}^{p-2}]^{b_{a_2}})^{b_{a_2}} \\
&= [b_{a_1},b_{a_2}][b_{a_1},b_{a_2}]^{b_{a_2}}[b_{a_1},b_{a_2}^{p-2}]^{b_{a_2}^2} \\
&= [b_{a_1},b_{a_2}][b_{a_1},b_{a_2}]^{b_{a_2}}[b_{a_1},b_{a_2}]^{b_{a_2}^2}[b_{a_1},b_{a_2}^{p-3}]^{b_{a_2}^3} \\
&\ \ \ldots \\
&= [b_{a_1},b_{a_2}][b_{a_1},b_{a_2}]^{b_{a_2}}[b_{a_1},b_{a_2}]^{b_{a_2}^2}\ldots[b_{a_1},b_{a_2}]^{b_{a_2}^{p-1}} \\
&= [b_{a_1},b_{a_2}]^{1+b_{a_2}+b_{a_2}^2+\ldots+b_{a_2}^{p-1}}.
\end{aligned}$$

Desta forma é conseqüência da demonstração do lema 4.6 (fatos *i*) e *ii*)) que $[b_{a_1},b_{a_2}^p] = 1$, o que prova que $S < Z(B)$. □

Observemos ainda que pelo teorema 2.14 B/B' é abeliano livre de expoente p^2, gerado livremente por $\{b_aB';a\in A\}$. Assim a imagem de S, no quociente por B', é um p-grupo abeliano elementar com base $\{b_a^pB';a\in A\}$. Logo $S\cap B'=\{1\}$.

Seja M o subgrupo de $\gamma_p(B)$ gerado pelos comutadores da forma $[[a_1,a_2,\ldots,a_p]]$, onde $\{a_1,a_2,\ldots,a_p\}$ é uma classe lateral de D, e L o subgrupo gerado por todos os outros comutadores do tipo $[[a_1,a_2,\ldots,a_p]]$. Como B é metabeliano satisfaz as seguintes relações:

$$\begin{array}{l}[[a_1,a_2,a_3,\ldots]][[a_2,a_3,a_1,\ldots]][[a_3,a_1,a_2,\ldots]]=1\\ [[a_1,a_2,\ldots,a_i,a_{i+1},\ldots]][[a_1,a_2,\ldots,a_{i+1},a_i,\ldots]]^{-1}=1\\ [[a_1,a_2,\ldots]][[a_2,a_1,\ldots]]=1.\end{array}\tag{4.2}$$

Além disso, temos a

Proposição 4.8. *$\gamma_p(B)$ é o produto direto de M e L.*

Demonstração: Seja $E=\{a_1,a_2,\ldots,a_p\}$ uma classe lateral de D. Como B é relativamente livre, existe um endomorfismo ϕ de B tal que:

1. $\phi(b_{a_i})=b_{a_i},\ i=1,2,\ldots,p$;
2. $\phi(b_a)=1,$ se $a\notin\{a_1,a_2,\ldots,a_p\}$.

Desta forma vemos que $\gamma_p(B)$ é o produto direto de dois subgrupos Γ_1 e Γ_2 gerados por comutadores de comprimento p; onde Γ_1 é gerado por comutadores onde todos os elementos pertencem ao conjunto E, e o Γ_2 é gerado por comutadores onde algum elemento não pertence à E. Isto é,

$$\begin{array}{rcl}\Gamma_1 &=& \langle\{[[a_{i_1},a_{i_2},\ldots,a_{i_p}]];a_i\in E\}\rangle,\\ \Gamma_2 &=& \langle\{[[a_{i_1},a_{i_2},\ldots,a_{i_p}]];a_i\notin E,\text{ para algum } i\}\rangle\end{array}$$

e

$$\gamma_p(B)=\Gamma_1\times\Gamma_2.$$

Basta verificar agora que não existem relações entre comutadores onde aparecem todos elementos de E e os que repetem algum elemento, ou seja,

$$\Delta_1\cap\Delta_2=\{1\},$$

onde

$$\Delta_1=\langle\ \{[[a_{i_1},a_{i_2},\ldots,a_{i_p}]];a_i\in E,i_r\neq i_s,\text{ se } r\neq s\}\ \rangle$$

e

$$\Delta_2 = \langle\ \{[[a_{i_1}, a_{i_2}, \ldots, a_{i_p}]]; a_i \in E, i_r = i_s, \text{ para alguns } r \neq s\}\ \rangle.$$

