Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre o Número de Dilworth e p-Grupos Metabelianos Delgados

por

Leonardo de Amorim e Silva

Brasília
2006

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre o número de Dilworth e p-Grupos Metabelianos Delgados

por

Leonardo de Amorim e Silva

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

MESTRE EM MATEMÁTICA

09 de agosto de 2006

Comissão Examinadora:

Prof. Norai Romeu Rocco - Orientador (MAT/UnB)

Paul Zalesski
Prof. Pavel Zalesski - Membro (MAT/UnB)

Rudolf Maier
Prof. Rudolf Richard Maier - Membro (MAT/UnB)

Agradecimentos

Agradeço a Deus por me dar forças para conseguir mais essa conquista.

À minha namorada e companheira, Gisliane, por todo seu amor, carinho, compreensão, por toda sua força e apoio nos momentos de maiores dificuldades.

Ao meu orientador, Prof. Noraí Romeu Rocco, pela orientação, pelo incentivo, pelas críticas construtivas e por toda ajuda.

Aos meus pais, Marise e Luiz por todo e apoio, carinho, compreensão e ensinamentos durante toda minha vida.

Aos meus irmãos, Leandro, Mirna, Luiza, Dudu e João Vitor.

À todos os meus amigos e colegas do Departamento de Matemática da UnB em especial ao Euro, por sempre me aconselhar, ajudar e lutar para que eu pudesse terminar o mestrado.

Finalmente agradeço a todas as pessoas que me ajudaram direta ou indiretamente durante esse período do curso.

Resumo

Neste trabalho abordamos questões relacionadas à largura do reticulado dos subgrupos de um grupo e estudamos p-grupos metabelianos delgados. Tais grupos, dentre os quais se inserem os p-grupos de classe maximal, são assim denominados pelo fato de apresentarem largura normal $p + 1$.

Abstract

In this work we approached subjects related to the width of the lattices of the subgroups of a group and we studied metabelian thin p-groups. Such groups, among which insert the maximal class p-groups, are denominated like this by the fact of they present width normal $p+1$.

Sumário

Introdução

Neste trabalho fazemos um estudo sobre p-grupos metabelianos delgados, que são grupos que possuem largura normal $p+1$. Nosso estudo tem como base os artigos de Brandl, Caranti e Scoppola *"Metabelian thin p-groups"*, Szekeres *"Metabelian groups with two generators"* e Brandl *"The Dilworth number of subgroup lattices"*.

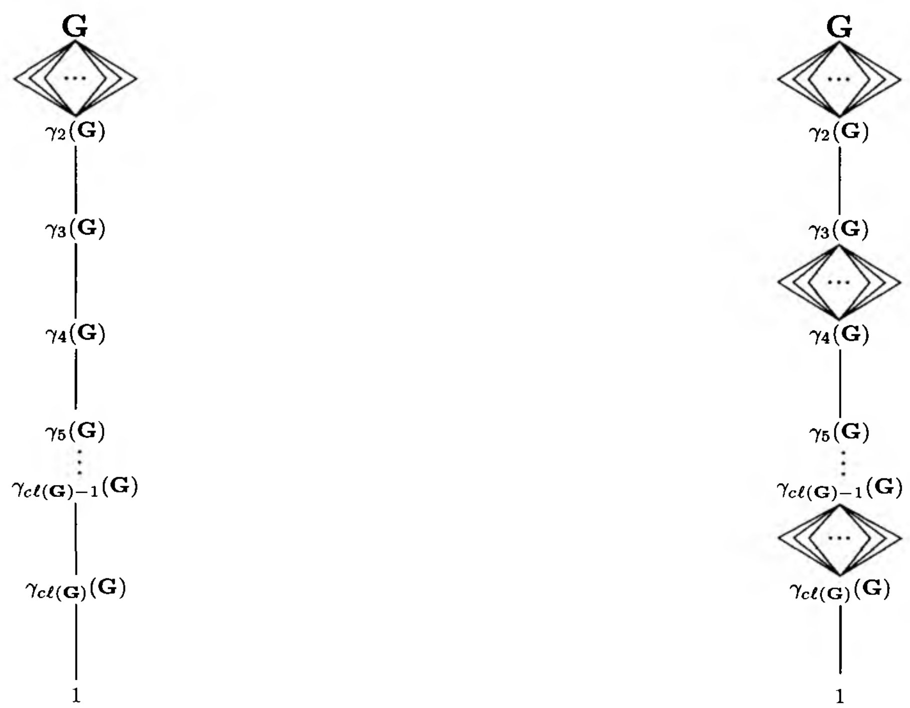
No capítulo 1, exibimos alguns resultados da teoria de p-grupos finitos e dos grupos metabelianos 2-gerados. O estudo a respeito desses grupos metabelianos 2-gerados tem como referência o artigo de Szekeres, o qual trata este assunto usando técnicas de anéis. Um exemplo de como usar tais técnicas para a construção de p-grupos metabelianos 2-gerados também é discutido neste capítulo.

Iniciamos o nosso objetivo de estudar os p-grupos delgados, com uma reflexão sobre os grupos de classe maximal. Blackburn estudou esses grupos em detalhes no seu artigo *"On a Special Class of p-Groups"*, razão pela qual neste trabalho não consideramos os grupos de classe maximal como grupos delgados.

No capítulo 3, onde falamos do número de Dilworth, expomos alguns resultados sobre a largura e a largura normal de um grupo. Tais resultados ajudam a entender a estrutura do reticulado dos subgrupos normais de um grupo de largura normal $p+1$, ou seja, dos grupos delgados. Exibimos, no final deste capítulo, um exemplo de um grupo de largura normal $p+1$ que não é de classe maximal, justificando assim que a classe dos p-grupos delgados abrange aquela dos p-grupos de classe maximal.

No capítulo 4, apresentamos o estudo sobre grupos metabelianos delgados. Em particular, mostramos que as séries centrais superior e inferior de um p-grupo delgado coincidem. No capítulo 2, onde foi feito o estudo dos grupos de classe maximal, observamos que estes grupos são caracterizados por possuírem um elemento cujo centralizador tem ordem p^2. Como veremos, a tentativa de caracterizar os p-grupos delgados como p-grupos contendo um elemento cujo centralizador tem de ordem p^3 falha. Mas mostramos que, se o grupo é tal que para cada $g \in \mathbf{G} - \mathbf{G}'$, o centralizador $C_{\mathbf{G}}(g)$ tem ordem p^3, então $\mathbf{G}$ é delgado. A recíproca está provada para p-grupos metabelianos delgados. Mostramos também que a ordem de um p-grupo metabeliano delgado $\mathbf{G}$ satisfaz $p^5 \leq |\mathbf{G}| \leq p^{2p}$ e um exemplo de que esta cota é atingida também é dado.

Um exemplo do diagrama do reticulado $\mathfrak{N}(\mathbf{G})$ de todos os subgrupos normais de um grupo de classe maximal e de um grupo delgado, é dado respectivamente logo a seguir, o que justifica o nome delgado:



Podemos observar que no reticulado de um grupo de classe maximal ocorre um diamante no topo, formado por seus $p+1$ subgrupos maximais, seguido por uma cadeia formada pelos termos da série central inferior. E no caso de um grupo delgado a ocorrência de diamantes não é muito bem controlada. Por um diamante nós entendemos um reticulado que tem um mínimo, um máximo e $p+1$ outros elementos intermediários.

Já no caso de um grupo metabeliano delgado, esse reticulado fica mais determinado, por uma conseqüência do Corolário 4.13, que assegura que os fatores centrais de um p-grupo metabeliano delgado têm ordem p^2, exceto $\gamma_2(\mathbf{G})/\gamma_3(\mathbf{G})$ e possivelmente $\gamma_{c\ell(\mathbf{G})}(\mathbf{G})$. A técnica de Szekeres também é utilizada como um método para a construção de p-grupos metabelianos delgados, que é descrito em [2]. Mas devido ao pouco tempo, essa técnica será estudada em outra ocasião.

Capítulo 1

Resultados Preliminares

Neste capítulo relacionamos alguns resultados que serão usados nos capítulos subseqüentes.

1.1 Comutadores, Subgrupo Comutador e Séries Centrais

Seja $\mathbf{G}$ um grupo. Definimos o comutador de $a, b \in \mathbf{G}$ como sendo $a^{-1}b^{-1}ab$ e denotaremos por $[a, b]$. O comutador $[a_1, a_2, a_3, ..., a_n]$ será definido recursivamente como sendo $[a_1, a_2, a_3, ..., a_n] = [[a_1, a_2, a_3, ..., a_{n-1}], a_n]$. Logo abaixo listamos algumas identidades básicas envolvendo comutadores:
(i) $[a, b] = [b, a]^{-1}$.
(ii) $[ab, c] = [a, c]^b[b, c] = [a, c][a, c, b][b, c]$.
(iii) $[a, bc] = [a, c][a, b]^c = [a, c][a, b][a, b, c]$.
(iv) $[a, b^{-1}, c]^b[b, c^{-1}, a]^c[c, a^{-1}, b]^a = 1$ (Identidade de Witt).

Sejam $\mathbf{G}$ um grupo e X um subconjunto de $\mathbf{G}$. A interseção $\langle X \rangle$ de todos os subgrupos de $\mathbf{G}$ contendo X é chamada o *subgrupo de $\mathbf{G}$ gerado* pelo conjunto X. Seja X um subconjunto contido em $\mathbf{G}$ tal que $\mathbf{G} = \langle X \rangle$, dizemos que $\mathbf{G}$ é gerado por X. Se X for finito dizemos que $\mathbf{G}$ é finitamente gerado.

Definição 1.1. Seja $\mathbf{G}$ um grupo. O subgrupo de $\mathbf{G}$ gerado por todos os comutadores, ou seja, $[a, b]$ para todo $a, b \in \mathbf{G}$ é chamado *subgrupo comutador* ou *grupo derivado* de $\mathbf{G}$

e será denotado por $\mathbf{G}'$. Podemos também definir o comutador $[L, M]$, onde L e M são subconjuntos de $\mathbf{G}$, como sendo

$$[L, M] = \langle [a, b] \mid a \in L, b \in M \rangle .$$

A série de um grupo $\mathbf{G}$, dada por

$$\mathbf{G} = \gamma_1(\mathbf{G}) \geq \gamma_2(\mathbf{G}) \geq ... \geq \gamma_i(\mathbf{G}) ... \geq ...$$

é definida recursivamente como sendo:

$$\begin{cases} \gamma_1(\mathbf{G}) & = \quad \mathbf{G} \\ \gamma_{i+1}(\mathbf{G}) & = \quad [\gamma_i(\mathbf{G}), \mathbf{G}], \quad i = 1, 2, ... \end{cases}$$

Esta série é chamada *série central inferior* do grupo $\mathbf{G}$ onde cada termo $\gamma_i(\mathbf{G})$ é totalmente invariante em $\mathbf{G}$, [[14] pág. 142], ou seja, é invariante por qualquer endomorfismo de $\mathbf{G}$. Além disso, tomando o quociente por $\gamma_{i+1}(\mathbf{G})$ na igualdade de $\gamma_{i+1}(\mathbf{G}) = [\gamma_i(\mathbf{G}), \mathbf{G}]$, obtém-se $[\gamma_i(\mathbf{G})/\gamma_{i+1}(\mathbf{G}), \mathbf{G}/\gamma_{i+1}(\mathbf{G})] = 1$, o que mostra que cada fator $\gamma_i(\mathbf{G})/\gamma_{i+1}(\mathbf{G})$ é um fator central.

A *série central superior* de um grupo $\mathbf{G}$

$$1 = \mathbf{Z}_0 \leq \mathbf{Z}_1(\mathbf{G}) \leq \mathbf{Z}_2(\mathbf{G}) \leq ... \mathbf{Z}_i(\mathbf{G}) \leq ...$$

é definida da seguinte maneira:

$$\mathbf{Z}_0(\mathbf{G}) = 1, \quad \mathbf{Z}_1(\mathbf{G}) = \mathbf{Z}(\mathbf{G}) \quad \text{e},$$

em geral, $\mathbf{Z}_{i+1}(\mathbf{G})$ é a pré-imagem em $\mathbf{G}$ de $\mathbf{Z}(\mathbf{G}/\mathbf{Z}_i(\mathbf{G}))$, isto é, $\mathbf{Z}_{i+1}(\mathbf{G})$ é aquele subgrupo de $\mathbf{G}$ para o qual $\mathbf{Z}_{i+1}(\mathbf{G})/\mathbf{Z}_i(\mathbf{G}) = \mathbf{Z}(\mathbf{G}/\mathbf{Z}_i(\mathbf{G}))$.

A proposição abaixo estabelece algumas propriedades da série central inferior e superior de um grupo.

Proposição 1.2. *Sejam G um grupo e i, j inteiros positivos.*
(i) $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$
(ii) $\gamma_i(\gamma_j(G)) \leq \gamma_{ij}(G)$
(iii) $[\gamma_i(G), Z_j(G)] \leq Z_{j-i}(G)$ *se* $j \geq i$.
Em particular, $[\gamma_i(G), Z_i(G)] = 1$.

Demonstração. A demonstração pode ser encontrada em [[14] pág. 144].

Proposição 1.3. *Seja G um grupo gerado por um conjunto X. Então*
(i) $\gamma_i(G) = \langle [x_1, ..., x_i]^g \mid x_j \in X, j = 1, ...i, g \in G \rangle$.
(ii) $\gamma_i(G) = \langle [x_1, ..., x_i], \gamma_{i+1}(G) \mid x_j \in X, j = 1, ...i, \rangle$.
(iii) Se $X = \{x, y\}$ *então* $\gamma_2(G) = \langle [x, y], \gamma_3(G) \rangle$ *e assim* $\gamma_2(G)/\gamma_3(G)$ *é cíclico.*
(iv) Se $X = \{x, y\}$ *então* $G'' := \gamma_2(G') \leq \gamma_5(G)$.

Demonstração. A demonstração pode ser encontrada em [[14] pág. 146].

Consideremos agora a seguinte lei de comutadores

$$[[x_1, ..., x_m], [x_{m+1}, ..., x_{m+n}]] = 1,$$

a qual denotaremos abreviadamente por $[m, n] = 1$.

Se o grupo satisfaz a lei

$$[x_1, x_2, x_3, ..., x_k] = [x_1, x_2, x_{\varphi(3)}, ..., x_{\varphi(k)}],$$

onde φ é uma permutação de $\{3, ..., k\}$, diremos que **G** satisfaz $C(k, \varphi)$, e se **G** satisfaz $C(k, \varphi)$ para toda permutação φ de $\{3, ..., k\}$, diremos que **G** satisfaz $C(k)$ (cf. F. Levin [9]).

Agora apenas citaremos alguns resultados de Levin [9] que são utilizados nos capítulos seguintes.

Lema 1.4. *[9] G satisfaz $C(n+2)$, $n \geq 2$ se, e somente se, G satisfaz $[n-k, 2+k] = 1$ para todo $k = 0, 1, 2..., n-2$.*

Teorema 1.5. *[9] Se G satisfaz*

$$[n, 2] = [n-1, 3] = ... = [n-k, 2+k] = 1,$$

para algum $k < s$, onde $2s = n-2$ se n é par e $2s = n-3$ se n é impar, então G satisfaz $C(2n-2k-1)$.

Em particular, para $k = 0$ temos o seguinte resultado:

Corolário 1.6. *Se G satisfaz $[n, 2] = 1$, $n > 3$, então G satisfaz $C(2n-1)$.*

Podemos observar que **G** satisfaz $[n, m] = 1$ se, e somente se, **G** satisfaz $[m, n] = 1$.

1.2 Grupos Nilpotentes, Subgrupo de Frattini e alguns resultados sobre p-Grupos

Definição 1.7. Um grupo $\mathbf{G}$ é dito *nilpotente* se $\mathbf{G}$ possui uma *série central* finita, isto é, uma série $1 = \mathbf{G}_0 < \mathbf{G}_1 < ... < \mathbf{G}_n = \mathbf{G}$ tal que:
(i) $\mathbf{G}_i \trianglelefteq \mathbf{G}, i = 0, ..., n$ (a série é normal);
(ii) $\mathbf{G}_{i+1}/\mathbf{G}_i \leq \mathbf{Z}(\mathbf{G}/\mathbf{G}_i)$ ($\mathbf{G}_{i+1}/\mathbf{G}_i$ é um fator central de $\mathbf{G}$).

Proposição 1.8. *Seja G um grupo nilpotente e $1 = G_0 < G_1 < ... < G_n = G$ uma série central em G. Então:*
(i) $\gamma_i(G) \leq G_{n+1-i}$, para $i = 1, ..., n+1$;
(ii) $G_i \leq Z_i(G)$ para $i = 0, ..., n$;
(iii) As séries centrais inferior e superior têm o mesmo comprimento.

Demonstração. (i) Para $i = 1$ temos $\gamma_i(\mathbf{G}) = \mathbf{G}_n = \mathbf{G}$. Para $i \geq 1$ observemos que $\mathbf{G}_{n+1-i}/\mathbf{G}_{n-i} \leq \mathbf{Z}(\mathbf{G}/\mathbf{G}_{n-i})$ fornece $[\mathbf{G}_{n+1-i}, \mathbf{G}] \leq \mathbf{G}_{n-i}$. Assim, admitindo por indução sobre i que $\gamma_i(\mathbf{G}) \leq \mathbf{G}_{n+1-i}$, obtemos

$$\gamma_{i+1}(\mathbf{G}) = [\gamma_i(\mathbf{G}), \mathbf{G}] \leq [\mathbf{G}_{n+1-i}, \mathbf{G}] \leq \mathbf{G}_{n-i}.$$

(ii) Demonstra-se de modo análogo ao anterior.
(iii) Se $\mathbf{G}$ tem classe c então existe uma série central $1 = \mathbf{G}_0 < \mathbf{G}_1 < ... < \mathbf{G}_c = \mathbf{G}$ e qualquer outra série central de 1 a $\mathbf{G}$ tem comprimento maior ou igual a c. Por (i) temos $\gamma_{c+1}(\mathbf{G}) = 1$, assim a série central inferior tem comprimento c, e por (ii) temos que $\mathbf{Z}_c(\mathbf{G}) = \mathbf{G}$. Logo a série central superior também tem comprimento c. ∎

Num grupo nilpotente, o comprimento das séries centrais superior e inferior são iguais, como foi provado acima. Este número é a classe de nilpotência de $\mathbf{G}$.

