UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO EM MATEMÁTICA

Francisco Carpegiani Medeiros Borges

SOBRE COBERTURAS MINIMAIS DE GRUPOS FINITOS POR SUBGRUPOS PRÓPRIOS

Fortaleza
2007

Francisco Carpegiani Medeiros Borges

SOBRE COBERTURAS MINIMAIS DE GRUPOS FINITOS POR SUBGRUPOS PRÓPRIOS

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática, da Universidade Federal do Ceará, para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. José Robério Rogério.

Fortaleza

2007

.

Aos meus queridos pais, Chagas e Rosa.

Agradecimentos

Agradeço, em primeiro lugar, a Deus.

Aos meus pais, Rosa e Chagas, pelo apoio incondicional, pelo amor e pela educação.

À minha irmã, Cleigiane, pelo incentivo e pelo amor.

Ao professor Abdênago Alves de Barros, pela oportunidade, apoio e orientação.

Ao professor Gervasio Gurgel Bastos, pela orientação na monografia de graduação, pelo apoio e incentivo.

Ao professor José Robério Rogério, pela orientação no mestrado, pela paciência, pelo apoio e pelo exemplo de humildade.

Ao professor Afonso(garoto), pelos valiosos ensinamentos e apoio.

Ao professor Luquésio, pelos ensinamentos e incentivo.

À amiga Andrea, pela eficiência, pela ajuda e amizade.

A todos os meus amigos, em especial, Darlan(manin), Jânio Kléo, Jobson(jobim), Ivy e Darlan, Gleydson, Jorge(deruba), Tony, Cristiane(cris), Laires(e lá?), Felipe(baiano), Ana Rocilda, Ronaldo(ronaldin) e Erlane, pela amizade dada e pelos vários momentos legais de curtição.

À CAPES, pelo apoio finaceiro.

.

“Uma cerveja antes do almoço é muito bom pra ficar pensando melhor”.
(Trecho de Praieira, Chico Science & Nação Zumbi)

.

Resumo

Estuda-se a quantidade mínima $\sigma(G)$ de subgrupos próprios de um grupo finito, não-cíclico G que cobre G. Calcula-se $\sigma(G)$ para grupos nilpotentes, solúveis e supersolúveis. Caracteriza-se grupos com $\sigma(G) = 3$, $\sigma(G) = 4$, $\sigma(G) = 5$. Caracteriza-se os grupos 6-primitivos e os grupos supersolúveis $(p + 1)$-primitivos, onde p é um número primo.

Sumário

Capítulo 1

Introdução

Quando podemos escrever um grupo como união de n subgrupos ?

Aparentemente este problema é simples. Os primeiros trabalhos relacionados a esse problema foram publicados por D. Greco, matemático italiano, na década de 50. D. Greco conseguiu caracterizar os grupos que podem ser cobertos por 2,3, 4 ou 5 subgrupos. Em 1954, B. H. Neumann foi mais adiante, estudou cobertura de grupos por classes laterais e por subconjuntos permutáveis. Daí por diante, vários trabalhos foram publicados relacionados a tal problema. Começou-se a estudar o problema de cobertura de grupos por subgrupos específicos, por exemplo, por subgrupos normais (M. A, Bradie, R. F. Chamberlain e L. C. Kappe), por subgrupos próprios (J. H. E. Cohn), etc.

Em 1994, J. H. E. Cohn estudou, em seu artigo [2], a quantidade mínima de subgrupos próprios que cobrem um grupo finito. Ele definiu $\sigma(G)$ como sendo o menor inteiro n para o qual G é união de n subgrupos próprios, e que G nestas condições, é um grupo n-soma. Conseqüentemente, todas as coberturas consideradas por Cohn são irredundantes, ou seja,

$$G = H_1 \cup H_2 \cup \ldots \cup H_n\,, \text{ onde } H_i \nsubseteq \bigcup_{j \neq i} H_j\,, \forall\, i.$$

Ele também define que G é um grupo n-primitivo, se $\sigma(G) = n$ e não existe nenhum subgrupo normal N, não-trivial, de G satisfazendo $\sigma(G) = \sigma\left(\frac{G}{N}\right)$. Com essas definições, Cohn calcula $\sigma(G)$ de diversos grupos; por exemplo, grupos nilpotentes, solúveis, supersolúveis, etc. Além disso, caracteriza os grupos n-soma, com $n \leq 5$. Neste artigo, Cohn conjectura que $\sigma(G)$,

onde G é um grupo solúvel, finito e não-nilpotente, é igual a $c+1$, onde c é a ordem do menor fator principal de G que possui mais que um complemento em G.

Em 1997, M. J. Tomkinson prova, em [8], a conjectura feita por Cohn. Esta dissertação de mestrado é baseada nestes dois artigos.

Falemos agora sobre a estrutura do texto, o que é feito em cada um dos capítulos que compõem este trabalho.

No capítulo 1, intoduzimos todos os pré-requesitos necessários para uma leitura inteligível do leitor. Definimos todos os subgrupos clássicos que aparecem no trabalho, também introduzimos resultados clássicos (Teorema de Lagrange, Teorema de Sylow, Teorema dos Isomorfismos, etc) que serão utilizados nos capítulos subseqüentes. Além disso, estabelecemos resultados sobre subgrupos comutadores, subgrupo Frattini e, finalizando o capítulo, falamos de séries derivado, central inferior e central superior; que serão importantes no apêndice sobre grupos solúveis e grupos nilpotentes.

O capítulo 2 é dedicado ao artigo de J. H. E. Cohn. No início do capítulo, definimos grupo n-soma e grupo n-primitivo, calculamos $\sigma(G)$ de um p-grupo não-cíclico:

Teorema A *Se G é um p-grupo não-cíclico, então $\sigma(G) = p+1$. Ademais, $C_p \times C_p$ é o único grupo $(p+1)$-primitivo,*

e calculamos $\sigma(G)$ de grupos nilpotentes (não-cíclicos):

Teorema B *Se G é um grupo nilpotente, não-cíclico. Então $\sigma(G) = p+1$, onde p é o menor primo para o qual $P \in Syl_p(G)$ é não-cíclico. Além disso, $C_p \times C_p$ é o único grupo $(p+1)$-primitivo nilpotente.*

Na seção 2.1, caracterizamos os grupos n-soma, com $n \leq 5$:

Teorema C *Seja G um grupo finito.*

(*i*) *G é um grupo 3-soma se, e somente se, possui pelo menos dois subgrupos de índice 2. Além disso, $C_2 \times C_2$ é o único grupo 3-primitivo;*

(*ii*) *G é um grupo 4-soma se, e somente se, $\sigma(G) \neq 3$ e possui pelo menos dois subgrupos de índice 3. Ademais, $C_3 \times C_3$ e S_3 são os únicos grupos 4-primitivos;*

(*iii*) *G é um grupo 5-soma se, e somente se, $\sigma(G) \neq 3$ ou 4 e G possui um subgrupo maximal de índice 4. Além disso, A_4 é o único grupo 5-primitivo.*

Na seção 2.2, mostramos que $\sigma(A_5) = 10$ e que $\sigma(S_5) = 16$, cuja a prova é trabalhosa e longa. Na seção 2.3, caracterizamos os grupos 6-primitivos:

Teorema D *$D_5, W = \langle a, b \,|\, a^5 = 1 = b^4\,,\, ba = a^2b\rangle$ e $C_5 \times C_5$ são os únicos grupos 6-primitivos.*

Na seção 2.4, calculamos $\sigma(G)$ para grupos supersolúveis e caracterizamos os grupos $(p+1)$-primitivos, supersolúveis:

Teorema E *Seja G um grupo $(p+1)$-primitivo supersolúvel. Então $G \simeq C_p \times C_p$ ou $G \simeq S$, onde $S = \{a^i b^j \,|\, a^p = 1 = b^N\,,\, bab^{-1} = a^r\}$ com $N \mid (p-1)$ e N é o menor inteiro positivo satisfazendo a congruência $r^n \equiv 1\,(mod\, p)$.*

A última seção 2.5 é dedicada ao resultado principal de [8], a demonstração de Tomkinson da conjectura feita por Cohn:

Teorema F *Se G é um grupo solúvel, finito e não-nilpotente. Se $\frac{H}{K}$ é o menor fator principal de G que possui mais que um complemento em G, então $\sigma(G) = \left|\frac{H}{K}\right| + 1$.*

Antes, introduzimos alguns resultados que são utilizados na demonstração, dentre estes, destacamos a definição de um grupo primitivo, quando existe um subgrupo maximal do grupo com núcleo normal trivial, e o Teorema de Gaschütz (veja [4]), que é fundamental na demonstração feita por Tomkinson, que diz:

Teorema G *Seja G um grupo solúvel finito e primitivo. Então, todo fator principal de G, distinto de N, tem ordem menor que $|N|$, onde N é o único subgrupo normal minimal de G.*

O apêndice é dedicado aos grupos nilpotentes, solúveis e supersolúveis, estes que são grupos estruturais da teoria dos grupos, nele fazemos todos os resultados envolvendo tais grupos que são utilizados no capítulo 2.

Capítulo 2

Preliminares

Esta é uma seção especial para consolidarmos a notação a ser usada no texto. Vejamos as definições:

- Se $x \in G$ definimos a ordem de x, indicada por $o(x)$ como sendo o menor natural tal que $x^{o(x)} = 1$ (caso não exista tal natural, diremos que x tem ordem infinita).

- Se $x, g \in G$ o conjugado de x por g será $x^g = g^{-1}xg$.

- se $x \in G$, a classe de conjugação de x é o subconjunto:

$$x^G = \{x^g \ \ ; \ \ g \in G\}.$$

- Se $N \leq G$, um subgrupo conjugado a N é dado por:

$$N^x = x^{-1}Nx = \{x^{-1}nx \ \ ; \ \ n \in N\}$$

  Caso $N^x = N, \ \ \forall x \in G$ diremos que N é normal em G e denotaremos $N \trianglelefteq G$. Observe que se $N^x \subseteq N$, para todo $x \in G$, então $N^x = N$, para todo $x \in G$.

- Se $x \in G$, o centralizador de x em G é o subgrupo formado pelos elementos em G que comutam com x, indicado por:

$$C_G(x) = \{g \in G; \ \ x^g = x\}$$

- Se $H \subseteq G$, o centralizador de H em G é o subgrupo:

$$C_G(H) = \{g \in G; \quad h^g = h, \quad \forall h \in H\} = \bigcap_{h \in H} C_G(h)$$

- O centro do grupo G é o subgrupo formado pelos elementos de G que comutam com todos os outros:

$$Z(G) = C_G(G) \trianglelefteq G.$$

- Se $H \leq G$, definimos o normalizador de H em G como sendo o subgrupo $N_G(H) = \{g \in G; \quad H^g = H\}$. Note que $H \trianglelefteq N_G(H) \leq G$.

- Se $x, y \in G$, definimos o *comutador* de x e y como sendo:

$$[x, y] = x^{-1}y^{-1}xy$$

  Observe que x e y comutam se e somente se seu comutador é 1.

- Definimos o derivado G' como sendo o subgrupo gerado por todos os comutadores de G:

$$G' = \langle [x, y]; \quad x, y \in G \rangle$$

  Lembrando que se $X \subset G$, o subgrupo gerado por X será $\langle X \rangle = \{x_1^{e_1}x_2^{e_2}...x_n^{e_n}; \quad x_i \in X, \quad e_i = \pm 1\}$. Observe ainda que $G' \trianglelefteq G$.

- Se $H, K \subset G$ defnimos $[H, K] = \langle [h, k]; \quad h \in H, \quad k \in K \rangle$. Note que $G' = [G, G]$.

- Um subgrupo H de G é *maximal* em G, se não existe nenhum subgrupo próprio de G que o contenha propriamente.

- Um subgrupo N de G é dito *normal minimal* de G, se $1 \neq N \trianglelefteq G$ e N não contém nenhum subgrupo normal, não-trivial, de G

- Um subgrupo H de G é *característico*, e denotamos $H \overset{\text{car}}{\trianglelefteq} G$, se $\varphi(H) = H$ para todo $\varphi \in \operatorname{Aut} G$.

- O Subgrupo *Frattini* de G é definido como sendo a interseção de todos os subgrupos maximais de G:

$$\Phi(G) = \bigcap_{\substack{M \leq G \\ M maximal}} M.$$

Se G não possui subgrupos maximais, então $\Phi(G) = G$.

Se $N \trianglelefteq G$, o conjunto das classes de N à direita (ou à esquerda) é um grupo com a operação $Nx \cdot Ny = Nxy$. Tal grupo é chamado grupo quociente de G por N e denotado por $\frac{G}{N}$. A cardinalidade das classes laterais de N à (ou à esquerda) chama-se o *índice de H em G* e é denotado por $|G : H|$. A proposição seguinte caracteriza os grupos quocientes abelianos.

Proposição 2.1 *Se $N \trianglelefteq G$, então $\frac{G}{N}$ é abeliano $\iff G' \leq N$.*

Prova: ($\Leftarrow$) Se $G' \leq N$, dados $a, b, \in G$ temos que $a^{-1}b^{-1}ab \in N$ e daí:

$$\begin{aligned} N = N(a^{-1}b^{-1}ab) &= (Na^{-1})(Nb^{-1})(Na)(Nb) \\ &= (Na)^{-1}(Nb)^{-1}(Na)(Nb) \\ \Rightarrow (Nb)(Na) = (Na)(Nb) &\Rightarrow \frac{G}{N} \text{ abeliano} \end{aligned}$$

($\Rightarrow$) Reciprocamente, se $\frac{G}{N}$ é abeliano:

$$\begin{aligned} & (Na)(Nb) = (Nb)(Na), \quad \forall a, b \in G \\ \Rightarrow \quad & (Na)(Nb)(Na)^{-1}(Nb)^{-1} = N \\ \Rightarrow \quad & N(aba^{-1}b^{-1}) = N.1 \Rightarrow aba^{-1}b^{-1} \in N, \quad \forall a, b \in G \\ \Rightarrow \quad & G' \leq N. \blacklozenge \end{aligned}$$

Teorema 2.1 (Lagrange) *Se $H \leq G$, temos*

$$|G| = |G : H|.|H|.$$

Prova: Veja [5]

Proposição 2.2 :

(i) $|G : K| = |G : H|.|G : K|$, *onde* $K \leq H \leq G$;

(ii) $|HK|.|H \cap K| = |H|.|K|$, *onde* $H, K, \leq G$;

(iii) $|G : H \cap K| \leq |G : H|.|G : K|$. *Em particular, se* $mdc\,(|G : K|, |G : H|) = 1$, *então* $|G : H \cap K| = |G : H|.|G : K|$;

(iv) se G *é um grupo finito,* $H, K \leq G$ *e* $mdc\,(|G : H|, |G : K|) = 1$, *então* $G = HK$.

Teorema 2.2 (Homomorfismos) *Sejam* G, G_1 *dois grupos,* $\varphi : G \to G_1$ *um homomorfismo e* π *a projeção canônica de* G *sobre* $\frac{G}{N}$. *Então, existe um único isomorfismo* $\bar{\varphi}$ *de* $\frac{G}{N}$ *sobre* $Im\,(\varphi)$ *tal que* $\varphi = \bar{\varphi} \circ \pi$. *Em particular,* $\frac{G}{N} \simeq Im\,(\varphi)$.

Prova: Veja [1]

Teorema 2.3 (Isomorfismos) :

(i) Sejam G *um grupo,* $H \leq G$ *e* $N \trianglelefteq G$. *Então*

$$H \cap N \trianglelefteq H \quad e \quad \frac{NH}{N} \simeq \frac{H}{H \cap N}.$$

(ii) Seja H *e* K *subgrupos normais em* G *com* $K \subset H$. *Então*

$$\frac{G/K}{H/K} \simeq \frac{G}{H}.$$

Prova: Veja [5]

Teorema 2.4 (Lei de Dedekind) *Sejam H,K,L subgrupos de G, então*

$$(HK) \cap L = (H \cap L)K, \quad se \quad K \leq L.$$

Prova: Seja $x \in (HK) \cap L$, então $x = hk$ com $h \in H, k \in K$ e $x = hk \in L$. Donde, obtemos $h = xk^{-1} \in L$ (pois $K \leq L$). Logo, $h \in H \cap L \Rightarrow x = hk \in (H \cap L)K$. Portanto, $(HK) \cap L \subseteq (H \cap L)K$.

Seja $y \in (H \cap L)K$, então $y = hk$ com $h \in H \cap L, k \in K$, o que implica $y \in HK$. Como $K \leq L$, temos $y \in L$. Assim, $(H \cap L)K \subseteq (HK) \cap L$. Portanto, temos a igualdade. ♦

A proposição, a seguir, define e caracteriza o núcleo normal de um subgrupo.

Proposição 2.3 *Se $H \leq G$ definimos:*

$$H_G = \langle X, \quad X \trianglelefteq G, \quad X \leq H \rangle \quad (\textit{núcleo normal}).$$

Então, $H_G = \bigcap_{g \in G} H^g$.

Prova: Vamos ver inicialmente que H_G é normal em G. Se $x \in H_G$, temos $x = y_1 y_2 ... y_n$ com $y_i \in Y_i \trianglelefteq G$ e $Y_i \leq H$. Daí, para qualquer $g \in G$:

$$\begin{aligned} g^{-1}xg = g^{-1}(y_1y_2...y_n)g &= (g^{-1}y_1g)(g^{-1}y_2g)...(g^{-1}y_ng) \\ &= y_1'y_2'...y_n' \in H_G \end{aligned}$$

pois cada $y_i' \in Y_i$ já que $Y_i \trianglelefteq G$. Logo $g^{-1}H_Gg \subset H_G \Rightarrow H_G$ é normal.
Seja $X = \bigcap_{g \in G} H^g$. Daí, como H_G é normal em G temos:

$$gH_Gg^{-1} = H_G \subset H \Rightarrow H_G \subset g^{-1}Hg = H^g$$

$$\Rightarrow H_G \subset \bigcap_{g \in G} H^g = X.$$

Por outro lado, veja que $X = \bigcap_{g \in G} H^g$ é normal em G, pois se $x \in X$ e $g, g_1 \in G$ podemos usar que $x \in H^{gg_1^{-1}}$ para concluir que:

$$g_1^{-1}xg_1 = g_1^{-1}(g_1g^{-1}hgg_1^{-1})g_1 = g^{-1}hg \Rightarrow x^{g_1} \in H^g, \quad \forall g \in G$$

Logo $x^{g_1} \in X \Rightarrow X^{g_1} \subset X \Rightarrow X$ é normal em G.
Por outro lado, $X \subset H^1 = H$ o que implica $X \subset H_G$, e portanto, $X = H_G$. ♦

Enunciaremos o Teorema de Sylow e algumas conseqüências, que serão muito utilizados neste trabalho.

Teorema 2.5 (Sylow) *Seja $|G| = p^n m$, onde $p \nmid m$. Então:*

(i) $Syl_p(G) = \{S \leq G\,;\, |S| = p^n\} \neq \varnothing$ *e* $n_p = |Syl_p(G)| \equiv 1 \,(mod\, p)$;

(ii) Se $|H| = p^r$, *com* $H \leq G$, *então* $H \leq S$ *para algum* $S \in Syl_p(G)$;

(iii) Os p-subgrupos de Sylow são conjugados. Em particular, $n_p = |G : N_G(P)|$ *e* n_p *divide* $|G : P|$.

Prova: Veja [6].

Corolário 2.1 :

(i) **(Argumento Frattini)** *Se* $N \trianglelefteq G$ *e* $P \in Syl_p(N)$*, então* $G = N.N_G(P)$*.*

(ii) Sejam $N \trianglelefteq G$ *e* $P \in Syl_p(G)$*, então:*

$$\frac{NP}{N} \in Syl_p\left(\frac{G}{N}\right) \quad e \quad P \cap N \in Syl_p(N).$$

A seguir, faremos alguns resultados básicos sobre subgrupos característicos.

Proposição 2.4 *Sejam* G *um grupo e* $H \leq G$*. Então:*

(i) $H \overset{\triangleleft}{_{car}} G \Rightarrow H \trianglelefteq G$*;*

(ii) $H \overset{\triangleleft}{_{car}} K \trianglelefteq G \Rightarrow H \trianglelefteq G$*;*

(iii) $H \overset{\triangleleft}{_{car}} K \overset{\triangleleft}{_{car}} G \Rightarrow H \overset{\triangleleft}{_{car}} G$*;*

(iv) se H *é o único subgrupo com ordem dada, então* $H \overset{\triangleleft}{_{car}} G$*;*

(v) se $P \in Syl_p(G)$ *e* $P \trianglelefteq G$*, então* $P \overset{\triangleleft}{_{car}} G$*;*

Prova: (i) Temos que $\varphi(H) = H$ para todo $\varphi \in \operatorname{Aut} G$. Em particular, considere $\varphi_g(x) = g^{-1}xg$. Daí, $g^{-1}Hg = H$ para todo $g \in G$, ou seja, $H \trianglelefteq G$.

(ii) Devemos mostrar que $g^{-1}Hg = H$ para todo $g \in G$. Com efeito, considere φ_g como no item (i). Como $K \trianglelefteq G$, segue que $\varphi_g|_K \in \operatorname{Aut} K$. Isto implica, juntamente com o fato de H ser característico em K, que $\varphi_g(H) = \varphi_g|_K(H) = H$, isto é, $g^{-1}Hg = H$ para todo $g \in G$.

(iii) Seja $\varphi \in \operatorname{Aut} G$. Como $K \overset{\triangleleft}{_{\text{car}}} G$, pelo item (i), temos que $K \trianglelefteq G$. Desse modo concluímos que $\varphi|K \in \operatorname{Aut} K$. Daí: $\varphi(H) = \varphi|_K(H) = H$ para todo $\varphi \in \operatorname{Aut} G$. Portanto, H é característico em G.

(iv) Seja $\varphi \in \operatorname{Aut} G$. Sabemos que $|\varphi(H)| = |H|$. Por hipótese, concluímos que $\varphi(H) = H$. Donde, $H \overset{\triangleleft}{_{\text{car}}} G$.

(v) Seja $P \in Syl_p(G)$ tal que $P \trianglelefteq G$. Logo, pelo Teorema de Sylow, P é o único p-subgrupo de Sylow. Do item (iv), concluímos que $P \overset{\triangleleft}{_{\text{car}}} G$. ♦

Agora, faremos alguns resultados básicos do subgrupo Frattini $\Phi(G)$.

Seja G um grupo qualquer. Dizemos que $g \in G$ é um elemento não-gerador(ou supérfluo), se $G = \langle X, g\rangle$ implicar que $G = \langle X\rangle$, onde X é um subcojunto de G.

Proposição 2.5 :

(i) $\Phi(G) = \{g \in G\,;\ g$ *é não-gerador*$\}$*;*

(ii) $\Phi(G) \overset{\lhd}{_{car}} G$*.*

Prova: (i) Suponha g não-gerador. Se $g \notin \Phi(G)$, então existiria um subgrupo maximal M tal que $g \notin M$. Então, $G = \langle M, g\rangle$ o que implica $G = M$, contradizendo o fato de M ser maximal. Agora, suponha que $g \in \Phi(G)$ e X é um subconjunto de G tal que $G = \langle X, g\rangle$. Suponha, por absurdo, que $G \neq \langle X\rangle$. Pelo Lema de Zorn, existe M maximal entre os subgrupos H de G satisfazendo: $\langle X\rangle \leq H$ e $g \notin H$. Afirmamos que M é um subgrupo maximal de G. De fato, seja $H \leq G$ tal que $M < H \leq G$. Como $\langle X\rangle \leq H$, pela maximalidade de M, devemos ter $g \in H$. Daí, $\langle X, g\rangle \leq H$ o que implica $H = G$, e portanto, segue a afirmação. Donde, concluímos que $g \in M$, o que é absurdo!