Para provar isto, tendo em vista o lema 3.3, definamos $\tilde{M}$ de forma semelhante à que foi definido $\bar{M}$. Sejam

$$\tilde{R} = \mathbb{Z}_p\langle \tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{q-1}\rangle,$$

a álgebra associativa livre com unidade, onde $q = |A|$, e $\tilde{J}_1, \tilde{J}_2, \tilde{J}_3$ os ideais de $\tilde{R}$ definidos tal como J_1, J_2, J_3. Agora definamos $\tilde{M}$ como o subgrupo do grupo das unidade de $\tilde{R}/\tilde{J}$, gerado por $y_i = 1 + \tilde{a}_i, i = 1, 2, \ldots, q-1$, onde $\tilde{J} = \tilde{J}_1 + \tilde{J}_2 + \tilde{J}_3$. Observe que, embora o fato de $\bar{M}$ ter expoente p dependa de $J > J_4$, o fato de $\bar{M}$ ser metabeliano e nilpotente de classe no máximo p segue de $J > J_1 + J_2 + J_3$. Analogamente $\tilde{M}$ é metabeliano e nilpotente de classe no máximo p. Seja $H = x^p(\tilde{M})\tilde{M}'$, isto é, o subgrupo de $\tilde{M}$ gerado por $\{g^p, [g_1, g_2]; g, g_1, g_2 \in \tilde{M}\}$. Pela definição de H temos que $\tilde{M}/H \in \mathbf{A}_p$. Por outro lado, como na demonstração do lema 3.5 não usamos que $J > J_4$, a forma análoga deste lema para $\tilde{M}$ é válida, o que implica que $H \in \mathbf{A}_p$. Logo $\tilde{M} \in \mathbf{A}_p\mathbf{A}_p \cap \mathbf{N}_p$. Como B é um grupo livre nesta variedade, segue que $\tilde{M}$ é um quociente de B, isto é, $\tilde{M} \cong B/N$, para algum subgrupo $N \lhd B$. Considerando a imagem de $\langle E\rangle$ neste quociente, o subgrupo Δ_1 é preservado (é isomorfo à sua imagem). De fato, isto segue de (3.4) e (3.5). No entanto, pela análoga da propriedade jj) de $\bar{M}$ para $\tilde{M}$, o subgrupo Δ_2 tem imagem trivial. Isto prova que a interseção acima é trivial. Assim a proposição está provada. □

Como $d = g_1^p \ldots g_k^p$, podemos considerar U um transversal de $D = \langle d\rangle$ em $x^p(A)$ tal que $1 \in U$, e T um transversal de $x^p(A)$ em A tal que $T \supset \left\{1, g_k, \ldots, {g_k}^{p-1}\right\}$.

Observemos que, pelo lema 4.4, os elementos

$$g(t,u,i) = [[tud^i, tu, tud, \ldots, tud^{p-1}]], i = 1, \ldots, p-1;\ t \in T \text{ e } u \in U;$$

são linearmente independentes. Por outro lado, um comutador de peso p, cujos elementos formam uma classe lateral de D, tem a forma

$$[[tud^i, tud^j, tu, \ldots, tud^{p-1}]] = g(t,u,i)g(t,u,j)^{-1},\ 0 \leq i, j \leq p-1 \tag{4.3}$$

onde $g(t,u,0) = 1;\ t \in T$ e $u \in U$.

De fato, de (4.2), temos

$$[[tud^i, tud^j, tu, \ldots, tud^{p-1}]][[tud^j, tu, tud^i, \ldots, tud^{p-1}]][[tu, tud^i, tud^j, \ldots, tud^{p-1}]] = 1.$$

Logo

$$[[tud^i, tud^j, tu, \ldots, tud^{p-1}]] = ([[tud^j, tu, tud^i, \ldots, tud^{p-1}]][[tu, tud^i, tud^j, \ldots, tud^{p-1}]])^{-1}.$$

Segue que

$$[[tud^i, tud^j, tu, \ldots, tud^{p-1}]] = [[tud^i, tu, \ldots, tud^{p-1}]]([[tud^j, tu, \ldots, tud^{p-1}]])^{-1}.$$

Logo

$$[[tud^i, tud^j, tu, \ldots, tud^{p-1}]] = g(t,u,i)g(t,u,j)^{-1}.$$

Segue da observação 4.5 e de (4.3) que os elementos $g(t,u,i)$ formam uma base para o subgrupo M. Estes são comutadores básicos para uma ordem tal que

$$tu < tud < \ldots < tud^{p-1}, \text{ para todos } t, u.$$

Logo, pelo lema 4.4, estes comutadores são linearmente independentes.