Teorema 1.9. *Todo subgrupo de um grupo nilpotente é subnormal. Mais precisamente, se G é nilpotente de classe c então, para qualquer subgrupo H, a série de normalizadores começando com H alcança G depois de no máximo c passos.*

Demonstração. Sejam

$$Z_i = Z_i(\mathbf{G}),\ H_0 = H,\ H_{j+1} = N_{\mathbf{G}}(Hj).$$

Para provar o teorema basta mostrar que $Z_i \leq H_i$. Para $i = 0$ isto é óbvio. Suponhamos então que o resultado seja válido para i e mostraremos que vale para $i+1$. Uma vez que $[\mathbf{G}, Z_{i+1}] \leq Z_i \leq H_i$, temos que

$$H_i^{Z_{i+1}} \subseteq H_i[H_i, Z_{i+1}] \leq H_i.$$

Então Z_{i+1} normaliza H_i, isto é, $Z_{i+1} \leq H_{i+1}$. ∎

Teorema 1.10. *Num grupo nilpotente $\mathbf{G}$, todo subgrupo normal não trivial intercepta o centro de $\mathbf{G}$ não trivialmente.*

Demonstração. Usaremos indução sobre a classe de nilpotência. Seja $\mathbf{G}$ um grupo nilpotente e H um subgrupo normal não trivial. Suponhamos, por indução, que o teorema seja válido para grupos de classe menor que $\mathbf{G}$. Se $H \leq Z_1(\mathbf{G})$ temos a conclusão desejada trivialmente. Tome $H \nleq Z_1(\mathbf{G})$. Então, por hipótese de indução para $\mathbf{G}/Z_1(\mathbf{G})$, a interseção $HZ_1(\mathbf{G}) \cap Z_2(\mathbf{G})$ contém um elemento $a \notin Z_1(\mathbf{G})$. Se $a = hz$ para algum $h \in H$, $z \in Z_1(\mathbf{G})$, então $h \in H \cap Z_2(\mathbf{G})$ e $h \notin Z_1(\mathbf{G})$. Seja $g \in \mathbf{G}$ um elemento tal que $[h, g] \neq e$. Então

$$[h, g] \in H \cap [Z_2(\mathbf{G}), \mathbf{G}] \leq H \cap Z_1(\mathbf{G}),$$

de modo que a interseção $H \cap Z_1(\mathbf{G})$ é não trivial, e o teorema está provado. ∎

Teorema 1.11. *Todo p-grupo finito é nilpotente.*

Demonstração. Sabemos que o centro de um p-grupo finito é não trivial, ou seja, $Z(\mathbf{G}) \neq 1$. Se, para algum i, temos que $Z_i(\mathbf{G}) < \mathbf{G}$, então $Z(\mathbf{G}/Z_i(\mathbf{G})) \neq 1$ e assim $Z_i(\mathbf{G}) < Z_{i+1}(\mathbf{G})$. Uma vez que $\mathbf{G}$ é finito, existirá um inteiro i com $Z_i(\mathbf{G}) = \mathbf{G}$. Portanto $\mathbf{G}$ é nilpotente. ∎

Definição 1.12. Seja $\mathbf{G}$ um grupo; definimos o seu *subgrupo de Frattini* $\Phi(\mathbf{G})$ como sendo a interseção de todos os subgrupos maximais de $\mathbf{G}$. Quando $\mathbf{G}$ não possui subgrupo maximal, definimos $\Phi(\mathbf{G}) = \mathbf{G}$.

Definição 1.13. Um elemento $x \in \mathbf{G}$ é dito um *não gerador* se ele pode ser omitido de todo conjunto gerador, isto é, se $\mathbf{G} = \langle x, Y \rangle$, então $\mathbf{G} = \langle Y \rangle$.

Teorema 1.14. *Para todo grupo $\mathbf{G}$, o subgrupo de Frattini $\Phi(\mathbf{G})$ é o conjunto de todos os elementos não geradores de $\mathbf{G}$.*

Demonstração. Sejam x um elemento não-gerador de $\mathbf{G}$ e M um subgrupo maximal em $\mathbf{G}$. Se $x \notin M$, então $\mathbf{G} = \langle x, M \rangle$, uma contradição. Conseqüentemente $x \in M$ para todo subgrupo maximal M, e assim $x \in \Phi(\mathbf{G})$. Reciprocamente, se $z \in \Phi(\mathbf{G})$, assuma que $\mathbf{G} = \langle z, Y \rangle$. Se $\langle Y \rangle \neq \mathbf{G}$, então existe um subgrupo maximal M com $\langle Y \rangle \leq M$. Mas $z \in M$, e assim $\mathbf{G} = \langle z, Y \rangle \leq M$, uma contradição. Portanto z não é um gerador. ∎

Teorema 1.15. *Seja $\boldsymbol{G}$ um grupo nilpotente. Se A é um subgrupo de $\boldsymbol{G}$ tal que $A[\boldsymbol{G}, \boldsymbol{G}] = \boldsymbol{G}$, então $A = \boldsymbol{G}$. Portanto*

$$[\boldsymbol{G}, \boldsymbol{G}] \leq \Phi(\boldsymbol{G}). \tag{1.1}$$

Demonstração. Suponha que $A \neq \mathbf{G}$. Seja $A_i = AZ_i(\mathbf{G})$, $i = 0, 1, 2....$ Temos que $A_i \lhd A_{i+1}$. Suponha que existe um n tal que $A_n < \mathbf{G}$, $A_{n+1} = \mathbf{G}$. Uma vez que o quociente A_{n+1}/A_n é abeliano temos que $[\mathbf{G}, \mathbf{G}] \leq A_n$, donde

$$A[\mathbf{G}, \mathbf{G}] \leq A_n < \mathbf{G},$$

uma contradição. A afirmação (1.1) segue diretamente da descrição dos elementos de $\Phi(\mathbf{G})$ como o conjunto dos não geradores de $\mathbf{G}$. ∎

Teorema 1.16. *Seja $\boldsymbol{G}$ um grupo finito.*
(i) $\Phi(\boldsymbol{G})$ é nilpotente.
(ii) Se $\boldsymbol{G}$ é um p-grupo finito, então $\Phi(\boldsymbol{G}) = \boldsymbol{G}'\boldsymbol{G}^p$, onde $\boldsymbol{G}^p$ é o subgrupo de $\boldsymbol{G}$ gerado por todas as p-ésimas potências de elementos de $\boldsymbol{G}$.
(iii) Se $\boldsymbol{G}$ é p-grupo finito, então $\boldsymbol{G}/\Phi(\boldsymbol{G})$ é um espaço vetorial sobre $\mathbb{Z}_p$.

Demonstração. (i) Seja P um p-subgrupo de Sylow de $\Phi(\mathbf{G})$ para algum p. Uma vez que $\Phi(\mathbf{G}) \lhd \mathbf{G}$, o argumento de Frattini nos fornece que $\mathbf{G} = \Phi(\mathbf{G})N_{\mathbf{G}}(P)$. Mas $\Phi(\mathbf{G})$ consiste de elementos não geradores, portanto $\mathbf{G} = N_{\mathbf{G}}(P)$, isto é, $P \lhd \mathbf{G}$, e assim $P \lhd \Phi(\mathbf{G})$. Portanto $\Phi(\mathbf{G})$ é o produto direto de seus subgrupos de Sylow, e assim, por [Teorema 5.39 [15]], $\Phi(\mathbf{G})$ é nilpotente.
(ii) Se M é um subgrupo maximal de $\mathbf{G}$, onde $\mathbf{G}$ é um p-grupo, então temos que $M \lhd \mathbf{G}$ e $[\mathbf{G} : M] = p$. Assim $\mathbf{G}/M$ é abeliano, de modo que $\mathbf{G}' \leq M$. Além disso $\mathbf{G}/M$ tem expoente p, de modo que $x^p \in M$ para todo $x \in \mathbf{G}$. Portanto $\mathbf{G}'\mathbf{G}^p \leq \Phi(\mathbf{G})$.

Para mostrar a outra inclusão, observe que $\mathbf{G}/\mathbf{G}'\mathbf{G}^p$ é um subgrupo abeliano de expoente p, assim abeliano elementar, e portanto um espaço vetorial sobre $\mathbb{Z}_p$. Claramente

$\Phi(\mathbf{G}/\mathbf{G}'\mathbf{G}^p) = 1$. Se $H \lhd \mathbf{G}$ e $H \leq \Phi(\mathbf{G})$, então $\Phi(\mathbf{G})$ é a imagem inversa (do homomorfismo canônico) de $\Phi(\mathbf{G}/H)$ (para subgrupos maximais correspondentes). Segue assim que $\Phi(\mathbf{G}) = \mathbf{G}'\mathbf{G}^p$.
(iii) Uma vez que $\mathbf{G}'\mathbf{G}^p = \Phi(\mathbf{G})$, o grupo quociente $\mathbf{G}/\Phi(\mathbf{G})$ é um grupo abeliano de expoente p, de modo que é espaço vetorial sobre $\mathbb{Z}_p$.

Definição 1.17. Um p-grupo $\mathbf{G}$ é dito ser *especial* se $\mathbf{G}$ é abeliano elementar ou $\mathbf{G}$ é de classe 2 e $\mathbf{G}' = Z(\mathbf{G}) = \Phi(\mathbf{G})$ é abeliano elementar.

Proposição 1.18. *Seja $\mathbf{G}$ um p-grupo, tal que para cada subgrupo abeliano H, $H/Z(\mathbf{G})$ é cíclico. Então $\mathbf{G}/Z(\mathbf{G})$ é abeliano elementar, diedral ou não abeliano de ordem p^3 e expoente p.*

Demonstração. Pode ser encontrada em [11].

Lema 1.19. *(Lei Modular). Sejam H, K e L subgrupos de um grupo $\mathbf{G}$ e assuma que $K \subseteq L$. Então $(HK) \cap L = (H \cap L)K$.*

Demonstração. Temos que $(H \cap L)K \subseteq HK$ e $(H \cap L) \subseteq LK = L$, assim $(H \cap L)K \subseteq (HK) \cap L$. Reciprocamente seja $x \in (HK) \cap L$ e escreva $x = hk$, $h \in H, k \in K$. Então $h = xk^{-1} \in LK = L$, de modo que $h \in H \cap L$. Portanto temos que $x \in (H \cap L)K$. ∎

Teorema 1.20. *(Teorema da Base de Burnside). Seja $\mathbf{G}$ um p-grupo finito e $\Phi(\mathbf{G})$ o subgrupo de Frattini. O grupo $A = \mathbf{G}/\Phi(\mathbf{G})$ é abeliano elementar. Se A tem ordem p^r, então todo conjunto $\{z_1, z_2, ...z_s\}$ de elementos que geram $\mathbf{G}$ contém um subconjunto de r elementos $\{x_1, ..., x_r\}$ o qual gera $\mathbf{G}$. Na aplicação $\mathbf{G} \to A$, os elementos $x_1, ..., x_r$ são aplicados numa base $\{a_1, ..., a_r\}$ de A. Reciprocamente, qualquer conjunto de r elementos de A, os quais são aplicados numa base de $\mathbf{G}$, geram $\mathbf{G}$.*

Demonstração. Pode ser encontrada em [[6] pág. 176].

1.3 Reticulados

Um conjunto parcialmente ordenado é um conjunto P junto com uma relação binária "$\leq$" tal que as seguintes condições são satisfeitas, para todo $x, y, z \in P$:
(1) $x \leq x$ (Reflexiva);

(2) Se $x \leq y$ e $y \leq x$, então $x = y$ (Antisimétrica);

(3) Se $x \leq y$ e $y \leq z$, então $x \leq z$ (Transitiva).

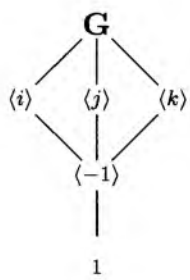
Um elemento x de um conjunto parcialmente ordenado $(P, \leq)$ é dito uma *cota inferior* para o subconjunto S de P se $x \leq s$ para todo $s \in S$. O elemento x é o *ínfimo* de S se x é uma cota inferior de S e $y \leq x$ para qualquer cota inferior y de S. Por (2), da definição anterior, tal ínfimo de S, se existir, será único e será denotado por $\cap S$. Analogamente as definições e observações aplicar-se-ão para as *cotas superiores* e *supremo*, e este será denotado por $\cup S$.

Definição 1.21. Um *reticulado* é um conjunto parcialmente ordenado no qual todo par de elementos tem um supremo e um ínfimo.

Exemplo 1.22. Se $\mathbf{G}$ é um grupo qualquer, o conjunto $\mathfrak{L}(\mathbf{G})$, de todos os subgrupos de $\mathbf{G}$, é um conjunto parcialmente ordenado com respeito à operação de inclusão, onde o supremo entre dois subgrupos desse reticulado é o subgrupo gerado pela união, e o ínfimo é a interseção desses subgrupos.

Dois elementos x e y num conjunto parcialmente ordenado são ditos *comparáveis* se $x \leq y$ ou $y \leq x$. Um subconjunto S de P é uma *cadeia* se quaisquer dois elementos em S são comparáveis; dizemos que S é uma *anti-cadeia* se quaisquer dois elementos de S não são comparáveis. O comprimento de uma cadeia finita S é, por definição, $|S| - 1$. Um conjunto parcialmente ordenado P tem *comprimento* n, onde n é um número natural, se existe uma cadeia finita em P de comprimento n e todas as cadeias em P são de comprimento no máximo n. Um conjunto parcialmente ordenado P é de *comprimento finito* se ele é de comprimento n para algum $n \in \mathbb{N}$. Analogamente, P é de *largura* n se existe uma anti-cadeia com n elementos em P e todas as anti-cadeias em P têm no máximo n elementos.

Exemplo 1.23. Seja $\mathbf{G}$ o grupo dos quatérnios de ordem 8 e seja $\mathfrak{N}(\mathbf{G})$ o reticulado dos subgrupos de $\mathbf{G}$. O diagrama desse reticulado é dado por:



Alguns exemplos de cadeias em $\mathfrak{N}(\mathbf{G})$ são: $\{\{1\},\langle -1\rangle,\langle i\rangle,\mathbf{G}\}$, $\{\{1\},\langle -1\rangle,\langle j\rangle,\mathbf{G}\}$, $\{\{1\},\langle -1\rangle,\langle k\rangle,\mathbf{G}\}$, $\{\{1\},\langle -1\rangle,\langle i\rangle\}$, etc. E suas anti-cadeias são: $\{\langle i\rangle,\langle j\rangle,\langle k\rangle\}$, $\{\langle i\rangle,\langle j\rangle\}$, $\{\langle i\rangle,\langle k\rangle\}$, $\{\langle j\rangle,\langle k\rangle\}$.

1.4 Módulos

Definição 1.24. Um *R-Módulo à esquerda* sobre o anel R consiste de um grupo abeliano $(\mathbf{G},+)$ e uma operação $R\times\mathbf{G}\to M$ (chamada multiplicação por escalar, usualmente escrita por justaposição, isto é, como rx, $r\in R$ e $x\in M$) tal que para todos $r,s\in R$, $x,y\in M$, temos:

1. $r(x+y)=rx+ry, r\in R;\ x,y\in\mathbf{G}$
2. $(r+s)x=rx+sx$
3. $(rs)x=r(sx)$
4. $1x=x$

Exemplo 1.25. Todo grupo abeliano $\mathbf{G}$ pode ser visto como um $\mathbb{Z}$-módulo, pois para $n>0$ temos que $nx=x+x+...+x$ (n vezes), $0x=0$ e $(-n)x=-(nx)$.

Definição 1.26. Um R-módulo M é chamado *cíclico* se $M=Rx$ para algum $x\in M$.

Exemplo 1.27. Todo grupo cíclico é um $\mathbb{Z}$-módulo cíclico.

O *aniquilador* de um módulo M é o conjunto $\{r\in R\mid rx=0\ \forall\ x\in\mathbf{G}\}$

Definição 1.28. Um módulo M *fiel* é um módulo onde o aniquilador é 0.

1.5 Grupos Metabelianos

Definição 1.29. Um grupo $\mathbf{G}$ é *metabeliano* se existe um subgrupo normal $N\trianglelefteq\mathbf{G}$ tal que N e $\mathbf{G}/N$ sejam ambos abelianos.

Exemplo 1.30. Todo grupo abeliano é metabeliano.

Lema 1.31. *G é metabeliano se, e somente se, $G''=1$.*

Demonstração. Suponha que $\mathbf{G}$ seja metabeliano. Uma vez que $\mathbf{G}/N$ é abeliano temos que $\mathbf{G}'\subseteq N$. E como N é abeliano, $\mathbf{G}''=1$.

Se $\mathbf{G}'' = 1$, mostraremos que $\mathbf{G}$ é metabeliano. Para isto provaremos a existência de um subgrupo normal abeliano em $\mathbf{G}$ e então mostraremos que o quociente de $\mathbf{G}$ por esse subgrupo também é abeliano. Se $\mathbf{G}$ é abeliano nada temos a se fazer, portanto podemos considerar o caso em que $\mathbf{G}$ é não abeliano, e portanto $\mathbf{G}' \neq 1$.

Se $\mathbf{G}'' = 1$, escolha $N = \mathbf{G}'$ e a afirmação segue, pois $\mathbf{G}/\mathbf{G}'$ e $\mathbf{G}'$ são abelianos. ∎

Teorema 1.32. *Se H é um subgrupo de um grupo metabeliano G, então H é metabeliano.*

Demonstração. Seja H um subgrupo do grupo metabeliano $\mathbf{G}$. Uma vez que $\mathbf{G}$ é metabeliano, pelo lema 1.31, $\mathbf{G}'' = 1$. Como H é um subgrupo de $\mathbf{G}$, temos que H'' é subgrupo de $\mathbf{G}''$ e portanto $H'' = 1$. Então, pelo lema 1.31, H é metabeliano. ∎

Teorema 1.33. *Se G é um grupo metabeliano e $\varphi : G \to K$ é um homomorfismo, então $\varphi(G)$ é metabeliano.*

Demonstração. Seja $\mathbf{G}$ um grupo metabeliano e φ como acima. Sabemos que $\varphi(H)' = \varphi(H')$ para qualquer grupo H. Assim $\varphi(\mathbf{G})'' = \varphi(\mathbf{G}')' = \varphi(\mathbf{G}'')$. Uma vez que $\mathbf{G}$ é metabeliano temos que $\mathbf{G}'' = 1$, e portanto $\varphi(\mathbf{G})'' = \varphi(\mathbf{G}'') = \varphi(1) = 1$. Assim, pelo lema 1.31, $\varphi(\mathbf{G})$ é metabeliano. ∎

1.6 Grupos Metabelianos a dois Geradores

Discutiremos nesta seção, em linhas gerais, uma técnica para construir grupos metabelianos com dois geradores cujo subgrupo comutador é finito. Esta técnica está apresentada no artigo de Szekeres [17], a qual é desenvolvida usando técnicas de anéis. Aqui trataremos somente os grupos metabelianos a dois geradores. Maiores detalhes podem ser encontrados em [17].