(ii) Sejam $\varphi \in \operatorname{Aut} G$ e M um subgrupo maximal de G. Afirmamos que $\varphi(M)$ é um subrupo maximal de G. De fato, considere $H \leq G$ tal que $\varphi(M) \leq H \leq G$. Daí, $\varphi^{-1}(\varphi(M)) \leq \varphi^{-1}(H) \leq \varphi(G)$ o que implica $M \leq \varphi^{-1}(H) \leq G$. Logo, $M = \varphi^{-1}(H)$ ou $\varphi^{-1}(H) = G$, isto é, $\varphi(M) = H$ ou $H = G$, o que prova a afirmação. Isto implica que $\{M\,;\ M \text{ maximal}\} = \{\varphi(M)\,;\ M \text{ maximal}\}$. Portanto,

$$\varphi(\Phi(G)) = \varphi\left(\bigcap_{\substack{M\leq G\\ M maximal}} M\right) = \bigcap_{\substack{M\leq G\\ M maximal}} \varphi(M) = \bigcap_{\substack{M\leq G\\ M maximal}} M = \Phi(G).$$

Como $\varphi \in \operatorname{Aut} G$ é arbitrário, concluímos que $\Phi(G) \overset{\lhd}{_{\text{car}}} G$. Em particular, da Proposição 2.4, segue que $\boxed{\Phi(G) \trianglelefteq G}$. ♦

No que segue, faremos algumas propriedades sobre comutadores e subgrupos comutadores, que serão importantes para grupos solúvies, grupos nilpotentes,séries centrais inferior e superior, e série derivada.

Lema 2.1 :

(i) $[x,y] = [y,x]^{-1}$;

(ii) $[xy,z] = [x,y]^z[y,z]$ *e* $[x,yz] = [x,z][x,y]^z$;

(iii) $[x,y^{-1}] = ([x,y]^{y^{-1}})^{-1}$ *e* $[x^{-1},y] = ([x,y]^{x^{-1}})^{-1}$;

(iv) $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$ **(Identidade de Hall-Witt)**.

A prova do Lema é imediata.

Proposição 2.6 (Lema dos três subgrupos) *Sejam H,K e L subgrupos de G. Se dois dos subgrupos* $[H,K,L],[K,L,H],[L,H,K]$ *estão contidos em um subgrupo normal de G, então o terceiro também estará.*

Prova: Seja $N \trianglelefteq G$. Suponhamos que $[H,K,L] \subseteq N$ e $[K,H,L] \subseteq N$. Do Lema 2.1, item (iv), temos $[h,k,l]^{k^{-1}}[k,l,h]^{l^{-1}}[l,h,k]^{h^{-1}} = 1$. Daí,

$$[l,h,k]^{h^{-1}} = ([k,l,h]^{l^{-1}})^{-1}([h,k,l]^{k^{-1}})^{-1} \in N \Rightarrow [l,h,k] \in N^h = N.$$

Logo, $[L,H,K] \subseteq N$. ♦

Sejam $H \leq G$ e $K \leq G$, definimos o subgrupo H^K por:

$$H^K = \langle h^k \mid h \in H\ ,\ k \in K \rangle.$$

De modo geral, se X é um subconjunto de G e $K \leq G$, então $[X,K]^K = [X,K]$. Basta usar o Lema 2.1, item (ii). Em particular, vemos que $\boxed{[N,G] \trianglelefteq G}$. Além disso, se $N \trianglelefteq G$, então $\boxed{[N,G] \subseteq N}$.

Proposição 2.7 :

(i) $\left[\frac{H}{N},\frac{K}{N}\right] = \frac{[H,K]N}{N}$;

(ii) se $H \trianglelefteq G$ *e* $K \trianglelefteq G$, *então* $[HK,G] = [H,G][K,G]$;

(iii) $[H,G] \leq K$ *se, e somente se,* $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$;

(iv) $[H_1 \times K_1, H_2 \times K_2] = [H_1,K_1] \times [H_2,K_2]$.

Prova: A prova segue das definições.

Uma série de G, é uma coleção de subgrupos H_i de G tal que $H_i \subseteq H_{i+1}$ para todo i, ou $H_{i+1} \subseteq H_i$ para todo i. Dizemos que uma série de G é *normal*, se todos os subgrupos da série são normais em G. Em particular, se todos os grupos quocientes satisfazem $\frac{H_{i+1}}{H_i} \leq Z\left(\frac{G}{H_i}\right)$, dizemos que a série é *central*.

Série Derivado de G

Definamos o subgrupo $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$, onde $G^{(0)} = G$ e $G^{(1)} = G'$. Note que:

- $G^{(i)} \overset{\text{car}}{\lhd} G$;

  Provemos por indução sobre i. Se $i = 0$, claramente $G \overset{\text{car}}{\lhd} G$. Se $i = 1$, temos $G' = [G, G]$. Seja $\varphi \in \operatorname{Aut} G$. Daí, $\varphi(G') = \varphi([G, G]) = [\varphi(G), \varphi(G)] = [G, G] = G'$, logo $G' \overset{\text{car}}{\lhd} G$. Suponhamos, por indução, que $G^{(i)} \overset{\text{car}}{\lhd} G$. Veja que $G^{(i+1)} = (G^{(i)})' \overset{\text{car}}{\lhd} G^{(i)}$. Donde, temos $G^{(i+1)} \overset{\text{car}}{\lhd} G^{(i)} \overset{\text{car}}{\lhd} G$. Da Proposição 2.4, item (iii), concluímos que $G^{(i+1)} \overset{\text{car}}{\lhd} G$.

  Portanto, $\boxed{G^{(i)} \trianglelefteq G}$.

- $\frac{G^{(i)}}{G^{(i+1)}}$ é abeliano.

$$\left[\frac{G^{(i)}}{G^{(i+1)}}, \frac{G^{(i)}}{G^{(i+1)}}\right] = \frac{[G^{(i)}, G^{(i)}]G^{(i+1)}}{G^{(i+1)}} = \frac{G^{(i+1)}G^{(i+1)})}{G^{(i+1)}} = \frac{G^{(i+1)}}{G^{(i+1)}} = 1.$$

Portanto, a série

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(n)} \geq \ldots \tag{2.1}$$

é uma série normal de G tal que todos os grupos quocientes $\frac{G^{(i)}}{G^{(i+1)}}$ são abelianos. Tal série de G é chamada de **Série Derivado** de G.

Série Central Inferior de G

Definamos os subgrupos $\gamma_1(G) = G$ e $\gamma_n(G) = [\gamma_{n-1}(G), G]$, com $n \geq 2$. Temos:

- $\gamma_n(G) \overset{\text{car}}{\lhd} G$.

  Provemos por indução sobre n. Se $n = 1$, é imediato. Agora suponha, por indução, que $\gamma_n(G) \overset{\text{car}}{\lhd} G$. Seja $\theta \in \operatorname{Aut} G$, então:

$$\theta(\gamma_{n+1}(G)) = \theta([\gamma_n(G), G]) = [\theta(\gamma_n(G)), \theta(G)] \leq [\gamma_n(G), G] = \gamma_{n+1}(G).$$

Donde, $\gamma_{n+1}(G) \overset{\lhd}{_{\text{car}}} G$. Em particular, $\boxed{\gamma_n(G) \trianglelefteq G}$. Isto implica que $\gamma_{n+1}(G) = [\gamma_n(G), G] \subseteq \gamma_n(G)$, i.e., $\boxed{\gamma_{n+1}(G) \subseteq \gamma_n(G)}$.

- $\frac{\gamma_n(G)}{\gamma_{n+1}(G)} \leq Z\left(\frac{G}{\gamma_{n+1}(G)}\right)$.

$$\left[\frac{\gamma_n(G)}{\gamma_{n+1}(G)}, \frac{G}{\gamma_{n+1}(G)}\right] = \frac{[\gamma_n(G), G]\gamma_{m+1}(G)}{\gamma_{n+1}(G)} = \frac{\gamma_{n+1}(G)}{\gamma_{n+1}(G)} = 1.$$

Logo, temos o resultado.

Desse modo, a série

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots \geq \gamma_n(G) \geq \ldots \tag{2.2}$$

é uma série central de G e é chamada de **Série Central Inferior** de G.

Série Central Superior de G

Definamos os subgrupos $Z_0(G) = 1, Z_1(G) = Z(G)$ e $Z_n(G)$ como um subgrupo de G tal que $\frac{Z_{n+1}(G)}{Z_n(G)} = Z\left(\frac{G}{Z_n(G)}\right)$. Temos:

- $Z_n(G) \overset{\lhd}{_{\text{car}}} G$.

Provemos por indução sobre n. Se $n = 2$, temos

$$[\varphi(Z_2(G)), G] = \varphi([Z_2(G), G]) = \varphi(Z_1(G)) = Z_1(G) \ , \ \varphi \in \operatorname{Aut} G.$$

Logo, $Z_2(G) \overset{\lhd}{_{\text{car}}} G$. Suponhamos, por indução, que $Z_n(G) \overset{\lhd}{_{\text{car}}} G$. Daí:

$$[\varphi(Z_{n+1}(G)), G] = \varphi([Z_{n+1}(G), G]) = \varphi(Z_n(G)) = Z_n(G),$$

ou seja, $Z_{n+1}(G) \overset{\lhd}{_{\text{car}}} G$. Donde, $\boxed{Z_n(G) \trianglelefteq G}$.

Assim, vemos que a série

$$1 = Z_0(G) \leq Z_1(G) = Z(G) \leq Z_2(G) \leq \ldots \leq Z_n(G) \leq \ldots \tag{2.3}$$

é uma série central de G. Chamamos de **Série Central Superior** de G.

Proposição 2.8 :

(i) Se $[H, G] \leq Z_i(G)$, então $H \leq Z_{i+1}(G)$;

(ii) $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$;

(iii) $\gamma_i(\gamma_j(G)) \leq \gamma_{ij}(G)$;

(iv) $[\gamma_i(G), Z_j(G)] \leq Z_{j-i}(G)$, *se* $j \geq i$;

(v) $Z_i\left(\frac{G}{Z_j(G)}\right) = \frac{Z_{i+j}(G)}{Z_j(G)}$;

(vi) $\gamma_n(A \times B) = \gamma_n(A) \times \gamma_n(B)$.

Prova: (i) Como $[H, G] \leq Z_i(G)$, segue que $\frac{HZ_i(G)}{Z_i(G)} \leq Z\left(\frac{G}{Z_i(G)}\right)$. Donde, $HZ_i(G) \leq Z_i(G)$ implicando que $H \leq Z_{i+1}(G)$.

Provemos por indução sobre i.

(ii) Se $i = 1$, temos $[\gamma_1(G), \gamma_j(G)] = [G, \gamma_j(G)] = \gamma_{j+1}(G)$. Suponha, por indução, que $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$. Daí, $[\gamma_{i+1}(G), \gamma_j(G)] = [[\gamma_i(G), G], \gamma_j(G)] = [\gamma_i(G), G, \gamma_j(G)]$. Pela Proposição 2.6, temos

$$\begin{aligned}
[\gamma_{i+1}(G), \gamma_j(G)] &\leq [G, \gamma_j(G), \gamma_i(G)][\gamma_j(G), \gamma_i(G), G] = \\
&= [\gamma_{j+1}(G), \gamma_i(G)][\gamma_j(G), \gamma_i(G), G] \leq \\
&\leq \gamma_{i+j+1}(G)[\gamma_{i+j}(G), G] = \gamma_{i+j+1}(G).
\end{aligned}$$

Logo, $[\gamma_{i+1}(G), \gamma_j(G)] \leq \gamma_{i+j+1}(G)$.

(iii) Se $i = 1$, temos $\gamma_1(\gamma_j(G)) = \gamma_j(G)$. Agora suponha o resultado válido para i, i.e., $\gamma_i(\gamma_j(G)) \leq \gamma_{ij}(G)$. Daí, da hipótese de indução e do item (ii), obtemos:

$$\gamma_{i+1}(\gamma_j(G)) = [\gamma_i(\gamma_j(G)), \gamma_j(G)] \leq [\gamma_{ij}(G), \gamma_j(G)] \leq \gamma_{(i+1)j}(G).$$

(iv) Para $i = 1$, temos $[\gamma_1(G), Z_j(G)] = [G, Z_j(G)] \leq Z_{j-1}(G)$. Suponha o resultado válido para $i \leq j$, i.e., $[\gamma_i(G), Z_j(G)] \leq Z_{j-i}(G)$. Da Proposição 2.6 e da hipótese de indução, temos

$$\begin{aligned}
[\gamma_{i+1}(G), Z_j(G)] = [\gamma_i(G), G, Z_j(G)] &\leq [G, Z_j(G), \gamma_i(G)][Z_j(G), \gamma_i(G), G] \\
&\leq [Z_{j-1}(G), \gamma_i(G)][Z_{j-i}(G), G] \\
&\leq Z_{j-i-1}(G).Z_{j-i-1}(G) = Z_{j-i-1}(G).
\end{aligned}$$

Donde, $[\gamma_{i+1}(G), Z_j(G)] \leq Z_{j-i-1}(G)$.

(v) Para $i = 1$, temos $Z_1\left(\frac{G}{Z_j(G)}\right) = \frac{Z_{j+1}(G)}{Z_j(G)}$. Suponha, por indução, que $Z_i\left(\frac{G}{Z_j(G)}\right) = \frac{Z_{i+j}(G)}{Z_j(G)}$. Seja $H \leq G$ tal que $Z_{i+1}\left(\frac{G}{Z_j(G)}\right) = \frac{H}{Z_j(G)}$. Mostraremos que $H = Z_{i+j+1}(G)$. Com efeito,

$$\frac{Z_{i+1}\left(\frac{G}{Z_j(G)}\right)}{Z_i\left(\frac{G}{Z_j(G)}\right)} = Z\left(\frac{\frac{G}{Z_j(G)}}{Z_i\left(\frac{G}{Z_j(G)}\right)}\right) = Z\left(\frac{\frac{G}{Z_j(G)}}{\frac{Z_{i+j}(G)}{Z_j(G)}}\right).$$

Porém,

$$\frac{\frac{H}{Z_j(G)}}{\frac{Z_{i+j}(G)}{Z_j(G)}} = Z\left(\frac{\frac{G}{Z_j(G)}}{\frac{Z_{i+j}(G)}{Z_j(G)}}\right) \iff \left[\frac{H}{Z_j(G)}, \frac{G}{Z_j(G)}\right] \leq \frac{Z_{i+j}(G)}{Z_j(G)}.$$

Como $\left[\frac{H}{Z_j(G)}, \frac{G}{Z_j(G)}\right] = \frac{[H,G]Z_j(G)}{Z_j(G)}$, temos que $\frac{[H,G]Z_j(G)}{Z_j(G)} \leq \frac{Z_{i+j(G)}}{Z_j(G)}$. Donde, segue que $[H, G]Z_j(G) \leq Z_{i+j}(G)$ o que implica $[H, G] \leq Z_{i+j}(G)$. Pelo item (i), vemos que $H \leq Z_{i+j+1}(G)$. Por outro lado,

$$\left[\frac{Z_{i+j+1}(G)}{Z_j(G)}, \frac{G}{Z_j(G)}\right] = \frac{[Z_{i+j+1}(G), G]Z_j(G)}{Z_j(G)} \leq \frac{Z_{i+j}(G)}{Z_j(G)}$$

pois $[Z_{i+j+1}(G), G] \leq Z_{i+j}(G)$. Logo,

$$\frac{\frac{Z_{i+j+1}(G)}{Z_j(G)}}{\frac{Z_{i+j}(G)}{Z_j(G)}} \leq Z\left(\frac{\frac{G}{Z_j(G)}}{\frac{Z_{i+j}(G)}{Z_j(G)}}\right) = \frac{\frac{H}{Z_j(G)}}{\frac{Z_{i+j}(G)}{Z_j(G)}}.$$

Donde concluímos que $\frac{Z_{i+j+1}(G)}{Z_j(G)} \leq \frac{H}{Z_j(G)}$, isto é, $Z_{i+j+1}(G) \leq H$.

Portanto, $H = Z_{i+j+1}(G)$, como queríamos.

(vi) Provemos por indução sobre n.

Se $n = 1$, então $\gamma_1(A \times B) = A \times B = \gamma_1(A) \times \gamma_1(B)$. Agora, suponha, por indução, que $\gamma_n(A \times B) = \gamma_n(A) \times \gamma_n(B)$. Daí,

$$\begin{aligned}
\gamma_{n+1}(A \times B) &= [\gamma_n(A \times B), A \times B] = \\
&\overset{\text{indução}}{=} [\gamma_n(A) \times \gamma_n(B), A \times B] = \\
&= [\gamma_n(A), A] \times [\gamma_n(B), B] = \\
&= \gamma_{n+1}(A) \times \gamma_{n+1}(B).
\end{aligned}$$

Portanto, segue o resultado. ♦

Capítulo 3

Sobre $\sigma(G)$

Nosso objetivo, neste capítulo, será obter propriedades de $\sigma(G)$.

Definição 3.1 *Diremos que G é um grupo n-soma se G é a união de n subgrupos próprios, onde n é o menor inteiro positivo com tal propriedade. Denotaremos este fato por $\sigma(G) = n$.*

Observação 3.1 *$\sigma(G) \geq 3$. De fato, suponha que G seja um grupo 2-soma, ou seja, $G = H \cup K$. Existe $h \in H \backslash K$ e $k \in K \backslash H$. Daí, $hk \in H$ ou $hk \in K$, o que é impossível, pois se $hk \in K$, teríamos $h \in K$ e se $hk \in H$, teríamos $k \in H$. Portanto, não existe nenhum grupo 2-soma, ou seja,* $\boxed{\sigma(G) \geq 3}$.

Exemplo 1 *Considere o grupo dos quatérnios Q_3, dado por:*

$$Q_3 = \langle a, b \,|\, a^4 = 1\,,\, a^2 = b^2\,,\, ba = a^3 b \rangle.$$

Note que $Q_3 = \langle a \rangle \cup \langle b \rangle \cup \langle ab \rangle \cup \langle a^2 b \rangle \cup \langle a^3 b \rangle$. Porém, $\langle b \rangle = \langle a^2 b \rangle$ e $\langle ab \rangle = \langle a^3 b \rangle$. Daí

$$Q_3 = \langle a \rangle \cup \langle b \rangle \cup \langle ab \rangle \quad \therefore \quad \boxed{\sigma(Q_3) = 3}.$$

De modo geral, qualquer grupo cíclico não pode ser escrito como união de subgrupos próprios, pois nenhum subgrupo contendo o gerador pode ser próprio. Contudo, qualquer grupo finito, não-cíclico G é a união de subgrupos próprios cíclicos, isto é,

$$G = \bigcup_{i=1}^{n} \langle a_i \rangle,\ a_i \in G.$$

Neste trabalho, todos os grupos considerados, salvo menção, serão finitos não-cíclicos. Quando G for cíclico, convencionamos que $\sigma(G) = \infty$.

Escreveremos $G = \bigcup_{r=1}^{n} H_r$, para indicar que G é a união de n subgrupos próprios. Suponha que $\sigma(G) = n$, ou seja, $G = H_1 \cup H_2 \cup \ldots \cup H_n$ onde n é o menor inteiro positivo com essa propriedade. Se H_1 não for maximal em G, substitua na cobertura H_1 por M_1, onde M_1 é um subgrupo maximal de G contendo H_1. Como a cobertura é mínima, segue que $H_j \nsubseteq M_1$ para todo $j = 2, 3, \ldots, n$. Prosseguindo, se H_2 não for maximal, substitua H_2 por M_2, onde M_2 é um subgrupo maximal de G contendo H_2. Portanto, podemos tomar os subgrupos da cobertura mínima todos maximais em G, quando conveniente. Denotaremos por $i(H_r) = i_r$ o índice de H_r em G. Podemos arranjar os H_r's de forma que os índices i_r estejam em ordem não-decrescente, ou seja, $i_1 \leq i_2 \leq \ldots \leq i_n$.

Feitas as considerações necessárias, vamos trabalhar!

Teorema 3.1 *Se $G = \bigcup_{r=1}^{n} H_r$ então $|G| \leq \sum_{r=2}^{n} H_r$. A igualdade ocorre se, e somente se, $H_1 H_r = G \; \forall\, r \neq 1$ e $H_r \cap H_s \subset H_1 \; \forall\, r \neq s$.*

Prova: Note que $|H_r| - |H_1 \cap H_r|$ é a quantidade de elementos de H_r que não pertencem a H_1, e que

$$\begin{aligned} |H_r| - |H_1 \cap H_r| &= |H_r| \left(1 - \frac{|H_1 \cap H_r|}{|H_r|}\right) \\ &= |H_r| \left(1 - \frac{|H_1|}{|H_1 H_r|}\right) \\ |H_r| - |H_1 \cap H_r| &\leq |H_r| \left(1 - \frac{|H_1|}{|G|}\right) \end{aligned}$$

Por outro lado,

$$\begin{aligned} |G| &\leq |H_1| + \sum_{r=2}^{n} (|H_r| - |H_1 \cap H_r|) \\ &\leq |H_1| + \sum_{r=2}^{n} |H_r| \left(1 - \frac{|H_1|}{|G|}\right) \\ \Rightarrow \quad |G| &\leq |H_1| + \left(1 - \frac{|H_1|}{|G|}\right) \sum_{r=2}^{n} |H_r| \; . \end{aligned}$$

Daí,

$$1 \leq \frac{|H_1|}{|G|} + \frac{1}{|G|} \sum_{r=2}^{n} |H_r| - \frac{|H_1|}{|G|^2} \sum_{r=2}^{n} |H_r| =$$

$$\begin{aligned} &= \frac{|H_1|}{|G|}\left(1-\frac{1}{|G|}\sum_{r=2}^{n}|H_r|\right)+\frac{1}{|G|}\sum_{r=2}^{n}|H_r| \\ \Rightarrow \quad 0 &\leq \frac{|H_1|}{|G|}\left(1-\frac{1}{|G|}\sum_{r=2}^{n}|H_r|\right)+\frac{1}{|G|}\sum_{r=2}^{n}|H_r|-1= \\ &= \left(1-\frac{1}{|G|}\sum_{r=2}^{n}|H_r|\right)\left(\frac{|H_1|}{|G|}-1\right) \end{aligned}$$

Assim,

$$\begin{aligned} &\left(1-\frac{|H_1|}{|G|}\right)\left(1-\frac{1}{|G|}\sum_{r=2}^{n}|H_r|\right)\leq 0 \\ \Rightarrow \quad &1-\frac{1}{|G|}\sum_{r=2}^{n}|H_r|\leq 0 \\ \therefore \quad &|G|\leq\sum_{r=2}^{n}|H_r|\ . \end{aligned}$$

Para o que resta, devemos provar a

AFIRMAÇÃO: $|G|=\sum_{r=2}^{n}|H_r|$ se, e somente se, $H_1H_r=G$ para todo $r\neq 1$ e $H_r\cap H_s\subset H_1$ para todo $r\neq s$.