Façamos $g_{t,i} = g(t,1,i)$. Sejam P o subgrupo de M gerado por $g_{t,i}$ ($t \in T$, $i = 1, \ldots, p-1$), e N o subgrupo de M gerado pelos produtos da forma $g(t,u,i){g_{t,i}}^{-1}$. Notemos que $P \cap N = \{1\}$. Com efeito, para $h \in P \cap N$, por um lado temos

$$h = g_{t_1,i_1}^{n_1} \cdot \ldots \cdot g_{t_r,i_r}^{n_r},$$

pois $h \in N$. Por outro lado

$$h = (g({t'}_1, u_1, {i'}_1) g_{t_{r+1},i_{r+1}}^{-1})^{m_1} \cdot \ldots \cdot (g({t'}_s, u_s, {i'}_s) g_{t_{r+1},i_{r+1}}^{-1})^{m_s},$$

pois $h \in P$. Isto implica que

$$g_{t_1,i_1}^{n_1} \cdot \ldots \cdot g_{t_r,i_r}^{n_r} \cdot g_{t_{r+1},i_{r+1}}^{m_1} \cdot \ldots \cdot g_{t_{r+s},i_{r+s}}^{m_s} = g({t'}_1, u_1, {i'}_1)^{m_1} \cdot \ldots \cdot g({t'}_s, u_s, {i'}_s)^{m_s}.$$

Como os elementos $g(t,u,i)$ são linearmente independentes segue que $u_1 = u_2 = \ldots = u_s = 1$, logo $n_1 = n_2 = \ldots = n_r = 0$. Portanto $h = 1$.

Por outro lado, é claro que P e N geram M. Logo M é o produto direto de P e N. Definamos $R \triangleleft B$ por $R = \langle S, N, L \rangle$, ou seja, $R = S \times N \times L$. É importante enfatizar que, por $S < R$, R contêm p-ésimas potências de geradores. Por $L < R$, R contém comutadores de comprimento p onde os elementos não formam uma classe lateral de D. Temos ainda que, por $N < R$, $g(t,u,i) =$

$g_{t,i}$ (mod R).

Consideremos um valor de u_l em C

$$(h_1b_1)^p \dots (h_lb_l)^p = h_1^p \dots h_l^p b = ab,$$

onde $a = h_1^p \dots h_l^p$ é um valor de u_l em A, $h_i \in A$ e $b,\ b_i \in B$. Assim um valor de u_l em C pode ser escrito na forma

$$f = ab_{a_1} \dots b_{a_r} \tag{4.4}$$

onde $b = b_{a_1} \dots b_{a_r}$ e $a_i \in A$.

Desta forma um valor de $u_l^{p^2}$ em C pode ser representado como segue

$$\begin{aligned} f^{p^2} &= (ab_{a_1} \dots b_{a_r})^{p^2} \\ &= [\underbrace{(ab_{a_1} \dots b_{a_r})(ab_{a_1} \dots b_{a_r}) \dots (ab_{a_1} \dots b_{a_r})}_{p\ fatores}]^p \\ &= (b_{a_1a^{p-1}} \dots b_{a_ra^{p-1}} b_{a_1a^{p-2}} \dots b_{a_ra^{p-2}} \dots b_{a_1} \dots b_{a_r})^p. \end{aligned}$$

Pelo lema 4.6 os geradores podem ser arbitrariamente rearranjados quando elevados à p-ésima potência. Assim, juntando geradores iguais e renumerando os a_i se necessário, podemos obter

$$f^{p^2} = (b_{a_1}^{\alpha_1} b_{a_1a}^{\alpha_1} \dots b_{a_1a^{p-1}}^{\alpha_1} \dots b_{a_n}^{\alpha_n} b_{a_na}^{\alpha_n} \dots b_{a_na^{p-1}}^{\alpha_n})^p, \tag{4.5}$$

onde $b_{a_i} \neq b_{a_ja^k}$ (ou, equivalentemente, $a_i \neq a_ja^k$) para $i \neq j$ e $k = 0, 1, \dots, p-1$, pois juntamos geradores iguais.

Lema 4.9. *Sejam $g_i \in B; \alpha_i \in \mathbb{N}; i = 1, 2, \dots, p$. Temos*

$$[g_1^{\alpha_1}, g_2^{\alpha_2}, \dots, g_p{}^{\alpha_p}] = [g_1, g_2, \dots, g_p]^{\alpha_1\alpha_2\dots\alpha_p}.$$

Demonstração: Segue diretamente da proposição 1.7.

□

Lema 4.10. *Sejam $b_1, b_2, \dots, b_p$ geradores livres de B, tais que $b_1 < b_2 < \dots < b_p$. Então*

$$(b_1b_2 \dots b_p)^p = b_1^p \cdot b_2^p \cdot \dots \cdot b_p^p \cdot c' \cdot c''.$$

Nesta expressão

$$c' = [b_2, b_1, b_3, \ldots, b_p]^{-1} \ldots [b_i, b_1, b_2, \ldots, b_{i-1}, b_{i+1}, \ldots, b_p]^{-1} \ldots [b_p, b_1, b_2, \ldots, b_{p-1}]^{-1}$$

e c'' é o produto dos demais comutadores básicos de comprimento p, isto é, comutadores básicos na forma $[b_{i_1}, \ldots, b_{i_p}]$, tal que $b_r = b_s$, para algum par (r,s), com $r \neq s$.