Sejam a, b geradores do grupo metabeliano $\mathbf{G}$ e $K = \mathbf{G}'$ finito. Temos que aK, bK são geradores de $\mathbf{G}/K$, de ordens r e s respectivamente.

Sejam α, β os automorfismos internos induzidos por a e b em K, isto é,

$$d^{\alpha} = a^{-1}da \quad d^{\beta} = b^{-1}db, \quad \forall\, d \in K. \tag{1.2}$$

Claramente α, β são independentes dos representantes a, b de aK, bK e

$$\alpha^r = \epsilon, \qquad \beta^s = \epsilon \tag{1.3}$$

onde ϵ indica o automorfismo identidade de K. Seja

$$R = \mathbb{Z}[\alpha, \beta] = \left\{ \sum_{i=0}^{m} \sum_{j=0}^{n} c_{i,j} \alpha^i \beta^j; \ m \geq 0, \quad n \geq 0, \quad c_{i,j} \in \mathbb{Z} \right\}, \tag{1.4}$$

onde $\alpha^0 = \beta^0 = \epsilon$. K é um R-grupo pela definição usual

$$d^{\rho\sigma} = (d^\rho)^\sigma, \quad d^{(\rho+\sigma)} = d^\rho d^\sigma, \quad d^\epsilon = d \ \ para \ \ d \in K, \quad \rho, \sigma \ \in \ R, \tag{1.5}$$

e

$$d^{m\rho} = (d^\rho)^m \ \ para \ \ m \in \mathbb{Z}. \tag{1.6}$$

Para conveniência de notação escreveremos K aditivamente. Defina um monomorfismo ψ de K no R-módulo $A = K^\psi$ tal que

$$d_1^\psi + d_2^\psi = (d_1 d_2)^\psi, \tag{1.7}$$

$$\rho d^\psi = (d^\rho)^\psi, \tag{1.8}$$

para todo $d_1, d_2, d \in K$, $\rho \in R$. Assim

$$(\rho\sigma) d^\psi = (d^{\rho\sigma})^\psi = \sigma(\rho d^\psi),$$

$$(\rho + \sigma) d^\psi = (d^{\rho+\sigma})^\psi = (d^\rho d^\sigma)^\psi = \rho d^\psi + \sigma d^\psi,$$

de modo que o R-módulo A carrega uma anti-representação de R. E também, é claro, uma representação direta já que R é comutativo.

Lema 1.34. *A é monogênico e é gerado por c^ψ onde*

$$c = a^{-1} b^{-1} a b. \tag{1.9}$$

Demonstração. Seja B o R-módulo gerado por c^ψ, $H = B^{\psi^*}$ onde $\psi\psi^* = \epsilon$. Uma vez que B admite α e β, $H^\alpha = H$, $H^\beta = H$, portanto $a^{-1} H a = H$, $b^{-1} H b = H$, além disso

$c \in H$. Então $\mathbf{G}/H$ é abeliano, gerado por aH, bH, portanto $H \supseteq K$; mas $H \subseteq K$, assim $K = H$. ∎

Seja $\mu : \mathbb{Z}[x,y] \to R$ o homomorfismo

$$F(x,y)^{\mu} = F(\alpha,\beta).$$

A estrutura de A é completamente determinada pelo ideal N de todo $F \in \mathbb{Z}[x,y]$ tal que F^{μ} age trivialmente sobre A, isto é,

$$F(\alpha,\beta).c^{\psi} = 0. \tag{1.10}$$

Uma vez que K é finito, N deve conter uma constante não nula h; além disso

$$x^r - 1 \;\in\; N, \quad y^s - 1 \;\in\; N. \tag{1.11}$$

De fato,

$$\begin{aligned} F(x,y) = x^r - 1 &\Rightarrow F(x,y)^{\mu} = \alpha^r - 1 \text{ (por 1.3, } \alpha^r = \epsilon) \\ &\Rightarrow (\alpha^r - 1)(c^{\psi}) = \alpha^r(c^{\psi}) - c^{\psi} = c^{\psi} - c^{\psi} = 0. \end{aligned}$$

A descrição completa de $\mathbf{G}$ requer, assim,

(a) uma especificação de $N \in \zeta_p[x,y]$ (onde $\zeta_p[x,y]$ representa os ideais p-primários de $\mathbb{Z}[x,y]$) e
(b) uma especificação dos elementos $a^r, b^s \in K$.

A parte (a) da afirmação acima está demonstrada na seção 4 de [17].

A respeito da parte (b), seja

$$(a^r)^{\psi} = \rho c^{\psi} \;\; e \;\; (b^s)^{\psi} = -\sigma c^{\psi}, \tag{1.12}$$

onde $\rho = \varphi(\alpha,\beta)$ e $\sigma = \eta(\alpha,\beta)$ são elementos convenientes de $\mathbb{Z}[\alpha,\beta]$.

Uma vez que a comuta com a^r, devemos ter $\alpha\rho = \rho$, isto é,

$$(x-1)\varphi(x,y) \in N_p \tag{1.13}$$

para cada p, onde N_p é a componente p-primária de N. Além disso, como $b^{-1}ab = ac$ por (1.9), temos para $r > 0$,

$$b^{-1}a^r b = (ac)^r = aca^{-1}a^2ca^{-2}...a^r ca^{-r}a^r,$$

assim por (1.12), $\beta\rho c^\psi = (b^{-1}a^r b)^\psi = (1 + \alpha + ... + \alpha^{r-1} + \rho)c^\psi$,

$$(y-1)\varphi(x,y) - (1 + x + ... + x^{r-1}) \in N_p. \tag{1.14}$$

Analogamente mostramos para $\eta(x,y)$,

$$(y-1)\eta(x,y) \in N_p, \tag{1.15}$$

$$(x-1)\eta(x,y) - (1 + y + ... + y^{s-1}) \in N_p, \tag{1.16}$$

se $s > 0$.

Cada componente p-primária de a^r e b^s é representada por polinômios $\varphi(x,y)$, $\eta(x,y)$ $mod\ N_p$, os quais satisfazem as condições acima. Se $r = 0$ então $\varphi(x,y) \equiv 0(mod\ N_p)$ para cada p e, similarmente, se $s = 0$ então $\eta(x,y) \equiv 0(mod\ N_p)$.

Temos que φ e η são independentes dos representantes a, b das classes laterais aK, bK. Se substituirmos a por ad, $d \in K$ onde $d^\psi = \Lambda(\alpha,\beta)c^\psi$, então fazendo cálculos mostra-se que c^ψ é substituído por $(c^\psi)^* = (1 + (\beta - 1)\Lambda(\alpha,\beta))c^\psi$, e $\varphi(x,y)$ por $\varphi^*(x,y)$, onde

$$\varphi(x,y) = \varphi^*(x,y)\left\{1 + (y-1)\Lambda(x,y)\right\} - (1 + x + ... + x^{r-1})\Lambda(x,y). \tag{1.17}$$

Mas $(y-1)\varphi^*(x,y) \equiv (1+x+...+x^{r-1})\ mod\ N_p$, por 1.14, assim $\varphi(x,y) \equiv \varphi^*(x,y)\ mod\ N_p$.

As equações (1.13)-(1.16) nem sempre têm solução. Uma condição necessária (contudo não suficiente) para a existência de solução é

$$(1 + x + ... + x^{r-1})(1 + y + ... + y^{s-1}) \in N_p$$

para todo p, como vimos de (1.14) ou (1.16). Para a existência de um sistema desses é necessário (contudo não suficiente) que

$$1 + x + ... + x^{r-1} \equiv 0,\ \ 1 + y + ... + y^{s-1} \equiv 0\ \ (mod\ N_p); \tag{1.18}$$

as condições são vazias se $r = 0$ ou $s = 0$. Pelo Teorema 2 [17] vemos que dado um $N \in \zeta_p[x,y]$ sempre existem valores $r = r_0$, $s = s_0$ para os quais (1.18) é satisfeito. Neste caso, ambos, φ e η estão no espaço vetorial determinado pelas equações

$$(x-1)\varphi(x,y) \equiv 0, \quad (y-1)\eta(x,y) \equiv 0 \ (mod\ N_p).$$

O resultado final pode ser resumido como segue. Para obter um grupo metabeliano com dois geradores e subgrupo comutador finito:

(a) Selecione um conjunto de ideais p-primários $N_p \in \zeta_p[x,y]$, um para cada p no conjunto finito P de números primos.
(b) Determine o menor par de inteiros $r_0 \geq 0, s_0 > 0$ tal que $x^{r_0} - 1 \in N_p$, $y^{s_0} - 1 \in N_p$ para cada $p \in P$. Tais inteiros sempre existem pelo Teorema 2 [17]. Tome múltiplos adequados $r = mr_0$, $s = ns_0$ tais que, se $m > 0$, então $r|s$, e se $m = 0$ então $n = 0$. Além disso, $1 + x + ... + x^{r-1} \in N_p$, se necessário.
(c) Tome soluções $\varphi_p(x,y), \eta_p(x,y)$ das equações (1.13)-(1.16). Pelo menos uma solução $(\varphi_p = \eta_p = 0)$ existe se (1.18) é satisfeito.

O grupo $\mathbf{G}$ correspondente consiste dos elementos

$$a^m b^n \prod_{p \in P} c_p^{F_p(\alpha,\beta)}, \quad 0 \leq m < r, \quad 0 \leq n < s,$$

onde $F_p(x,y)$ é considerado módulo N_p gerando as relações seguintes:

$$c_p c_q = c_q c_p \text{ para todo } p,\ q\ \in P;$$
$$a^{-1} c_p a = c_p^{\alpha}, \quad b^{-1} c_p b = c_p^{\beta};$$
$$a^{-1} b^{-1} a b = \prod_{p \in P} c_p;$$
$$a^r = \prod_{p \in P} c^{\varphi_p(\alpha,\beta)}, \quad b^r = \prod_{p \in P} c^{\eta_p(\alpha,\beta)},$$

$\mathbf{G}$ é unicamente determinado por essas relações.

Agora faremos alguns comentários do que foi feito acima e daremos um exemplo de como esta técnica pode ser utilizada para construirmos p-grupos metabelianos 2-gerados.

Se $\mathbf{G} = \langle a, b \rangle$ é metabeliano 2-gerado, empregando as técnicas acima e tomando $c = [a, b]$, sejam x e y automorfismos do grupo abeliano $\mathbf{G}'$ induzidos por a e b, respectivamente, e A o anel (comutativo) de endomorfismos de $\mathbf{G}'$ gerado por x e y, temos que $\mathbf{G}'$ é um A-módulo cíclico gerado por c. Seja também I o ideal de A gerado por $X = x - 1$, $Y = y - 1$. Desta forma

$$\gamma_i(\mathbf{G}) = cI^{i-2},$$

para $i \geq 2$, onde $I^0 = A$.

De fato, temos pelos resultados acima que

$$\gamma_2(\mathbf{G}) = \mathbf{G}' = c.A.$$

Para $i = 3$ temos, por definição, que

$$\gamma_3(\mathbf{G}) = [\gamma_2(\mathbf{G}), \mathbf{G}].$$

Com efeito, $\mathbf{G}' = c.A$. Temos que $\forall\ w \in \mathbf{G}'$ implica $w = c^{\eta}$, onde $\eta \in A$, e que $\mathbf{G} = \langle a, b \rangle$. Assim

$$[w, a] = [c^{\eta}, a] = c^{-\eta}c^{\eta a},$$

e lembrando que $c^{\eta a} = c^{\eta x} = c^{x\eta}$ obtemos que

$$[w, a] = c^{\eta(-1+x)} = c^{\eta(x-1)} = c^{\eta X},$$

e assim observamos que X age pegando um elemento de $\mathbf{G}'$ e fazendo o comutador desse elemento com a. Analogamente temos que

$$[w, b] = c^{\eta(-1+y)} = c^{\eta(y-1)} = c^{\eta Y},$$

e portanto Y age pegando um elemento de $\mathbf{G}'$ e fazendo o comutador desse elemento com b. Observamos também que $\eta X, \eta Y \in I$, e assim $[w, a], [w, b] \in cI$. Para o comutador abaixo temos que

$$[w, ab] = [c^{\eta}, ab] = [c^{\eta}, b][c^{\eta}, a]^b = c^{\eta Y}(c^{\eta X})^x = c^{\eta Y + \eta x X},$$

e novamente $\eta Y + \eta x X \in I$. Portanto $c^{\eta Y + \eta x X} \in cI$. Fazendo cálculos análogos aos que foram feitos acima podemos deduzir que, para todos $w \in \gamma_2(\mathbf{G})$ e $g \in \mathbf{G}$, o comutador $[w, g] \in cI$. Logo $\gamma_3(\mathbf{G}) = cI$.

Supondo por indução que $\gamma_i(\mathbf{G}) = cI^{i-2}$, temos que

$$\gamma_{i+1}(\mathbf{G}) = [\gamma_i(\mathbf{G}), \mathbf{G}] = [cI^{i-2}, \mathbf{G}].$$

Para quaisquer $w \in \gamma_i(\mathbf{G})$ temos que $w = c^\sigma$, com $\sigma \in I^{i-2}$. Assim

$$[w, a] = [c^\sigma, a] = c^{-\sigma} c^{\sigma a} = c^{-\sigma} c^{\sigma x} = c^{-\sigma + x\sigma} = c^{\sigma(x-1)} = c^{\sigma X},$$

onde $\sigma X \in I^{(i+1)-2}$. Conseqüentemente $c^{\sigma X} \in cI^{(i+1)-2}$. E seguindo o raciocínio acima, deduzimos que $[w, g] \in I^{(i+1)-2}$, $\forall \sigma \in I^{i-2}$ e $\forall g \in \mathbf{G}$. Donde concluímos que $\gamma_{i+1}(\mathbf{G}) = cI^{(i+1)-2}$, como afirmamos.

Sejam agora $\varphi, \psi \in A$ tais que

$$\begin{cases} a^p &= c\varphi, \\ b^p &= c\psi. \end{cases}$$

Temos então, por resultados anteriores, que as seguintes relações valem:

$$X\varphi = 0, \quad Y\psi = 0, \quad -X\psi = N(y), \quad Y\varphi = N(x). \tag{1.19}$$

Aqui a norma $N(z)$ de um elemento z em A é definida como

$$N(z) = 1 + z + ... + z^{p-1} = p + \binom{p}{2}(z-1) + ... + \binom{p}{i}(z-1)^{i-1} + ... + (z-1)^{p-1}.$$

Um exemplo de como construir grupos metabelianos 2-gerados especificando os dados acima e usando o método de extensão apresentado em [[18] pág. 130-133] é dado a seguir.

Exemplo 1.35. [2] Seja $p > 3$ um número primo e seja

$$M = \langle c_0, u_1, v_1, u_2, w_2, v_2 \rangle$$

um p-grupo abeliano elementar de ordem p^6, escrito aditivamente. Observe que este é um caso particular do desenvolvimento acima, pois aqui estamos trabalhando num p-grupo.

Defina dois endomorfismos X, Y de M por

$$\begin{cases} c_0X & = & u_1, & c_0Y & = & v_1 \\ u_1X & = & u_2, & u_1Y & = & w_2 \\ v_1X & = & w_2, & v_1Y & = & v_2 \\ u_2X & = & w_2X & = v_2X & = & 0 \\ u_2Y & = & w_2Y & = v_2Y & = & 0. \end{cases}$$

É fácil ver que X e Y comutam, e que $X^3 = Y^3 = 0$. Então $x = 1 + X$ e $y = 1 + Y$ são automorfismos comutando em M. Seja A o anel dos endomorfismos de M gerado por x e y, e I o ideal gerado por X e Y. Assim M é um A-módulo cíclico gerado por c_0, e $pA = 0$, pois M é de expoente p.

Podemos agora construir um grupo metabeliano $F = \langle a, b \rangle$ como uma extensão de M por um grupo abeliano elementar de ordem p^2, escolhendo $\varphi, \psi \in I^2$ e colocando

$$\begin{cases} [a,b] & = & c_0, & & & \\ c_0^a & = & c_0x, & c_0^b & = & c_0y, \\ a^p & = & c_0\varphi, & b^p & = & c_0\psi, \end{cases}$$

de modo que as relações 1.19 são satisfeitas. Mas este de fato é o caso, pois

$$X\varphi,\ Y\psi,\ X\psi,\ Y\varphi\ \in\ I^3\ =\ 0,$$

e

$$N(x) = p + \binom{p}{2} X + \ldots + \binom{p}{i} X^{i-1} + \ldots + X^{p-1} = 0,$$

uma vez que $pA = 0$ e $X^{p-1} = 0$, pois $p > 3$, e analogamente para N(y). Temos dessa forma construído F, acima mencionado.

Capítulo 2

Grupos de Classe Maximal

Neste capítulo damos a definição de grupos de classe maximal e estudamos algumas de suas propriedades. Tais grupos foram primeiramente estudados por Blackburn e tais resultados foram apresentados em [1].

2.1 Grupos de Classe Maximal

Definição 2.1. Seja $\mathbf{G}$ um p-grupo de ordem p^n com $n \geq 2$. Uma vez que $|\mathbf{G}/\gamma_2(\mathbf{G})| \geq p^2$ então a classe $c\ell(\mathbf{G})$ de $\mathbf{G}$ é no máximo $n-1$. Dizemos que $\mathbf{G}$ é um *p-grupo de classe maximal* se $\mathbf{G}$ tem ordem p^n e classe $n-1$.

A estrutura do reticulado dos subgrupos normais de um p-grupo de classe maximal fica totalmente determinada pelo lema a seguir.