De fato, se $|G|=\sum_{r=2}^{n}|H_r|$ podemos escrever:

$$\begin{aligned} |G| &= |G|+|H_1|-\frac{|H_1|}{|G|}|G| \\ \Rightarrow \quad |G| &= |H_1|+\left(1-\frac{|H_1|}{|G|}\right)\sum_{r=2}^{n}|H_r|\ . \end{aligned}$$

Suponha, por absurdo, que $H_1H_k\neq G$ para algum k. Então

$$\begin{aligned} |G| &\leq |H_1|+\sum_{r=2}^{n}\left(1-\frac{|H_1|}{|H_1H_r|}\right)|H_r|= \\ &= |H_1|+\sum_{\substack{r=2\\ r\neq k}}^{n}\left(1-\frac{|H_1|}{|G|}\right)|H_r|+\left(1-\frac{|H_1|}{|H_1H_r|}\right)|H_k|< \\ &< |H_1|+\left(1-\frac{|H_1|}{|G|}\right)\sum_{\substack{r=2\\ r\neq k}}^{n}|H_r|+\left(1-\frac{|H_1|}{|G|}\right)|H_k|=|G| \\ \Rightarrow \quad |G| &< |G| \quad \text{(Absurdo!)} \end{aligned}$$

Assim, $H_1H_r=G\ \forall\, r\neq 1$. Considere $K_i=H_i-H_i\cap H_1$. Como $H_i\cap H_j\subset H_1 \ \Leftrightarrow\ K_i\cap K_j=\varnothing$, basta mostrar que $K_i\cap K_j=\varnothing$. Com efeito, suponha por absurdo, que $K_i\cap K_j\neq\varnothing$.

Daí, como $G = H_1 \cup K_2 \cup \ldots \cup K_n$, segue que

$$\begin{aligned} |G| &< |K_2| + \ldots + |K_n| + |H_1| = \\ &= (|H_2| - |H_2 \cap H_1|) + \ldots + (|H_n| - |H_n \cap H_1|) + |H_1| = \\ &= |G| - \frac{|H_1|}{|G|}(|H_2| + \ldots + |H_n|) + |H_1| \end{aligned}$$

$$\Rightarrow |G| < |G| - \frac{|H_1|}{|G|}|G| + |H_1| = |G| \quad \Rightarrow \quad |G| < |G| \quad \text{(Absurdo!)}.$$

Portanto, $H_i \cap H_j \subset H_1 \ \forall\, r \neq s$.

Reciprocamente, se $H_1 H_r = G$ para todo $r \neq 1$ e $H_i \cap H_j \subset H_1$ para todo $r \neq s$; suponha por absurdo, que $|G| < \sum_{r=2}^{n} |H_r|$. Então

$$\begin{aligned} |G| &= |H_1| + \sum_{r=2}^{n} |K_r| \\ &= |H_1| + \sum_{r=2}^{n} (|H_r| - |H_1 \cap H_r|) \\ &= |H_1| + \sum_{r=2}^{n} |H_r| \left(1 - \frac{|H_1|}{|G|}\right) \\ &> |H_1| + \left(1 - \frac{|H_1|}{|G|}\right)|G| \\ \Rightarrow \quad |G| &> |G| \quad \text{(Absurdo!). } \blacklozenge \end{aligned}$$

Lema 3.1 *Se $\sigma(G) = n$, então $i_2 \leq n - 1$.*

Prova: Considere $G = \bigcup_{r=1}^{n} H_r$, com $i_1 \leq i_2 \leq \ldots \leq i_n$. Pelo Teorema 3.1, tem-se:

$$|G| \leq \sum_{r=2}^{n} |H_r|.$$

Por outro lado, como $i_1 \leq i_2 \leq \ldots \leq i_n$, segue que

$$|G| \leq \sum_{r=2}^{n} |H_r| = \sum_{r=2}^{n} \frac{|G|}{i_r} \leq \sum_{r=2}^{n} \frac{|G|}{i_2} = (n-1)\frac{|G|}{i_2} \quad \Rightarrow \quad i_2 \leq n - 1. \ \blacklozenge$$

Lema 3.2 *Se $N \trianglelefteq G$, então $\sigma(G) \leq \sigma\left(\frac{G}{N}\right)$.*

Prova: Seja $\sigma(G) = n$ e $\sigma\left(\frac{G}{N}\right) = m$. Então

$$\frac{G}{N} = \frac{H_1}{N} \cup \frac{H_2}{N} \cup \ldots \cup \frac{H_m}{N}.$$

Seja $g \in G$, daí $gN \in \frac{H_i}{N}$ para algum i, donde $g \in H_i$ para algum i. Assim, $G = H_1 \cup H_2 \cup \ldots \cup H_m$ e portanto, $n \leq m$. ♦

Desse lema, segue o

Corolário 3.1 $\sigma(H \times K) \leq \min\{\sigma(H), \sigma(K)\}$.

De fato, podemos identificar H com $H \times \{1\}$ e K com $\{1\} \times K$. Então, $H \trianglelefteq H \times K$ e $K \trianglelefteq H \times K$. Logo, pelo Lema 3.1;

$$\begin{aligned} & \sigma(H \times K) \leq \sigma\left(\frac{H \times K}{K}\right) = \sigma(H) \\ e \quad & \sigma(H \times K) \leq \sigma\left(\frac{H \times K}{H}\right) = \sigma(K) \\ \therefore \quad & \sigma(H \times K) \leq \min\{\sigma(H), \sigma(K)\}. \blacklozenge \end{aligned}$$

O Corolário 3.1 mostra que podemos construir, a partir de grupos n-soma, novos grupos n-soma. Isso sugere a seguinte

Definição 3.2 *Um grupo G é dito n-primitivo se, $\sigma(G) = n$ e não existe subgrupo normal N, não-trivial, de G tal que $\sigma\left(\frac{G}{N}\right) = n$.*

Observação 3.2 *Suponha que G é um grupo n-soma primitivo onde todos elementos da cobertura sejam maximais em G e $G = H_1 \cup \ldots \cup H_n$. Considere o subgrupo Frattini $\Phi(G)$. Temos que $\Phi(G) \lhd G$. Pelo Lema* 3.1*, $\sigma(G) \leq \sigma\left(\frac{G}{\Phi(G)}\right)$. Por outro lado,*

$$\frac{G}{\Phi(G)} = \frac{H_1}{\Phi(G)} \cup \frac{H_2}{\Phi(G)} \cup \ldots \cup \frac{H_n}{\Phi(G)}.$$

Daí, $\sigma\left(\frac{G}{\Phi(G)}\right) \leq n$ e portanto, $\sigma(G) = \sigma\left(\frac{G}{\Phi(G)}\right)$. Mas, sendo G um grupo n-primitivo, segue que $|\Phi(G)| = 1$.

No que segue, obteremos alguns resultados que nos permitirão classificar os grupos 3-soma, 4-soma e 5-soma.

3.1 Caracterização dos grupos n-soma, $n \leq 5$

Lema 3.3 *$C_p \times C_p$ é um grupo $(p+1)$-primitivo, onde p é primo.*

Prova: Qualquer subgrupo próprio de $C_p \times C_p$ tem índice p. Logo, pelo Lema 3.1, temos $\sigma(C_p \times C_p) \geq p+1$. Por outro lado,

$$\begin{aligned} C_p \times C_p &= \langle \alpha, \beta \,|\, \alpha^p = \beta^p = 1\,,\ \alpha\beta = \beta\alpha \rangle \\ &= \{\alpha^i\beta^j \mid 0 \leq i \leq p-1 \quad e \quad 0 \leq j \leq p-1\}. \end{aligned}$$

Se considerarmos $H_i = \langle \alpha\beta^i \rangle$ e $H_p = \langle \beta \rangle$, então

$$C_p \times C_p = H_0 \cup H_1 \cup \ldots \cup H_p \quad \Rightarrow \quad \sigma(C_p \times C_p) \leq p+1.$$

$$\therefore \quad \sigma(C_p \times C_p) = p+1.$$

Do fato de $C_p \times C_p$ ser abeliano e todo subgrupo próprio ter índice p, concluímos que $C_p \times C_p$ é $(p+1)$-primitivo. ♦

Teorema 3.2 *Se G é um p-grupo não-cíclico, então $\sigma(G) = p+1$. Além disso, $C_p \times C_p$ é o único grupo $(p+1)$-primitivo.*

Prova: Seja $|G| = p^k$. Como qualquer subgrupo próprio de G tem, no mínimo, índice p, o Lema 3.1 garante que $\sigma(G) \geq p+1$.

Se G é abeliano, pelo Teorema dos Grupos Abelianos Finitamente Gerados, temos

$$G \simeq C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \ldots \times C_{p^{\alpha_n}},$$

onde $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n$ e $\alpha_1 + \alpha_2 + \ldots + \alpha_n = k$. Logo, existe um subgrupo K de G tal que $\frac{G}{K} \simeq C_p \times C_p$. Dos Lemas 3.2 e 3.3 temos

$$\begin{aligned} \sigma(G) &\leq \sigma\left(\frac{G}{K}\right) = \sigma(C_p \times C_p) = p+1 \\ \therefore \quad \sigma(G) &= p+1. \end{aligned}$$

Provaremos por indução sobre k, que $\sigma(G) \leq p+1$.

Se $k = 2$, então $G = C_p \times C_p$ o que implica $\sigma(G) = p+1$. Assuma o resultado válido para qualquer p-grupo com ordem menor ou igual que p^k. Se $k \geq 3$ e G é abeliano, pela primeira parte segue o resultado. Então, considere G não-abeliano. Temos que $\frac{G}{Z(G)}$ é um

p-grupo não-cíclico (se $\frac{G}{Z(G)}$ fosse cíclico, teríamos G abeliano) com ordem menor que $|G|$. Logo, por hipótese de indução, $\sigma\left(\frac{G}{Z(G)}\right) \leq p+1$. Daí,

$$\sigma(G) \leq \sigma\left(\frac{G}{Z(G)}\right) \leq p+1.$$

Donde concluímos que, $\sigma(G) = p+1$.

Se G é $(p+1)$-primitivo então G é abeliano, pois caso contrário, teríamos que $\sigma\left(\frac{G}{Z(G)}\right) = p+1$, contradizendo o fato de G ser $(p+1)$-primitivo (visto que $Z(G)$ tem pelo menos p elementos). Assim, pelo que foi feito anteriormente, G possui um subgrupo K tal que $\frac{G}{K} \simeq C_p \times C_p$. Sendo G $(p+1)$-primitivo, necessariamente K é o subgrupo trivial e portanto, $G \simeq C_p \times C_p$. ♦

Exemplo 2 *Consideremos o grupo Q_n dos quatérnios generalizados, dado por*

$$Q_n = \langle a, b \,|\, a^{2^{n-1}} = 1\,,\, b^2 = a^{2^{n-2}}\,,\, bab^{-1} = a^{2^{n-1}-1} \rangle \quad e \quad |Q_n| = 2^n,\ n \geq 3.$$

Claramente, Q_n é um 2-grupo não-cíclico. Do Teorema 3.2, obtemos que $\boxed{\sigma(Q_n) = 3}$.

Proposição 3.1 *Seja $G = H \times K$, com $mdc(|H|, |K|) = 1$, e $S \leq G$. Então:*

(i) $S = (H \cap S) \times (K \cap S)$;

(ii) se M é maximal em G então: $M = H \times L$ com L maximal em K, ou $M = L \times K$ com L maximal em H.

Prova: Suponha que $G = HK$, com $H \trianglelefteq G, K \trianglelefteq G$ e $H \cap K = 1$. Como $|G : H|$ e $|G : K|$ são relativamente primos, temos também, $|S : H \cap S|$ e $|S : K \cap S|$ relativamente primos. Logo, $S = (H \cap S).(K \cap S)$. Por outro lado, temos $H \cap S \trianglelefteq S$ (pois $H \trianglelefteq G$), $K \cap S \trianglelefteq S$ (pois $K \trianglelefteq G$) e $(H \cap S) \cap (K \cap S) = (H \cap K) \cap S = 1$. Donde, $S = (H \cap S) \times (K \cap S)$.

Seja M um subgrupo maximal de G. Pelo item (i), $M = (H \cap M).(K \cap M)$. Temos duas possibilidades; $H \subseteq M$ ou $H \nsubseteq M$. Se $H \nsubseteq M$, temos $G = HM$. Então

$$HK = G = HM = H[(H \cap M).(K \cap M)] = H.(K \cap M).$$

Logo, $K \cap M = K \Rightarrow K \leq M$, o que implica $M = (H \cap M)K$. Afirmamos que $H \cap M$ é maximal em H. De fato, seja $N \leq H$ tal que $H \cap M \leq N$. Então

$$NK = G \quad ou \quad NK = M, \text{ pois } M \leq NK.$$

- Se $NK = G \Rightarrow H = H \cap NK = N(H \cap K) = N \quad \therefore \quad H = N.$
- Se $NK = M \Rightarrow N = N \cap M \leq H \cap M \quad \therefore \quad N = H \cap M.$

Logo, segue a afirmação. Agora, se $H \subseteq M$ segue que $M = H(K \cap M)$. Para o que resta, devemos mostrar que $K \cap M$ é maximal em K. Com efeito, seja $L \leq K$ tal que $K \cap M \leq L$. Daí

$$HL = G \quad ou \quad HL = M.$$

- Se $HL = G$, temos $K = K \cap G = K \cap HL = L(K \cap M) = L$, i.e., $L = K$.
- Se $HL = M$, temos $L = L \cap M \leq K \cap M$, e portanto, $L = K \cap M$.

Assim, de fato, $K \cap M$ é um subgrupo maximal de K, o que prova a proposição. ♦

Lema 3.4 *Se* $mdc(|H|, |K|) = 1$ *então* $\sigma(H \times K) = \min\{\sigma(H), \sigma(K)\}$.

Prova: Sendo $G = H \times K$ cíclico se, e somente se, H e K são cíclicos, não há nada a provar! Suponha que $\sigma(G) = n$. Pela proposição 3.1, qualquer subgrupo maximal de G é da forma $H \times Y$ com Y maximal em K, ou da forma $X \times K$ com X maximal em H. Então

$$G = \bigcup_{r=1}^{p}(H \times Y_r) \cup \bigcup_{s=1}^{q}(X_s \times K) = G_1 \cup G_2,$$

onde $p + q = n$, $p \geq 0, q \geq 0$.

Mostraremos que $p = 0$ ou $q = 0$. Se $q \neq 0$ então $G_1 \neq G$, ou seja, existe $(h_1, k_1) \notin G_1$. Logo, $(h, k_1) \notin G_1$ para todo $h \in H$, o que implica $(h, k_1) \in G_2$ para todo $h \in H$. Donde, $(h, k) \in G_2$ para todo $h \in H$ e para todo $k \in K$. Daí, $G = G_2$ e portanto, $p = 0$. Dessa forma,

$$G = G_2 = \bigcup_{s=1}^{n}(X_s \times K) = \left(\bigcup_{s=1}^{n} X_s\right) \times K$$

$$\therefore \quad H = \bigcup_{s=1}^{n} X_s \Rightarrow \sigma(H) \leq n.$$

Analogamente, se $q = 0$ então $\sigma(K) \leq n$. Portanto,

$$\min\{\sigma(H), \sigma(K)\} \leq \sigma(G).$$

Do Corolário 3.1, segue a igualdade. ♦

Teorema 3.3 *Se G é um grupo nilpotente não-cíclico, então $\sigma(G) = p+1$ onde p é o menor primo para o qual $S_0 \in Syl_p(G)$ não é cíclico. Além disso, $C_p \times C_p$ é o único grupo nilpotente $(p+1)$-primitivo.*

Prova: Como G é nilpotente finito, G é o produto direto dos seus subgrupos de Sylow. Pelo Teorema 3.2, temos $\sigma(S_0) = p + 1$ e, pelo Lema 3.4;

$$\begin{aligned} \sigma(G) &= \min\{\sigma(S) \mid \text{S subgrupo de Sylow}\} \\ &= \sigma(S_0) = p + 1. \end{aligned}$$

Também do Teorema 3.2, segue que $C_p \times C_p$ é o único nilpotente $(p+1)$-primitivo. ♦

Observação 3.3 *A hipótese do Teorema* 3.3 *é equivalente a dizer que G possui, pelo menos, dois subgrupos maximais de índice p. De fato, se p é o menor primo para o qual $P \in Syl_p(G)$ é não-cíclico, existe pelo menos dois subgrupos maximais de P com índice p, digamos M_1 e M_2. Como G é nilpotente, G é o produto direto de seus subgrupos de Sylow. Seja $P_i \in Syl_{p_i}(G)$, com $p_i \neq p$. Consideremos os subgrupos $H_1 = P_1 \times \ldots \times M_1 \times \ldots \times P_n$ e $H_2 = P_1 \times \ldots \times M_2 \times \ldots \times P_r$. Veja que $|G : H_1| = |G : H_2| = p$, implicando que H_1 e H_2 são dois subgrupos maximais de G com índice p. Reciprocamente, sejam M_1, M_2 dois subgrupos maximais de G com índice p e $P \in Syl_p(G)$. Logo, $P \nsubseteq M_1$ e $P \nsubseteq M_2$. Portanto, $PM_1 = G$ e $PM_2 = G$. Afirmamos que $P \cap M_1 \neq P \cap M_2$. Com efeito, se $P \cap M_1 = P \cap M_2$, então $P \cap M_1 \subseteq M_1 \cap M_2$. Daí,*

$$p = |M_1 : M_1 \cap M_2| \Big| |M_1 : P \cap M_1| = |G : P|,$$

e teríamos p dividindo $|G : P|$, o que é absurdo. Desse modo, $P \cap M_1$ e $P \cap M_2$ são dois subgrupos de P com mesma ordem, ou seja, P não é cíclico.

Lema 3.5 *Se $G = \bigcup_{r=1}^{n} H_r$, onde $\sigma(G) = n$, e L um subgrupo de H_r para todo $r \neq k$, possivelmente. Então L é subgrupo de todos os H_r's.*

Prova: Por hipótese, $L \leqslant H_r$ para cada $r \neq k$. Como $G = H_1 \cup \ldots \cup H_r$ é uma cobertura mínima e, conseqüentemente, irredundante; isto é, $H_k \nsubseteq \bigcup_{r \neq k} H_r$, existe $a \in H_k$ tal que $a \notin H_r$

para todo $r \neq k$. Então $aL \cap H_r = \varnothing$ para todo $r \neq k$, pois se $b \in aL \cap H_r \Rightarrow b = a\ell (\ell \in L)$ e $b \in H_r$. Como $L \leq H_r$, tem-se $a = b\ell^{-1} \in H_r$, o que não ocorre! Logo $aL \subset H_k \Rightarrow L \leq H_k$. ♦

Teorema 3.4 *Se G é um grupo n-primitivo então; ou, $G \simeq C_p \times C_p$ para algum p primo ou, $Z(G)$ é o subgrupo trivial.*

Prova: Se G é abeliano então G é nilpotente e, pelo Teorema 3.3, temos $G \simeq C_p \times C_p$. Agora considere G não-abeliano e suponha, por absurdo, que $Z(G)$ seja não-trivial. Seja p um primo que divide $|Z(G)|$, então existe $u \in Z(G)$ com ordem p. Considere $U = \langle u \rangle$ e suponha que $G = \bigcup_{r=1}^{n} H_r$, com cada H_r maximal em G. Como $U \lhd G$ e G é n-primitivo, temos $\sigma\left(\frac{G}{U}\right) > n$. Logo, existe no mínimo um H_r tal que $U \not\subset H_r$. Porém, pelo Lema 3.5, devem existir no mínimo dois subgrupos H_r's com tal propriedade, digamos H e K (pois se existe apenas um, teríamos $U \leq H_r \ \forall r$, o que é absurdo!). Pela maximalidade de H, temos

$$G = HU \ \Rightarrow \ G = \bigcup_{i=0}^{p-1} Hu^i.$$

Além disso,

$$H^G = H^{HU} = (H^H)^U = H^U = H \ \Rightarrow \ H \lhd G.$$

$$\therefore \quad \frac{G}{H} \simeq U \ \Rightarrow \ i(H) = p.$$

Analogamente, $K \lhd G$ e $i(K) = p$.

Assim, $G \simeq H \times U$. Por hipótese, G é um grupo n-primitivo, isso implica que $\sigma(G) < \sigma(H)$. Sendo H e K subgrupos normais e maximais de G, temos $X = H \cap K \lhd G$ e

$$\begin{aligned} i(X) &= |HK : X| = |HK : K|.|K : X| \\ &= |HK : K|.|HK : K| = i(K)^2 = p^2 \\ \therefore \quad i(X) &= p^2. \end{aligned}$$

Então $X \lhd H$ e $|\ \frac{H}{X}\ | = p$, o que implica que $\frac{H}{X} \simeq C_p$. Se $X = 1$, segue que $G \simeq C_p \times C_p$. Portanto, suponha $X \neq 1$. Então

$$H = \bigcup_{j=0}^{p-1} Xv^j\ , \ \text{onde}\, v \in H, v, v^2, \ldots, v^{p-1} \notin X \,\text{e}\, v^p \in X.$$

Daí

$$\begin{aligned} G &= \bigcup_{i=0}^{p-1} Hu^i = \bigcup_{i=0}^{p-1} \left(\bigcup_{j=0}^{p-1} Xv^j \right) u^i \\ &= \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-1} Xv^j u^i \overset{u \in Z(G)}{=} \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-1} Xu^i v^j \end{aligned}$$

Porém, para cada $0 < j \leq p-1$, existe um único $0 < k \leq p-1$ tal que $ik \equiv j \, (mod\, p)$. Logo, $Xu^i v^j = X(uv^k)^i$. Assim, podemos reescrever

$$\begin{aligned} G &= \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-1} Xu^i v^j \\ &= \left(\bigcup_{j=0}^{p-1} Xv^j \right) \bigcup \left\{ \bigcup_{i=1}^{p-1} \left(\bigcup_{j=0}^{p-1} Xu^i v^j \right) \right\} \\ &= \left(\bigcup_{j=0}^{p-1} Xv^j \right) \bigcup \left\{ \bigcup_{k=0}^{p-1} \left(\bigcup_{i=1}^{p-1} X(uv^k)^i \right) \right\} \\ &= \left(\bigcup_{j=0}^{p-1} Xv^j \right) \bigcup \left\{ \bigcup_{k=0}^{p-1} \left(\bigcup_{i=1}^{p-1} (X(uv^k)^i \cup X) \right) \right\} \\ &= \left(\bigcup_{j=0}^{p-1} Xv^j \right) \bigcup \left\{ \bigcup_{k=0}^{p-1} \left(\bigcup_{i=1}^{p-1} (X(uv^k)^i \cup X(uv^k)^0) \right) \right\} \\ &= \left(\bigcup_{j=0}^{p-1} Xv^j \right) \bigcup \left\{ \bigcup_{k=0}^{p-1} \left(\bigcup_{i=0}^{p-1} X(uv^k)^i \right) \right\} \\ &= H \cup \left(\bigcup_{k=0}^{p-1} B_k \right), \end{aligned}$$

onde $B_k = \bigcup_{i=0}^{p-1} X(uv^k)^i$. Note que $B_k = X\langle uv^k \rangle$, implicando que B_k é um subgrupo de G, para todo $k \in \{0, 1, \ldots, p-1\}$. Afirmamos que B_k tem índice p em G. De fato, como $|G : X| = p^2$ e $X \leq B_k$, segue que $|G : B_k| = 1, p$ ou p^2. Se $|G : B_k| = 1$, então $G = B_k$. Logo, $h = x(uv^k)^i$ para todo $h \in H$ e $0 < i \leq p-1$. Daí, $u^i = x^{-1} h v^{-ki}$, implicando que $u^i \in H \cap U = 1$, isto é, $i = 0$, o que não ocorre. Se $|G : B_k| = p^2$, então $X = B_k = X\langle uv^k \rangle \Rightarrow uv^k \in X$. Como $X \leq H$ e $v^k \in H$, segue que $u \in H$, o que é absurdo. Portanto, $|G : B_k| = p$ para todo $0 \leq k \leq p-1$.

Se $(uv^k)^i \in X$ para algum $1 \leq i \leq p-1$, como $X \subseteq H$ e $v \in H$, teríamos $u^i \in H$, contradizendo o fato de que $U \cap H = 1$. Logo, as classes $X(uv^k)^i$ são disjuntas, duas a duas.