Demonstração: Recordemos que aplicando o processo de coleção surgem apenas comutadores básicos. Como B é nilpotente, obtemos

$$(b_1 b_2 \ldots b_p)^p = b_1^p \cdot b_2^p \cdot \ldots \cdot b_p^p \cdot c_1^{e_1} \cdot \ldots \cdot c_t^{e_t}$$

onde os elementos c_i são comutadores e os expoentes e_j são dados por

$$e_j = b_1 n^{(1)} + b_2 n^{(2)} + \ldots + b_l n^{(l)}.$$

Nesta expressão n é a potência a qual estamos elevando, neste caso p, l é o comprimento de comutador c_j, $b_i \in \mathbb{Z}$ e $n^{(k)} = \frac{n(n-1)\ldots(n-k+1)}{k!}$. Desta fórmula segue que os comutadores de comprimento $l \leq p-1$ aparecem com expoente múltiplo de p. Assim

$$(b_1 b_2 \ldots b_p)^p = b_1^p \cdot b_2^p \cdot \ldots \cdot b_p^p \pmod{\gamma_p(B)}.$$

Para obter a expressão de c', calcularemos o expoente do comutador $[b_p, b_1, \ldots, b_{p-1}]$. Haja vista que, permutando os geradores b_i, obtemos que os expoentes dos comutadores do tipo $[b_{i_1}, b_1, b_{i_3} \ldots b_{i_p}], \{i_1, \ldots i_p\} = \{1, 2, \ldots, p\}$, são todos iguais. Passemos aos cálculos.

$$(b_1 b_2 \ldots b_p)^p = \underbrace{(b_1 b_2 \ldots b_p) \ldots (b_1 b_2 \ldots b_p)}_{p}$$

$$\begin{aligned} = \; & b_1^p b_2 [b_2, b_1^{p-1}] \ldots b_p [b_p, b_1^{p-1}] b_2 [b_2, b_1^{p-2}] \ldots b_p [b_p, b_1^{p-2}] \ldots b_2 [b_2, b_1] \ldots b_p \\ & \times [b_p, b_1] \ldots b_2 \ldots b_p. \end{aligned}$$

Como estamos interessados no expoente do comutador $[b_p, b_1 \ldots b_{p-1}]$, não vamos nos preocupar com os comutadores onde não aparece o elemento b_p. Em outras palavras vamos explicitar

os comutadores com o elemento b_p e ocultar os demais comutadores. Temos

$$(b_1b_2\dots b_p)^p = b_1^p\dots b_p[b_p,b_1^{(p-1)}]\dots b_p[b_p,b_1]\dots b_p$$

$$= b_1^pb_2^p\dots b_p[b_p,b_2^{(p-1)}][b_p,b_1^{(p-1)}][b_p,b_1^{(p-1)},b_2^{(p-1)}]\dots b_p[b_p,b_2][b_p,b_1][b_p,b_1,b_2]\dots b_p$$

$$= b_1^pb_2^pb_3^p\dots b_pc_1[b_p,b_1^{(p-1)},b_2^{(p-1)}][b_p,b_1^{(p-1)},b_2^{(p-1)},b_3^{(p-1)}]\dots b_pc_2[b_p,b_1,b_2] \times[b_p,b_1,b_2,b_3]\dots b_p,$$

onde

$$c_1 = [b_p,b_2^{(p-1)}][b_p,b_2^{(p-1)},b_3^{(p-1)}][b_p,b_1^{(p-1)}][b_p,b_1^{(p-1)},b_3^{(p-1)}]$$

e

$$c_2 = [b_p,b_2^{(p-1)}][b_p,b_2^{(p-1)},b_3^{(p-1)}][b_p,b_1^{(p-1)}][b_p,b_1^{(p-1)},b_3^{(p-1)}].$$

Observe que os elementos c_1 e c_2 não colaborarão com o expoente de $[b_p,b_1\dots b_{p-1}]$, haja vista que, continuando o processo de coleção, comutadores obtidos de c_1 e c_2 não conterão um dos elementos b_1,b_2.

Desta forma, continuando este processo, obtemos

$$(b_1b_2\dots b_p)^p$$

$$= b_1^pb_2^p\dots b_{p-1}^p\dots b_pc_3[b_p,b_1^{(p-1)},\dots,b_{p-2}^{(p-1)}][b_p,b_1^{(p-1)},\dots,b_{p-2}^{(p-1)},b_{p-1}^{(p-1)}]\dots b_pc_4 \times[b_p,b_1,\dots,b_{p-2}][b_p,b_1,\dots,b_{p-1}]\dots b_p$$