Lema 2.2. *Seja $\boldsymbol{G}$ um p-grupo de classe maximal de ordem p^n. Então:*
(i) Temos que $|\boldsymbol{G}/\gamma_2(\boldsymbol{G})| = p^2$ e $|\gamma_i(\boldsymbol{G}) : \gamma_{i+1}(\boldsymbol{G})| = p$ para $2 \leq i \leq n-1$. Assim $|\boldsymbol{G} : \gamma_i(\boldsymbol{G})| = p^i$ para $2 \leq i \leq n$.
(ii) A não ser que $\boldsymbol{G}$ seja cíclico de ordem p^2, temos que $\Phi(\boldsymbol{G}) = \boldsymbol{G}'$ e $d(\boldsymbol{G}) = 2$ (onde $d(\boldsymbol{G})$ é o número mínimo de geradores de $\boldsymbol{G}$).
(iii) Os únicos subgrupos normais de $\boldsymbol{G}$ são os $\gamma_i(\boldsymbol{G})$ e os subgrupos maximais de $\boldsymbol{G}$. Mais precisamente, se N é um subgrupo normal de $\boldsymbol{G}$ de índice $p^i \geq p^2$ então $N = \gamma_i(\boldsymbol{G})$.
(iv) Se N é um subgrupo normal de $\boldsymbol{G}$ de índice $\geq p^2$ então $\boldsymbol{G}/N$ também tem classe maximal.

(v) $Z_i(\boldsymbol{G}) = \gamma_{n-i}(\boldsymbol{G})$ *para* $0 \leq i \leq n-1$.

Demonstração. (i) Temos que

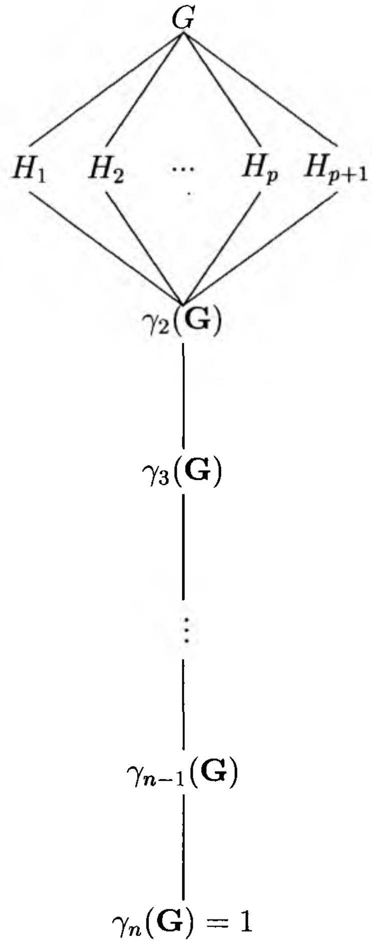
$$|\mathbf{G}| = |\mathbf{G} : \mathbf{G}'| \prod_{i=2}^{n-1} |\gamma_i(\mathbf{G}) : \gamma_{i+1}(\mathbf{G})|$$

Agora é suficiente observar que $|\mathbf{G}| = p^n$, e por outro lado, $|\mathbf{G} : \mathbf{G}'| \geq p^2$ e $|\gamma_i(\mathbf{G}) : \gamma_{i+1}(\mathbf{G})| \geq p$ para $2 \leq i \leq n-1$.
(ii) Sabemos que $\mathbf{G}' \leq \Phi(\mathbf{G})$, por (i) temos que $|\mathbf{G} : \Phi(\mathbf{G})| \leq p^2$. Se $|\mathbf{G} : \Phi(\mathbf{G})| = p$ então $\mathbf{G}/\Phi(\mathbf{G})$ é cíclico e $\mathbf{G}$ também é cíclico e de ordem p^2. Caso contrário $|\mathbf{G} : \Phi(\mathbf{G})| = p^2$ e $d(\mathbf{G}) = 2$.
(iii) Seja N um subgrupo normal de $\mathbf{G}$ tal que $|\mathbf{G} : N| = p^i$ com $0 \leq i \leq n$. Se $i = 0$ ou $i = 1$ então $N = \mathbf{G}$ ou N é maximal em $\mathbf{G}$ respectivamente. Caso Contrário, se $i \geq 2$ temos que $\gamma_i(\mathbf{G}) \leq N$. Uma vez que $|\mathbf{G} : \gamma_i(\mathbf{G})| = p^i$, concluímos que $N = \gamma_i(\mathbf{G})$.
(iv) Isto é imediato de (iii) e (i), uma vez que a classe de $\mathbf{G}/\gamma_i(\mathbf{G})$ é $i-1$ sempre que $i \leq n$.
(v) O resultado é óbvio para $n = 2$, podemos então assumir que $n \geq 3$. Então o grupo fator $\mathbf{G}/Z_{n-3}(\mathbf{G})$ não é abeliano e conseqüentemente o quociente deste grupo pelo centro não é cíclico. Assim $|\mathbf{G} : Z_{n-2}(\mathbf{G})| \geq p^2$. Uma vez que $|Z_{i+1}(\mathbf{G}) : Z_i(\mathbf{G})| \geq p$ para $0 \leq i \leq n-3$ e

$$p^n = |\mathbf{G}| = |\mathbf{G} : Z_{n-2}(\mathbf{G})| \prod_{i=0}^{n-3} |Z_{i+1}(\mathbf{G}) : Z_i(\mathbf{G})|,$$

todas desigualdades acima, de fato, são igualdades. Segue que $|\mathbf{G} : Z_i(\mathbf{G})| = p^{n-i}$ para $0 \leq i \leq n-2$ e pela parte (iii), $Z_i(\mathbf{G}) = \gamma_{n-i}(\mathbf{G})$. ■

Um diagrama do reticulado dos subgrupos normais $\mathfrak{N}(\mathbf{G})$ de um p-grupo $\mathbf{G}$ de classe maximal de ordem p^n pode ser apresentado como segue, no qual podemos observar que $\mathbf{G}$ tem exatamente $p+1$ subgrupos maximais, $H_1, H_2, ..., H_{p+1}$ e o restante dos subgrupos normais são os $\gamma_i(\mathbf{G})$.



2.2 Grau de Comutatividade

Falaremos agora de um importante conceito que tem um papel fundamental no estudo de p-grupos de classe maximal.

No que segue, quando $\mathbf{G}$ for um p-grupo de classe maximal, escreveremos $\mathbf{G}_i = \gamma_i(\mathbf{G})$ para $i \geq 2$ e $\mathbf{G}_0 = \mathbf{G}$.

Definição 2.3. Seja $\mathbf{G}$ um p-grupo de classe maximal de ordem p^n. Definimos $\mathbf{G}_1 = C_{\mathbf{G}}(\mathbf{G}_2/\mathbf{G}_4)$. Em outras palavras, $\mathbf{G}_1$ é composto pelos elementos $x \in \mathbf{G}$ tal que $[x, \mathbf{G}_2] \leq \mathbf{G}_4$.

Se N é um subgrupo normal de $\mathbf{G}$ tal que $|\mathbf{G}/N| \geq p^4$, temos pela definição que $(\mathbf{G}/N)_1 = \mathbf{G}_1/N$.

Teorema 2.4. *Seja G um p-grupo de classe maximal. Então G_1 é um subgrupo maximal característico de G.*

Demonstração. Seja $\varphi \in Aut(\mathbf{G})$. Uma vez que $\mathbf{G}_2$ e $\mathbf{G}_4$ são subgrupos característicos de $\mathbf{G}$, temos que

$$[\varphi(x), \mathbf{G}_2] = [\varphi(x), \varphi(\mathbf{G}_2)] = \varphi([x, \mathbf{G}_2]) \leq \mathbf{G}_4.$$

Isto mostra que $\mathbf{G}_1$ é característico em $\mathbf{G}$.

Por outro lado, temos que $\mathbf{G}/\mathbf{G}_1$ mergulha em $Aut(\mathbf{G}_2/\mathbf{G}_4)$. Mas $|\mathbf{G}_2 : \mathbf{G}_4| = p^2$, assim $\mathbf{G}_2/\mathbf{G}_4 \cong C_{p^2}$ ou $C_p \times C_p$. No primeiro caso, $|Aut(\mathbf{G}_2/\mathbf{G}_4)| = p.(p-1)$, no segundo caso $|Aut(\mathbf{G}_2/\mathbf{G}_4)| = |GL_2(p)| = (p^2-p).(p^2-1)$. Em quaisquer casos, a maior potência de p que divide $|Aut(\mathbf{G}_2/\mathbf{G}_4)|$ é p, assim deduzimos que $|\mathbf{G} : \mathbf{G}_1| \leq p$. Se $\mathbf{G}_1 = \mathbf{G}$ então $\mathbf{G}_3 = [\mathbf{G}, \mathbf{G}_2] = [\mathbf{G}_1, \mathbf{G}_2] \leq \mathbf{G}_4$. Isso é possível somente se $\mathbf{G}_3 = 1$, o que contradiz o fato que $|\mathbf{G}| \geq p^4$. ∎

Segue que, com a notação introduzida acima, $|\mathbf{G}_i : \mathbf{G}_{i+1}| = p$ para $0 \leq i \leq n-1$ e $\mathbf{G}_i = 1$ para $i \geq n$.

Definimos agora o grau de comutatividade, esse invariante pode ser considerado como a chave para a análise da estrutura de um p-grupo de classe maximal, o qual mede o quanto os termos da série $\{\mathbf{G}_i\}_{i \geq 1}$ comutam com cada outro.

Definição 2.5. Seja $\mathbf{G}$ um p-grupo de classe maximal. Definimos o *grau de comutatividade* de $\mathbf{G}$, o qual denotamos por $\ell(\mathbf{G})$ ou simplesmente por ℓ, como sendo

$$\ell(\mathbf{G}) = max\,\{k \leq m-2 | [\mathbf{G}_i, \mathbf{G}_j] \leq \mathbf{G}_{i+j+k} \text{ para todo } i, j \geq 1\}.$$

Definição 2.6. Um p-grupo de classe maximal será chamado *excepcional* se $\ell(\mathbf{G}) = 0$.

Lema 2.7. *Seja G um p-grupo de classe maximal com $|G| = p^n$ e $n \geq 4$. E suponha que G não é um grupo excepcional. Nós escolhemos elementos s e s_1 em G com*

$$G = \langle G_1, s\rangle \quad e \quad G_1 = \langle G_2, s_1\rangle.$$

Definimos o elemento s_i $(i \geq 2)$ de G recursivamente como $s_i = [s_{i-1}, s]$. Então temos que $G_i = \langle G_{i+1}, s_i\rangle$ para $2 \leq i \leq n-1$.

Demonstração. Temos que

$$\mathbf{G} = \langle \mathbf{G}_1, s \rangle = \langle \mathbf{G}_2, s_1, s \rangle .$$

Uma vez que $\mathbf{G}_2 = \mathbf{G}' \leq \Phi(\mathbf{G})$ temos que $\mathbf{G} = \langle s_1, s \rangle$. Pela proposição (1.3) temos que

$$\mathbf{G}_2 = \gamma_2(\mathbf{G}) = \langle [s_1, s], \gamma_3(\mathbf{G}) \rangle = \langle s_2, \mathbf{G}_3 \rangle .$$

Suponha por indução que $\mathbf{G}_{i-1} = \langle \mathbf{G}_i, s_{i-1} \rangle$. Uma vez que $\mathbf{G} = \langle s, s_1 \rangle$ segue que

$$\mathbf{G}_i = [\mathbf{G}_{i-1}, \mathbf{G}] = \langle \mathbf{G}_{i+1}, [s_{i-1}, s], [s_{i-1}, s_1] \rangle .$$

Como $\mathbf{G}$ não é excepcional, existe $i \leq n-1$

$$[s_{i-1}, s_1] \in [\mathbf{G}_{i-1}, \mathbf{G}_1] \leq \mathbf{G}_{i+1}$$

Como $[s_{i-1}, s] = s_i$ temos que $\mathbf{G}_i = \langle \mathbf{G}_{i+1}, s_i \rangle$, o que mostra o resultado. ∎

2.3 Elementos Uniformes

Seja $\mathbf{G}$ um grupo de classe maximal de ordem p^n. Da mesma maneira que definimos o subgrupo $\mathbf{G}_1 = C_{\mathbf{G}}(\mathbf{G}_2/\mathbf{G}_4)$, podemos considerar, mais geralmente, os centralizadores de 2-passos $C_{\mathbf{G}}(\mathbf{G}_i/\mathbf{G}_{i+2})$ para $1 \leq i \leq n-2$. Assim como $\mathbf{G}_1$, todos esses subgrupos são característicos e maximais em $\mathbf{G}$. Uma vez que $[\mathbf{G}_1, \mathbf{G}_1] = [\mathbf{G}_1, \mathbf{G}_2] \leq \mathbf{G}_4$, segue que $C_{\mathbf{G}}(\mathbf{G}_1/\mathbf{G}_4) = \mathbf{G}_1$ e, conseqüentemente, é suficiente considerar os centralizadores de 2-passos para $2 \leq i \leq n-2$.

Definição 2.8. Seja $\mathbf{G}$ um p-grupo de classe maximal de ordem p^n. Dizemos que $s \in \mathbf{G}$ é um *elemento uniforme* se $s \notin \cup_{i=2}^{n-2} C_{\mathbf{G}}(\mathbf{G}_i/\mathbf{G}_{i+2})$.

Podemos imediatamente nos perguntarmos se qualquer p-grupo de classe maximal possui elementos uniformes, isto é, se é verdade ou não que $\mathbf{G} \neq \cup_{i=2}^{n-2} C_{\mathbf{G}}(\mathbf{G}_i/\mathbf{G}_{i+2})$. Blackburn mostrou juntamente com algumas propriedades sobre o grau de comutatividade que isso é sempre verdadeiro.

Teorema 2.9. *(Blackburn). Seja G um p-grupo de classe maximal, de ordem p^n. Então valem as seguintes afirmações:*

(i) Se $\ell(G) = 0$ *então* $p \geq 5$, n *é par e* $6 \leq n \leq p+1$.
(ii) $\ell(G/Z(G)) \geq 1$.
(iii) G *tem elementos uniformes.*

Demonstração. A demonstração está feita em detalhes em ([4], capítulo 4, 47-55)

As partes (i) e (ii) no Teorema 2.9 justifica o termo "grupo excepcional" que é usado para grupos de grau de comutatividade zero.

Lema 2.10. *Seja* G *um p-grupo de classe maximal, de ordem* p^n *e* s *um elemento uniforme de* G. *Se* $1 \leq i \leq n-2$ *e* $x \in G_i - G_{i+1}$, *então* $[s,x] \in G_{i+1} - G_{i+2}$.

Demonstração. Como $x \in \mathbf{G}_i$, é óbvio que $[s,x] \in \mathbf{G}_{i+1}$ e temos somente então que mostrar que $[s,x] \notin \mathbf{G}_{i+2}$. Suponha por contradição que $[s,x] \in \mathbf{G}_{i+2}$. Escrevendo $\bar{\mathbf{G}} = \mathbf{G}/\mathbf{G}_{i+2}$, isto significa que $\bar{s}$ e $\bar{x}$ comutam em $\bar{\mathbf{G}}$. Temos também que $[s, \mathbf{G}_{i+1}] \leq \mathbf{G}_{i+2}$ ou seja, $\bar{s}$ centraliza $\mathbf{G}_{i+1}$. Uma vez que $\mathbf{G}_i = \langle x, \mathbf{G}_{i+1}\rangle$, segue que $\bar{s}$ centraliza $\bar{\mathbf{G}}_i$. Então $[s, \mathbf{G}_i] \leq \mathbf{G}_{i+2}$ e $s \in C_{\mathbf{G}}(\mathbf{G}_i/\mathbf{G}_{i+2})$, o que contradiz o fato de s ser um elemento uniforme.
∎

Teorema 2.11. *Seja* G *um p-grupo de classe maximal de ordem* p^n *e* s *um elemento uniforme de* G. *Então valem as seguintes propriedades:*
(i) $C_G(s) = \langle s\rangle Z(G)$.
(ii) $s^p \in Z(G)$ *e conseqüentemente* $o(s) \leq p^2$ *e* $|C_G(s)| = p^2$.
(iii) Os conjugados de s *são exatamente os elementos na classe lateral* sG_2.
(iv) Para $0 \leq t \leq n-4$, *o subgrupo* $H = \langle s, G_{t+1}\rangle$ *é um p-grupo de classe maximal de ordem* p^{n-t} *tal que* $H_i = G_{i+t}$ *para* $i \geq 1$. *Assim temos que* $\ell(H) = n-t-2$ *ou* $\ell(H) \geq \ell(G) + t$.

Demonstração. (i) Seja g um elemento qualquer de $\mathbf{G}$. Como $\mathbf{G} = \langle s\rangle \mathbf{G}_1$ podemos escrever $g = s^i x$, onde $i \in \mathbb{Z}$ e $x \in \mathbf{G}_1$. Então $g \in C_{\mathbf{G}}(s)$ se, e somente se, $[s,x] = 1$. Mas, de acordo com Lema 2.10, se $x \in \mathbf{G}_i - \mathbf{G}_{i+1}$ com $1 \leq i \leq n-2$ então $[s,x] \in \mathbf{G}_{i+1} - \mathbf{G}_{i+2}$ e, em particular, $[s,x] \neq 1$. Segue que $x \in \mathbf{G}_{n-1} = Z(\mathbf{G})$(de acordo com 2.2). Conseqüentemente $C_{\mathbf{G}}(s) = \langle s\rangle Z(\mathbf{G})$.

(ii) Na prova de (i) vimos que $C_{\mathbf{G}_1}(s) = Z(\mathbf{G})$. Como $s^p \in \mathbf{G}_1$ comuta com s, segue que $s^p \in Z(\mathbf{G})$.

(iii) A cardinalidade da classe de conjugação de s em $\mathbf{G}$ é $|\mathbf{G} : C_{\mathbf{G}}(s)| = p^{n-2} = |s\mathbf{G}_2|$.

Uma vez que qualquer conjugado de s pertence a $s\mathbf{G}_2$ ($s^g = s[s,g]$), deduzimos que os elementos na classe lateral $s\mathbf{G}_2$ são precisamente os conjugados de s.