Donde, $\sigma(G) \leq p+1$ e se $k > 0$, então $U \nsubseteq B_k$. Além disso, como B_k tem índice p em G, segue que B_k é um subgrupo maximal de G e daí, $G = UB_k$. Como $U \subseteq Z(G)$, temos que $B_k \trianglelefteq G$ e $B_k \cap U = 1$. Assim, $G \simeq U \times B_k$ e daí, $\sigma(B_k) > n$. Por outro lado,

$$G = \bigcup_{r=1}^{n} H_r \Rightarrow B_k = G \cap B_k = \bigcup_{r=1}^{n} (H_r \cap B_k).$$

Então, se $H_r \cap B_k \neq B_k$ para todo r, teríamos $\sigma(B_k) \leq n$, o que é absurdo! Donde, $H_r \cap B_k = B_k$ para algum r. Daí, para cada $k \geq 1$ existe um único inteiro r tal que $B_k \subseteq H_r$. Porém, B_k tem índice p em G e H_r é um subgrupo próprio de G, logo $B_k = H_r$. Assim, $p-1$ valores distintos de k dão $p-1$ valores distintos de r, logo na representação $G = \bigcup_{i=1}^{n} H_r$ existem no mínimo p termos distintos, a saber; $H, B_1, B_2, \ldots, B_{p-1}$, onde U não está contido em nenhum de tais subgrupos. Dessa forma, $\sigma(G) \geq p+1$ e portanto, $\sigma(G) = p+1$. Como $\frac{H}{X}$ e $\frac{K}{X}$ tem ordem igual a p, segue que $\frac{G}{X}$ não é cíclico e daí, $\frac{G}{X} \simeq C_p \times C_p \Rightarrow \sigma(G) = \sigma(\frac{G}{X}) = p+1$, o que é absurdo!

Portanto $|Z(G)| = 1$. ♦

Lema 3.6 *Se H é um subgrupo maximal de G, então: ou H tem $i(H)$ conjugados em G, ou $H \lhd G$ e $i(H)$ é primo.*

Prova: Seja $N_G(H)$ o normalizador de H em G. Como H é maximal em G, temos que $N_G(H) = H$ ou $N_G(H) = G$.

- Se $N_G(H) = H$, então H tem exatamente $i(N_G(H)) = i(H)$ conjugados em G.
- Se $N_G(H) = G$, então $H \lhd G$. Assim, $\frac{G}{H}$ é um grupo que não possui subgrupos próprios. Logo, $\frac{G}{H} \simeq C_p$ e portanto $i(H) = p$. ♦

Exemplo 3 *Considere o grupo $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. Se tomarmos os subgrupos $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$ e $\langle(123)\rangle$, concluímos que:*

$$S_3 = \langle(12)\rangle \cup \langle(13)\rangle \cup \langle(23)\rangle \cup \langle(123)\rangle.$$

Como qualquer subgrupo próprio de S_3, que contenha uma transposição, só pode conter esta e como um subgrupo que contenha um 3-ciclo e uma tranposição, não pode ser próprio; concluímos que tal cobertura de S_3 é mínima, ou seja, $\boxed{\sigma(S_3) = 4}$.

Observação 3.4 *Consideremos o grupo S_4 e K grupo de Klein. Sabemos que $K \lhd S_4$. O grupo $\frac{S_4}{K}$ não é abeliano, pois $(S_4)' = A_4 \not\subset K$, onde $(S_4)'$ denota o subgrupo derivado de S_4. Assim, $\frac{S_4}{K} \simeq S_3$ e portanto, pelo Exemplo 3, concluímos que $\sigma\left(\frac{S_4}{K}\right) = 4$.*

Exemplo 4 *Consideremos o grupo alternado A_4. Temos que $A_4 = \langle 3\text{-}ciclos \rangle$. Note que:*

$$A_4 = K \cup \langle (123) \rangle \cup \langle (124) \rangle \cup \langle (134) \rangle \cup \langle (234) \rangle,$$

onde K é o grupo de Klein. Do fato de um subgrupo próprio de A_4 que contém um 3-ciclo, poder conter no máximo dois 3-ciclos e do fato de K ser maximal em A_4, concluímos que $\boxed{\sigma(A_4) = 5}$.

Com os resultados estabelecidos até aqui, estamos em condições de caracterizar todos os grupos 3-soma, 4-soma e 5-soma.

Teorema 3.5 (Caracterização dos grupos 3-soma,4-soma e 5-soma) *:*

(*i*) *G é um grupo 3-soma se, e somente se, possui pelo menos dois subgrupos de índice 2. Além disso, $C_2 \times C_2$ é o único grupo 3-primitivo;*

(*ii*) *G é um grupo 4-soma se, e somente se, $\sigma(G) \neq 3$ e possui pelo menos dois subgrupos de índice 3. Ademais, $C_3 \times C_3$ e S_3 são os únicos grupos 4-primitivos;*

(*iii*) *G é um grupo 5-soma se, e somente se, $\sigma(G) \neq 3$ ou 4 e G possui um subgrupo maximal de índice 4. Além disso, A_4 é o único grupo 5-primitivo.*

Prova: (*i*) Se $\sigma(G) = 3$, pelo Lema 3.1, $2 \leq i_1 \leq i_2 \leq 2 \Rightarrow i_2 = i_3 = 2$. Reciprocamente, se G possui dois subgrupos H_1 e H_2 de índice 2, então ambos são normais em G. Então

$$N = H_1 \cap H_2 \lhd G \quad e \quad |H_1 : N| = |H_1 H_2 : H_2| = 2 \Rightarrow$$
$$\Rightarrow \quad i(N) = i(H_1)|H_1 : N| = 2.2 = 4.$$

Assim, $\frac{G}{N}$ é abeliano $\Rightarrow$ $\frac{G}{N} \simeq C_4$ ou $\frac{G}{N} \simeq C_2 \times C_2$. Porém, $\frac{H_1}{N}$ e $\frac{H_2}{N}$ são subgrupos de $\frac{G}{N}$ de ordem igual a 2. Logo, $\frac{G}{N}$ não é cíclico, donde;

$$\frac{G}{N} \simeq C_2 \times C_2 \Rightarrow \sigma\left(\frac{G}{N}\right) = 3.$$

Os Lemas 3.1 e 3.2 nos dão que $\sigma(G) = 3$. Ademais, sendo G um grupo 3-primitivo, necessariamente $|N| = 1$, e portanto, $G \simeq C_2 \times C_2$.

(ii) Se $\sigma(G) = 4$, pelo Lema 3.1, $i_2 \leq 3$. Porém, se $i_2 = 2$ então $i_1 = i_2 = 2$, o que implicaria, pelo item (i), que $\sigma(G) = 3$, o que não ocorre! Então, $i_2 = 3$. Pelo Teorema 3.1,

$$\begin{aligned} & 1 \leq \frac{1}{i_2} + \frac{1}{i_3} + \frac{1}{i_4} \leq \frac{1}{3} + \frac{2}{i_3} \\ \Rightarrow \quad & \frac{2}{3} \leq \frac{2}{i_3} \quad \Rightarrow \quad i_3 \leq 3 \quad \therefore \ i_3 = 3. \end{aligned}$$

Aplicando, novamente, o Teorema 3.1, segue que $i_4 = 3$. Reciprocamente, suponha que $\sigma(G) \neq 3$ e que G possui dois subgrupos, A e B, de índice 3. Então: ou A e B são subgrupos normais de G, ou pelo menos um deles não é normal.

- Se $A \lhd G$ e $B \lhd G$, segue que $X = A \cap B \lhd G$, e portanto, $\frac{G}{X} \simeq C_3 \times C_3 \Rightarrow \sigma(G) = 4$. Em particular, se G é 4-primitivo, temos que $G \simeq C_3 \times C_3$.

- Se $A \not\lhd G$, seja $X = A_G$ o núcleo normal de A. Então, defina a ação

$$\begin{aligned} \varphi : G \quad & \to \quad S_{G:A} \\ g \quad & \mapsto \quad \varphi_g : g_1 A \mapsto g(g_1 A). \end{aligned}$$

  Dessa forma, o grupo $\frac{G}{X}$ é isomorfo a um subgrupo de S_3. Como A não é normal em G, A tem exatamente 3 subgrupos conjugados em G. Se $\frac{G}{X}$ fosse cíclico, então A seria normal em G, o que não ocorre. Portanto, $\frac{G}{X} \simeq S_3 \Rightarrow \sigma\left(\frac{G}{X}\right) = \sigma(S_3) = 4 \Rightarrow \sigma(G) = 4$. Em particular, se G é 4-primitivo, segue que $G \simeq S_3$.

(iii) Se $\sigma(G) = 5$, pelo Lema 3.1, $i_2 \leq 4$. Pelo item (i), temos $i_2 \neq 2$. Se $i_2 = 3$, pelo Teorema 3.1,

$$\begin{aligned} & 1 \leq \frac{1}{i_2} + \frac{1}{i_3} + \frac{1}{i_4} + \frac{1}{i_5} \leq \frac{1}{3} + \frac{3}{i_3} \Rightarrow \\ \Rightarrow \quad & \frac{2}{3} \leq \frac{3}{i_3} \Rightarrow i_3 \leq \left\lfloor \frac{9}{2} \right\rfloor \quad \therefore \quad i_3 \leq 4. \end{aligned}$$

Pelo item (ii), $i_3 \neq 3 \Rightarrow i_3 = 4$. Reciprocamente, suponha que $\sigma(G) \neq 3$ ou 4, e que G possui um subgrupo maximal B de índice 4. Pelo Lema 3.6, B tem exatamente 4 subgrupos

conjugados em G e $B \not\trianglelefteq G$. Seja $X = B_G$ o núcleo normal de B. Defina a ação

$$\begin{aligned} \varphi : G &\rightarrow S_{G:B} \\ g &\mapsto \varphi_g : g_1B \mapsto g(g_1B). \end{aligned}$$

Então, o grupo $\frac{G}{X}$ é isomorfo a um subgrupo de S_4. Como B tem quatro conjugados em G, segue que $\frac{G}{X}$ não é cíclico. Note:

$$\left|\frac{G}{X}\right| = \left|\frac{G}{X} : \frac{B}{X}\right| \left|\frac{B}{X}\right| \quad \Rightarrow \quad i(B) = \left|\frac{G}{X} : \frac{B}{X}\right| = 4.$$

Como B não é normal em G, temos $X \neq B$. Assim, $\left|\frac{G}{X}\right| = 8, 12$ ou 24.

- Se $\left|\frac{G}{X}\right| = 8$, então $\frac{G}{X}$ é um 2-grupo não-cíclico. Pelo Teorema 3.2, temos $\sigma\left(\frac{G}{X}\right) = 3 \Rightarrow \sigma(G) = 3$, o que é absurdo!

- Se $\left|\frac{G}{X}\right| = 24$, então $\frac{G}{X} \simeq S_4$. Porém, pela Observação 3.4, temos $\frac{S_4}{K} \simeq S_3$, onde K é subgrupo de Klein. Daí, pelo Lema 3.2, $\sigma\left(\frac{G}{X}\right) = \sigma(S_4) \leq \sigma\left(\frac{S_4}{K}\right) = \sigma(S_3) = 4 \Rightarrow \sigma(G) \leq 4$, o que é absurdo!

Donde concluímos que $\left|\frac{G}{X}\right| = 12$, e portanto, $\frac{G}{X} \simeq A_4$. Portanto

$$\sigma\left(\frac{G}{X}\right) = \sigma(A_4) = 5 \quad \Rightarrow \quad \sigma(G) = 5.$$

Em particular, se G é 5-primitivo, temos $G \simeq A_4$. ♦

3.2 $\sigma(S_5)$ e $\sigma(A_5)$

O Teorema 3.5 induz, naturalmente, que podemos supor que os grupos 6-soma possam ser caracterizados, similarmente, pela existência de dois subgrupos de índice 5. Porém, os grupo A_5 e S_5 mostram que isso não é possível, pois ambos contêm cinco subgrupo de índice 5, a saber; em A_5, todos isomorfos a A_4, e em S_5, todos isomorfos a S_4.

Observação 3.5 *Se G é um grupo de ordem 12, então ou, existe $\alpha \in G$ de ordem 6 ou, G é isomorfo a A_4. De fato, seja $P \in Syl_3(G)$. Defina a ação*

$$\begin{aligned} \varphi : G &\rightarrow S_{G:P} \\ g &\mapsto \varphi_g : hP \mapsto g(hP). \end{aligned}$$

Sabemos que $\ker\varphi \trianglelefteq G$ *e* $\ker\varphi \subseteq P$. *Daí,* $\ker\varphi = 1$ *ou* $\ker\varphi = P$.

- *Se* $\ker\varphi = 1$, *então* $G \lesssim S_4$. *Como o único subgrupo de* S_4 *de índice* 2 *é* A_4, *segue que* $G \simeq A_4$.

- *Se* $\ker\varphi = P$, *então* $P \lhd G$. *Considere* $P = \langle a\rangle$, *com* $o(a) = 3$. *Assim, os únicos elementos de* G *de ordem* 3 *são* a *e* a^2. *Daí,* $|G : C_G(a)| = |a^G| = 2$, *implicando que* $|C_G(a)| = 6$. *Logo, existe* $b \in C_G(a)$ *de ordem* 2. *Como* $o(a)$ *e* $o(b)$ *são primos entre si e* $ab = ba$, *segue que* $o(ab) = 6$.

Observação 3.6 *Se* H *é um subgrupo de* S_5 *com ordem* 24, *então* $H \simeq S_4$. *De fato, consideremos a ação*

$$\begin{aligned} \varphi : S_5 &\to S_{S_5:H} \\ g &\mapsto \varphi_g : \alpha H \mapsto g(\alpha H). \end{aligned}$$

Então, $\ker\varphi \trianglelefteq S_5$ *e* $\ker\varphi \subseteq H$. *Contudo, os únicos subgrupos normais de* S_5 *são* $1, A_5$ *e* S_5. *Assim,* $\ker\varphi = 1$. *Agora, consideremos* $\tilde{\varphi} = \varphi|_H$. *Observe que* $\tilde{\varphi}_h(H) = H$ *para todo* $h \in H$, *donde* $\tilde{\varphi}(H) \subseteq S_4$. *Por outro lado,* $\ker\tilde{\varphi} = \ker\varphi \cap H \Rightarrow \ker\tilde{\varphi} = 1$. *Portanto,*

$$H \simeq \frac{H}{\ker\tilde{\varphi}} = \tilde{\varphi}(H) = S_4 \Rightarrow H \simeq S_4.$$

Proposição 3.2 *Não existe subgrupo de* S_5 *com ordem* $15, 30$ *e* 40.

Prova: Como, a menos de isomorfismos, C_{15} é o único subgrupo de ordem 15 e S_5 não possui elemento de ordem 15, segue que não existe subgrupo de S_5 com ordem 15. Se existisse $H \leq S_5$ com ordem 30, então $H \cap A_5$ seria um subgrupo de ordem 15, o que não ocorre!

Seja H de ordem 40. Defina a ação

$$\begin{aligned} \varphi : S_5 &\to S_{S_5:H} \\ \gamma &\mapsto \varphi_\gamma : \alpha H \mapsto \gamma(\alpha H). \end{aligned}$$

Então $\ker\varphi$ é um subgrupo normal não-trivial de S_5 contido em H . Porém, os únicos subgrupos normais de S_5 são $1, A_5$ e S_5. Donde, teríamos $\ker\varphi = 1 \Rightarrow S_5 \leq S_3$, o que é absurdo!

Lema 3.7 *$\sigma(A_5) = 10$ e $\sigma(S_5) = 16$.*

Prova: Temos

GRUPO A_5:

- 15 elementos de ordem 2; por exemplo, (12)(34), etc.
- 20 elementos de ordem 3; por exemplo, (234), etc.
- 24 elementos de ordem 5; por exemplo, (12345), etc.

Seja X um subgrupo próprio de A_5, contendo um elemento α de ordem 5. Daí, se existisse $\beta \in X$ com ordem 3, teríamos $|X| \geq 15$ o que implicaria $|X| = 15, 20$ ou 30, o que não ocorre(pois A_5 não possui subgrupos com tais ordens). Analogamente, os únicos elementos de ordem 5 são potências de α. Assim, $|X| = 5$ ou $|X| = 10$ e são necessários seis subgrupos próprios para conter todos elementos de ordem 5. Logo, podemos tomar todos com ordem 10, donde todos são isomorfos a D_5, pois S_5 não contém elementos de ordem 10. Dessa forma, tais subgrupos contêm, entre eles, todos os elementos de ordem 2.

Agora, seja Y um subgrupo próprio contendo um elemento de ordem 3. Então $|Y| = 3, 6$ ou 12 e Y contém 2 ou 8 elementos de ordem 3. Porém, os elementos de ordem 3 em Y podem envolver no máximo quatro dos cinco símbolos, pois caso contrário, se (123) e (145) pertencessem a Y, teríamos (145)(123) = (12345) pertencendo a Y, o que não ocorre. Logo, são necessários pelo menos quatro subgrupos para conter, entre eles, todos os elementos de ordem 3. Porém, quatro subgrupos é suficiente, pois basta considerar os grupos alternados dos símbolos $\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{1, 2, 4, 5\}$ e $\{2, 3, 4, 5\}$. Portanto, segue que $\boxed{\sigma(A_5) = 10}$.

GRUPO S_5:

- 10 transposições; por exemplo, $(12), (45)$, etc.
- 15 produtos de duas transposições; por exemplo, (23)(45), etc.
- 20 3-ciclos; por exemplo, (134), etc.
- 30 4-ciclos; por exemplo, (1452), etc.

- 24 5-ciclos; por exemplo, (13524), etc.
- 20 elementos de ordem 6, por exemplo; (13)(245), etc.

Seja X um subgrupo próprio de S_5 contendo α de ordem 6. Então;

▶ se $\beta \in X$, β de ordem 5

Então $|X| \geq |\langle\alpha\rangle\langle\beta\rangle| = 30 \Rightarrow |X| = 60$ e $X \simeq A_5$. Porém, A_5 não possui elemento de ordem 6. Donde $\beta \notin X$.

▶ se $\gamma \in X$, γ de ordem 4

Então $|X| \geq |\langle\alpha\rangle\langle\gamma\rangle| = 12 \Rightarrow |X| = 12, 20, 24$ ou 60. Como A_5 e S_4 não possuem elementos de ordem 6, temos que $|X| \neq 60$ e $|X| \neq 24$. Além disso, $|\langle\alpha\rangle| = 6 \nmid 20 \Rightarrow |X| \neq 20$. Donde, $|X| = 12$ e portanto, $X \simeq D_6$. No entanto, D_6 não possui elemento de ordem 4. Logo, $\gamma \notin X$.

▶ No entanto, se X possui elemento de ordem 2 ou de ordem 3, seque que $|X| = 6$ ou $|X| = 12$. Se X possuísse outro elemento de ordem 6 que não fosse potência de α, então $|X| \geq 12 \Rightarrow |X| = 12$. Assim

$$X \simeq C_6 \times C_2 \quad ou \quad X \simeq D_6.$$

Por outro lado, $X \not\simeq D_6$ visto que X possui quatro elementos de ordem 6, enquanto que D_6 possui apenas dois elementos de ordem 6. E ainda, como um elemento de ordem 6 envolve os cinco símbolos, ele não comuta com nenhum elemento de S_5. Logo, $X \not\simeq C_6 \times C_2$. Dessa forma, os únicos elementos de ordem 6 são potências de α.

Logo são necessários 10 subgrupos próprios para conter todos os elementos de ordem 6. Podemos tomar tais subgrupos com ordem igual a 12, e portanto, todos isomorfos a D_6. Assim, tais subgrupos contém, entre eles, todos os 3-ciclos, todas as transposições e todos os produtos de duas tranposições.

Por fim, seja Y um subgrupo contendo um elemento α de ordem 5 e um elemento β de ordem 4. Então $|Y| \geq |\langle\alpha\rangle\langle\beta\rangle| = 20 \Rightarrow |Y| = 20$ e $Y = \langle\alpha, \beta\rangle$. Assim, os únicos

elementos de ordem 5 são potências de α. Donde, são necessários 6 subgrupos para conter todos elementos de ordem 5. Ademais,

$$\langle\alpha\rangle \lhd Y \;\Rightarrow\; \beta\alpha\beta^{-1} \in \langle\alpha\rangle = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}.$$

Temos que $\beta\alpha\beta^{-1} \neq \alpha$, pois α envolve todos os cinco símbolos.

Se $\beta\alpha\beta^{-1} = \alpha^4 = \alpha^{-1}$, então:

$$\beta(\beta\alpha\beta^{-1})\beta^{-1} = \beta(\alpha^{-1})\beta^{-1} = (\beta\alpha\beta^{-1})^{-1} = (\alpha^{-1})^{-1} = \alpha$$

$$\Rightarrow \quad \alpha\beta^2 = \beta^2\alpha \quad \therefore\ o(\alpha\beta^2) = 10 \quad \text{(Absurdo!)}.$$

Assim, $\beta\alpha\beta^{-1} = \alpha^2$ ou α^3. Daí, podemos considerar Y da forma

$$Y = \langle\alpha, \beta \,|\, \alpha^5 = 1 = \beta^4\,,\ \beta\alpha\beta^{-1} = \alpha^2\rangle.$$

Dessa forma, podemos tomar os seis subgrupos como o subgrupo Y. E, além disso, tais subgrupos contêm, entre eles, todos os 4-ciclos.

Portanto, $\boxed{\sigma(S_5) = 16}$. ♦

3.3 Caracterização dos grupos 6-primitivos

COMENTÁRIO: De um modo geral, se $G = H_1 \cup H_2 \cup \ldots \cup H_n$, temos que $|G| \leq \sum_{r=1}^{n} |H_r|$.

Lema 3.8 *Se* $\sigma(G) = n$ *e* $G = \left(\bigcup_{r=1}^{m} H_r\right) \bigcup \left(\bigcup_{r=m+1}^{n} K_r\right)$, *onde cada subgrupo da cobertura é maximal em* G *e* $H_r \trianglelefteq G$, *com* $|H_r| \neq |H_s|\ \forall\, r \neq s$. *Então* $|G| \leq \sum_{r=m+1}^{n} |K_r|$.