$$= b_1^pb_2^p\dots b_{p-1}^p\dots b_pc_3[b_p,b_1^{(p-1)},\dots,b_{p-2}^{(p-1)}][b_p,b_1,\dots,b_{p-1}]^{(p-1)^{p-1}}\dots b_pc_4 \times[b_p,b_1,\dots,b_{p-2}][b_p,b_1,\dots,b_{p-1}]\dots b_p,$$

onde os elementos c_3 e c_4 tem as mesmas propriedades de c_1 e c_2, isto é, são produtos de comutadores que contêm o elemento b_p mas não colaboram com o expoente de $[b_p,b_1\dots b_{p-1}]$. No último passo apareceram comutadores que contêm o elemento b_p na última posição, isto é, elementos do tipo $[b_{i_1},b_{i_2},\dots,b_{i_{p-1}},b_p]$. Todavia, pelo lema 4.4, estes comutadores não mudam o expoente de $[b_p,b_1,\dots,b_{p-1}]$. Assim

$$(b_1b_2\dots b_p)^p = b_1^pb_2^p\dots b_p^p\dots c_5[b_p,b_1,\dots,b_{p-1}]^{(p-1)^{p-1}}\dots c_6[b_p,b_1,\dots,b_{p-1}]^{(p-2)^{p-1}}\dots b_p \times c_7[b_p,b_1,\dots,b_{p-1}]\dots b_p.$$

Assim o expoente deste comutador é

$$(p-1)^{p-1}+(p-2)^{p-1}+\ldots+2^{p-1}+1.$$

Pelo pequeno teorema de Fermat, temos

$$a^{p-1}\equiv 1 \pmod{p},$$

desde que $mdc(a,p)=1$. Logo tal expoente é

$$p-1=-1 \pmod{p}.$$

Portanto,

$$(b_1b_2\ldots b_p)^p = b_1^p\cdot b_2^p\cdot\ldots\cdot b_p^p\cdot\prod_i[b_i,b_1,b_2,\ldots,b_{i-1},b_{i+1},\ldots,b_p]^{-1}\cdot c''.$$

□

Denotaremos por $\overline{g}$ a imagem de $g\in A$ no grupo quociente $A/x^p(A)$.

Lema 4.11. *O elemento $f^{p^2}\in R$ se, e somente se, $D\cap\langle a\rangle=\{1\}$ ou, para cada $k\in A/x^p(A)$, o número de a_i presentes na representação de f em 4.4 tal que $\overline{a_i}=k$ é múltiplo de p.*

Demonstração: Os geradores de B podem ser ordenados satisfazendo a condição

$$tu<tud<\ldots<tud^{p-1}, \text{ para todos } t,u.$$

Aplicando o processo de coleção, surgirão apenas comutadores básicos. Entre esses, assim como no lema anterior, os de comprimento $l\leq p-1$ aparecem com expoente múltiplo de p. Isto se deve a fórmula para o expoente e_j de um comutador c_j, pois

$$e_j=b_1n^{(1)}+b_2n^{(2)}+\ldots+b_ln^{(l)},$$

onde n a é a potência a qual estamos elevando, l é o comprimento de comutador c_j, $b_i\in\mathbb{Z}$ e $n^{(k)}=\frac{n(n-1)\ldots(n-k+1)}{k!}$. Como neste caso $n=p$, é claro que para $l<p$ o expoente e_j é múltiplo de p.

Como B é metabeliano e nilpotente de classe p restam, na representação de f^{p^2}, comutadores

básicos de comprimento p. Esses elementos são da forma

$$[[a_{i(1)}a^{j(1)},\ldots,a_{i(p)}a^{j(p)}]]. \tag{4.6}$$

Assumamos primeiramente que $D\cap\langle a\rangle=\{1\}$, assim comutadores na forma (4.6) nos quais aparecem a_ia^j e a_ia^k estão contidos em R. Com efeito, caso contrário, pela definição de R, a_ia^j e a_ia^k estariam na mesma classe lateral de D, ou seja, $a_ia^j=a_ia^kd^r$, o que é uma contradição.

Por outro lado, seja $[[a_{i(1)}a^{j(1)},\ldots,a_{i(p)}a^{j(p)}]]$ é um comutador na forma (4.6) tal que o conjunto $\{a_{i(1)}a^{j(1)},\ldots,a_{i(p)}a^{j(p)}\}$ é uma classe lateral de D. Renumerando os a_i e substituindo a_ia^k por a_i podemos assumir que

$$\{a_{i(1)}a^{j(1)},\ldots,a_{i(p)}a^{j(p)}\}=\{a_1,a_2,\ldots,a_p\}=\{a_1,a_1d,\ldots,a_1d^{p-1}\}.$$