(iv) Não há nada a se provar se $t = 0$, assim podemos assumir que $t \geq 1$. Está claro pela parte (ii) que $|H| = p\,|\mathbf{G}_{t+1}| = p^{n-t}$. Aplicando 2.10 repetidamente, para qualquer $x \in \mathbf{G}_{t+1} - \mathbf{G}_{t+2}$ temos que

$$[x, s, \overset{i-1}{\ldots}, s] \in \mathbf{G}_{i+t} - \mathbf{G}_{i+t+1} \text{ para } 2 \leq i \leq n-t-1.$$

Em particular, para $i = n-t-1$ segue que $1 \neq [x, s, \overset{n-t-2}{\ldots}, s] \in H_{n-t-1}$ e H têm classe maximal. Em ordem, para provar que $H_i = \mathbf{G}_{i+t}$, suporemos primeiro que $i \geq 2$. Por 2.3 temos que H_i tem um elemento em $\mathbf{G}_{i+t} - \mathbf{G}_{i+t+1}$. Usando esta propriedade não somente com H_i, mas também com qualquer H_j contido em H_i, deduzimos que H_i tem elementos em $\mathbf{G}_k - \mathbf{G}_{k+1}$ para $i+t \leq k \leq n-1$. Conseqüentemente $\mathbf{G}_{i+t} \leq H_i$ e, uma vez que ambos os subgrupos têm a mesma ordem, segue a igualdade. Por outro lado, $[\mathbf{G}_{t+1}, H_2] = [\mathbf{G}_{t+1}, \mathbf{G}_{t+2}] \leq \mathbf{G}_{2t+3} \leq \mathbf{G}_{t+4} = H_4$ e obtemos que $H_1 = \mathbf{G}_{t+1}$. Finalmente, se $\ell = \ell(\mathbf{G})$ então $[H_i, H_j] = [\mathbf{G}_{i+t}, \mathbf{G}_{j+t}] \leq \mathbf{G}_{i+j+\ell+2t} = H_{i+j+\ell+t}$ para quaisquer $i, j \geq 1$ e conseqüentemente ou $\ell(H) = n-t-2$ ou $\ell(H) \geq \ell(\mathbf{G}) + t$. ∎

Para finalizar esta seção, vamos mostrar que p-grupo de classe maximal pode ser caracterizado como sendo um grupo que possui um elemento cujo centralizador tem ordem p^2.

Lema 2.12. *Seja $\boldsymbol{G}$ um p-grupo com $|\boldsymbol{G}| = p^n$, $n \geq 3$. Então $\boldsymbol{G}$ é um p-grupo de classe maximal se, e somente se, existir um elemento g de $\boldsymbol{G}$ tal que*

$$\left|\{g^h \mid h \in \boldsymbol{G}\}\right| = p^{n-2}.$$

(O lema também vale para $n = 2$)

Demonstração. (1) Seja $g \in \mathbf{G}$ tal que

$$\left|\{g^h \mid h \in \mathbf{G}\}\right| = p^{n-2} = |\mathbf{G} : \mathbf{C}_G(g)|$$

Para n=3, como $\mathbf{G}$ não é abeliano, $\mathbf{G}$ tem classe 2. Provaremos para $n > 3$ por indução sobre n.

Como $\mathbf{Z(G)} \leq \mathbf{C}_G(g)$ e $g \notin \mathbf{Z(G)}$ temos que $|\mathbf{Z(G)}| = p$. Seja $\mathbf{B} = \mathbf{Z(G)}$ e $\mathbf{C}_{G/B}(gB) = L/B$ com

$$L = \left\{h \mid g^h = gz \text{ com } z = [g,h] \in \mathbf{B}\right\}.$$

Então a aplicação $h \to [g,h]$ é um homomorfismo de L em $\mathbf{B}$ com núcleo $\mathbf{C}_G(g)$. Conseqüentemente segue que

$$|L| \leq p\,|\mathbf{C}_G(g)| = p^3.$$

Seja $\bar{\mathbf{G}} = \mathbf{G}/\mathbf{B}$ e $\bar{g} = g\mathbf{B}$, então

$$\left|\left\{\bar{g}^{\bar{h}} \mid \bar{h} \in \bar{\mathbf{G}}\right\}\right| = \left|\bar{\mathbf{G}} : \mathbf{C}_{\bar{G}}(\bar{g})\right| = |\mathbf{G} : L| \geq p^{n-3}$$

Uma vez que

$$\left\{\bar{g}^{\bar{h}} \mid \bar{h} \in \bar{\mathbf{G}}\right\} \subseteq \bar{g}\bar{\mathbf{G}}' \text{ pois } \bar{g}^{\bar{h}} = \bar{h}^{-1}\bar{g}\bar{h} = h^{-1}Z(\mathbf{G})gZ(\mathbf{G})hZ(\mathbf{G}) = h^{-1}ghZ(\mathbf{G}) = \\ h^{-1}hg[g,h]Z(\mathbf{G}) = gZ(\mathbf{G})[g,h]Z(\mathbf{G}) \in \bar{g}\bar{\mathbf{G}}'$$

e

$$\left|\left\{\bar{g}^{\bar{h}} \mid \bar{h} \in \bar{\mathbf{G}}\right\}\right| \leq \left|\bar{\mathbf{G}}'\right| \leq p^{n-3},$$

temos então que

$$\left|\left\{\bar{g}^{\bar{h}} \mid \bar{h} \in \bar{\mathbf{G}}\right\}\right| = p^{n-3}$$

e conseqüentemente pela nossa hipótese de indução

$$e \neq \gamma_{n-2}(\mathbf{G}/\mathbf{B}) = \gamma_{n-2}(\mathbf{G})\mathbf{B}/\mathbf{B}.$$

Logo $\gamma_{n-2}(\mathbf{G}) \nleq \mathbf{B} = \mathbf{Z(G)}$ e assim $\gamma_{n-1}(\mathbf{G}) \neq e$. Segue que $\mathbf{G}$ é um p-grupo de classe maximal.

(2) Seja $\mathbf{G}$ um p-grupo de classe maximal. Se $p > 2$, então pelo Teorema 2.11, existe um $g \in \mathbf{G}$ com $|\mathbf{C}_G(g)| = p^2$, então

$$\left|\{g^h \mid h \in \mathbf{G}\}\right| = |\mathbf{G} : \mathbf{C}_G(g)| = p^{n-2}.$$

Se $p = 2$, por [[7] III 11.9] $\mathbf{G} = \langle a, b \rangle$ com $a^{2^{n-1}} = e$ e $a^b = a^{-1+2^{n-2}}$ ou $a^b = a^{-1}$, então

$$\left|\{b^h \mid h \in \mathbf{G}\}\right| = |\{ba^{2j} \mid j = 0, 1, 2...\}| = 2^{n-2}.$$

Assim tomamos $g = b$. ∎

Capítulo 3

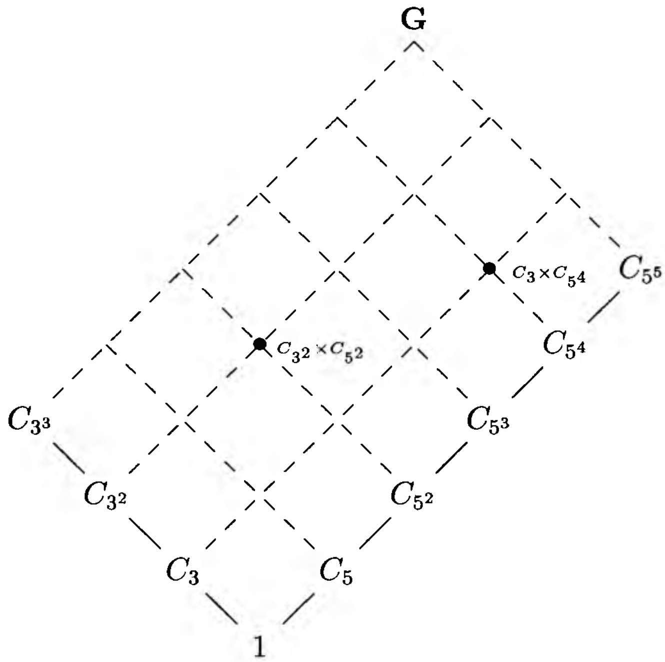
O Número de Dilworth

O *número de Dilworth* D($\mathfrak{V}$) de um conjunto parcialmente ordenado $\mathfrak{V}$ é definido como a máxima cardinalidade possível de uma anti-cadeia em $\mathfrak{V}$.

Definição 3.1. Seja $\mathbf{G}$ um grupo.
a) A *largura* $w(\mathbf{G})$ é definida como o número de Dilworth do reticulado $\mathfrak{L}(\mathbf{G})$, de todos os subgrupos de $\mathbf{G}$.
b) A *largura normal* $w_n(\mathbf{G})$ é o $D(\mathfrak{N}(\mathbf{G}))$, onde $\mathfrak{N}(G)$ é o reticulado de todos subgrupos normais de $\mathbf{G}$.

Para melhor elucidar a definição de largura de um grupo, vejamos o exemplo a seguir:

Exemplo 3.2. Seja $\mathbf{G} = C_{3^3} \times C_{5^5}$. Aqui temos um grupo abeliano, e assim todo subgrupo é normal. Conseqüentemente, $\mathfrak{L}(\mathbf{G}) = \mathfrak{N}(\mathbf{G})$. O diagrama de Hasse desse reticulado pode ser visualizado a seguir, onde observamos que $w(\mathbf{G}) = w_n(\mathbf{G}) = 4$. Para ver isto basta considerar a anti-cadeia $C_{3^3}, C_{3^2} \times C_{5^2}, C_3 \times C_{5^4}$ e C_{5^5}.



Podemos observar algumas conclusões imediatas da largura de um grupo: seja $\mathbf{U}$ um subgrupo de um grupo $\mathbf{G}$; temos que $w(\mathbf{U}) \leq w(\mathbf{G})$ e se $\mathbf{N}$ é um subgrupo normal de G então $w(\mathbf{G}/\mathbf{N}) \leq w(\mathbf{G})$ e $w_n(\mathbf{G}/\mathbf{N}) \leq w_n(\mathbf{G})$.

Lema 3.3. *Seja $G = \mathbb{Z}_{p^a} \times \mathbb{Z}_{q^b}$ onde p e q são primos distintos e $1 \leq a \leq b$. Então $w(G) = a + 1$.*

Lema 3.4. *Seja p um primo.*
(a) Se G é um p-grupo abeliano elementar de posto c, então $w(G) \geq 1 + p + ... + p^{c-1}$.
(b) Se $G = \mathbb{Z}_p \times \mathbb{Z}_{p^a}$ onde a é um inteiro positivo, então $w(G) \geq a(p-1) + 2$.
(c) Para qualquer n dado existe somente uma quantidade finita de p-grupos finitos abelianos e não cíclicos de largura n.

Demonstração. (a) Esse limite inferior dado é igual a quantidade de subgrupos de ordem p em $\mathbf{G}$. Estes claramente formam uma anti-cadeia.

(b) Se $a = 1$, segue da parte (a). Podemos então considerar $a \geq 2$. Um simples argumento de contagem mostra que $\mathbf{G}$ contém exatamente p subgrupos cíclicos de ordem p^b para todo $2 \leq b \leq a$. De fato, temos que $\mathbf{G} = \mathbb{Z}_p \times \mathbb{Z}_{p^a} = \langle x, y \mid x^p = 1, y^{p^a} = 1, [x, y] = 1 \rangle$. Um subgrupo cíclico de $\mathbf{G}$ é gerado por um único elemento $z = x^i y^j$, $0 \leq i \leq p-1, 0 \leq j \leq p^a - 1$. Observe que

$$\forall\ n \in \mathbb{N},\ \ z^n = x^{in} y^{jn}, \text{uma vez que } [x, y] = 1,$$

como queremos que a ordem do subgrupo seja p^b para $b \geq 2$, devemos ter então que $z^{p^b} = 1$ e $z^{p^b - 1} \neq 1$. Se $i = 0$ então o único subgrupo obtido é o único subgrupo de $\mathbb{Z}_{p^a}$ de ordem p^b. Os demais são obtidos compondo

$$x^i, \ 1 \leq i \leq p-1, \text{ com o } y^{p^{a-b}}, \text{ isto é, } z = x^i y^{p^{a-b}} \text{ pois } z^{p^b} = x^{ip^b}.y^{p^a} = 1.$$

Portanto os subgrupos de ordem p^b são, precisamente, os gerados por $x^i.y^{p^{a-b}}$.

Se b é menor que a, exatamente um desses subgrupos de ordem p^b está contido em $\mathbf{G}^p$, e seja $W_{b,1}, ..., W_{b,p-1}$ os subgrupos restantes. Seja $W_{a,1}, ..., W_{a,p}$ os subgrupos isomorfos com $\mathbb{Z}_{p^a}$ e seja $W_{1,1}, ..., W_{1,p}$ os subgrupos de ordem p de $\mathbf{G}$ que não estão contidos em $\mathbf{G}^p$. Afirmamos que o conjunto de todos $W_{i,j}$ formam uma anti-cadeia em $\mathfrak{L}(\mathbf{G})$.

De fato, $W_{i,j}$ é cíclico de ordem p^i e conseqüentemente se $W_{i,j} \lneqq W_{k,\ell}$ implica $i < k$ e então $W_{i,j} \leq (W_{k,\ell})^p \leq \mathbf{G}^p$ contrariando a escolha de $W_{i,j}$.

Isso mostra que $w(\mathbf{G}) \geq p + (a-2)(p-1) + p = a(p-1) + 2$.

(c) Seja n dado. Temos que existe um c tal que

$$\begin{aligned} \tfrac{p^c-1}{p-1} &= 1 + p + p^2 + ... + p^{c-1} > n \\ p^c - 1 &> n(p-1) \\ c &> \log_p(n(p-1)+1). \end{aligned}$$

Portanto se $\mathbf{G}$ for um p-grupo abeliano elementar de posto c, tal que $c > \log_p(n(p-1)+1)$, temos por (a) que $w(\mathbf{G}) > n$. Assim para que $w(\mathbf{G}) = n$ devemos escolher um c, onde $c < \log_p(n(p-1)+1)$, o que nos da uma quantidade finita de possibilidades.

Se $\mathbf{G}$ for um p-grupo abeliano finito não cíclico, que não é abeliano elementar, temos que

$$G = C_{p^\beta} \times C_{p^\alpha} \times ... \times C_{p^\sigma}$$

então existe um subgrupo $N \leq \mathbf{G}$ tal que

$$\mathbf{G}/N \cong C_p \times C_{p^a}.$$

Portanto se tomarmos $a > \frac{n-2}{p-1}$ temos por (b) que $w(\mathbf{G}) > n$. Assim temos que tomar $a < \frac{n-2}{p-1}$, o que novamente nos da um número finito de possibilidades.

Portanto temos um número finito de p-grupos abelianos finitos não cíclicos de largura n. ∎

Proposição 3.5. *Sejam p um primo e G um p-grupo não-cíclico finito.*
(a) Temos que $w(G) \geq p+1$.
(b) Se $w(G) = p+1$ então ou G é isomorfo ao grupo dos quatérnios de ordem 8 ou $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Demonstração. (a) Como $\mathbf{G}$ é não cíclico, por (1.20) $\mathbf{G}/\Phi(\mathbf{G}) = \langle g_1\Phi(\mathbf{G})\rangle_p \times \langle g_2\Phi(\mathbf{G})\rangle_p \times \dots \times \langle g_r\Phi(\mathbf{G})\rangle_p$, com $r \geq 2$. Seja $N = \langle g_3\Phi(\mathbf{G})\rangle_p \times \dots \times \langle g_r\Phi(\mathbf{G})\rangle_p$. Então temos que $\Phi(\mathbf{G}) \leq N$ e sabemos também pelo teorema (1.15) que $\mathbf{G}' \leq \Phi(\mathbf{G})$ e portando $\mathbf{G}' \leq N$. Tome $g \in \mathbf{G}$ e $n \in N$, temos que

$$gng^{-1} = gg^{-1}n[n, g^{-1}] = nn_1 \in N$$

assim, $N \triangleleft \mathbf{G}$. Conseqüentemente, $\mathbf{G}/\Phi(\mathbf{G})/N/\Phi(\mathbf{G}) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. E pelo terceiro teorema de isomorfismo temos que

$$\mathbf{G}/\Phi(\mathbf{G})/N/\Phi(\mathbf{G}) \cong \mathbf{G}/N$$

e portanto $\mathbf{G}/N \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Portanto a afirmação segue do lema anterior.

(b) Se $\mathbf{G}$ é um grupo quatérnio generalizado, então imediatamente obtemos $|\mathbf{G}| = 8$. Agora suponha que existe algum grupo ausente em nossa lista e seja $\mathbf{G}$ uma cópia de menor ordem possível. Temos então que existe um subgrupo maximal M de $\mathbf{G}$ contendo um subgrupo isomorfo com $\mathbb{Z}_p \times \mathbb{Z}_p$. Por indução temos que $M \cong \mathbb{Z}_p \times \mathbb{Z}_p$ e assim $\mathbf{G}$ é de ordem p^3.

Então podemos observar que se $\exp(\mathbf{G}) = p$, então $w(\mathbf{G}) \geq p^2+p+1 > p+1$. Agora, o Lema 3.4 (b) mostra que $w(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \geq 2p$. Por fim, seja $\mathbf{G}$ não abeliano e de expoente p^2, um argumento análogo ao usado na prova do Lema 3.4 (b) mostra que $w(\mathbf{G}) \geq 2p$. ∎

Observemos que para todo p-grupo finito não cíclico $\mathbf{G}$, temos $w_n(\mathbf{G}) \geq w(\mathbf{G}/\mathbf{G}') \geq p+1$. A segunda desigualdade e dada por 3.5 (a) e a primeira desigualdade é observada pelo seguinte fato: sejam $\theta : \mathbf{G} \to \bar{\mathbf{G}} = \mathbf{G}/\mathbf{G}'$ (o homomorfismo canônico) e $\bar{M} \in \bar{\mathbf{G}}$, assim temos um subgrupo M em $\mathbf{G}$ da seguinte forma: $M = \{g \in \mathbf{G} \mid \theta(g) \in \bar{M}\}$. Tome $m \in M$ e $g \in \mathbf{G}$, então $\theta(gmg^{-1}) = \theta(g)\theta(m)\theta(g)^{-1}$, como $\bar{M}$ é normal em $\bar{\mathbf{G}}$ temos que $\theta(g)\theta(m)\theta(g)^{-1} \in \bar{M}$, assim $gmg^{-1} \in M$ o que implica que M é normal em $\mathbf{G}$. Donde se verifica a primeira desigualdade.