Prova: Pelo comentário podemos supor $m \geq 1$. Pelo Lema 3.6, $i(H_r) = p_r$ onde p_r é um número primo e $r \in \{1, \ldots, m\}$. Por hipótese, $p_1, \ldots, p_r$ são todos distintos dois a dois. Daí,

$$\left| G : \bigcap_{r=1}^{m} H_r \right| = p_1 p_2 \cdot \ldots \cdot p_r.$$

Se $D = \bigcup_{r=1}^{m} H_r$, então:

$$|D| \;=\; \sum_{r=1}^{m} |H_r| - \sum_{\substack{r,s \\ 1\leq r<s}}^{m} |H_r \cap H_s| + \sum_{\substack{r,s,t \\ 1\leq r<s<t}}^{m} |H_r \cap H_s \cap H_t| -$$

$$
\begin{aligned}
&- \sum_{\substack{r,s,t,k \\ 1\le r<s<t<k}}^{m} |H_r \cap H_s \cap H_t \cap H_k| + \ldots + (-1)^{m-1}|H_1 \cap H_2 \cap \ldots \cap H_m| \\
|D| &= \sum_{r=1}^{m} \frac{|G|}{p_r} - \sum_{\substack{r,s \\ 1\le r<s}}^{m} \frac{|G|}{p_r p_s} + \sum_{\substack{r,s,t \\ 1\le r<s<t}}^{m} \frac{|G|}{p_r p_s p_t} - \sum_{\substack{r,s,t,k \\ 1\le r<s<t<k}}^{m} \frac{|G|}{p_r p_s p_t p_k} + \\
&+ \ldots + (-1)^{m-1}|G| \prod_{r=1}^{m} \frac{1}{p_r} \\
|D| &= |G| \left\{ \sum_{r=1}^{m} \frac{1}{p_r} - \sum_{\substack{r,s \\ 1\le r<s}}^{m} \frac{1}{p_r p_s} + \ldots + (-1)^{m-1} \prod_{r=1}^{m} \frac{1}{p_r} \right\} \\
\Rightarrow |D| &= |G| \left\{ 1 - \prod_{r=1}^{m} \left(1 - \frac{1}{p_r} \right) \right\}
\end{aligned}
$$

Seja k_r o número de elementos de K_r que não pertencem a D. Como $H_s \trianglelefteq G$ e K_r é maximal em G, implica que $G = H_s K_r$ e daí:

$$
\begin{aligned}
|H_s \cap K_r| &= \frac{|H_s||K_r|}{|H_s K_r|} = \frac{|H_s||K_r|}{|G|} = \frac{|H_s||K_r|}{p_s.|H_s|} = \frac{|K_r|}{p_s} \\
&\Rightarrow |H_s \cap K_r| = \frac{|K_r|}{p_s}.
\end{aligned}
$$

Analogamente, $|H_t \cap K_r| = \frac{|K_r|}{p_t}$. Além disso,

$$
|H_s \cap H_t \cap K_r| \Big| \frac{|K_r|}{p_s} \quad e \quad |H_s \cap H_t \cap K_r| \Big| \frac{|K_r|}{p_t}.
$$

Temos que $|K_r| = p_s.a = p_t.b$. Como p_s e p_t são primos entre si, segue que $p_s \mid b$ e daí, $|K_r| = |H_s \cap H_t \cap K_r| p_s p_t.c$, o que implica que $|H_s \cap H_t \cap K_r| \Big| \frac{|K_r|}{p_s p_t}$. Por outro lado,

$$
\begin{aligned}
|H_s \cap H_t \cap K_r| &= \frac{|K_r||H_s \cap H_t|}{|K_r(H_s \cap H_t)|} \\
&= \frac{|K_r||G|}{p_s p_t |K_r(H_s \cap H_t)|} \\
&\geq \frac{|K_r||G|}{p_s p_t |G|} = \frac{|K_r|}{p_s p_t}
\end{aligned}
$$

Donde concluímos que, $|H_s \cap H_t \cap K_r| = \frac{|K_r|}{p_s p_t}$. Ademais,

$$
\begin{aligned}
k_r &= |K_r \backslash D| = |K_r| - |K_r \cap D| = \\
k_r &= |K_r| - \left| K_r \cap \left(\bigcup_{s=1}^{m} H_s \right) \right| \\
k_r &= |K_r| - \left| \bigcup_{s=1}^{m} (H_s \cap K_r) \right|
\end{aligned}
$$

$$\begin{aligned} k_r &= |K_r| - \sum_{s=1}^{m} |H_s \cap K_r| + \sum_{\substack{s,t \\ 1\leq s<t}}^{m} |H_s \cap H_t \cap K_r| - \\ &- \sum_{\substack{s,t,k \\ 1\leq s<t<k}}^{m} |H_s \cap H_t \cap H_k \cap K_r| + \ldots + (-1)^{m-1}|H_1 \cap H_2 \cap \ldots \cap H_m \cap K_r| \\ k_r &= |K_r| - \sum_{s=1}^{m} \frac{|K_r|}{p_s} + \sum_{\substack{s,t \\ 1\leq s<t}}^{m} \frac{|K_r|}{p_s p_t} - \sum_{\substack{s,t,k \\ 1\leq s<t<k}}^{m} \frac{|K_r|}{p_s p_t p_k} + \ldots + (-1)^{m-1}|K_r| \prod_{s=1}^{m} \frac{1}{p_s} \\ k_r &= |K_r| \left(1 - \sum_{s=1}^{m} \frac{1}{p_s} + \sum_{\substack{s,t \\ 1\leq s<t}}^{m} \frac{1}{p_s p_t} - \sum_{\substack{s,t,k \\ 1\leq s<t<k}}^{m} \frac{1}{p_s p_t p_k} + \ldots + (-1)^{m-1} \prod_{s=1}^{m} \frac{1}{p_s} \right) \\ \Rightarrow \quad k_r &= |K_r|. \prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right). \end{aligned}$$

Assim,

$$|G| \leq |D| + \sum_{r=m+1}^{n} k_r = |G| - |G|. \prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right) + \sum_{r=m+1}^{n} \left\{ |K_r|. \prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right) \right\}$$

Donde,

$$\begin{aligned} |G|. \prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right) &\leq \left\{ \prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right) \right\}. \sum_{r=m+1}^{n} |K_r| \\ \therefore \quad |G| &\leq \sum_{r=m+1}^{n} |K_r|. \blacklozenge \end{aligned}$$

Lema 3.9 *Se $\sigma(G) = 6$, então $i_1 = 2$ ou 5 e $i_r = 5$ para $2 \leq r \leq 6$.*

Prova: O Teorema 3.5 nos garante que G não possui subgrupo maximal de índice 4 e que G tem, no máximo, um subgrupo maximal de índice 2 e um subgrupo maximal de índice 3. Assim, $i_3 \geq 5$. Se $i_1 = 2$ e $i_2 = 3$, pelo Lema 3.8,

$$\begin{aligned} 1 &\leq \frac{1}{i_3} + \frac{1}{i_4} + \frac{1}{i_5} + \frac{1}{i_6} \leq \frac{4}{i_3} \Rightarrow i_3 \leq 4 \text{ (absurdo!)} \\ \therefore \quad & \boxed{(i_1 = 2 \ e \ i_2 \neq 3) \quad ou \quad (i_1 \neq 2 \ e \ i_2 = 3) \quad ou \quad (i_1 \neq 2 \ e \ i_2 \neq 3)}. \end{aligned}$$

Porém, se $i_2 = 3 \Rightarrow i_1 = i_2 = 3$, o que não ocorre! Portanto, se $i_1 = 2, 3$ ou 5, concluímos que $i_2 = 5$. Daí, pelo Lema 3.1,

$$\begin{aligned} & 1 \leq \frac{1}{5} + \frac{1}{i_3} + \frac{1}{i_4} + \frac{1}{i_5} + \frac{1}{i_6} \Rightarrow 1 \leq \frac{1}{5} + \frac{4}{i_3} \\ \Rightarrow \quad & \frac{4}{5} \leq \frac{4}{i_3} \Rightarrow i_3 \leq 5 \quad \therefore \quad \boxed{i_3 = 5}. \end{aligned}$$

Aplicando o Lema 3.1 repetidamente, concluímos que $\boxed{i_4 = i_5 = i_6 = 5}$. Suponha, por absurdo, que $i_1 = 3$. Então H_1 é o único subgrupo de G de índice 3, logo $H_1 \trianglelefteq G$. Do Teorema 3.1, sabemos que $|G| \leq \sum_{r=2}^{6} |H_r|$. Se $|G| < \sum_{r=2}^{6} |H_r|$, teríamos

$$1 < \frac{1}{i_2} + \frac{1}{i_3} + \frac{1}{i_4} + \frac{1}{i_5} + \frac{1}{i_6} = \frac{5}{5} = 1, \text{ absurdo!}$$

Então, $|G| = \sum_{i=2}^{6} |H_r|$ e, portanto, $H_1 H_r = G$ para todo $r \neq 1$ e $H_r \cap H_s \subset H_1$ para todo $r \neq s$. Em particular, $H_2 \cap H_3 \subset H_1$. Daí $3 = i_1 | i(H_2 \cap H_3)$ e $5 = i_2 | i(H_2 \cap H_3)$, o que implica que $15 | i(H_2 \cap H_3)$. Por outro lado,

$$\begin{aligned} |H_2 \cap H_3| &= \frac{|H_2||H_3|}{|H_2 H_3|} \geq \frac{|H_2||H_3|}{|G|} = \frac{|G|^2}{i_2 i_3 |G|} = \frac{|G|}{25} \\ &\Rightarrow \quad i(H_2 \cap H_3) \leq 25 \\ &\therefore \quad i(H_2 \cap H_3) = 15. \end{aligned}$$

Além disso,

$$\begin{aligned} |H_1 \cap H_2| &= \frac{|H_1||H_2|}{|H_1 H_2|} = \frac{|H_1||H_2|}{|G|} = \frac{|G|}{i_1 i_2} \\ \Rightarrow \quad i(H_1 \cap H_2) &= i_1 i_2 = 15. \end{aligned}$$

Donde, $X = H_1 \cap H_2 = H_2 \cap H_3 = H_r \cap H_s$ para todo $r \neq s$. Como $H_1 \trianglelefteq G$, tem-se $X \trianglelefteq H_2$ e $X \trianglelefteq H_3$, e $G = \langle H_2, H_3 \rangle$; segue que $X \trianglelefteq G$. Assim,

$$\begin{aligned} \frac{G}{X} &= \frac{H_1}{X} \cup \frac{H_2}{X} \cup \frac{H_3}{X} \cup \frac{H_4}{X} \cup \frac{H_5}{X} \cup \frac{H_6}{X} \\ &\therefore \quad \sigma\left(\frac{G}{X}\right) = 6. \end{aligned}$$

Contudo, todo grupo de ordem 15 é cíclico. Portanto, $i_1 \neq 3$ e segue o resultado. ♦

Exemplo 5 *Consideremos o grupo dihedral D_5, dado por*

$$D_5 = \langle a, b \,|\, a^5 = 1 = b^2 \,,\, bab^{-1} = a^{-1} \rangle \quad e \quad |D_5| = 10.$$

Temos que $D_5 = \langle a \rangle \cup \langle b \rangle \cup \langle ab \rangle \cup \langle a^2 b \rangle \cup \langle a^3 b \rangle \cup \langle a^4 b \rangle$, o que implica $\sigma(D_5) \leq 6$. Por outro lado, $\langle a \rangle$ é o único subgrupo de D_5 de índice 2 e D_5 não possui nenhum subgrupo de índice 3 ou 4. Pelo Teorema 3.5, concluímos que $\boxed{\sigma(D_5) = 6}$.

Exemplo 6 *Agora considere o grupo W, dado por*

$$W = \langle a, b \,|\, a^5 = 1 = b^4 \,,\, ba = a^2b \rangle \quad e \quad |W| = 20.$$

Temos que $W = \langle a \rangle \cup \langle b \rangle \cup \langle ab \rangle \cup \langle a^2b \rangle \cup \langle a^3b \rangle \cup \langle a^4b \rangle \Rightarrow \sigma(W) \leq 6$. *Sendo* $\langle a, b^2 \rangle$ *o único subgrupo de* W *de índice* 2, *segue que* $\sigma(W) \neq 3$. *Como* $3 \nmid |W| = 20$, *não existe nenhum subgrupo de índice* 3 *e, portanto,* $\sigma(W) \neq 4$. *Além disso,* $\langle a \rangle$ *é o único subgrupo de* W *de índice* 4. *Veja que* $\langle a \rangle$ *não é um subgrupo maximal de* W, *pois* $\langle a \rangle < \langle a, b^2 \rangle \neq W$; *donde,* $\sigma(W) \neq 5$. *Desse modo, concluímos que* $\boxed{\sigma(W) = 6}$.

Lema 3.10 *Se* G *é um grupo* 6*-primitivo e* $i_1 = 2$, *então* $G \simeq D_5$ *ou* $G \simeq W$.

Prova: Pelo Lema 3.9, $i_r = 5$ para $2 \leq r \leq 6$ e, além disso, $|G| = \sum_{r=2}^{6} |H_r|$. Donde, $H_1H_r = G$ para todo $r \neq 1$ e $H_r \cap H_s \subset H_1$ para todo $r \neq s$. Temos que $2 = i_1 \mid i(H_r \cap H_s)$ e $5 = i_r \mid i(H_r \cap H_s)$, o que implica que $10 \mid i(H_r \cap H_s)$. Por outro lado,

$$|H_r \cap H_s| = \frac{|H_r||H_s|}{|H_rH_s|} \geq \frac{|H_r||H_s|}{|G|} = \frac{|G|}{25}$$
$$\Rightarrow \quad i(H_r \cap H_s) \leq 25 \quad \Rightarrow \quad i(H_r \cap H_s) = 10 \text{ } ou \text{ } 20.$$

Ademais, como $H_1H_r = G$ segue que $i(H_1 \cap H_r) = 10$, para todo $r \neq 1$.

caso 1. Existem inteiros r, s, com $r \neq 1$ e $r \neq s$, tais que $i(H_r \cap H_s) = 10$.

Então $X = H_1 \cap H_r = H_r \cap H_s = H_1 \cap H_s$. Temos $|G| = i(X).|X|$ e $|G| = i_r.|H_r|$, donde $|X| = \frac{|H_r|}{2}$, ou seja, $X \trianglelefteq H_r$. Analogamente, $X \trianglelefteq H_s$. Como $G = \langle H_r, H_s \rangle$, implica que $X \trianglelefteq G$. Sendo $\frac{H_r}{X}$ e $\frac{H_s}{X}$ dois subgrupos distintos de $\frac{G}{X}$ de ordem 2, vemos que $\frac{G}{X}$ é não-cíclico. Donde $\frac{G}{X} \not\simeq C_{10}$ e, portanto, $\frac{G}{X} \simeq D_5$. Logo, $\sigma\left(\frac{G}{X}\right) = \sigma(D_5) = 6$. Como G é 6-primitivo, devemos ter $|X| = 1$ e daí, $G \simeq D_5$.

caso 2. $i(H_r \cap H_s) = 20$ para todo $r \neq s$, com $r \neq 1$.

Em particular, $H_2 \cap H_3 \subset H_1$. Considere $B_r = H_1 \cap H_r$ e $X = B_2 \cap B_3$. Note: $B_2 \cap B_3 = (H_1 \cap H_2) \cap (H_1 \cap H_3) = H_1 \cap (H_2 \cap H_3) = H_2 \cap H_3$. Temos

$$|H_1 : B_2| = |H_1 : H_1 \cap H_2| = |H_1H_2 : H_2| = |G : H_2| = i_2 = 5$$

Donde, B_2 é maximal em H_1. Além disso,

$$|B_2 : X| = \frac{|G : X|}{|G : B_2|} = \frac{i(H_2 \cap H_3)}{i(H_1 \cap H_2)} = 2 \quad \Rightarrow \quad X \trianglelefteq B_2.$$

Analogamente, X é normal em B_3 e B_3 é maximal em H_1. Como $H_1 = \langle B_2, B_3 \rangle$, segue que $X \trianglelefteq H_1$. Daí, $H_1 \subseteq N_G(X)$ e, portanto, $N_G(X) = H_1$ ou $N_G(X) = G$. Se $N_G(X) = H_1$, então X tem exatamente dois subgrupos conjugados em G, digamos X e Y. Como $X \trianglelefteq H_1$ e $X \ntrianglelefteq H_2$ (pois se $X \trianglelefteq H_2$, sendo $G = H_1H_2$, teríamos $X \trianglelefteq G$ o que implicaria $N_G(X) = G$, absurdo!), existe $b \in H_2$ tal que $bXb^{-1} \neq X$, ou seja, $bXb^{-1} = Y$. Como $X \subset H_2$, então $Y = bXb^{-1} \subseteq H_2$. Analogamente, $X \ntrianglelefteq H_3$ e $Y \subseteq H_3$, donde $Y \subseteq H_2 \cap H_3 = X$, o que é absurdo! Logo $N_G(X) = G$, o que implica $X \trianglelefteq G$. Considere $K = \frac{G}{X}$. Sendo $\frac{H_2}{X}$ e $\frac{H_3}{X}$ dois subgrupos distintos de K de ordem 4, vemos que K é não-cíclico.

Provaremos que $\sigma(K) = 6$ e $K \simeq W$. Com efeito, já sabemos que $\sigma(K) \geq 6$. Veja:

$$|K : K_1| = \left| \frac{G}{X} : \frac{H_1}{X} \right| = |G : H_1| = 2 \quad \Rightarrow \quad \frac{H_1}{X} = K_1 \trianglelefteq K.$$

Se K possuísse dois subgrupos de índice 2, pelo Teorema 3.5, teríamos $\sigma(K) = 3$, o que não ocorre! Então, K_1 é o único subgrupo de K de índice 2, ou seja, K_1 é o único subgrupo de K com ordem igual a 10. Pelo Teorema de Sylow, existe um único $F \in Syl_5(K)$ o que implica $F \trianglelefteq K$. Logo K_1 contém todos os elementos de K de ordem múltipla de 5, e é único. Assim, restam dez elementos de K de ordem dividindo 4, e daí existem exatamente cinco 2-subgrupos de Sylow contendo, entre eles, tais elementos. Dessa forma, devemos ter $\sigma(K) \leq 6$ e, portanto, $\sigma(K) = 6$. Implicando, pelo fato de G ser um grupo 6-primitivo, que $X = 1$, donde $G = K$. Ademais, $\left|\frac{K}{F}\right| = 4$, segue que $\frac{K}{F} \simeq C_2 \times C_2$ ou $\frac{K}{F} \simeq C_4$. Se $\frac{K}{F} \simeq C_2 \times C_2$, teríamos $\sigma\left(\frac{K}{F}\right) = 3$, o que é absurdo! Portanto, $\frac{K}{F} \simeq C_4$. Seja a gerador de F e Fb gerador de $\frac{K}{F}$, temos que $a^5 = 1$ e $b^4 \in F$. Se $b^4 \neq 1$, K seria gerador por b donde, K seria cíclico, o que não ocorre! Dessa forma, $b^4 = 1$. Como F é normal em K, temos que $ba \in Fb = \{b, ab, a^2b, a^3b, a^4b\}$. Claramente, devemos ter $ba \neq b$ e $ba \neq ab$.

- Se $ba = a^4b$, então b^2 comuta com a e daí, $L = \langle b^2 \rangle \subseteq Z(G)$, donde L é normal

em G. Assim,

$$\begin{aligned}\frac{G}{L} = \frac{K}{L} &\simeq \langle \alpha, \beta \,|\, \alpha^5 = 1 = \beta^2 \,,\, \beta\alpha\beta^{-1} = \alpha^{-1} \rangle \simeq D_5 \\ &\Rightarrow \sigma\left(\frac{G}{L}\right) = 6 = \sigma(G).\end{aligned}$$

Como G é 6-primitivo, necessariamente $|L| = 1$ e daí, $G \simeq D_5$.

- Se $ba = a^2b$, então $K = \langle a, b \,|\, a^5 = 1 = b^4 \,,\, ba = a^2b \rangle = W$, ou seja, $G = W$.
- Se $ba = a^3b$, considere $c = b^3$. Daí:

$$\begin{aligned}ca &= b^3a = b^2(ba) = b^2(a^3b) = b(ba)a^2b = b(a^3b)a^2b = \\ &= (ba)a^2(ba)ab = (a^3b)a^2(a^3b)ab = a^3b^2ab = a^3b(ba)b = \\ &= a^3b(a^3b)b = a^3(ba)a^2b^2 = a^3(a^3b)a^2b^2 = aba^2b^2 = \\ &= a(ba)ab^2 = a^4bab^2 = a^4(a^3b)b^2 = a^2b^3 = a^2c \\ &\Rightarrow ca = a^2c.\end{aligned}$$

Assim, $K = \langle a, c \,|\, a^5 = 1 = c^4 \,,\, ca = a^2c \rangle = W$, ou seja, $G = W$.

Portanto segue o resultado. ♦

Lema 3.11 *Se G é um grupo não-cíclico tal que $|G|$ divide 24, então $\sigma(G) \leq 5$.*

Prova: Pelo Teorema 3.2, basta considerarmos os grupos de ordem 6, 12 ou 24. Se $|G| = 6$ e G é não-cíclico, então $G \simeq S_3$ e, portanto, $\sigma(G) = 4$. Se $|G| = 12$, pelo Teorema de Sylow, $n_2 = 1$ ou 3 e $n_3 = 1$ ou 4. Temos os seguintes casos:

(i) se $n_2 = 3$, então G tem exatamente três subgrupos de índice 3. Do Teorema 3.5, segue que $\sigma(G) = 3$ ou 4;

(ii) se $n_2 = 1$ e $n_3 = 1$, então $H \trianglelefteq G$ e $K \trianglelefteq G$ onde $H \in Syl_2(G)$ e $K \in Syl_3(G)$. Como $H \cap K = 1$, concluímos que G é o produto direto dos subgrupos de Sylow H e K, dessa forma o Teorema 3.3 nos garante que $\sigma(G) = 3$;

(iii) se $n_3 = 4$, então $n_2 = 1$. Logo, G tem exatamente quatro 3-subgrupos de Sylow e um 2-subgrupo de Sylow, que cobrem G. Donde, $\sigma(G) \leq 5$.

Se $|G| = 24$, pelos casos anteriores basta considerar o caso em que G tem um único T, 2-subgrupo de Sylow, e quatro 3-subgrupos de Sylow, digamos V_1, V_2, V_3 e V_4. Notemos que nenhum dos V_i's pode ser maximal, pois caso contrário, pelo Lema 3.6, V_i teria 8 subgrupos conjugados em G, o que não ocorre! Dessa forma, seja K um subgrupo maximal de G contendo V_i, para algum i. Então $i(K) = 2$ ou 4.

- $i(K) = 2$

  Se G possuir outro subgrupo de índice 2, pelo Teorema 3.5, temos $\sigma(G) = 3$. Então, suponha que K é o único subgrupo de G de índice 2, ou seja, $K \trianglelefteq G$. Daí, K e T contêm todos os elementos de G com ordem $2, 3, 4$ e 8. Logo existe $\beta \notin T$ e $\beta \notin K$ de ordem 6. Considere $L = \langle\beta\rangle$, o que implica que $i(L) = 4$. Se L não fosse maximal em G, existiria um subgrupo maximal de índice 2, distinto de K (pois $\beta \notin K$), o que é absurdo! Donde, L é um subgrupo maximal de G de índice 4. Do Teorema 3.5, segue que $\sigma(G) \leq 5$.