Segue que os comutadores contendo $a_{\bar{i}(1)}a^{\bar{j}(1)}$ e $a_{\bar{i}(2)}a^{\bar{j}(2)}$, onde $\bar{i}(1)\leq p<\bar{i}(2)$ (em outras palavras $\bar{i}(1)\in\{i(1),\ldots,i(p)\}$ e $\bar{i}(2)\notin\{i(1),\ldots,i(p)\}$), pertencem à R. De fato, se $a_{\bar{i}(1)}a^{\bar{j}(1)}$ e $a_{\bar{i}(2)}a^{\bar{j}(2)}$ pertencesse a mesma classe lateral de D teríamos

$$a_{\bar{i}(1)}a^{\bar{j}(1)}d^m=a_{\bar{i}(2)}a^{\bar{j}(2)},$$

como $a_{\bar{i}(1)}d^ma^{\bar{j}(1)-\bar{j}(2)}=a_{\bar{i}}a^{\bar{j}(1)-\bar{j}(2)}$, para algum $\bar{i}\leq p$, segue que

$$a_{\bar{i}}a^{\bar{j}(1)-\bar{j}(2)}=a_{\bar{i}(2)}.$$

Isto não pode ocorrer, pois, pela representação de f^{p^2}, $a_i\neq a_ja^k$ para $i\neq j$ e $k=0,1,\ldots,p-1$.

Resta-nos agora considerar comutadores na forma (4.6) nos quais os elementos formam o conjunto $\{a_1a^j,a_1da^j,\ldots,a_1d^{p-1}a^j\}$. Estes são comutadores do tipo

$$[[tud^ia^j,tua^j,tuda^j,\ldots,tud^{p-1}a^j]]=g(t,u,i)^{a^j} \tag{4.7}$$

onde $tu=a_1,t\in T,u\in U,0\leq j\leq p-1,0\leq i\leq p-1$. Observe que utilizamos o fato de que, se G é um grupo, então

$$[a_1,\ldots,a_s]^c=[a_1^c,\ldots,a_s^c],$$

para todos $a_i,c\in G$.

O expoente de tal comutador não depende de i ou j. Com efeito, não depende de j, pois estamos apenas conjugando por a^j. Para ver que não depende de i, para $j=0$ por exemplo,

podemos supor que eles são provenientes da expressão $b_{a_1}^{\alpha_1} b_{a_1 d}^{\alpha_2} \dots b_{a_1 d^{p-1}}^{\alpha_p}$. Desta forma verificaremos isto para a expressão

$$(b_1^{\alpha_1} b_2^{\alpha_2} \ \dots \ b_p^{\alpha_p})^p = (y_1 y_2 \ \dots \ y_p)^p,$$

onde $y_i = b_i^{\alpha_i}$. Aplicando o processo de coleção a esta última expressão temos que a quantidade de comutadores na forma

$$[y_i, y_1, \dots, y_p] = [b_i^{\alpha_i}, b_2^{\alpha_2}, \dots, b_p^{\alpha_p}]$$

não depende de i. Desta forma, pelo lema 4.9, o expoente de um comutador em (4.7) não depende de i. Logo, pelo que foi dito acima, a imagem do elemento f^{p^2} no quociente B/R é igual à um produto de elementos do tipo

$$\prod_{i=1,j=0}^{i,j=p-1} g(t,u,i)^{\alpha a^j} = \left(\prod_{i=1}^{p-1} \prod_{j=0}^{p-1} g(t,u,i)^{a^j} \right)^{\alpha}.$$

Assim, para que f^{p^2} pertença à R, é suficiente que

$$\prod_{j=0}^{p-1} g(t,u,i)^{a^j} \in R, \text{para todos } t \in T, u \in U, 1 \leq i \leq p-1.$$

Como $x^p(A)$ é um p-grupo abeliano elementar, podemos assumir que U é um grupo. Desta forma, se $v \in U$, então $g(t,u,i)^v = g(t,uv,i) = g(t,u,i) \pmod R$. Logo $a = vd^k$, e

$$\prod_{j=0}^{p-1} g(t,u,i)^{a^j} = \prod_{j=0}^{p-1} g(t,u,i)^{v^j d^{kj}} = \prod_{j=0}^{p-1} g(t,u,i)^{d^j}.$$

De (4.3) podemos obter

$$g(t,u,i)^{d^j} = [[tud^{i+j}, tud^j, tu, \dots, tud^{p-1}]] = g_{i,i+j} g_{i,j}^{-1} \pmod R,$$

finalmente temos

$$\prod_{j=0}^{p-1} g(t,u,i)^{a^j} = \prod_{j=0}^{p-1} g_{i,i+j} g_{i,j}^{-1} = \prod_{j=0}^{p-1} g_{i,i+j} \prod_{j=0}^{p-1} g_{i,j}^{-1} = \prod_{j=0}^{p-1} g_{i,j} \prod_{j=0}^{p-1} g_{i,j}^{-1} = 1 \pmod R.$$

Isto completa a prova de que $D \cap \langle a \rangle = \{1\}$ implica que $f^{p^2} \in R$.