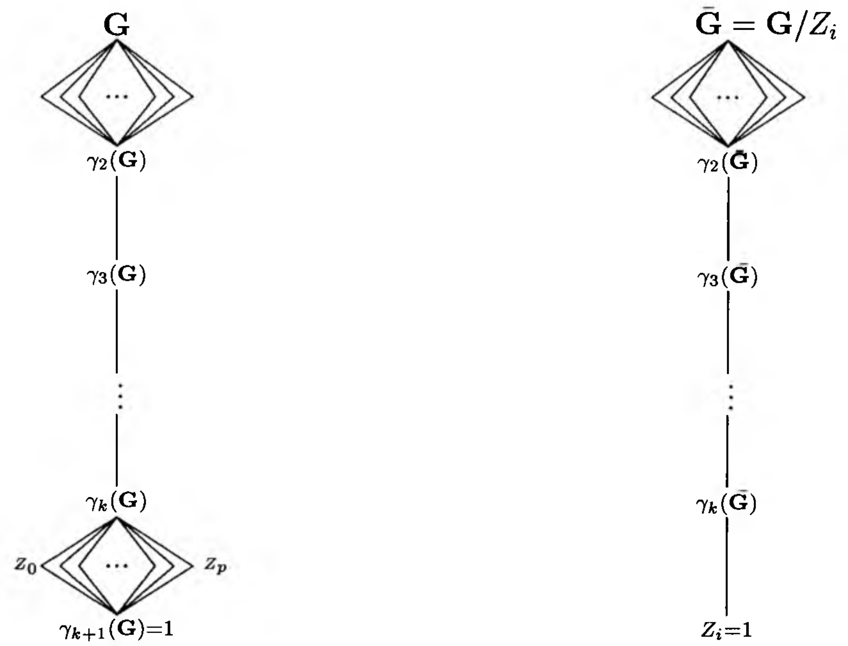
Podemos observar que $w_n(\mathbf{G}) = p+1$ se, e somente se, $\mathfrak{N}(\mathbf{G})$ consiste de um número de diamantes que são ligados por cadeias (onde por um diamante nós estamos querendo dizer um reticulado que tem um mínimo, um máximo e $p+1$ outros elementos intermediários). E como já vimos, $\mathbf{G}$ é de classe maximal se, e somente se, $\mathfrak{N}(\mathbf{G})$ consiste de exatamente um diamante no topo de uma cadeia.

Proposição 3.6. *Seja G um p-grupo finito de largura normal $p+1$. Seja $k \geq 4$ um inteiro.*
(a) Se $p = 2$, então G é de classe maximal.
(b) Se $G/\gamma_k(G)$ é de classe maximal e $k > p$, então G é de classe maximal.
(c) Se $G/\gamma_k(G)$ é de classe maximal e k é par, então $G/\gamma_{k+1}(G)$ é de classe maximal.
(d) Se $G/\gamma_k(G)$ é de classe maximal e se $[\gamma_2(G), \gamma_{k-2}(G)] \leq \gamma_{k+1}(G)$ então $G/\gamma_{k+1}(G)$ é de classe maximal.
(e) Se $G/\gamma_4(G)$ é de classe maximal e se G é metabeliano, então G é de classe maximal.

Demonstração. Pela observação acima temos que $w_n(\mathbf{G}) \geq w(\mathbf{G}/\mathbf{G}') \geq p+1$ e, por hipótese, $w_n(\mathbf{G}) = p+1$, temos que $w(\mathbf{G}/\mathbf{G}') = p+1$ e portanto, pela proposição 3.5, segue que $\mathbf{G}/\mathbf{G}' \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Assim todos os fatores centrais de $\mathbf{G}$ são abelianos elementares de posto ≤ 2. Em particular, $|\mathbf{G}'/\gamma_3(\mathbf{G})| \leq p$.

Para $p = 2$ temos que $\mathbf{G}$ é de classe maximal [[7]; pág. 339], assim podemos assumir que p é ímpar. Se $|\mathbf{G}| \leq p^4$, então temos que $\mathbf{G}$ é de classe maximal. De fato, se $\mathbf{G}$ tem ordem p^2, $\mathbf{G}$ é abeliano e portanto de classe 1; se $\mathbf{G}$ tem ordem p^3 e não é abeliano, então $c\ell(\mathbf{G}) > 1$, e como $|\mathbf{G}/\mathbf{G}'| = p^2$ e $\gamma_2(\mathbf{G})/\gamma_3(\mathbf{G})$ é cíclico de ordem p (pela proposição 1.3) temos que $c\ell(\mathbf{G}) = 2$; e se $\mathbf{G}$ tem ordem p^4, temos também que $|\mathbf{G}/\mathbf{G}'| = p^2$ e $|\gamma_2(\mathbf{G})/\gamma_3(\mathbf{G})| = p$, portanto se $c\ell(\mathbf{G}) = 2$ então temos que $|\mathbf{G}| = |\mathbf{G}/\mathbf{G}'|\,|\gamma_2(\mathbf{G})/\gamma_3(\mathbf{G})| = p^3$, uma contradição, assim temos que $c\ell(\mathbf{G}) = 3$. Assim para o restante da prova assumimos que $|\mathbf{G}| \geq p^5$.

Para provar (b) e (c), podemos admitir que $\gamma_{k+1}(\mathbf{G}) = 1$. Suponhamos, por contradição, que $\mathbf{G}$ não é de classe maximal. Então $\gamma_k(\mathbf{G}) \cong \mathbb{Z}_p \times \mathbb{Z}_p$, e sejam $Z_0, ..., Z_p$ seus subgrupos de ordem p. Claramente $\mathbf{G}/Z_i$ é de classe maximal.



Por nossas hipóteses, temos que $|\mathbf{G}| = p^{k+2}$. Assim, $|\mathbf{G}/Z_i| = p^{k+1}$. Observemos que, se $k > p$ temos que $k+1 > p+1$, e pelo Teorema 2.9 $\mathbf{G}/Z_i$ não é excepcional para nenhum $i = 0, ..., p$. Agora, se k é par, $k+1$ é ímpar, novamente pelo Teorema 2.9, temos que $\mathbf{G}/Z_i$ não é excepcional. Portanto, seja $\mathbf{G}_1 = C_{\mathbf{G}}(\gamma_2(\mathbf{G})/\gamma_4(\mathbf{G}))$, e escolha $s \in \mathbf{G} \backslash \mathbf{G}_1$ e $s_1 \in G_1 \backslash \gamma_2(\mathbf{G})$ e seja $t = [s_{1,k-1}\, s]$. Então o Lema 2.7 garante que $\gamma_k(\mathbf{G}) = \langle Z_i, t \rangle$ para todo $0 \leq i \leq p$. Mas $\gamma_k(\mathbf{G})$ é o conjunto união dos Z_i e chegamos em $\gamma_k(\mathbf{G}) = Z_i$ para ao menos um índice i, uma contradição.

Para provar (d), primeiro mostraremos que $\mathbf{G}$ pode ser gerado por dois elementos x e y tal que $[x, y, y] \in \gamma_4(\mathbf{G})$. Seja $\mathbf{G} = \langle x, z \rangle$ com $x, z \in \mathbf{G}$. Assim

$$\gamma_3(\mathbf{G})/\gamma_4(\mathbf{G}) = \langle [x, z, x]\gamma_4(\mathbf{G}), [x, z, z]\gamma_4(\mathbf{G}) \rangle$$

Por hipótese, este grupo é cíclico, e assim podemos assumir sem perda de generalidade que

$$[x, z, x] \equiv [x, z, z]^a mod \gamma_4(\mathbf{G}) \tag{3.1}$$

Módulo $\gamma_4(\mathbf{G})$ temos as seguintes congruências

$$[x, z^a, x] \equiv [x, z, x]^a = [x, z, z]^{a^2} \text{por } 3.1$$

e

$$[x, z^a, z^a] \equiv [x, z, z]^{a^2}.$$

Após substituir z por z^a, temos $\mathbf{G} = \langle x, z \rangle$ e

$$[x, z, x] \equiv [x, z, z] \ mod \gamma_4(\mathbf{G}). \tag{3.2}$$

Seja $z = xy$ para algum $y \in \mathbf{G}$. Então $\mathbf{G} = \langle x, y \rangle$ e temos

$$[x, z, x] \equiv [x, y, x]$$

e

$$[x, z, z] \equiv [x, y, x][x, y, y]$$

Isso, junto com 3.2 nos dá que

$$[x, y, y] \in \gamma_4(\mathbf{G}) \tag{3.3}$$

Agora $\gamma_k(\mathbf{G})$ é gerado por todos os comutadores $c = [x, y, z_1, z_2, ..., z_{k-2}]$ onde $z_i = x$ ou $z_i = y$. Pelas nossas hipóteses e corolário 1.6, podemos re-arranjar os z_i e escrever $c = [x, y,_t y,_{k-t-2} x]$ para qualquer inteiro t. Se $t \geq 1$, então por (3.3) temos que $c \in \gamma_{k+1}(\mathbf{G}) = 1$, e portanto $\gamma_k(\mathbf{G}) = \langle [x, y,_{k-2} x] \rangle$ é cíclico de ordem p, uma contradição.

Finalmente a parte (e) segue imediatamente de (d). ∎

Para finalizar este capítulo exibiremos um exemplo de um p-grupo que tem largura normal $p + 1$ mas que não é de classe maximal.

Exemplo 3.7. [3] Seja p um primo, $p \geq 5$, e seja $\mathbf{G}$ um grupo livre de expoente p e classe 3 nos geradores livres x e y. Então $\gamma_2(\mathbf{G})/\gamma_3(\mathbf{G}) = \langle [x, y]\gamma_3(\mathbf{G}) \rangle$ é cíclico de ordem p e $\gamma_3(\mathbf{G}) = \langle [x, y, x], [x, y, y] \rangle = Z(\mathbf{G})$ é abeliano elementar de ordem p^2. Assim $|\mathbf{G}| = p^5$.

Agora determinaremos os subgrupos normais de $\mathbf{G}$. Seja $N \trianglelefteq \mathbf{G}$ com $|N| = p^a$. Se $a = 1$ então $N \leq Z(\mathbf{G})$ e assim existem $p+1$ subgrupos N. Se $a = 3$ então $N = \mathbf{G}'$, com isso $\mathbf{G}$ possui exatamente $p + 1$ subgrupos de índice p. Finalmente se $a = 2$, suponha por contradição que $N \neq \gamma_3(\mathbf{G})$. Temos $N \leq Z_2(\mathbf{G}) = \mathbf{G}'$ e assim $N\gamma_3(\mathbf{G})/\gamma_3(\mathbf{G}) = \mathbf{G}'/\gamma_3(\mathbf{G})$. Conseqüentemente $[x, y] = nz$ para algum $n \in N$ e $z \in \gamma_3(\mathbf{G})$. Isso implica que $[x, y, x] = [nz, x] = [n, x] \in N$ e analogamente obtemos $[x, y, y] \in N$, uma contradição. Assim $\gamma_3(\mathbf{G})$ é o único subgrupo normal de ordem p^2 em $\mathbf{G}$. Isso mostra que $w_n(\mathbf{G}) = p+1$. Mas claramente, $\mathbf{G}$ não é de classe maximal.

Os grupos que têm largura normal $p+1$, como no exemplo anterior, serão chamados de grupos delgados. Na próxima seção estabeleceremos alguns resultados para tais grupos.

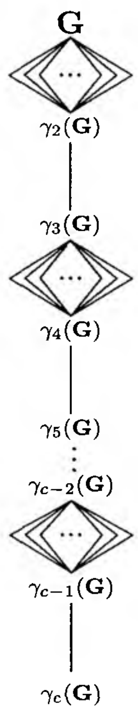
Capítulo 4

p-Grupos Metabelianos Delgados

Nessa seção trataremos os p-grupos delgados; daqui para frente, sempre que falarmos em um grupo $\mathbf{G}$, estaremos nos referindo a um p-grupo finito.

No capítulo 3 falamos sobre o número de Dilworth, aqui estaremos trabalhando os grupos onde toda anti-cadeia em $\mathfrak{N}(\mathbf{G})$ contém no máximo $p+1$ elementos, ou seja, grupos que têm *largura normal* $p+1$.

Um exemplo do diagrama do reticulado dos subgrupos normais de um p-grupo delgado é dado logo abaixo:



onde cada diamante no reticulado acima tem $p+1$ elementos.

Ao longo desta seção mostraremos os seguintes resultados:

Teorema 4.1. *Seja G um p-grupo metabeliano delgado. Então*
(a) $\gamma_{p+1}(G)$ é cíclico, e $\gamma_{p+2}(G) = 1$.
(b) $\mathfrak{N}(G)$ consiste de um diamante no topo, seguido por uma cadeia de comprimento 1, no máximo $p-2$ diamantes, mais um possível outra cadeia de comprimento 1.

O Teorema acima nos dá imediatamente que:

Corolário 4.2. *Para todo primo p, existe somente um quantidade finita de p-grupos metabelianos delgados.*

Teorema 4.3.
(a) Um p-grupo metabeliano G é delgado se, e somente se, $G/\gamma_5(G)$ é delgado.
(b) Um p-grupo metabeliano G com G/G' abeliano elementar de ordem p^2 o qual é de classe 4 e ordem p^7 (máxima possível) é delgado se, e somente se, os geradores a, b podem ser escolhidos tal que

$$[a, b, a, a] = [a, b, b, b]^k,$$

onde k não é um quadrado módulo p.

4.1 p-Grupos Delgados

Um grupo será considerado delgado quando toda anti-cadeia no reticulado dos subgrupos normais tiver no máximo $p+1$ elementos. Observe que os grupos de classe maximal satisfazem isso, mas tais grupos já foram bem estudados, por exemplo em [[7] III]. Portanto definimos um grupo delgado excluindo a classe dos grupos de classe maximal.

Definição 4.4. Um p-grupo não cíclico $\mathbf{G}$ é *delgado* se as duas condições seguintes são satisfeitas:
(i) toda anti-cadeia em $\mathfrak{N}(\mathbf{G})$ contém no máximo $p+1$ elementos, e
(ii) $\mathbf{G}$ não é de classe maximal.

Relembremos agora um conhecido resultado de Meier-Wunderli [12]:

Lema 4.5. *Um grupo 2-gerado metabeliano de expoente um primo p tem classe de nilpotência no máximo p − 1. Em outras palavras, se* G *é um p-grupo 2-gerado metabeliano, então* $G^p \geq \gamma_p(G)$.

Lema 4.6. *Seja* G *um p-grupo. Se* $G/\gamma_{i+1}(G)$ *tem expoente p, para* $1 \leq i \leq p-1$*, então* $\gamma_j(G)/\gamma_{j+i}(G)$ *tem expoente p.*

Demonstração. Em [[7], 2.3(b)] mostra o caso $i = 1$; o caso $i = 2$ foi demonstrado em [10].

Usaremos indução sobre i, e então sobre j. Para $i = 1, 2$, sabemos que o resultado é verdadeiro. Suponha por contradição que $g \in \gamma_j(\mathbf{G})$ tal que $g^p \notin \gamma_{j+i}(\mathbf{G})$. Então g é um produto de comutadores de peso j e maior. Agora pelo processo de coleta de P. Hall mostramos, com nossa hipótese de indução sobre i, que nós podemos assumir que $g = [u, v]$ é ele mesmo um comutador de peso peso j. Aplicando novamente o processo, nos podemos escrever $[u, v]^p = [u^p, v]P_1P_2$, onde P_1 é o produto de p-ésimas potências de comutadores de peso maior que j, e P_2 é o produto de comutadores de peso no mínimo $j + i$. Assim, $P_2 \in \gamma_{j+i}(\mathbf{G})$, e novamente por nossa hipótese de indução sobre i, temos também que $P_1 \in \gamma_{j+i}(\mathbf{G})$. Finalmente, nossa hipótese de indução sobre j mostra que $[u^p, v] \in \gamma_{j+i}(\mathbf{G})$, a assim $g^P \in \gamma_{j+i}(\mathbf{G})$, uma contradição. ∎

Lema 4.7. *Seja* G *um p-grupo finito, com p primo.*
(i) G é delgado ou de classe maximal se, e somente se, o comprimento máximo de uma anti-cadeia no reticulado dos subgrupos normais é $p + 1$.
(ii) Se G *é delgado e* N *é um subgrupo normal de* G*, então* N *é um termo da série central inferior de* G *se, e somente se,* N *é o único subgrupo normal desta ordem.*
(iii) Se G *é um grupo metabeliano delgado, então* $\gamma_3(G)/\gamma_4(G)$ *não é cíclico.*
(iv) Se G *é delgado, então* $|G| \geq p^5$, $cl(G) > 2$ *e* $G/\gamma_3(G)$ *tem expoente p.*

4.2 Séries Centrais e Centralizadores

Apresentaremos nesta seção alguns resultados sobre p-grupos delgados que como veremos são similares às propriedades dos p-grupos de classe maximal.

Lema 4.8. *Seja* G *um p-grupo delgado. Seja* $h \in \gamma_i(G) - \gamma_{i+1}(G)$*. Então* $\gamma_{i+1}(G) = [h, G]\gamma_{i+2}(G)$.

Demonstração. Podemos assumir $\gamma_{i+2}(\mathbf{G}) = 1$. Temos que $[h, \mathbf{G}] \leq \gamma_{i+1}(\mathbf{G})$, pela definição de $\gamma_{i+1}(\mathbf{G})$. Temos que mostrar agora que $\gamma_{i+1}(\mathbf{G}) = [h, \mathbf{G}]$. Assuma por contradição que $H = [h, \mathbf{G}] < \gamma_{i+1}(\mathbf{G})$ (com o símbolo $<$ queremos dizer que H está estritamente contido em $\gamma_{i+1}(\mathbf{G})$). Temos que $H \trianglelefteq \mathbf{G}$, uma vez que $H \leq \gamma_{i+1}(\mathbf{G}) \leq Z(\mathbf{G})$.