- $i(K) = 4$

  É imediato do Teorema 3.5. ♦

Lema 3.12 *O único grupo 6-soma primitivo com $i_1 = 5$ é $C_5 \times C_5$.*

Prova: Suponha que $G = \bigcup_{r=1}^{6} H_r$, onde todos os H_r's são maximais em G. Pelo Lema 3.9, $i_r = 5$ para todo $r \in \{1, 2, \ldots, 6\}$ e, pelo Teorema 3.1, temos que $H_1 H_r = G$ para todo $r \neq 1$ e que $H_r \cap H_s \subset H_1$ para todo $r \neq s$. Temos $H_r \cap H_s \subseteq H_1 \cap H_r \Rightarrow |H_r \cap H_s| \leq |H_1 \cap H_r|$. Por outro lado,

$$|H_1 \cap H_r| = \frac{|H_1||H_r|}{|H_1 H_r|} = \frac{|H_1||H_r|}{|G|} = \frac{|G|}{i_1 i_r} \quad \Rightarrow \quad i(H_1 \cap H_r) = 25$$

$$e \quad |H_r \cap H_s| = \frac{|H_r||H_s|}{|H_r H_s|} = \frac{|H_1||H_r|}{|H_r H_s|} \geq \frac{|H_1||H_r|}{|G|} = |H_1 \cap H_r|$$

Daí $|H_1 \cap H_r| = |H_r \cap H_s|$, o que implica $i(H_r \cap H_s) = 25$ e $H_1 \cap H_r = H_r \cap H_s = H_1 \cap H_s$ para todo $r \neq s$ e $r \neq 1$. Note que $X = H_r \cap H_s$ não contém nenhum subgrupo normal em G não-trivial, pois caso contrário, se $\{1\} \neq K \subset X$ com $K \trianglelefteq G$, teríamos

$$\frac{G}{K} = \bigcup_{r=1}^{6} \frac{H_r}{K} \quad \Rightarrow \quad \sigma\left(\frac{G}{K}\right) = 6,$$

contradizendo o fato de G ser 6-primitivo. Seja Y_r o maior subgrupo normal de H_r que é normal em G (a saber, $Y_r = (H_r)_G$). Como $i_1 = 5$, segue que o grupo $\frac{G}{Y_1}$ é isomorfo a um subgrupo de S_5, o que acarreta que $\left|\frac{G}{Y_1}\right|$ divide 5!. Então

$$|G : Y_1| = 5.\frac{|H_1|}{|Y_1|} \Rightarrow \frac{|H_1|}{|Y_1|} = k\Big|24.$$

Seja $Z_1 = X \cap Y_1$. Note $Z_1 = X \cap Y_1 = (H_1 \cap H_2) \cap Y_1 = H_2 \cap Y_1$. Além disso,

$$\begin{aligned} & h_2 Z_1 h_2^{-1} = h_2(H_2 \cap Y_1)h_2^{-1} \subseteq H_2 \quad e \quad h_2 Z_1 h_2^{-1} \subseteq Y_1, \quad \text{pois } Y_1 \trianglelefteq G \\ \Rightarrow \quad & h_2 Z_1 h_2^{-1} \subseteq H_2 \cap Y_1 = Z_1, \ \forall\, h_2 \in H_2 \quad \Rightarrow \quad Z_1 \trianglelefteq H_2. \end{aligned}$$

Analogamente $Z_1 \trianglelefteq H_3$, como $G = \langle H_2, H_3\rangle$, temos $Z_1 \trianglelefteq G$. Porém, $Z_1 \subseteq X$ o que implica que $Z_1 = \{1\}$. Daí $|X||Y_1| = |X \cap Y_1||XY_1| = |Z_1||XY_1| = |XY_1|$. Também XY_1 é um subgrupo de H_1 contendo propriamente X(pois caso contrário, se $XY_1 = X \Rightarrow Y_1 \subseteq X$, o que não ocorre, visto que Y_1 é normal em G). Mas

$$\begin{aligned} & i(X) = i_1.|H_1 : X| \quad \Rightarrow \quad |H_1 : X| = 5 \\ \Rightarrow \quad & XY_1 = H_1 \quad \Rightarrow \quad 5 = |H_1 : X| = |XY_1 : X| \\ \Rightarrow \quad & 5 = |Y_1 : X \cap Y_1| = |Y_1| \quad \therefore \quad |Y_1| = 5. \end{aligned}$$

Além disso, como $k \mid 24$ e $|H_1| = k.|Y_1| \Rightarrow 5 \mid |H_1|$ e mais, sendo $Y_1 \trianglelefteq G$, Y_1 é o único 5-subgrupo de Sylow de H_1. Sendo $|Y_1| = 5$, tem-se que Y_1 tem quatro elementos de ordem 5 e são os únicos elementos de ordem 5 de H_1. Analogamente, cada Y_r contém exatamente quatro elementos de ordem 5. Como $Y_r \cap Y_s = 1 (r \neq s)$, segue que G possui exatamente 24 elementos de ordem 5 e nenhum de ordem 25, pois $G = \bigcup_{r=1}^{6} H_r$. Logo, G possui um único 5-subgrupo de Sylow, digamos F, com $F \simeq C_5 \times C_5$. Se o grupo $\frac{G}{F}$ não fosse cíclico, pelo Lema 3.11, teríamos $\sigma\left(\frac{G}{F}\right) \leq 5$ e, conseqüentemente, $\sigma(G) \leq 5$, o que não ocorre! Assim, $\frac{G}{F} \simeq C_k$.

Se $k = 1$, então $G = F$ e, portanto, $\boxed{G \simeq C_5 \times C_5}$. Suponha, por absurdo, que $k > 1$. Então, se Y_1 e Y_2 são gerados por a e b, respectivamente, segue que Y_3, Y_4, Y_5 e Y_6 são gerados por $\langle ab^s\rangle$ para $s = 1, 2, 3, 4$, onde $ab = ba$ e $a^5 = 1 = b^5$. Seja Fc gerador de $\frac{G}{F}$. Sem perda de generalidade, podemos supor que $c^k = 1$, pois se $c^k \neq 1$, considere $\frac{G}{F}$ gerado por Fd, onde

$d = c^5$, daí $d^k = (c^5)^k = (c^k)^5 = 1$. Como $Y_1 \trianglelefteq G$ e $Y_2 \trianglelefteq G$, temos $ca = a^r c$, para algum $1 \leq r \leq 4$ e $cb = b^s c$, para algum $1 \leq s \leq 4$. Analogamente, $c(ab) = (ab)^t c$ para algum $1 \leq t \leq 4$. Mas,

$$c(ab) = (ca)b = a^r(cb) = a^r b^s c \Rightarrow a^r b^s = a^t b^t$$

$$\Rightarrow \quad a^{r-t} = b^{t-s} \quad \Rightarrow \quad 5 \mid r-t \quad e \quad 5 \mid t-s$$

Donde, $5 \mid r - s$. Como $r - s < 5$, segue que $r - s = 0$, isto é, $r = s = t$.

- $r = 1$:

  Então $ca = ac$ e $cb = bc$. Considere $K = \langle c \rangle \Rightarrow |K| = k$. Como $K \cap F = 1$ e $F \trianglelefteq G$, segue que $KF \leq G$ e $|KF| = 5^2.k$, ou seja, $G = KF$. Além disso, $K \trianglelefteq G$ e, portanto, $G \simeq K \times F$. Donde, $\frac{G}{K} \simeq F \Rightarrow \sigma\left(\frac{G}{K}\right) = 6$, contradizendo o fato de G ser 6-primitivo.

- $r = 4$:

  Temos $ca = a^4 c$ e $cb = b^4 c$. Se $k \neq 2$, então:

  $$\begin{aligned} c^2 a &= c(ca) = c(a^4 c) = (ca)a^3 c = (a^4 c)a^3 c = \\ &= a^4(ca)a^2 c = a^3(ca)ac = a^2(ca)c = ac^2 \\ &\Rightarrow c^2 a = ac^2. \end{aligned}$$

  Analogamente, $c^2 b = bc^2$, o que implica $c^2 \in Z(G)$ e $Z(G) \neq 1$. Pelo Teorema 3.4, $G \simeq C_5 \times C_5$, o que é absurdo. No entanto, se $k = 2$; temos

  $$\frac{G}{Y_1} \simeq \langle \alpha, \beta \,|\, \alpha^5 = 1 = \beta^2 \,,\, \beta\alpha\beta^{-1} = \alpha^{-1} \rangle \simeq D_5.$$

  Logo, $\sigma(G) = \sigma\left(\frac{G}{Y_1}\right)$, contradizendo o fato de G ser 6-primitivo.

- $r = 2$ ou 3:

  Então $ca = a^2 c$ e $cb = b^2 c$. Se $k \neq 2$ e 4, então:

  $$\begin{aligned} c^4 a &= c^3(ca) = c^3(a^2 c) = c^2(ca)ac = c^2(a^2 c)ac = \\ &= c(ca)a(ca)c = c(a^2 c)a(a^2 c)c = (ca)a(ca)a^2 c^2 = \\ &= (a^2 c)a(a^2 c)a^2 c^2 = a^2(ca)a^2(ca)ac^2 = a^2(a^2 c)a^2(a^2 c)ac^2 = \\ &= a^4(ca)a^3(ca)c^2 = a^4(a^2 c)a^3(a^2 c)c^2 = ac^4 \\ &\Rightarrow c^4 a = ac^4. \end{aligned}$$

Analogamente, $c^4b = bc^4$, o que implica $c^4 \in Z(G)$, o que é absurdo, pelo Teorema 3.4. Donde, $k = 2$ ou 4. Se $k = 4$, segue que $\frac{G}{Y_1} \simeq W \Rightarrow \sigma\left(\frac{G}{Y_1}\right) = 6$, contradizendo o fato de G ser 6-primitivo. Dessa forma, concluímos que $k = 2$ e daí, $c^2 = 1$. Note:

$$c^2a = c(ca) = c(a^2c) = (ca)ac = a^2(ca)c = a^4c^2 \quad \Rightarrow$$
$$\Rightarrow a = a^4 \quad \Rightarrow \quad a^3 = 1 \text{ (absurdo!)}.$$

O mesmo raciocínio se aplica, caso $ca = a^3c$ e $cb = b^3c$. ♦

Portanto, os Lemas 3.10 e 3.12 nos dão que

Teorema 3.6 *Os únicos grupos* 6*-primitivos são* $C_5 \times C_5, D_5$ *e* W.

3.4 $\sigma(G)$ de grupos supersolúveis

O Teorema 3.3 garante que todo grupo G não-cíclico e nilpotente é $(p+1)$-soma, onde p é o menor primo para o qual G possui, pelo menos, dois subgrupos maximais de índice p. Este resultado não é válido, de modo geral, como mostra o Lema 3.7. No que segue, mostraremos que podemos enfraquecer a hipótese, supondo G supersolúvel (Teorema 3.7).

Lema 3.13 *Sejam* G *um grupo não-cíclico,* $X \trianglelefteq G$ *e* p *um número primo. Se* $X \simeq C_p$ *e* $\frac{G}{X}$ *é cíclico, então* $\sigma(G) = p + 1$.

Prova: Seja $\frac{G}{X} \simeq C_m$. Temos dois casos a estudar:

- G abeliano

  Então $G \simeq C_p \times C_m$. Como G é não-cíclico, seque que $p \mid m$ e daí,

  $$G \simeq (C_p \times C_{p^n}) \times C_r, \quad \text{onde } p \nmid r.$$

  Logo, pelo Teorema 3.3, concluímos que $\sigma(G) = p + 1$.

- G não-abeliano

Considere $X = \langle a \rangle$ com $a^p = 1$ e $\frac{G}{X} = \langle bX \rangle$, onde $b^m \in X$. Temos que $G = \langle a \rangle \langle b \rangle$. Como $\langle a \rangle \cap \langle b \rangle \subseteq \langle a \rangle$, segue que $\langle a \rangle \cap \langle b \rangle = 1$ ou $\langle a \rangle \cap \langle b \rangle = \langle a \rangle$. Se $\langle a \rangle \cap \langle b \rangle = \langle a \rangle$, teríamos $\langle a \rangle \subseteq \langle b \rangle$, o que acarretaria $G = \langle b \rangle$, absurdo!

$$\therefore \quad \langle a \rangle \cap \langle b \rangle = 1 \quad \Rightarrow \quad b^m = 1.$$

Além disso, como X é normal em G, temos que $bab^{-1} = a^r$, onde $1 < r \leq p-1$. Dessa forma, $G = \{a^i b^j \,|\, a^p = 1 = b^m \,,\, bab^{-1} = a^r\}$. Note:

$$\begin{aligned}
b^2ab^{-2} &= b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = a^{r^2} \\
b^3ab^{-3} &= b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = a^{r^3} \\
&\vdots \\
b^kab^{-k} &= a^{r^k} \\
\Rightarrow \quad a &= b^mab^{-m} = a^{r^m} \quad \Rightarrow \quad r^m \equiv 1\,(mod\,p).
\end{aligned}$$

Além disso,

$$\begin{aligned}
(a^ib)^k &= (a^ib)(a^ib)\cdot\ldots\cdot(a^ib) \\
(a^ib)^k &= a^i(ba^ib^{-1})(b^2a^ib^{-2})\cdot\ldots\cdot(b^{k-1}a^ib^{-k+1})b^k \\
(a^ib)^k &= a^ia^{ir}a^{ir^2}\cdot\ldots\cdot a^{ir^{k-1}}.b^k \\
(a^ib)^k &= a^{i(1+r+\ldots+r^{k-1})}b^k \quad \Rightarrow \quad o(a^ib) \geq m.
\end{aligned}$$

Por outro lado, $1 + r + r^2 + \ldots + r^{m-1} = \frac{r^m-1}{r-1} \equiv 0\,(mod\,p) \;\Rightarrow\; o(a^ib) \leq m$, e portanto, $o(a^ib) = m$. Assim, $X_i = \langle a^ib \rangle$ é um subgrupo maximal de G para cada $i = 0, 1, \ldots, p-1$. E mais, cada X_i é um subgrupo de qualquer cobertura de G por subgrupos próprios. Se $a \in X_i$, para algum $i \in \{0, 1, \ldots, p-1\}$, então $a = (a^ib)^s = a^{i(1+r+\ldots+r^{s-1})}b^s \;\Rightarrow\; b^s = a^{i(1+r+\ldots+r^{s-1})-1} \in \langle a \rangle \cap \langle b \rangle$. Logo, $b^s = 1$ e $s = m$, donde $a = 1$, o que é absurdo! Dessa forma, nenhum dos X_i's contém a. Com isso, concluímos que $\sigma(G) \geq p + 1$. Para o que resta, devemos mostrar que $\sigma(G) \leq p + 1$. Com efeito, considere k o menor inteiro positivo satisfazendo à congruência $r^s \equiv 1\,(mod\,p)$. Então $k \mid m$ e $k \neq 1$, visto que $r \neq 1$. Se $k = m$, então para $0 < M < m$, tem-se $1 + r + \ldots + r^{M-1} \not\equiv 0\,(mod\,p)$. Daí, todo elemento $a^Nb^M = (a^ib)^M$ pertence a X_i,

para algum i. Donde, $G = X_0 \cup X_1 \cup \ldots \cup X_{p-1} \cup X \;\Rightarrow\; \sigma(G) \leq p+1$. Se $k < m$, considere $B = \langle b^k \rangle$. Como $b^k a b^{-k} = a^{r^k} = a$, concluímos que $B \leq Z(G)$, e portanto, $B \trianglelefteq G$. Daí:

$$\frac{G}{B} \simeq \{\alpha^i \beta^j \mid \alpha^p = \bar{1} = \beta^k \,,\, \beta\alpha\beta^{-1} = \alpha^r\}.$$

Logo, pelo caso anterior, $\sigma\left(\frac{G}{B}\right) \leq p+1$, o que implica, $\sigma(G) \leq p+1$, como queríamos. ♦

Lema 3.14 *Suponha que G é um grupo supersolúvel com ordem $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, onde $p_1 < p_2 < \ldots < p_r$ são números primos e $\alpha_i > 0$ para todo i. Então $\sigma(G) \leq p_r + 1$.*

Prova: Pelo Teorema de Zappa, existe uma série central onde todos os fatores são cíclicos

$$1 = B_R \leq B_{R-1} \leq \ldots \leq B_1 \leq B_0 = G,$$

onde $R = \alpha_1 + \ldots + \alpha_r$ e $p_1 = \left|\frac{B_0}{B_1}\right| \leq \left|\frac{B_1}{B_2}\right| \leq \ldots \leq \left|\frac{B_{R-1}}{B_R}\right| = p_r$. Seja k o menor inteiro positivo para o qual $\frac{G}{B_{k+1}}$ é não-cíclico. Como $\frac{B_0}{B_1} = \frac{G}{B_1}$ é cíclico e $\frac{G}{B_R} = G$, segue que $1 \leq k \leq R-1$. Além disso,

$$\frac{G}{B_k} \simeq \frac{\frac{G}{B_{k+1}}}{\frac{B_k}{B_{k+1}}} \text{ é cíclico} \quad \text{e} \quad \frac{B_k}{B_{k+1}} \simeq C_{p_m}.$$

Aplicando o Lema 3.13 para $\bar{G} = \frac{G}{B_{k+1}}$ e $\bar{X} = \frac{B_k}{B_{k+1}}$, concluimos que $\sigma(\bar{G}) = p_m + 1$. Donde,

$$\begin{aligned} \sigma(G) &\leq \sigma\left(\frac{G}{B_{k+1}}\right) = \sigma(\bar{G}) = p_m + 1 \leq p_r + 1. \\ &\therefore \quad \sigma(G) \leq p_r + 1. \blacklozenge \end{aligned}$$

Proposição 3.3 *Seja G um grupo supersolúvel finito. Então $H \lhd G$, onde $H \in Syl_p(G)$ e p é o maior primo que divide $|G|$.*

Prova: Provaremos, por indução, sobre a ordem $|G|$.

Seja N um subgrupo normal minimal de G. Como G é supersolúvel, temos que $N \simeq C_q$. Temos que $N \subseteq H$ ou $N \nsubseteq H$. Se $N \subseteq H$, então $N = H$ ou $N < H$. Caso $N = H$, não há nada a provar. Então suponha que $N < H$. Temos que $\frac{H}{N} \in Syl_p\left(\frac{G}{N}\right)$. Logo, por indução, $\frac{H}{N} \lhd \frac{G}{N}$, e portanto, $H \lhd G$. Se $N \nsubseteq H$, então $|N| = q$ com $q < p$ e q primo. Temos:

$$|NH| = \frac{|N||H|}{|N \cap H|} = |N||H| = q.p^m \;,\; q < p.$$

Pelo Teorema de Sylow, $n_p \equiv 1\,(mod\,p)$ e $n_p \mid q \;\Rightarrow\; n_p = 1$, donde $H \lhd NH$, e portanto, $H \overset{\lhd}{_{\text{car}}} NH$. Por outro lado, $\frac{NH}{N} \in Syl_p\left(\frac{G}{N}\right)$. Logo, por indução, tem-se $\frac{NH}{N} \lhd \frac{G}{N} \;\Rightarrow\; NH \lhd G$. Do fato de $H \overset{\lhd}{_{\text{car}}} NH$ e $NH \lhd G$, concluimos que $H \lhd G$. ♦

Lema 3.15 *Nas mesmas condiçoes do Lema* 3.14*, se G possui pelo menos dois subgrupos de índice p, então* $\sigma(G) \leq p+1$.

Prova: Sejam A e B dois subgrupos de G de índice p, e portanto, maximais em G. Temos duas possibilidades;

- A e B são normais em G.

  Logo $X = A \cap B$ é normal em G e

  $$|X| = |A \cap B| = \frac{|A||B|}{|AB|} = \frac{|A||B|}{|G|} \quad \Rightarrow \quad i(X) = p^2.$$

  Como $\frac{A}{X}$ e $\frac{B}{X}$ são dois subgrupos distintos de $\frac{G}{X}$ com ordem igual a p, segue que $\frac{G}{X}$ não é cíclico. Donde, $\frac{G}{X} \simeq C_p \times C_p$, e portanto, $\sigma(G) \leq p+1$.

- A ou B é normal em G.

  Digamos que A não seja normal em G. Então, A tem exatamente $p = p_m$ conjugados em G. Se $m = r$, o resultado segue do Lema 3.14. Se $m < r$, considere $H \in Syl_{p_r}(A)$. Como $|A| = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m - 1} \cdot \ldots \cdot p_r^{\alpha_r}$, segue que $H \in Syl_{p_r}(G)$. Pela Proposição 3.3, temos H normal em G com $|H| = p_r^{\alpha_r}$. Além disso, H está contido em todos os conjugados de A em G. Dessa forma, $\frac{G}{H}$ é um grupo supersolúvel não-cíclico com ordem igual a $p_1^{\alpha_1} \cdot \ldots \cdot p_{r-1}^{\alpha_{r-1}}$, e possui p subgrupos de índice p; a saber, $\frac{A^c}{H}$ onde A^c é conjugado de A em G. Agora considere $\bar{H} \in Syl_{p_{r-1}}\left(\frac{G}{H}\right) = Syl_{p_{r-1}}(\bar{G})$, temos $\bar{H} \lhd \bar{G}$ (Proposição 3.3), e portanto, $\frac{\bar{G}}{\bar{H}}$ é um grupo supersolúvel não-cíclico com ordem igual a $p_1^{\alpha_1} \cdot \ldots \cdot p_{r-2}^{\alpha_{r-2}}$. Prosseguindo com esse raciocínio, obteremos um grupo fator K supersolúvel não-cíclico de ordem $p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$. Então

  $$\sigma(G) \leq \sigma\left(\frac{G}{H}\right) \leq \sigma\left(\frac{\bar{G}}{\bar{H}}\right) \leq \ldots \leq \sigma(K) \leq p_m + 1,$$

  onde a última desigualdade é válida devido ao Lema 3.14. ♦

Nota: Na prova do Teorema abaixo, utilizaremos o Teorema 3.10, que provaremos na próxima seção 2.5.

Teorema 3.7 *Seja G um grupo supersolúvel finito. Se para fator primo p que divide $|G|$, G possui, no máximo, um subgrupo de índice p, então G é cíclico. Caso contrário, se p é o menor primo para o qual G possui mais que um subgrupo de índice p, então $\sigma(G) = p + 1$.*

Prova: Suponhamos que para fator primo p que divide $|G|$, G possui, no máximo, um subgrupo de índice p. Logo, segue que todo subgrupo maximal de G é normal, e portanto, G é nilpotente. Afirmamos que G é cíclico. De fato, se G não fosse cíclico, existiria $P \in Syl_p(G)$ não-cíclico. Donde, pela Observação 3.3, encontraríamos dois subgrupos maximais de G com índice p, o que não ocorre. Portanto, G é cíclico.

Agora, suponha que p é o menor primo para o qual G possui, pelo menos, dois subgrupos maximais de índice p. Logo, G é um grupo supersolúvel, finito e não-cíclico. Pelo Lema 3.15, temos $\sigma(G) \leq p+1$. Por outro lado, sendo G um grupo solúvel, finito e não-nilpotente, o Teorema 3.10 nos garante que $\sigma(G) = \left|\frac{H}{K}\right| + 1$, onde $\frac{H}{K}$ é o menor fator principal de G que possui mais que um complemento em G. Da Proposição A.4, concluímos que $\left|\frac{H}{K}\right| = q$. Além disso, qualquer complemento de $\frac{H}{K}$ em G é um subgrupo maximal de G, implicando que $q \geq p$. Donde, $\sigma(G) = q + 1 \geq p + 1$ e, portanto, $\sigma(G) = p + 1$. ♦

Com os resultados estabelecidos até agora, estamos em condições de caracterizar os grupos $(p + 1)$-soma primitivos supersolúveis.

Teorema 3.8 *Seja G um grupo $(p + 1)$-primitivo supersolúvel. Então $G \simeq C_p \times C_p$ ou $G \simeq S$, onde $S = \{a^i b^j \mid a^p = 1 = b^N, bab^{-1} = a^r\}$ com $N \mid (p - 1)$ e N é o menor inteiro positivo satisfazendo a congruência $r^n \equiv 1 \,(mod\, p)$.*

Prova: Seja $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, com $p_1 < p_2 < \ldots < p_r$ primos e $\alpha_i > 0$ para todo i. O Teorema 3.7 nos garante que G possui, pelo menos, dois subgrupos maximais de índice p, digamos A e B.

Se A e B são normais em G, então $\frac{G}{A \cap B} \simeq C_p \times C_p$, o que implica $\sigma(G) = \sigma\left(\frac{G}{A \cap B}\right)$. Como G é $(p + 1)$-primitivo, concluímos que $G \simeq C_p \times C_p$.