No outro caso temos que $a = d^k$ para algum $k \in \mathbb{N}$. Refaçamos as contas para f^{p^2}.

$$\begin{aligned}
f^{p^2} &= (d^k b_{a_1} \dots b_{a_r})^{p^2} \\
&= [\underbrace{(d^k b_{a_1} \dots b_{a_r})(d^k b_{a_1} \dots b_{a_r}) \dots (d^k b_{a_1} \dots b_{a_r})}_{p \ fatores}]^p \\
&= (b_{a_1 d^{k(p-1)}} \dots b_{a_r d^{k(p-1)}} b_{a_1 d^{k(p-2)}} \dots b_{a_r d^{k(p-2)}} \dots b_{a_1} \dots b_{a_r})^p \\
&= (b_{a_1 d^{(p-1)}} \dots b_{a_r d^{(p-1)}} b_{a_1 d^{(p-2)}} \dots b_{a_r d^{(p-2)}} \dots b_{a_1} \dots b_{a_r})^p \\
&= (b_{a_1} b_{a_1 d} \dots \ b_{a_1 d^{p-1}} \dots b_{a_r} b_{a_r d} \dots b_{a_r d^{p-1}})^p, \\
&= (b_{a_1}^{\alpha_1} b_{a_1 d}^{\alpha_1} \dots \ b_{a_1 d^{p-1}}^{\alpha_1} \dots b_{a_n}^{\alpha_n} b_{a_n d}^{\alpha_n} \dots b_{a_n d^{p-1}}^{\alpha_n})^p,
\end{aligned}$$

onde $a_i \neq a_j d^k$ para $i \neq j$; $k = 0, 1, \dots, p-1$ e $0 < \alpha_i \leq p^2$. O expoente α_j é igual ao número de a_i aparecendo na representação de f em (4.4) pertencendo a mesma classe lateral de D que a_j.

Façamos $a_j = t_j u_j d^{i_j}$, $j = 1, 2, \dots, n$. Apliquemos novamente o processo de coleção à expressão de f^{p^2}. A imagem do elemento f^{p^2} no quociente B/R, assim como anteriormente, é um produto de comutadores básicos de comprimento p, onde elementos formam uma classe lateral de D. Em outras palavras, a imagem de f^{p^2} neste quociente é igual a um produto de elementos do tipo

$$[[tud^i, tu, \dots \ , tud^{p-1}]] = g(t,u,i) = g_{t,i} \ (\text{mod } R). \tag{4.8}$$

Como na expressão de f^{p^2} acima juntamos geradores cujos índices pertencem à mesma classe lateral de D, segue que um comutador $[[a_{i(1)} d^{j(1)}, \dots, a_{i(p)} d^{j(p)}]]$ tal que $a_{i(r)} \neq a_{i(s)}$, para alguns r, s, pertencem à R. Logo

$$\begin{aligned}
f^{p^2} &= (b_{a_1}^{\alpha_1} b_{a_1 d}^{\alpha_1} \dots \ b_{a_1 d^{p-1}}^{\alpha_1})^p \dots (b_{a_n}^{\alpha_n} b_{a_n d}^{\alpha_n} \dots b_{a_n d^{p-1}}^{\alpha_n})^p \\
&= ((b_{a_1} b_{a_1 d} \dots \ b_{a_1 d^{p-1}})^{\alpha_1})^p \dots ((b_{a_n} b_{a_n d} \dots \ b_{a_n d^{p-1}})^{\alpha_n})^p \\
&= (b_{a_1} b_{a_1 d} \dots \ b_{a_1 d^{p-1}})^{\alpha_1 p} \dots (b_{a_n} b_{a_n d} \dots \ b_{a_n d^{p-1}})^{\alpha_n p}.
\end{aligned}$$

Por outro lado, como um comutador em (4.8) não depende de u, podemos substituir a_j por

$t_j d^{i_j}$. Desta forma, reordenando se necessário, obtemos

$$f^{p^2} = (b_{t_1} b_{t_1 d} \dots\ b_{t_1 d^{p-1}})^{\alpha_1 p} \dots (b_{t_n} b_{t_n d} \dots\ b_{t_n d^{p-1}})^{\alpha_n p}.$$

Observemos que mesmo para $j_1 \neq j_2$ podemos ter $t_{j_1} = t_{j_2}$. Mais ainda, $t_{j_1} = t_{j_2}$ se, e somente se, $\bar{a}_{j_1} = \bar{a}_{j_2} = \bar{t}_{j_1}$. Assim, juntando na expressão acima potências com mesmo t_j, temos

$$f^{p^2} = (b_{t_1} b_{t_1 d} \dots\ b_{t_1 d^{p-1}})^{\beta_1 p} \dots (b_{t_n} b_{t_n d} \dots\ b_{t_n d^{p-1}})^{\beta_n p}.$$