Seja $\bar{\mathbf{G}} = \mathbf{G}/H$. Tome $\bar{h} \in Z(\bar{\mathbf{G}})$ (onde $\bar{h}$ é a classe lateral hH) e seja $g \in \gamma_{i+1}(\mathbf{G}) - H$; então temos que

$$\bar{g} \neq \bar{1} \text{ e } Z(\bar{\mathbf{G}}) \geq \langle \bar{g}, \bar{h} \rangle = \bar{K}.$$

Pelo Lema 4.7 (iv) temos que $\mathbf{G}/\gamma_3(\mathbf{G})$ tem expoente p e pelo Lema 4.6 fazendo $i = 2$ e $j = i$ obtemos que $\gamma_i(\mathbf{G})/\gamma_{i+2}(G)$ tem expoente p, mas $\gamma_{i+2}(\mathbf{G}) = 1$, portanto temos que $\gamma_i(\mathbf{G})$ tem expoente p. Como $h \in \gamma_i(\mathbf{G})$ e $g \in \gamma_{i+1}(\mathbf{G}) \leq \gamma_i(\mathbf{G})$, temos que h e g têm expoente p e portanto $\bar{K}$ tem expoente p. Assim $\bar{K}$ é abeliano elementar, $|\bar{K}| = p^2$ e todo subgrupo de $\bar{K}$ de ordem p é normal em $\bar{\mathbf{G}}$. Assim temos $p+1$ subgrupos normais em $\bar{\mathbf{G}}$ de ordem p. Como $\mathbf{G}$ é delgado temos que $|\gamma_{i+1}(\mathbf{G})/\gamma_{i+2}(\mathbf{G})| \leq p^2$, e como $H \neq 1$ e por hipótese $H < \gamma_{i+1}(\mathbf{G})$ temos que $|\gamma_{i+1}(\mathbf{G})| = p^2$. Sejam $Z_0, Z_1, ..., Z_p$ os subgrupos de $\bar{\mathbf{G}}$ de ordem p e θ o homomorfismo canônico de $\mathbf{G}$ em $\bar{\mathbf{G}}$. Como Z_k tem ordem p, com $k = 0, 1, 2, ..., p$ temos que $Z_k = \langle zH \rangle$, onde $z \notin H$, ou seja, $Z_k = \{H, zH, z^2H, ..., z^{p-1}H\}$.

Afirmação: $\theta^{-1}(Z_k) = \langle z, h \rangle$, onde $z, h \in \mathbf{G}$, $H = \langle h \rangle$ e $Z_k = \langle zH \rangle$. E portanto $|\theta^{-1}(Z_k)| = |\langle z, h \rangle| = p^2$.

De fato, tome $g \in \theta^{-1}(Z_k)$, onde $\theta^{-1}(Z_k) = \{g \in \mathbf{G} \,|\, \theta(g) \in Z_k\}$, temos então que $\theta(g) = z^iH$ o que implica que $g = z^ih^j$, com $i = 0, 1, ..., p-1$ e $j = 0, 1, ..., p-1$ donde podemos concluir que $g \in \langle z, h \rangle$ e portanto $\theta^{-1}(Z_k) \subseteq \langle z, h \rangle$. Por outro lado, tome $w \in \langle z, h \rangle$, então temos que $w = z^ih^j$. Mas temos que $\theta(w) = wH = z^ih^jH = z^iH$ e portanto $\theta(w) \in Z_k$ o que implica que $w \in \theta^{-1}(Z_k)$, donde segue que $\langle z, h \rangle \subseteq \theta^{-1}(Z_k)$. Portanto $\theta^{-1}(Z_k) = \langle z, h \rangle$, donde segue que $|\theta^{-1}(Z_k)| = |\langle z, h \rangle| = p^2$.

Portanto as pré-imagens dos Z_k, $k = 1, 2, ..., p-1$, são $p+1$ subgrupos de ordem $|\gamma_{i+1}(\mathbf{G})|$ em $\mathbf{G}$, o que é um absurdo pois contraria o fato de $\mathbf{G}$ ser delgado e ter somente um subgrupo normal de ordem $|\gamma_{i+1}(\mathbf{G})|$, Lema 4.7(ii). ∎

Corolário 4.9. *As séries centrais inferior e superior de um p-grupo delgado coincidem.*

Demonstração. Faremos indução sobre a classe c de $\mathbf{G}$. Assim, basta mostrar que $Z(\mathbf{G}) = \gamma_c(\mathbf{G})$. Como $\mathbf{G}$ é delgado temos que $|\gamma_c(\mathbf{G})| \leq p^2$. Suponhamos primeiramente que $|\gamma_c(\mathbf{G})| = p^2$. Temos que $\gamma_c(\mathbf{G}) \leq Z(\mathbf{G})$, supondo $\gamma_c(\mathbf{G}) < Z(\mathbf{G})$ teríamos $|Z(\mathbf{G})| \geq p^3$, mas como todo subgrupo de $Z(\mathbf{G})$ é normal em $\mathbf{G}$, teríamos uma anti-cadeia com mais de $p+1$ elementos, contrariando o fato de que $\mathbf{G}$ é delgado. Podemos assumir também $|\gamma_c(\mathbf{G})| = p$ e por contradição supor que $\gamma_c(\mathbf{G}) < Z(\mathbf{G})$.

Temos pelo Lema 4.7(ii) que $Z(\mathbf{G}) \leq \gamma_{c-1}(\mathbf{G})$. Então se $g \in Z(\mathbf{G}) - \gamma_c(\mathbf{G})$, tal que $g \in \gamma_{c-1}(\mathbf{G})$, pelo Lema 4.8 $\gamma_c(\mathbf{G}) = [g, \mathbf{G}] = 1$. Contradição. ∎

Como vimos no capítulo 2, Lema 2.12, os p-grupos de classe maximal são caracterizados por possuírem um elemento cujo centralizador tem ordem p^2. Uma tentativa parecida para caracterizar os p-grupos delgados como grupos que têm um elemento cujo centralizador tem ordem p^3 falha. Pois como veremos no exemplo a seguir, um grupo pode possuir um elemento cujo centralizador tem ordem p^3 sem necessariamente ser delgado.

Exemplo 4.10. Seja $\mathbf{G} = \langle a, b \mid a^5 = b^5 = [b,a,a,a] = 1, \gamma_5(\mathbf{G}) = 1\rangle$.

Onde $Z(\mathbf{G}) = \gamma_4(\mathbf{G}) = \langle [b,a,a,b], [b,a,b,b]\rangle$, o centralizador de b é $\langle b, Z(\mathbf{G})\rangle$ de ordem 5^3, mais $\mathbf{G}$ não é delgado, pois o subgrupo $\langle [b,a,a], [b,a,a,b]\rangle$ é normal de ordem 5^2, mas ele é diferente de $\gamma_4(\mathbf{G})$, contrariando assim 4.7(ii).

Contudo, podemos caracterizar os p-grupos metabelianos delgados como grupos onde a ordem do centralizador de qualquer elemento $g \in \mathbf{G} - \mathbf{G}'$ é p^3. O teorema a seguir mostra a primeira parte dessa caracterização sem a necessidade do grupo ser metabeliano, mas para provar sua recíproca precisamos adicionar a hipótese do grupo ser metabeliano.

Teorema 4.11. *Seja $\mathbf{G}$ um p-grupo não-abeliano. Se $|C_G(g)| = p^3$, para todo $g \in \mathbf{G} - \mathbf{G}'$. Então $\mathbf{G}$ é delgado.*

Demonstração. Seja $\mathbf{G}$ um contra-exemplo mínimo. Dividimos a demonstração em três passos.

Passo 1: $cl(\mathbf{G}) \geq 3$

Se $\mathbf{G}$ tem classe 2, temos que $\mathbf{G}' \leq Z(\mathbf{G})$; se $z \in Z(\mathbf{G}) - \mathbf{G}'$, $C_{\mathbf{G}}(z) = G$, e $|\mathbf{G}| = p^3$, e portanto teríamos $\mathbf{G} = Z(\mathbf{G})$, então $\mathbf{G}$ é abeliano, contradição. De modo que $\mathbf{G}' = Z(\mathbf{G})$.

Usaremos agora um resultado de [1] ou [7]: se $\mathbf{G}$ é um p-grupo de classe 2, tal que para todo $g \in \mathbf{G} - \mathbf{G}'$, temos $[g, \mathbf{G}] = \mathbf{G}'$, então $\mathbf{G}/\mathbf{G}'$ é abeliano elementar de posto par. De fato nossas hipóteses dão que $|\mathbf{G}'| = p$ ou $|\mathbf{G}'| = p^2$, pois, como $\mathbf{G}$ não é abeliano existe pelo menos um $g \in \mathbf{G}$ tal que $g \notin Z(\mathbf{G})$ e então temos que $Z(\mathbf{G}) < C_{\mathbf{G}}(g)$ e como $|C_{\mathbf{G}}(g)| = p^3$ então $|Z(\mathbf{G})| \leq p^2$. Se $|\mathbf{G}'| = p$, por $\mathbf{G}' = Z(\mathbf{G})$ podemos aplicar o resultado acima, pois tomando $g \in \mathbf{G} - \mathbf{G}'$, $|[g, \mathbf{G}]| > 1$ e como $[g, \mathbf{G}] \leq \mathbf{G}'$ obtemos que $|[g, \mathbf{G}]| = p$; mas neste caso $[\mathbf{G} : C_{\mathbf{G}}(g)] = p$ para $g \in \mathbf{G} - \mathbf{G}'$ e $|\mathbf{G}| = p^4$, uma contradição.

Se $|\mathbf{G}'| = p^2$, por nossas hipóteses e Proposição 1.18, $\mathbf{G}$ é um grupo especial. De fato, temos que $\mathbf{G}$ não é abeliano, portanto para que ele seja especial ele deve ter classe 2 e $\mathbf{G}' = Z(\mathbf{G}) = \Phi(\mathbf{G})$ é abeliano elementar. Já temos que $\mathbf{G}$ é de classe 2 e que $\mathbf{G}' = Z(\mathbf{G})$, falta mostrar que $\Phi(\mathbf{G}) = \mathbf{G}'$ e que é abeliano elementar. Observe que $\mathbf{G}$ não pode conter um subgrupo abeliano de ordem maior ou igual a p^4, pois caso contrário, poderíamos tomar um elemento g nesse subgrupo e fora de $\mathbf{G}'$ e teríamos $|C_{\mathbf{G}}(g)| \geq p^4$, o que não pode acontecer. Assim se H é um subgrupo abeliano de $\mathbf{G}$, então $|H| \leq p^3$, e portanto $|H/Z(\mathbf{G})| \leq p$. Então pela Proposição 1.18 temos que $\mathbf{G}/Z(\mathbf{G})$ é abeliano elementar o que implica que $\forall\, g \in \mathbf{G}$, $g^p \in \mathbf{G}'$, assim pelo Teorema 1.16 temos que $\Phi(\mathbf{G}) = \mathbf{G}'$. Agora para mostrar que $Z(\mathbf{G})$ é abeliano elementar basta mostrar que $exp(Z(\mathbf{G})) = p$. Dado qualquer elemento $[x, y] \in \mathbf{G}'$ temos que $[x, y]^p = [x^p, y]$, pois $c\ell(\mathbf{G}) = 2$, e como já vimos que $x^p \in \mathbf{G}' = Z(\mathbf{G})$ temos que $[x, y]^p = [x^p, y] = 1$. Portanto $Z(\mathbf{G})$ é abeliano elementar. Observemos agora que $|\mathbf{G}/Z(\mathbf{G})| \geq p^2$, pois caso contrário teríamos que $\mathbf{G}$ é abeliano, assim existem $x, y \in \mathbf{G} - \mathbf{G}'$, tal que $[g, x] \neq 1$ e $[g, y] \neq 1$, como $[g, x]$ e $[g, y] \in [g, \mathbf{G}]$ e cada um deles têm ordem p temos que $[g, \mathbf{G}] \geq p^2$ e $[g, \mathbf{G}] \subseteq \mathbf{G}'$ então $[g, \mathbf{G}] = \mathbf{G}'$. Portanto $p^2 = |[g, \mathbf{G}]| = |\mathbf{G} : C_{\mathbf{G}}(g)| = |\mathbf{G} : \langle g \rangle\, Z(\mathbf{G})|$, de modo que $|\mathbf{G}| \leq p^5$. Se $|\mathbf{G}| = p^5$ podemos aplicar novamente o resultado enunciado acima, obtendo uma contradição; se $|\mathbf{G}| = p^4$, então $\mathbf{G}$ é 2-gerado e pela Proposição 1.3 $\mathbf{G}' = Z(\mathbf{G})$ é cíclico, novamente uma contradição. Assim $\mathbf{G}$ deve ter classe no mínimo 3.

Passo 2: Se $M, N \trianglelefteq G$, $M \neq 1$, $|N| = p$, $N \leq \gamma_c(\mathbf{G})$ e $N \nleq M$, então $|M| = p$; e tal M sempre existe.

Por indução $\mathbf{G}/N$ é delgado ou de classe maximal, pois

$$|C_{\mathbf{G}/N}(gN)| \leq |C_{\mathbf{G}}(g)|$$

Para mostrar que $|M| = p$ procedemos por contradição, e podemos assumir que $|M| = p^2$. Uma vez que $M \cap Z(\mathbf{G}) \neq 1$, temos que $C_{\mathbf{G}}(M)$ é maximal. Pois caso contrário, se $C_{\mathbf{G}}(M)$ não é maximal, existe um subgrupo maximal H de $\mathbf{G}$ tal que $C_{\mathbf{G}}(M) \leq H$. Assim tome $h \in H - \mathbf{G}'$. Temos que $|C_H(h)| = |M \cap Z(\mathbf{G})|\,|N|\,|\langle h \rangle| = p^3$. Mas H não é delgado pois $M \leq H$ e $N \leq H$ e assim existe uma anti-cadeia de largura maior do que $p + 1$, o que contrária a minimalidade de $\mathbf{G}$. Assim, seja $g \in C_{\mathbf{G}}(M) - \mathbf{G}'$; então

$MN \leq C_{\mathbf{G}}(g)$, pois $M \leq C_{\mathbf{G}}(g)$ e $N \leq Z(\mathbf{G})$. Temos $|MN| = p^3$, assim $MN = C_{\mathbf{G}}(g)$, conseqüentemente $g \in MN \leq Z_2(\mathbf{G})$ e $gN \in Z_2(\mathbf{G}/N)$. Como $\mathbf{G}/N$ é ou delgado ou de classe maximal, temos $Z_2(\mathbf{G}/N) \leq \mathbf{G}'/N$ e $g \in \mathbf{G}'$, uma contradição. Uma vez que $\mathbf{G}$ não é delgado, tal M deve existir.

Passo 3: Conclusão

Nós agora temos que $Z(\mathbf{G}) = MN$ e existe $h \in \gamma_{c-1}(\mathbf{G}) - (\gamma_{c-1}(\mathbf{G}) \cap Z(\mathbf{G}))$. Se $\gamma_c(\mathbf{G}) = N$, nós teríamos que $C_{\mathbf{G}}(h)$ é maximal, e $\langle h \rangle Z(\mathbf{G})$ centralizaria algum $g \in C_{\mathbf{G}}(h) - \mathbf{G}'$; uma vez que $|\langle h \rangle Z(\mathbf{G})| = p^3$, $\langle h \rangle Z(\mathbf{G}) \leq \gamma_{c-1}(\mathbf{G})Z(\mathbf{G})$, poderíamos encontrar uma contradição como no *Passo 2*. Assim $N < \gamma_c(\mathbf{G})$. Uma vez que $\gamma_c(\mathbf{G}) \leq Z(\mathbf{G})$ temos $\gamma_c(\mathbf{G}) = NM$. Portanto $\mathbf{G}$ é delgado, uma contradição. ∎

4.3 p-Grupos Metabelianos Delgados

Lema 4.12. *Seja G um p-grupo metabeliano delgado. Assuma que $\gamma_i(G)/\gamma_{i+1}(G)$ é cíclico, para algum $i \geq 4$. Então $\gamma_i(G)$ é uma imagem epimórfica de G'.*

Demonstração. Usando as técnicas de anéis apresentadas no capítulo 1, temos que $\mathbf{G}'$ é um A-módulo cíclico fiel. Mostraremos que, com nossas hipóteses, $\gamma_i(\mathbf{G})$ é também um A-módulo cíclico, pois $\gamma_{i+1}(\mathbf{G})$ é seu único submódulo maximal. Como $\gamma_i(\mathbf{G})/\gamma_{i+1}(\mathbf{G})$ é cíclico, temos que $\gamma_i(\mathbf{G}) = \langle h, \gamma_{i+1}(\mathbf{G}) \rangle$, onde $\gamma_i(\mathbf{G})/\gamma_{i+1}(\mathbf{G}) = \langle h\gamma_{i+1}(\mathbf{G}) \rangle$.

Afirmação: Se um A-módulo M finitamente gerado contém um único submódulo maximal N então qualquer elemento de N pode ser retirado do conjunto gerador.

De fato, seja $C = \{x_1, x_2, ...x_n, y\}$ um conjunto gerador de M onde $y \in N$. Suponha por contradição que $C' = \{x_1, x_2, ..., x_n\}$ não gere M, então C' gera um submódulo próprio contido ou igual a N. Como $y \in N$ temos que C gera um submódulo próprio de M, o que é uma contradição. Portanto C' gera M como um A-módulo.

Portanto, qualquer elemento de $\gamma_{i+1}(\mathbf{G})$ pode ser omitido do conjunto gerador de $\gamma_i(\mathbf{G})$, e assim podemos concluir que $\gamma_i(\mathbf{G}) = \langle h \rangle$. Assim $\gamma_i(\mathbf{G})$ é uma imagem epimórfica de $\mathbf{G}'$ (como um A-módulo). ∎

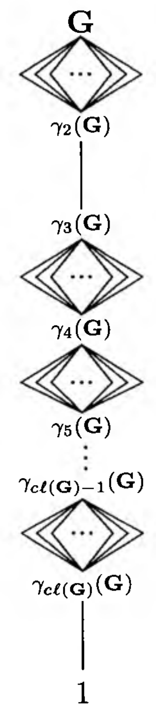
Uma conseqüência do Lema anterior é o seguinte Corolário:

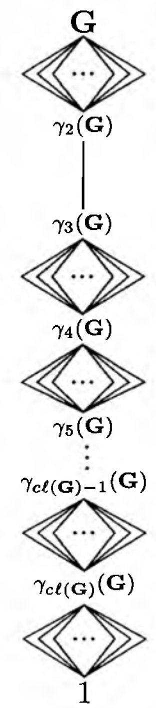
Corolário 4.13. *Seja G um p-grupo metabeliano delgado, e seja $\gamma_i(G)/\gamma_{i+1}(G)$ cíclico, para algum $i \geq 4$. Então $\gamma_{i+1}(G) = 1$, de modo que $c\ell(G) \leq i$.*

Demonstração. Seja $N \trianglelefteq \mathbf{G}$ tal que $[N : \gamma_i(\mathbf{G})] = p$. Temos que N é um A-módulo cíclico, pois $\gamma_i(\mathbf{G})$ é seu único submódulo maximal. Portanto N é uma imagem epimórfica de $\mathbf{G}'$; e uma vez que $\gamma_3(\mathbf{G})/\gamma_4(\mathbf{G})$ não é cíclico, temos que $\gamma_{i+1}(\mathbf{G}) = 1$. De fato, temos que existe um homomorfismo φ do A-módulo $\mathbf{G}'$ sobre o A-módulo cíclico N. O núcleo desse homomorfismo é um A-submódulo de $\mathbf{G}'$, que é, um subgrupo normal de $\mathbf{G}$ contido em $\mathbf{G}'$. Se este núcleo estiver contido em $\gamma_4(\mathbf{G})$, então os $p+1$ subgrupos normais (A-submódulos) intermediários entre $\gamma_3(\mathbf{G})$ e $\gamma_4(\mathbf{G})$ são aplicados em $p+1$ subgrupos normais (A-submódulos) com a mesma ordem de $\gamma_{i+1}(\mathbf{G})$. Mas isso contraria o fato do grupo ser delgado (Lema 4.7 (ii)). De modo que o núcleo deve ser um dos subgrupos intermediários acima, e esta imagem (que é $\{1\}$) é $\gamma_{i+1}(\mathbf{G})$. ∎

Assim todos os fatores centrais inferiores (e superiores) de um p-grupo metabeliano delgado têm ordem p^2, exceto possivelmente $\gamma_2(\mathbf{G})/\gamma_3(\mathbf{G})$ e $\gamma_{c\ell(\mathbf{G})}(\mathbf{G})$.