Agora, suponhamos que $A \not\trianglelefteq G$ e, neste caso, G é não-abeliano. Se $p < p_r$, pela prova do Lema 3.13, encontraríamos um grupo K (a saber, $K \simeq \frac{G}{N}$) supersolúvel não-cíclico tal que $\sigma(K) \leq p+1$, o que implica $\sigma(G) = \sigma(K) = p+1$, contradizendo o fato de G ser $(p+1)$-primitivo. Donde, temos $p = p_r$. Pelo Teorema de Zappa, existe uma série normal onde todos os fatores são cíclicos

$$1 = B_R \leq B_{R-1} \leq \ldots \leq B_1 \leq B_0 = G,$$

onde $R = \alpha_1 + \ldots + \alpha_r$ e $p_1 = \left|\frac{B_0}{B_1}\right| \leq \left|\frac{B_1}{B_2}\right| \leq \ldots \leq \left|\frac{B_{R-1}}{B_R}\right| = p_r = p$. Seja k o menor inteiro para o qual $\frac{G}{B_{k+1}}$ é um grupo não-cíclico. Então $1 \leq k \leq R-1$. O Lema 3.13 nos garante que $\sigma\left(\frac{G}{B_{k+1}}\right) \leq p+1$, donde $\sigma(G) = \sigma\left(\frac{G}{B_{k+1}}\right)$. Como G é $(p+1)$-primitivo, segue que $B_{k+1} = 1$, e portanto, $k = R-1$. Desse modo, temos que $\frac{G}{B_{R-1}}$ é um grupo cíclico, $B_{R-1} \trianglelefteq G$ e $B_{R-1} \simeq C_p$. Pela prova do Lema 3.13, concluímos que $G = \{a^i b^j \mid a^p = 1 = b^N,\ bab^{-1} = a^r\}$, onde $N \mid (p-1)$ e N é o menor inteiro satisfazendo a congruência $r^n \equiv 1\,(mod\,p)$, com $1 < r \leq p-1$. ♦

3.5 $\sigma(G)$ de grupos solúveis

Em 1994, J. H. E. Cohn conjecturou que se G é um grupo solúvel finito, então $\sigma(G) = c+1$, onde c é a ordem do menor fator principal de G para o qual G possui dois subgrupos de índice c. Porém, em 1997, M. J. Tomkinson provou tal conjectura. Nesta seção faremos a demonstração de Tomkinson.

Definição 3.3 *Dizemos que $\frac{H}{K}$ é um fator principal de G, se $\frac{H}{K}$ é um subgrupo normal minimal do grupo quociente $\frac{G}{K}$.*

Definição 3.4 *Seja $\frac{H}{K}$ um fator principal de G. Se $\frac{H}{K} \leq \Phi\left(\frac{G}{K}\right)$, dizemos que $\frac{H}{K}$ é Frattini.*

Definição 3.5 *Se $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$, dizemos que $\frac{H}{K}$ é um fator central de G.*

Pela Proposição 2.7, podemos dizer que $\frac{H}{K}$ é um fator central de G se, e somente se, $[H, G] \leq K$.

Sejam H e K subgrupos de G. Dizemos que H é um complemento de K em G, se $G = HK$ e $H \cap K = 1$.

Proposição 3.4 *Seja G um grupo solúvel finito. Se $\frac{H}{K}$ é um fator principal de G que possui um complemento normal em G, então $\frac{H}{K}$ é um fator central de G. Conseqüentemente, todo complemento de $\frac{H}{K}$ será normal.*

Prova: Sejam N um subgrupo normal minimal de G e M um complemento normal de N em G, isto é; $G = NM, N \cap M = 1$ e $M \trianglelefteq G$. Isto implica que $[N, M] = 1$. Por outro lado, como N é abeliano, temos $[N, N] = 1$. Então $[N, G] = [N, NM] = [N, N][N, M] = 1$, o que implica $N \leq Z(G)$.

Ademais, seja $L \neq M$ um complemento de N em G. Como $N \leq Z(G)$, segue que $L^n = L$ para todo $n \in N$. Daí, $L^g = L^{nl} = (L^n)^l = L^l = L$ para todo $g \in G$. Donde, $L \trianglelefteq G$. ♦

Definição 3.6 *Dizemos que um grupo G é primitivo, se existe um subgrupo maximal de G com núcleo normal trivial.*

Sejam G um grupo e M um subgrupo maximal de G. É fácil ver que $\frac{M}{M_G}$ é um subgrupo maximal de $\frac{G}{M_G}$, com núcleo normal trivial. E portanto,

$$\boxed{\frac{G}{M_G} \text{ é um grupo primitivo, se } M \text{ é um subgrupo maximal de } G}.$$

Proposição 3.5 *Todo grupo finito,solúvel e primitivo possui um único subgrupo normal minimal.*

Prova: A existência é garantida pelo fato de G ser solúvel finito. Sejam N um subgrupo normal minimal de G e M um subgrupo maximal de G tal que $M_G = 1$. Como $N \trianglelefteq G$, segue que $N \nsubseteq M$, o que implica $G = MN$. Temos que $N \cap M \trianglelefteq M$ (pois $N \trianglelefteq G$) e $N \cap M \trianglelefteq N$ pois N é abeliano, donde $N \cap M \trianglelefteq G$. Logo, devemos ter $N \cap M = 1$, implicando que M é um complemento de N em G. Seja $C = C_G(N) \trianglelefteq G$. Como N é abeliano, segue que $N \leq C$. Note: $C \cap M \trianglelefteq M$ (pois $C \trianglelefteq G$) e $C \cap M \trianglelefteq N$, o que implica $C \cap M \trianglelefteq G$, e portanto, $C \cap M = 1$. Daí, $C = C \cap G = C \cap (MN) = N(C \cap M) = N$, isto é, $\boxed{N = C_G(N)}$.

Agora considere L um subgrupo normal minimal de G. Devemos provar que $L = N$. Com efeito, temos que $L \cap N \trianglelefteq G$, o que implica $L \cap N = 1$ ou $L \cap N = N$ (i.e., $L = N$). Se $L \cap N = 1$, temos que $[L, N] = 1$, donde $L \leq C_G(N) = N$, e portanto, $L = N$, o que é absurdo. Desse modo, segue que $L = N$, como queríamos. ♦

Proposição 3.6 *Seja G um grupo finito, solúvel e primitivo. Se N é um subgrupo normal minimal de G tal que $\frac{G}{N}$ é cíclico, então $\sigma(G) = |N| + 1$.*

Prova: Seja M um subgrupo maximal de G tal que $M_G = 1$. Logo, devemos ter $M \ntrianglelefteq G$ e $N \nleq M$. Assim, M é um complemento de N em G. Como $M \ntrianglelefteq G$, M possui exatamente $r = |G : M| = |N|$ conjugados em G, digamos $M_1, M_2, \ldots, M_r$. Além disso, os M_i's são todos cíclicos, pois $M_i \simeq \frac{G}{N}$ é cíclico e também são complementos de N em G. Note:

$$(M_i)_G = \bigcap_{y\in G} M_i^y = \bigcap_{y\in G} M^{xy} = \bigcap_{g\in G} M^g = M_G = 1 \;\Rightarrow\; \boxed{(M_i)_G = 1}\; \forall\, i = 1, \ldots, r.$$

Seja $G = X_1 \cup \ldots \cup X_{\sigma(G)}$, então $M_i = \bigcup_{j=1}^{\sigma(G)} (M_i \cap X_j)$. Como M_i é um grupo cíclico, temos $M_i = X_j$ para algum j. Do fato de $N \nsubseteq M_1 \cup \ldots \cup M_r$, concluímos que $\sigma(G) \geq |N| + 1$.

Por outro lado, $M_i \cap M_j \trianglelefteq \langle M_i, M_j\rangle = G$. Como $(M_i)_G = 1$, devemos ter $M_i \cap M_j = 1$, para todo $i \neq j$. Daí

$$\begin{aligned} |M_1 \cup \ldots \cup M_r| &= |\{1\} \cup (M_1\backslash\{1\}) \cup \ldots \cup (M_r\backslash\{1\})| = 1 + |N|(|M| - 1) = |G| - |N| + 1 \\ &\Rightarrow\; |G| = |M_1 \cup \ldots \cup M_r| + |N| - 1. \end{aligned}$$

Porém,

$$|M_1 \cup \ldots \cup M_r \cup N| = |(M_1 \cup \ldots \cup M_r) \cup (N\backslash\{1\})| = |M_1 \cup \ldots \cup M_r| + |N| - 1 = |G|.$$

Donde, concluímos que $G = M_1 \cup \ldots \cup M_r \cup N$, e portanto, $\sigma(G) \leq |N| + 1$. ♦

O teorema a seguir é devido a Gaschütz [4], este será de fundamental importância na demonstração de Tomkinsom.

Teorema 3.9 (Gaschütz) *Seja G um grupo finito, solúvel e primitivo. Então, todo fator principal de G, distinto de N, tem ordem menor que $|N|$, onde N é o único subgrupo normal minimal de G.*

Prova: Veja [4].

Se G é um grupo solúvel finito, onde todo fator principal de G é Frattini ou central, então G é um grupo nilpotente (Proposição A.10) e, neste caso, sabemos que $\sigma(G) = p + 1$ (Teorema 3.3). Portanto, se G é um grupo solúvel, finito e não-nilpotente, então existe um fator principal de G que possui mais que um complemento em G.

Teorema 3.10 (Tomkinson) *Sejam G um grupo solúvel, finito,não-nilpotente e $\frac{H}{K}$ é o menor fator principal de G que possui mais que um complemento em G. Então $\sigma(G) = \left|\frac{H}{K}\right| + 1$.*

Prova: Considere $\left|\frac{H}{K}\right| = p^n$.

(i) $\sigma(G) \leq p^n + 1$.

Seja $\frac{V}{W}$ um fator principal de G, com ordem igual a p^n, tal que $\frac{V}{W}$ tem mais que um complemento em G e que $\left|\frac{G}{V}\right|$ é mínima com essas propriedades. Portanto, se $\frac{S}{T}$ é um fator principal de G que possui complemento em G, com $S > V$ e $\left|\frac{S}{T}\right| \leq p^n$, segue que $\frac{S}{T}$ possui um único complemento C em G. Donde, $C \trianglelefteq G$ e, pela Proposição 3.4, concluímos que $\frac{S}{T}$ é um fator central de G com ordem $\left|\frac{S}{T}\right| = p$.

Seja M um complemento de $\frac{V}{W}$ em G e considere $Y = M_G \geq W$. Logo, $\frac{G}{Y}$ é um grupo solúvel primitivo, e portanto, seja $\frac{X}{Y}$ o único subgrupo normal minimal de $\frac{G}{Y}$. Afirmamos que $\frac{X}{Y} \simeq \frac{V}{W}$. De fato, como $\frac{YV}{Y} \trianglelefteq \frac{G}{Y}$, temos que $X \leq YV$. Note:

$$YV = YV \cap G = YV \cap (MX) = (YV \cap M)X = Y(V \cap M)X = YWX = X.$$

Logo, $\boxed{X = YV}$. Temos que $W \leq Y \cap V$. Daí, $\frac{Y\cap V}{W} \trianglelefteq \frac{G}{W}$ e $\frac{Y\cap V}{W} \leq \frac{V}{W}$. Do fato de $\frac{V}{W}$ ser normal minimal, segue que $Y \cap V = W$ ou $Y \cap V = V$. Se $Y \cap V = V$, então $V \subseteq Y$. Donde, teríamos $X = YV = Y$, o que não ocorre. Desse modo, concluímos que $\boxed{Y \cap V = W}$. Daí,

$$\frac{X}{Y} = \frac{YV}{Y} \simeq \frac{V}{Y \cap V} = \frac{V}{W} \;\Rightarrow\; \frac{X}{Y} \simeq \frac{V}{W},$$

o que prova a afirmação. Se $X > V$, pela primeira parte, concluímos que $\frac{X}{Y}$ tem um único complemento normal em G, o que implica que $\frac{X}{Y}$ é um fator central de G com ordem $\left|\frac{X}{Y}\right| = p$. Afirmamos que $\frac{V}{W}$ é um fator central de G. De fato, sabemos que $X = YV$ e que $[X, G] \leq Y$. Daí, $Y \geq [X, G] = [YV, G] = [Y, G][V, G]$. Como $Y \trianglelefteq G$, temos $[Y, G] \leq Y$. Donde, $[V, G] \leq Y$. Por outro lado, $[V, G] \leq V$ (pois $V \trianglelefteq G$), o que implica $[V, G] \leq Y \cap V = W$, logo segue a afirmação. Desse modo, todo complemento de $\frac{V}{W}$ em G é normal. Sejam M_1 e M_2 dois tais complementos. Temos que $\left|\frac{G}{M_1\cap M_2}\right| = p^2$. Como $\frac{M_1}{M_1\cap M_2}$ e $\frac{M_2}{M_1\cap M_2}$ são dois subgrupos distintos com ordem p, vemos que $\frac{G}{M_1\cap M_2}$ é não-cíclico. Donde, $\frac{G}{M_1\cap M_2} \simeq C_p \times C_p$ e daí $\sigma(G) \leq \sigma\left(\frac{G}{M_1\cap M_2}\right) = p + 1 \leq p^n + 1$. Assim, podemos assumir que $X = V$ e $Y = W$,

e portanto, que $\frac{G}{W}$ é um grupo solúvel primitivo com um único normal minimal $\frac{V}{W}$. Pelo Teorema 3.9, todo fator principal de $\frac{G}{W}$ tem ordem menor que p^n. Como todo fator principal de $\frac{G}{V}$ é isomorfo a um fator principal de $\frac{G}{W}$, segue que todo fator principal de $\frac{G}{V}$ tem ordem menor que p^n. Da definição de $\frac{V}{W}$, concluímos que todo fator principal de $\frac{G}{V}$ ou é Frattini, ou é central. Pela Proposição A.10, vemos que $\frac{G}{V}$ é um grupo nilpotente. Assim, pela Proposição A.11, obtemos que todo fator primo q de $\left|\frac{G}{V}\right|$ é menor que p^n. Se $\frac{G}{V}$ não é cíclico concluímos, pelo Teorema 3.3, que $\sigma\left(\frac{G}{V}\right) = q+1$, onde q é o menor primo para o qual $\frac{Q}{V} \in Syl_q\left(\frac{G}{V}\right)$ não é cíclico. Logo, $\sigma(G) < p^n + 1$. Se $\frac{G}{V}$ é cíclico, apliquemos a Proposição 3.6 para $\bar{G} = \frac{G}{W}$ e $\bar{N} = \frac{V}{W}$, donde obtemos que $\sigma(G) \leq \sigma\left(\frac{G}{W}\right) = \left|\frac{V}{W}\right| + 1 = p^n + 1$.

(ii) $p^n + 1 \leq \sigma(G)$.

Seja N o maior subgrupo normal de G satisfazendo a condição $\sigma(G) = \sigma\left(\frac{G}{N}\right)$. Então, se $\frac{K}{N}$ é um subgrupo normal minimal de $\frac{G}{N}$, devemos ter $\frac{G}{K}$ cíclico ou $\sigma\left(\frac{G}{K}\right) > \sigma(G)$.

Considere $G = X_1 \cup \ldots \cup X_{\sigma(G)}$, onde os X_i's são subgrupos maximais de G, que contém N. Afirmamos que $K \nsubseteq X_i$ para algum j. Suponhamos, por absurdo, que todos os X_i's contêm K. Se $\sigma\left(\frac{G}{K}\right) > \sigma(G)$, teríamos $\frac{G}{K} = \frac{X_1}{K} \cup \ldots \cup \frac{X_{\sigma(G)}}{K}$, implicando que $\sigma\left(\frac{G}{K}\right) \leq \sigma(G)$, o que não ocorre. Agora se $\frac{G}{K}$ é cíclico, então $\frac{G}{K}$ não possui cobertura por subgrupos próprios, logo $G = X_j$ para algum j, contradizendo o fato de X_j ser um subgrupo próprio de G. Desse modo, existe X_j tal que $K \nsubseteq X_j$, ou seja, $\frac{K}{N}$ possui um complemento em G. Contudo, se X_j fosse o único complemento de $\frac{K}{N}$ em G, pelo Lema 3.5, teríamos que $K \subseteq X_i$, para todo $i \in \{1, \ldots, \sigma(G)\}$, o que é absurdo. Portanto, $\frac{K}{N}$ tem mais que um complemento em G.

Se $\frac{K}{N}$ possui algum complemento normal, pela Proposição 3.4, segue que todos os complementos são normais. Da definição de N, concluímos que o grupo quociente $\frac{G}{N}$ é $\sigma(G)$-primitivo. Além disso, pela Proposição 3.4, temos $\bar{1} \neq \frac{K}{N} \subseteq Z\left(\frac{G}{N}\right)$. Desse modo, pelo Teorema 3.4, vemos que $\frac{G}{N} \simeq C_q \times C_q$, para algum primo q. Daí, $\sigma(G) = \sigma\left(\frac{G}{N}\right) = q+1 = \left|\frac{K}{N}\right|+1$. No entanto, se todos os complementos de $\frac{K}{N}$ são não-normais, então $\frac{K}{N}$ possui exatamente $r = \left|\frac{K}{N}\right|$ complementos em G, digamos $M_1, M_2, \ldots, M_r$. Note:

$$M_i = \bigcup_{j=1}^{\sigma(G)} (M_i \cap X_j) \quad \text{e} \quad \frac{M_i}{N} = \frac{\frac{G}{N}}{\frac{K}{N}} \simeq \frac{G}{K}.$$

Se $\frac{G}{K}$ é cíclico, então $\frac{M_i}{N}$ não possui cobertura por subgrupos próprios, o que implica que $M_i = X_j$, para algum j. Se $\sigma\left(\frac{G}{K}\right) > \sigma(G)$; suponhamos, por absurdo, que $M_i \neq X_j$ para

todo j. Daí, teríamos $\frac{M_i}{N} = \frac{X_1}{N} \cup \ldots \cup \frac{X_{\sigma(G)}}{N}$ implicando que $\sigma\left(\frac{M_i}{N}\right) = \sigma\left(\frac{G}{K}\right) \leq \sigma(G)$, o que é absurdo. Logo, $M_i = X_j$ para algum j. Como $K \nsubseteq X_j$ para todo j, segue que $\sigma(G) > \left|\frac{K}{N}\right|$, ou seja, $\sigma(G) \geq \left|\frac{K}{N}\right| + 1$. Donde,

$$\sigma(G) \geq \left|\frac{K}{N}\right| + 1 \geq p^n + 1.$$

Portanto, segue o teorema. ♦

Exemplo 7 (Aplicação do Teorema de Tomkinson) *Consideremos o grupo S_4. Os únicos subgrupo normais, não-triviais, de S_4 são: A_4 e K (grupo de Klein). Temos $\left|\frac{A_4}{K}\right| = 3$. Desse modo, K e $\frac{A_4}{K}$ são os únicos fatores principais de S_4. Em S_4, temos 4 subgrupos isomorfos a S_3 que complementam K. Por outro lado, $\frac{S_4}{K} \simeq S_3$ e $\frac{A_4}{K} \simeq A_3$. Como A_3 é complementado por qualquer transposição, segue que $\frac{A_4}{K}$ tem 3 complementos em S_4. Do Teorema 3.10, concluímos que $\sigma(S_4) = \left|\frac{A_4}{K}\right| + 1 = 3 + 1 = 4$. Portanto,* $\boxed{\sigma(S_4) = 4}$.

Referências Bibliográficas

[1] BASTOS, G. G., **Notas de Álgebra**, Fortaleza: Editora Premius - Edições Livro Técnico, 2002. 160p.

[2] COHN, J. H. E., On n-sum groups, **Mathematica Scandinavica Kobenhavn**, DK, v.75, p.44-58, 1994.

[3] DOERK, K., HAWKES, T., **Finite soluble groups**. Berlin: Nerw York: Walter de Gruyter, 1992. 891p.

[4] GASCHÜTZ, W., Existenz und Konjugiertsein von Untergruppen, die in endlichen auflösbaren Gruppen durch gewisse Indexschranken definiert sind, **Journal of Algebra**, New York, v.53, p.1-20, 1978.

[5] GARCIA, ARNALDO, LEQUAIN, YVES, **Elementos de Álgebra**. Rio de Janeiro: IMPA, 2002. 326p. (Projeto Euclides)

[6] ROBINSON, DEREK. J. S., **A Course in the Theory of Groups**, 2nd ed., New York: Springer Verlag, c1996. 499p(Graduate texts in mathematics, 80)

[7] ROSE, JOHN S., **A course on group theory**, Cambridge. Cambridge University Press, 1978. 310p.

[8] TOMKINSON, M. J., Groups as the union of proper subgroups. **Mathematica Scandinavica Kobenhavn**, DK, v.81, p.189-198, 1997.

Apêndice A

Grupos Nilpotentes e Grupos Solúveis

Neste apêndice, fazemos alguns resultados, utilizados nesse trabalho, sobre grupos nilpotentes e grupos solúveis.

A.1 Grupos Solúveis

Definição A.1 *Um grupo G é dito solúvel, se existe uma série subnormal*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G, \tag{A.1}$$

(não necessariamente $G_i \trianglelefteq G$) onde todos os grupos quocientes $\frac{G_{i+1}}{G_i}$ são abelianos.

Proposição A.1 *Seja G um grupo solúvel. Então:*

(i) todo subgrupo de G é solúvel;

(ii) se $N \trianglelefteq G$, então o grupo $\frac{G}{N}$ é solúvel;

(iii) se $N \trianglelefteq G$, com N e $\frac{G}{N}$ solúveis, então G é solúvel.

Prova: (i) Como G é solúvel, existe uma série subnormal $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$, onde todos os grupos quocientes $\frac{G_{i+1}}{G_i}$ são abelianos. Seja H um subgrupo de G, e considere $H_i = G_i \cap H$. Seja $h \in H_{i+1} = G_{i+1} \cap H$, daí $H_i^h = (G_i \cap H)^h = G_i^h \cap H^h = G_i \cap H$, o que implica $H_i \trianglelefteq H_{i+1}$. Além disso,

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{(G_{i+1} \cap H) \cap G_i} \simeq \frac{(G_{i+1} \cap H)G_i}{G_i} \leq \frac{G_{i+1}}{G_i}.$$

Logo, $\frac{H_{i+1}}{H_i}$ é abeliano, e portanto, H é solúvel.

(ii) Seja $N \trianglelefteq G$. Então $G_iN \trianglelefteq G_{i+1}N$, o que implica $\frac{G_iN}{N} \trianglelefteq \frac{G_{i+1}N}{N}$. Daí

$$\frac{\frac{G_{i+1}N}{N}}{\frac{G_iN}{N}} \simeq \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \simeq \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \simeq \frac{\frac{G_{i+1}}{G_i}}{\frac{G_{i+1} \cap (G_iN)}{G_i}}$$

$$\therefore \quad \frac{\frac{G_{i+1}N}{N}}{\frac{G_iN}{N}} \text{ é abeliano.}$$

Logo, $\bar{1} = N \trianglelefteq \frac{G_1N}{N} \trianglelefteq \ldots \trianglelefteq \frac{G_nN}{N} = \frac{G}{N}$ é uma série subnormal de $\frac{G}{N}$, como em $(A.1)$. Portanto, $\frac{G}{N}$ é solúvel.

(iii) Como N e $\frac{G}{N}$ são solúveis, temos

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = N \ , \ \frac{N_{i+1}}{N_i} \text{ é abeliano}$$

$$\text{e} \quad \bar{1} = N \trianglelefteq \frac{H_1}{N} \trianglelefteq \ldots \trianglelefteq \frac{H_s}{N} = \frac{G}{N} \ , \ \frac{\frac{H_{i+1}}{N}}{\frac{H_i}{N}} \text{ é abeliano.}$$

Porém, $\frac{\frac{H_{i+1}}{N}}{\frac{H_i}{N}} \simeq \frac{H_{i+1}}{H_i}$. Portanto , $1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = N \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_s = G$ é uma série subnormal da forma $(A.1)$, ou seja, G é solúvel. ♦

Proposição A.2 *Sejam G um grupo solúvel e $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ uma série subnormal onde todos os grupos quocientes $\frac{G_{i+1}}{G_i}$ são abelianos. Então $G^{(i)} \subseteq G_{n-i}$, para todo i.*

Prova: Provaremos por indução sobre i.