Observe que o expoente β_j é igual ao número de a_i aparecendo na representação de f pertencendo a mesma classe lateral de $x^p(A)$ que a_j. Desta forma é claro que se o número de a_i presentes na representação de f em (4.4) tal que $\overline{a_i} = k$ é múltiplo de p, então $f^{p^2} \in R$. Para provar o lema no outro sentido suponhamos, por exemplo, que β_1 não é múltiplo de p. Como estes comutadores são linearmente independentes, é suficiente provar que o expoente de um comutador de comprimento p, quando aplicamos o processo de coleção à expressão

$$(b_{t_1} b_{t_1 d} \dots\ b_{t_1 d^{p-1}})^p,$$

não é múltiplo de p. No entanto, segue diretamente do lema 4.10 que este expoente é -1, o que prova o lema. □

Demonstração do teorema 4.1: Como V é o subgrupo verbal relativo à palavra $u_{k-1}^{p^2}$, temos que $u_{k-1}^{p^2}$ é uma identidade em C/V. Provemos agora que $u_k^{p^2}$ não é uma identidade em C/V. Segue imediatamente do lema 4.11 que R contêm todos os valores de u_l em C quando $l < k$. Haja vista que, neste caso, a é um valor de u_l e d não o é. Assim $V \subseteq R$. Por outro lado, considerando os elementos $g_1, \dots, g_{k-1}, g_k b$, temos

$$(g_1^p \dots g_{k-1}^p (g_k b)^p)^{p^2} = (d b_{g_k^{p-1}} \cdot b_{g_k^{p-2}} \cdot \dots \cdot b)^{p^2},$$

pelo lema 4.11 este elemento não se encontra em R. Logo o subgrupo verbal W, relativo à palavra $u_k^{p^2}$, não está contido em R. Isto implica que $V \subsetneq W$. Portanto $u_k^{p^2}$ não é uma identidade em C/V. □

Referências Bibliográficas

[1] S. I. Adyan, *Infinite irreducible systems of group identities*, Dokl. Akad. Nauk SSSR **190** (1970), 499–501.

[2] Y. A. Bahturin, *Basic structures of modern algebra*, Mathematics and its Applications, vol. 265, Kluwer Academic Publishers Group, Dordrecht, 1993.

[3] R. M. Bryant, *Some infinitely based varieties of groups*, J. Austral. Math. Soc. **16** (1973), 29–32, Collection of articles dedicated to the memory of Hanna Neumann. I.

[4] D. E. Cohen, *On the laws of a metabelian variety*, J. Algebra **5** (1967), 267-273.

[5] C. K. Gupta and A. N. Krasilnikov, *Metanilpotent varieties without torsion and varieties of groups of prime power exponent*, International Jornal of Algebra and Computation, vol. 6, no. 3 (1996), 325–338.

[6] C. K. Gupta and A. N. Krasilnikov, *The finite basis question for varieties of groups—some recent results*, Illinois J. Math. **47** (2003), no. 1-2, 273–283, Special issue in honor of Reinhold Baer (1902–1979).

[7] M. Hall Jr., *The theory of groups*, Chelsea Publishing Co., New York, 1976, Reprinting of the 1968 edition.

[8] M. I. Kargapolov and Ju. I. Merzljakov, *Fundamentals of the theory of groups*, Graduate Texts in Mathematics, vol. 62, Springer-Verlag, New York, 1979, Translated from the second Russian edition by Robert G. Burns.

[9] A. N. Krasilnikov, *On the group of units of a ring, whose associative lie ring is metabelian*, Usp. Mat. Nauk **47** 6 (1992) 217-218.

[10] Ju. G. Kleiman, *The basis of a product variety of groups. I, II*, Izv. Akad. Nauk SSSR Ser. Mat. Tom **38** (1974), 481 –489; ibid. **38** (1974).

[11] P. A. Kozhevinikov, *Varieties of groups of prime expoent and identities with large power*, Ph. D. Thesis, Moscow State University, 2000.

[12] R. C. Lyndon, *Two notes on nilpotents groups*, Proc. Amer. Math. Soc. **3** (1952), 579-583. MR 14,242a.

[13] H. Meier-Wunderli, *Metabelische gruppen*, Comm. Math. Helv. **25** (1951) 1-10.

[14] H. Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967.

[15] A. Ju. Olshanskii, *The finite basis problem for identities in groups*, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 376–384.

[16] A. Ju. Olshanskii, *Geometry of defining relations in groups*, Kluwer Akad. Publishers, (1991).

[17] D. J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996.

[18] J. J. Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[19] S. K. Sharma and J. B. Srivastava, *Lie centrally metabelian groups*, J. Algebra **151** (1992) 476-486.

[20] M. R. Vaughan-Lee, *Uncountably many varieties of groups*, Bull. London Math. Soc. **2** (1970), 280–286.