Então o reticulado dos subgrupos normais de um p-grupo metabeliano delgado seria dado por um dos seguintes tipos abaixo.





Lema 4.14. *Seja G um p-grupo metabeliano delgado, e seja $g \in G - \gamma_2(G)$. Assuma que $g^p \in \gamma_i(G) - \gamma_{i+1}(G)$. Então $\gamma_{i+1}(G)$ é cíclico e $c\ell(G) \leq i+1$.*

Demonstração. Pelo Lema 4.8, temos que $[g^p, \mathbf{G}]\gamma_{i+2}(\mathbf{G}) = \gamma_{i+1}(\mathbf{G})$. Trabalhando módulo $\gamma_{i+2}(\mathbf{G})$, temos que:

$$[g^p, \mathbf{G}] \equiv \langle [g^p, g], [g^p, h] \rangle \equiv \langle [g^p, h] \rangle$$

onde escolhemos $h \in \mathbf{G} - \gamma_i(\mathbf{G})$ tal que $\langle g, h \rangle = \mathbf{G}$. O limite sobre a classe é uma conseqüência imediata do Corolário 4.13. ∎

Teorema 4.15. *Seja G um p-grupo metabeliano delgado. Então $c\ell(G) \leq p+1$, $G^{p^2} = 1$, $\gamma_2(G)^p \leq \gamma_{c\ell(G)}(G)$ e $\gamma_3(G)^p = 1$.*

Demonstração. Seja ℓ o maior inteiro tal que $\mathbf{G}^p \leq \gamma_\ell(\mathbf{G})$. Pelo Lema 4.7(iv), $\ell \geq 3$. Além disso, se $\mathbf{G}^p \leq \gamma_p(\mathbf{G})$, então pelo resultado de Meier-Wunderli (Lema 4.5) $\mathbf{G}^p = \gamma_p(\mathbf{G})$, de modo que $\ell \leq p$.

Como $\mathbf{G}/\gamma_\ell(\mathbf{G})$ tem expoente p, podemos aplicar o Lema 4.6 para obter que $\gamma_2(\mathbf{G})/\gamma_{\ell+1}(\mathbf{G})$ e $\gamma_3(\mathbf{G})/\gamma_{\ell+2}(\mathbf{G})$ têm expoente p, de modo que $\gamma_2(\mathbf{G})^p \leq \gamma_{\ell+1}(\mathbf{G})$ e $\gamma_3(\mathbf{G})^p \leq \gamma_{\ell+2}(\mathbf{G})$. Conseqüentemente existe um elemento $g \in \mathbf{G} - \gamma_2(\mathbf{G})$ com $g^p \in \gamma_\ell(\mathbf{G}) - \gamma_{\ell+1}(\mathbf{G})$. Pelo Lema 4.14, $\gamma_{\ell+2}(\mathbf{G}) = 1$, e a classe de $\mathbf{G}$ ou é ℓ ou $\ell+1$. ∎

Agora podemos demonstrar a recíproca do Teorema 4.11 no caso de grupos metabelianos:

Teorema 4.16. *Seja G um grupo metabeliano delgado e $g \in G - G'$. Então $|C_G(g)| = p^3$.*

Demonstração. Seja $a \in \mathbf{G} - \mathbf{G}'$, e escolha um elemento $b \in \mathbf{G}$ de modo que $\mathbf{G} = \langle a, b \rangle$. Temos que $C_{\mathbf{G}'}(a) = C_{\mathbf{G}}(a) \cap \mathbf{G}'$ e portanto $\langle a \rangle C_{\mathbf{G}'}(a) = \langle a \rangle (C_{\mathbf{G}}(a) \cap \mathbf{G}')$ e pela lei modular (Lema 1.19) temos $\langle a \rangle C_{\mathbf{G}'}(a) = C_{\mathbf{G}}(a) \cap \mathbf{G}' \langle a \rangle$. Mas podemos observar que $\mathbf{G}' \langle a \rangle$ é um subgrupo maxímal contendo $\langle a \rangle$. E como $\mathbf{G}$ é nilpotente temos que $C_{\mathbf{G}}(a)$ é subnormal, e portanto existe uma seqüência $C_{\mathbf{G}}(a) \lhd H_1 \lhd ... \lhd H_m \lhd \mathbf{G}$. Mas como $\mathbf{G}'$ não contém $\langle a \rangle$ e por outro lado $\langle a \rangle \subseteq C_{\mathbf{G}}(a)$ temos que a sequência acima se reduz $C_{\mathbf{G}}(a) \lhd H_1 \lhd \mathbf{G}$, onde H_1 é um subgrupo maxímal de $\mathbf{G}$. Mas $\mathbf{G}' \langle a \rangle$ é o único subgrupo maxímal de $\mathbf{G}$ contendo $\langle a \rangle$. Portanto temos que $C_{\mathbf{G}}(a) \subseteq \mathbf{G}' \langle a \rangle$. Assim obtemos $C_{\mathbf{G}}(a) = C_{\mathbf{G}'}(a) \langle a \rangle$. Além disso, $C_{\mathbf{G}'}(a)$ é normal em $\mathbf{G}$, pois as ações de a e b sobre $\mathbf{G}'$ comutam por conjugação.

Agora, se $C_{\mathbf{G}'}(a) \leq Z(\mathbf{G})$, então $C_{\mathbf{G}'}(a) = Z(\mathbf{G})$. Se $|Z(\mathbf{G})| = p$, temos que:

$$|C_{\mathbf{G}}(a)| = |\langle a\rangle|\,|C_{\mathbf{G}'}(a)| = p^2$$

assim pelo Lema 2.12 temos que $\mathbf{G}$ é de classe maximal. Contradição.

Por outro lado temos que, se $C_{\mathbf{G}'}(a)$ não está contido em $Z(\mathbf{G})$, então pelo Lema 4.8 $C_{\mathbf{G}'}(a) \leq Z_2(\mathbf{G})$ e $Z(\mathbf{G})$ é cíclico. De fato, suponha que $Z_2(\mathbf{G}) < C_{\mathbf{G}'}(a)$. Então existe $g \in C_{\mathbf{G}'}(a) - Z_2(\mathbf{G})$ e pelo Lema 4.8 temos que $Z_2(\mathbf{G}) = [g, \mathbf{G}]Z(\mathbf{G})$. Trabalhando módulo $Z(\mathbf{G})$ temos que

$$Z_2(\mathbf{G}) = [g, \mathbf{G}] = \langle [g, a], [g, b]\rangle = \langle [g, b]\rangle$$

e portanto $Z_2(\mathbf{G})/Z(\mathbf{G})$ é cíclico. Contradição, pois $\mathbf{G}$ é delgado. Assim $C_{\mathbf{G}'}(a) \leq Z_2(\mathbf{G})$.

Portanto, tome $g \in C_{\mathbf{G}'}(a) - Z(\mathbf{G})$, novamente pelo Lema 4.8 temos que $Z(\mathbf{G}) = [g, \mathbf{G}] = \langle [g, b]\rangle$. Assim obtemos que $Z(\mathbf{G})$ é cíclico.

Assuma por contradição que $C_{\mathbf{G}'}(a) = Z_2(\mathbf{G})$ de ordem p^3. Uma vez que $[Z_2(\mathbf{G}), b] \leq Z(\mathbf{G})$, e $|Z(\mathbf{G})| = p$, existe um elemento $u \in Z_2(\mathbf{G}) - Z(\mathbf{G})$ o qual é centralizado por b, de modo que $u \in Z(\mathbf{G})$, uma contradição. Portanto, $|C_{\mathbf{G}'}(a) = p^2|$ e conseqüentemente $|C_{\mathbf{G}}(a)| = p^3$. ∎

Podemos agora provar o Teorema 4.3. Primeiramente, se $\mathbf{G}$ é delgado, seus grupos fatores ou são delgados ou de classe maximal.

Observamos também que em um p-grupo metabeliano delgado, nós temos, por resultados anteriores que

$$|\mathbf{G}| = |\mathbf{G}/\gamma_2(\mathbf{G})|\,.\,|\gamma_2(\mathbf{G})/\gamma_3(\mathbf{G})|\,.\left(\prod_{i=3}^{p}|\gamma_i(\mathbf{G})/\gamma_{i+1}|\right).\,|\gamma_{p+1}(\mathbf{G})| \leq p^2.p.(p^2)^{p-2}.p = p^{2p}.$$

Exemplo 4.17. Um exemplo de um 3-grupo onde esta cota é realmente atingida, ou seja, um grupo metabeliano delgado de ordem 3^6, é dado a seguir.

Seja $\mathbf{G}$ um grupo com a seguinte apresentação:

$$\mathbf{G} = \langle a, b \mid a^3 = b^3 = [a,b,b,b] = [a,b,a,a] = [a,b,a,b] = [a,b,a,b,a] = [a,b,a,b,b] = 1, \\ [a,b,a,b] = [a,b,b,a]\rangle\,.$$

Este grupo é metabeliano delgado de classe 4 e ordem 3^6. Esses resultados foram verificados utilizando o programa GAP [5]. O algoritmo utilizado para fazer estas verificações foi o seguinte:

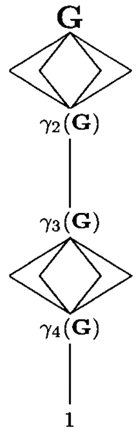
```
Entrando com a apresentação do grupo:
f:=FreeGroup("a", "b");
r:=[f.1^3, f.2^3,
Iterated([f.1, f.2, f.1, f.1], Comm),
Iterated([f.1, f.2, f.2, f.2], Comm),
Iterated([f.1, f.2, f.1, f.2], Comm)^3,
Iterated([f.1, f.2, f.1, f.2, f.1], Comm),
Iterated([f.1, f.2, f.1, f.2, f.2], Comm),
Iterated([f.1, f.2, f.1, f.2], Comm)/Iterated([f.1, f.2, f.2, f.1], Comm)];
g:=f/r;
```

Para verificar se o grupo é delgado, mostraremos que: $\mathbf{G}/\mathbf{G}' \approx \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbf{G}'/\gamma_3(\mathbf{G}) \approx \mathbb{Z}_3$, $\gamma_3(\mathbf{G})/\gamma_4(\mathbf{G}) \approx \mathbb{Z}_3 \times \mathbb{Z}_3$ e $\gamma_4(\mathbf{G}) \approx \mathbb{Z}_3$. Para fazer tais verificações no GAP, utilizamos o seguinte procedimento:

```
gap> IsElementaryAbelian(l[2]);
true
gap> AbelianIvariants(g);
[3 3]
gap> AbelianInvariants(l[2]/l[3]);
[3]
gap> AbelianInvariants(l[3]/l[4]);
[3 3]
gap> AbelianInvariants(l[4]);
[3]
```

onde l[i]=$\gamma_i(\mathbf{G})$.

Com isso, podemos exibir o reticulado dos subgrupos normais deste grupo, como a seguir:



Este reticulado também pode ser construído utilizando uma ferramenta do GAP, chamada xgap, através do procedimento:

`Executar dentro do ambiente xgap:`
`gap> g:=Image(EpimorphismPGroup(g,3));`(transformar um grupo finitamente apresentado em policíclico)
`gap> s:=GraphicSubgroupLattice(g);`(cria o reticulado do grupo)
`gap> MenuSelected(4,2,17);`(marca os grupos normais de g)

Seja agora $\mathbf{G} = \langle a, b\rangle$ um p-grupo delgado de classe 4 e ordem p^7. Todo grupo 2-gerado com $\mathbf{G}^P \leq \gamma_4(\mathbf{G})$ é um quociente de um grupo F com as mesmas propriedades, e $\gamma_4(F)/\gamma_5(F)$ abeliano elementar de posto 3, como construído no capítulo 1.

Usando a teoria de anéis descrita no capítulo 1, deve haver uma identidade não trivial da forma

$$\alpha X^2 + \beta XY + \gamma Y^2 = 0 \tag{4.1}$$

em A. Isso decorre do fato que $\gamma_4(\mathbf{G}) = cI^2$ e que $\gamma_4(\mathbf{G}) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Assim, como cX^2, cXY e $cY^2 \in \gamma_4(\mathbf{G})$ e como vimos acima $\gamma_4(\mathbf{G})$ tem posto 2, existem α, β e γ tais que $\alpha X^2 + \beta XY + \gamma Y^2 = 0$. Mudando os geradores de $\mathbf{G}$ de modo que a mudança de base sobre $\mathbf{G}/\mathbf{G}'$ é dada por um elemento de $SL(2,p)$, o lado esquerdo de (4.1) é transformado correspondentemente como uma forma quadrática em X, Y. Conseqüentemente, se a forma tem um vetor isotrópico, podemos escolher geradores de modo que em (4.1) temos que $XY = 0$. Mas assim $\langle X, X^2\rangle$ e $I^2 = \langle X^2, Y^2\rangle$ são dois submódulos distintos de ordem igual a $|\gamma_4(\mathbf{G})|$, e portanto $\mathbf{G}$ não é delgado.

Portanto, podemos admitir que a forma quadrática é anisotrópica. Logo, pode ser colocada na forma $X^2 - kY^2$, onde k não é um quadrado módulo p. Portanto, $cX^2 = ckY^2$ e assim, $[a, b, a, a] = [a, b, b, b]^k$.

Agora, se $\mathbf{G} = \langle a, b \rangle$ é um grupo metabeliano e no anel associado A, vale a relação

$$X^2 - kY^2 \in I^3, \tag{4.2}$$

onde k não é um quadrado módulo p, então $\mathbf{G}$ é delgado. De fato, seja c a classe de $\mathbf{G}$, de modo que $I^{c-1} = 0$. Então claramente $I^{c-2} = \langle XY^{c-3},\ Y^{c-2} \rangle \neq 0$ é de posto no máximo 2, pois, todas as potências pares de X pode ser reescritas em termos de Y de acordo com (4.2). Nós mostraremos que qualquer A-submódulo N de $\mathbf{G}'$ ou contém, ou está contido em I^{c-2}. Indução sobre c dará que $\mathbf{G}$ é delgado.

Portanto assuma que o submódulo N não está contido em I^{c-2}, de modo que em N existe um elemento congruente a $\alpha XY^{i-3} + \beta Y^{i-2}$ módulo I^{i-1} para algum $i < c$, onde α, β não são ambos zero. Multiplicando por XY^{c-i-1} e Y^{c-i}, temos que N contém

$$\alpha X^2 Y^{c-4} + \beta XY^{c-3} = \beta XY^{c-3} + k\alpha Y^{c-2} \quad \text{e} \quad \alpha XY^{c-3} + \beta Y^{c-2}.$$

Agora $\beta^2 - k\alpha^2$ desaparece somente para $\alpha = \beta = 0$, pois k não é um quadrado módulo p, de forma que estes dois elementos geram I^{c-2}, como queríamos. ∎

Referências Bibliográficas

[1] N. Blackburn, *On a Special Class of p-Groups*, Acta Math. 100(1958), 45-92.

[2] R. Brandl, A. Caranti e C. M. Scoppola, *Metabelian Thin p-Groups*, Quart. J. Oxford (2), 43 (1992), 157-173.

[3] R. Brandl, *The Dilworth number of subgroupos lattices*, Arch. Math., vol 50, 502-510 (1988).

[4] G. A. Fernández-Alcober, *An Introduction to Finite p-groups: Regular p-groups and Groups of Maximal Class*, XVI Escola de Algebra, Brasília, July 2000.

[5] The GAP Group, GAP - *Groups, Algorithms, and Programming*, Version 4.4; 2006. (http://www.gap-system.org)

[6] M. Hall Jr., *The Theory of Groups*, 2th edn., Macmillan, New York (1976).

[7] B. Huppert, *Endliche Gruppen I*, Springer, Berlin Heidelberg New York (1967).

[8] N. Jacobson, *Lectures in Abstract Algebra: I. Basic Concepts*, Springer, New York (1951).

[9] F. Levin, *On Some Varieties of Soluble Groups II*, Math. Zeitschr. 103, 103-162 (1968).

[10] A. Mann, *Regular p-groups and groups of maximal class*, J. Algebra 42 (1976), 136-141.

[11] A. Mann, *Groups with small abelian subgroups*, Arch. Math 50 (1988), 210-213.

[12] H. Meier-Wunderli, *Metabelsche Gruppen*, Comment, Math. Helv. 25(1951).1-10.

[13] J.S. Robinson, *A course in the Theory of Groups*, 2th edn., Springer (1995).

[14] N. R. Rocco, *Métodos de Lie em Teoria dos Grupos*, Atas da IX Escola de Algebra (segundo volume), Brasília, Coleção Atas nº 17 (1986).

[15] J.J. Rotman, *An Introdutction to the Theory of Groups*, 4th edn., Speinger-Verlag, New York (1995).

[16] R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter, Berlin (1994).

[17] G. Szekeres, *Metabelian Groups with Two Generators*, Proc. Internat. Conf. Theory of Groups, Austral. Nat. Univ. Canberra, August 1965, 323-346 (1967).

[18] H. Zassenhaus, *The Theory of Groups*, 2º ed, Chelsea, New York, 1958.