Se $i = 0$, então $G^{(0)} = G = G_n$. Suponha, por indução, que $G^{(i)} \subseteq G_{n-i}$. Como $\frac{G_{n-i}}{G_{n-i+1}}$ é um grupo abeliano, segue que $G'_{n-i} \subseteq G_{n-i+1}$. Por outro lado, $G^{(i)} \subseteq G_{n-i}$ por indução. Isto implica $G^{(i+1)} \subseteq G'_{n-i}$. Donde, $G^{(i+1)} \subseteq G_{n-i+1}$.

Em particular, para $i = n$, temos que $G^{(n)} \subseteq G_0 = 1$, ou seja, $G^{(n)} = 1$. ♦

Corolário A.1 *G é um grupo solúvel se, e somente se, existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$.*

Lema A.1 *Suponha que $G = HA$, onde $H \leq G, A \trianglelefteq G$ e A abeliano. Então H é maximal em G se, e somente se, $\frac{A}{H \cap A}$ é um subgrupo normal minimal de $\frac{G}{H \cap A}$.*

Prova: Temos que $H \cap A \trianglelefteq H$ (pois $A \trianglelefteq G$) e $H \cap A \trianglelefteq A$ pois A é abeliano. Como $G = HA$, segue que $H \cap A \trianglelefteq G$.

Suponha que H é um subgrupo maximal de G. Seja $\frac{K}{H\cap A} \trianglelefteq \frac{G}{H\cap A}$ tal que $\frac{K}{H\cap A} \leq \frac{A}{H\cap A}$. Então, $H \leq HK \leq G$ o que implica $H = HK$ ou $HK = G$. Se $HK = H$, temos $K \leq H$ o que acarreta $K \leq H \cap A$, e portanto, $K = H \cap A$. Se $HK = G$, temos $A = A \cap G = A \cap (HK) = K(H \cap A) = K$, donde $K = A$. Deste modo, concluímos que $\frac{A}{H\cap A}$ é um subgrupo normal minimal de $\frac{G}{H\cap A}$.

Reciprocamente, suponha que $\frac{A}{H\cap A}$ é um subgrupo normal minimal de $\frac{G}{H\cap A}$. Seja $H \leq L \leq G$. Logo, $G = LA$ e $L \cap A \trianglelefteq G$, o que implica $\frac{L\cap A}{H\cap A} \trianglelefteq \frac{G}{H\cap A}$. Donde, $\frac{L\cap A}{H\cap A} = \bar{1}$ ou $\frac{L\cap A}{H\cap A} = \frac{A}{H\cap A}$, isto é, $L \cap A = H \cap A$ ou $L \cap A = A$. Se $L \cap A = A$, temos $A \leq L$ o que acarreta $G = L$. Se $L \cap A = H \cap A$, então $L = L \cap G = L \cap (HA) = H(L \cap A) = H(H \cap A) = H$, ou seja, $L = H$. Portanto, concluímos que H é maximal em G. ♦

Dizemos que um grupo G é n-abeliano elementar, se G é um grupo abeliano e, além disso, todo elemento de G tem ordem n.

Teorema A.1 *Seja G um grupo finito e solúvel. Então:*

(i) todo fator de composição [1] *de G tem ordem prima;*

(ii) todo fator principal de G é p-abeliano elementar (p primo).

(iii) todo maximal de G tem índice em G igual a potência de um algum primo p.

Prova: (i) Basta mostrar que todo grupo solúvel simples N tem ordem prima. Com efeito, temos $N' \trianglelefteq N$ o que implica $N' = 1$ ou $N' = N$. Como N é solúvel, temos $N' \neq N$. Donde, $N' = 1$, ou seja, N é abeliano. Seja $x \in N, x \neq 1$. Então $\langle x\rangle \trianglelefteq N$. Sendo N simples, concluímos que $\langle x\rangle = N$ e $o(x) = p$, com p primo.

(ii) Seja N um subgrupo normal minimal de G. Temos que $N' \overset{\trianglelefteq}{\text{car}} N \trianglelefteq G$, implicando que $N' \trianglelefteq G$, conseqüentemente, $N' = 1$ (i.e., N é abeliano). Sejam p um número primo e $N[p] = \{x \in N\,;\, o(x) = p\}$. Então $N[p] \overset{\trianglelefteq}{\text{car}} N$, o que implica $N[p] \trianglelefteq G$. Assim, $N[p] = 1$ ou $N[p] = N$. Como G é finito, segue que $N[p] = N$, donde N é p-abeliano elementar. .

(iii) Provaremos por indução sobre o comprimento derivado n. Se $G' = 1$, temos G abeliano. Logo M é um maximal normal em G, conseqüentemente, temos $|G : M| = p$. Suponha o resultado válido para comprimento derivado igual a $n > 1$.

[1] Dizemos que $\frac{H}{K}$ é um fator de composição de G, se H é subnormal, $K \trianglelefteq H$ e $\frac{H}{K}$ é um subgrupo simples.

Temos que $G^{(n-1)} \subseteq M$ ou $G^{(n-1)} \nsubseteq M$. Se $G^{(n-1)} \subseteq M$, temos que $\frac{M}{G^{(n-1)}}$ é um subrupo maximal de $\frac{G}{G^{(n-1)}}$. Logo, por indução, $p^r = \left|\frac{G}{G^{(n-1)}} : \frac{M}{G^{(n-1)}}\right| = |G : M|$. Se $G^{(n-1)} \nsubseteq M$, segue que $G = MG^{(n-1)}$. Temos que $[G^{(n-1)} : G^{(n-1)}] = G^n = 1$. Donde, G^{n-1} é abeliano. Ademais, temos $G^{(n-1)} \trianglelefteq G$ e $\frac{G^{(n-1)}}{M \cap G^{(n-1)}}$ é um subgrupo normal minimal de $\frac{G}{M \cap G^{(n-1)}}$. Do item (ii), concluímos que

$$|G^{(n-1)} : M \cap G^{(n-1)}| = p^r \quad ou \quad |G^{(n-1)} : M \cap G^{(n-1)}| = \infty.$$

Porém, $|G^{(n-1)} : M \cap G^{(n-1)}| = |MG^{(n-1)} : M| = |G : M|$. Portanto, $|G : M| = p^r$. ♦

A.2 Grupos Supersolúveis

Definição A.2 *Um grupo G é supersolúvel, se existe uma série normal*

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G, \tag{A.2}$$

onde $G_i \trianglelefteq G$ e todos os grupos quocientes $\frac{G_{i+1}}{G_i}$ são cíclicos.

Observe que todo grupo supersolúvel é solúvel. Mas a recíproca não é válida, por exemplo, o grupo alternado A_4 é solúvel pois $1 \lhd K \lhd A_4$, onde K é o grupo de Klein, é uma série subnormal da forma (A.1). Porém, A_4 é supersolúvel, pois A_4 não possui subgrupo cíclico normal.

Proposição A.3 *Seja G um grupo supersolúvel. Então:*

(i) todo subgrupo de G é supersolúvel;

(ii) se $N \trianglelefteq G$, então $\frac{G}{N}$ é supersolúvel;

(iii) se N é um subgrupo, normal, cíclico de G, com N e $\frac{G}{N}$ solúveis; então G é solúvel.

Prova: (i) Seja H um subgrupo qualquer de G. Como G é supersolúvel, seja $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ uma série normal onde $\frac{G_{i+1}}{G_i}$ é cíclico para todo i. Considere $H_i = H \cap G_i$. Então:

$$\frac{H_{i+1}}{H_i} = \frac{H \cap G_{i+1}}{H \cap G_i} = \frac{H \cap G_{i+1}}{(H \cap G_{i+1}) \cap G_i} \simeq \frac{G_i(H \cap G_{i+1})}{G_i} \leq \frac{G_{i+1}}{G_i},$$

implicando que $\frac{H_{i+1}}{H_i}$ é cíclico. Além disso, temos $H_i = H \cap G_i \trianglelefteq H$ (pois $G_i \trianglelefteq G$) para todo i. Desse modo, H é supersolúvel.

(ii) Considere $\overline{N}_i = \frac{NG_i}{N}$. Temos que $\overline{N}_i \trianglelefteq \frac{G}{N}$ e $\overline{N}_i \leq \overline{N}_{i+1}$ para todo i. Daí

$$\frac{\overline{N}_{i+1}}{\overline{N}_i} = \frac{\frac{NG_{i+1}}{N}}{\frac{NG_i}{N}} \simeq \frac{NG_{i+1}}{NG_i} = \frac{(NG_i)G_{i+1}}{NG_i} \simeq \frac{G_{i+1}}{(NG_i) \cap G_{i+1}} \simeq \frac{\frac{Gi+1}{G_i}}{\frac{(NG_i) \cap G_{i+1}}{G_i}},$$

implicando que $\frac{\overline{N}_{i+1}}{\overline{N}_i}$ é cíclico. Portanto, $\frac{G}{N}$ é supersolúvel.

(iii) Sendo $\frac{G}{N}$ supersolúvel, temos $\bar{1} \leq \frac{N_1}{N} \leq \ldots \leq \frac{N_s}{N} = \frac{G}{N}$, onde $\frac{N_i}{N} \trianglelefteq \frac{G}{N}$ e $\frac{\frac{N_{i+1}}{N}}{\frac{N_i}{N}}$ é cíclico para todo i. Temos que $N_i \trianglelefteq G$ e, além disso,

$$\frac{\frac{N_{i+1}}{N}}{\frac{N_i}{N}} \simeq \frac{N_{i+1}}{N_i}.$$

Logo, $\frac{N_{i+1}}{N_i}$ é cíclico. Assim, $1 \leq N \leq N_1 \leq N_2 \leq \ldots \leq N_s = G$ é uma série normal de G onde todos os fatores são cíclicos, isto é, G é supersolúvel. ♦

Proposição A.4 *Seja G um grupo supersolúvel finito. Então, todo fator principal de G tem ordem prima e todo subgrupo maximal de G tem índice primo.*

Prova: Seja N um subgrupo normal minimal de G. Considere $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$, onde $G_i \trianglelefteq G$ e $\frac{G_{i+1}}{G_i}$ é cíclico. Seja k o menor inteiro tal que $G_k \cap N \neq 1$. Isto implica que $G_{k-1} \cap N = 1$. Ademais, $G_k \cap N \trianglelefteq G$ e $1 \neq G_k \cap N \leq N$ o que acarreta $G_k \cap N = N$. Donde, $N \leq G_k$. Daí,

$$N \simeq \frac{NG_{k-1}}{G_{k-1}} \leq \frac{G_k}{G_{k-1}} \quad \Rightarrow \quad N \text{ é cíclico.}$$

Sendo N é um subgrupo normal minimal de G, concluímos que $|N| = p$, para algum primo p.

Agora, considere M um subgrupo maximal de G. Provemos por indução sobre o comprimento derivado r. Se $G' = 1$, temos G abeliano. Logo M é um maximal normal em G, donde o índice de M em G é primo. Suponha o resultado válido para comprimento derivado $r > 1$. Se $G^{(r-1)} \subseteq M$, temos que $\frac{M}{G^{(r-1)}}$ é um subgrupo maximal de $\frac{G}{G^{(r-1)}}$. Por indução, concluímos que

$$p = \left| \frac{G}{G^{(r-1)}} : \frac{M}{G^{(r-1)}} \right| = |G : M|.$$

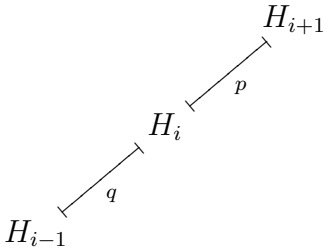
Se $G^{(r-1)} \not\subseteq M$, segue que $G = MG^{(r-1)}$. Da hipótese de indução e do Lema A.1, segue que $|G : M| = p$. ♦

Teorema A.2 (Zappa) *Seja G um grupo supersolúvel. Então existe uma série normal $1 = G_0 < G_1 < G_2 < \ldots < G_n = G$, onde podemos colocar:*

$$\left|\frac{G_1}{G_0}\right| = p_1 \geq \left|\frac{G_2}{G_1}\right| = p_2 \geq \ldots \geq \left|\frac{G_s}{G_{s-1}}\right| = p_s \ (p_i > 2);$$
$$\frac{G_{s+1}}{G_s} \simeq \frac{G_{s+2}}{G_{s+1}} \simeq \ldots \simeq \frac{G_t}{G_{t-1}} \simeq C_\infty \quad e$$
$$\frac{G_{t+1}}{G_t} \simeq \frac{G_{t+2}}{G_{t+1}} \simeq \ldots \simeq \frac{G_n}{G_{n-1}} \simeq C_2.$$

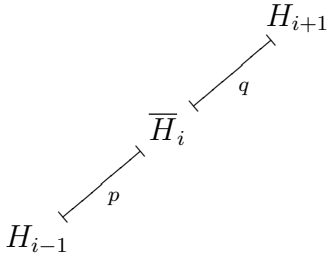
Prova: Como G é supersolúvel, seja $1 = G_0 < G_1 < \ldots < G_n = G$ uma série normal onde todos os fatores são cíclicos. Refinando esta série, obtemos $1 = H_0 < H_1 < \ldots < H_m = G$ outra série normal onde os grupos quocientes $\frac{H_{i+1}}{H_i}$ ou tem ordem prima, ou tem ordem infinita.

caso 1. $\frac{H_{i+1}}{H_i} \simeq C_p$ e $\frac{H_i}{H_{i-1}} \simeq C_q$, com $q < p$.

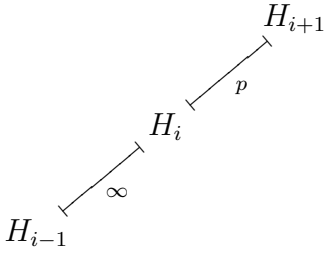


Neste caso, temos $\left|\frac{H_{i+1}}{H_{i-1}}\right| = pq$. Logo, $\frac{H_i}{H_{i-1}}$ é um q-subgrupo normal de Sylow de $\frac{H_{i+1}}{H_{i-1}}$. Seja $\frac{\overline{H}_i}{H_{i-1}}$ um p-subgrupo de Sylow de $\frac{H_{i+1}}{H_{i-1}}$. Como $p > q$, segue que $\frac{\overline{H}_i}{H_{i-1}} \trianglelefteq \frac{H_{i+1}}{H_{i-1}}$ o que implica $\frac{\overline{H}_i}{H_{i-1}} \underset{\text{car}}{\trianglelefteq} \frac{H_{i+1}}{H_{i-1}}$. Do fato de $\frac{H_{i+1}}{H_{i-1}} \trianglelefteq \frac{G}{H_{i-1}}$, concluímos que $\frac{\overline{H}_i}{H_{i-1}} \trianglelefteq \frac{G}{H_{i-1}}$. Donde, $\overline{H}_i \trianglelefteq G$.

CONCLUSÃO: Substitua H_i por $\overline{H}_i$.



caso 2. $\frac{H_{i+1}}{H_i} \simeq C_p$ e $\frac{H_i}{H_{i-1}} \simeq C_\infty$, $p > 2$.



Neste caso, $\mathrm{Aut}\left(\frac{H_i}{H_{i-1}}\right) \simeq C_2$ o que implica $\left|\mathrm{Aut}\left(\frac{H_i}{H_{i-1}}\right)\right| = 2$. Então

$$\left|\frac{\frac{H_{i+1}}{H_{i-1}}}{C_{\frac{H_{i+1}}{H_{i-1}}}\left(\frac{H_i}{H_{i-1}}\right)}\right| \leq 2. \tag{A.3}$$

Como $\frac{H_i}{H_{i-1}}$ é cíclico, e portanto, abeliano; segue que $\frac{H_i}{H_{i-1}} \leq C_{\frac{H_{i+1}}{H_{i-1}}}\left(\frac{H_i}{H_{i-1}}\right)$. Por outro lado, $\left|\frac{H_{i+1}}{H_{i-1}} : \frac{H_i}{H_{i-1}}\right| = |H_{i+1} : H_i| = p$, donde:

$$\frac{H_i}{H_{i-1}} = C_{\frac{H_{i+1}}{H_{i-1}}}\left(\frac{H_i}{H_{i-1}}\right) \quad \text{ou} \quad \frac{H_{i+1}}{H_{i-1}} = C_{\frac{H_{i+1}}{H_{i-1}}}\left(\frac{H_i}{H_{i-1}}\right).$$

Se $\frac{H_i}{H_{i-1}} = C_{\frac{H_{i+1}}{H_{i-1}}}\left(\frac{H_i}{H_{i-1}}\right)$, por (A.3), teríamos $2 < p \leq 2$, o que é absurdo. Portanto, $\frac{H_{i+1}}{H_{i-1}} = C_{\frac{H_{i+1}}{H_{i-1}}}\left(\frac{H_i}{H_{i-1}}\right)$ implicando que $\frac{H_{i+1}}{H_{i-1}} \leq Z\left(\frac{H_{i+1}}{H_{i-1}}\right)$, donde concluímos que $\frac{H_{i+1}}{H_{i-1}}$ é abeliano. Se $\frac{H_{i+1}}{H_{i-1}}$ for cíclico, apenas retire H_i da série ! Caso contrário, temos $\frac{H_i}{H_{i-1}} = \langle xH_{i-1}\rangle$ com $o(xH_{i-1}) = \infty$ e $\frac{H_{i+1}}{H_i} = \langle yH_i\rangle$ com $o(yH_i) = p$, i.e., $y^p \in H_i$. Daí $H_{i+1} = \langle x, y, H_{i-1}\rangle$, o que implica $\frac{H_{i+1}}{H_{i-1}} = \langle xH_{i-1}\rangle\langle yH_i\rangle$, onde $y^p \in H_i$.

Estamos com a seguinte situação: $K = \langle\alpha\rangle\langle\beta\rangle$, com K abeliano, $o(\alpha) = \infty$ e $|K : \langle\alpha\rangle| = p$. Temos que $\beta^p \in \langle\alpha\rangle \cap \langle\beta\rangle$ e que $|\langle\beta\rangle : \langle\beta^p\rangle| = p$, isto implica que $\langle\alpha\rangle \cap \langle\beta\rangle = \langle\beta^p\rangle$. Vamos mostrar que o conjunto $\{g \in K\,;\, o(g) = p\}$ é não-vazio. Com efeito, temos duas possibilidades; $|K : \langle\beta\rangle| = \infty$ ou $|K : \langle\beta\rangle| < \infty$. Se $|K : \langle\beta\rangle| = \infty$, então $\langle\alpha\rangle \cap \langle\beta\rangle = 1$, donde $\beta^p = 1$. Se $|K : \langle\beta\rangle| = r$, temos que $\alpha^r \in \langle\alpha\rangle \cap \langle\beta\rangle$. Como $|\langle\alpha\rangle : \langle\alpha^r\rangle| = r$, segue que $\langle\alpha^r\rangle = \langle\alpha\rangle \cap \langle\beta\rangle = \langle\beta^p\rangle$. Daí, $\alpha^r = \beta^{ps}$ e $\beta^p = \alpha^{rt}$ o que implica $r = rst$, isto é, $s = 1$ e $t = 1$. Donde, $\alpha^r = \beta^p$. Se $p \mid r$, então $r = pr'$ implicando $(\alpha^{r'}\beta^{-1})^p = 1$. Caso contrário, existem inteiros u, v tais que $up + vr = 1$. Logo,

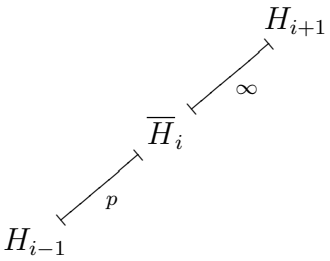
$$\alpha = \alpha^{up+vr} = \alpha^{up}.\alpha^{br} = (\alpha^u\beta^v)^p \quad \text{e} \quad \beta = \beta^{up+vr} = \beta^{up}.\beta^{vr} = (\alpha^u\beta^v)^r.$$

Desse modo, teríamos G cíclico, o que não ocorre. Assim, segue a afirmação.

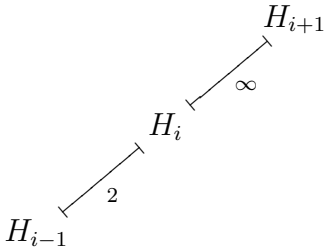
Seja $N = \{g \in K\,;\, o(g) = p\} \neq \varnothing$. Sabemos que $N \overset{\text{car}}{\lhd} K$. Além disso, temos que $\langle\alpha\rangle \cap N = 1$. Logo, $K = N\langle\alpha\rangle$ o que implica $p = \left|\frac{K}{\langle\alpha\rangle}\right| = |N|$, donde $|N| = p$.

Portanto, concluímos que $\frac{H_{i+1}}{H_{i-1}} \simeq C_p \times C_\infty$ e que existe um subgrupo $\frac{\overline{H}_i}{H_{i-1}}$ tal que $\frac{\overline{H}_i}{H_{i-1}} \overset{\text{car}}{\lhd} \frac{H_{i+1}}{H_{i-1}}$ e $\left|\frac{\overline{H}_i}{H_{i-1}}\right| = p$.

CONCLUSÃO: Substitua H_i por $\overline{H}_i$.

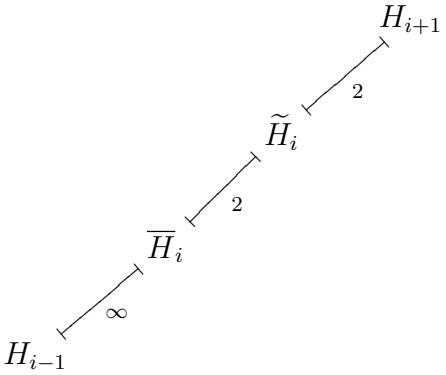


caso 3. $\frac{H_{i+1}}{H_{i-1}} \simeq C_\infty$ e $\frac{H_i}{H_{i-1}} \simeq C_2$.



Neste caso, Aut $\left(\frac{H_i}{H_{i-1}}\right)$ é trivial, e portanto, $\frac{H_{i+1}}{H_{i-1}} = C_{\frac{H_{i+1}}{H_{i-1}}}\left(\frac{H_i}{H_{i-1}}\right)$ o que implica $\frac{H_{i+1}}{H_{i-1}} \subseteq Z\left(\frac{H_{i+1}}{H_{i-1}}\right)$. Logo, $\frac{H_{i+1}}{H_{i-1}}$ é abeliano. Se $\frac{H_{i+1}}{H_{i-1}}$ for cíclico, apenas retire H_i da série. Dessa modo, considere $\frac{H_{i+1}}{H_{i-1}}$ não-cíclico.

Temos a seguinte situação: $K = \langle\alpha\rangle\langle\beta\rangle$, com K abeliano, $o(\alpha) = 2$ e $o(\beta) = \infty$. Como no **caso 2**, temos que $K \simeq C_2 \times C_\infty$. Considere $1 \neq K^2 = \{g^2\,;\, g \in K\}$. Logo, $K^2 \overset{\triangleleft}{}_{\text{car}}\, K$ e, além disso, $K^2 \subseteq \langle\beta\rangle$. Ou seja, $\frac{\overline{H}_i}{H_{i-1}} = K^2 \overset{\triangleleft}{}_{\text{car}}\, K = \frac{H_{i+1}}{H_{i-1}}$. Como $\frac{H_{i+1}}{H_{i-1}} \trianglelefteq \frac{G}{H_{i-1}}$, segue que $\overline{H}_i \trianglelefteq G$. Ademais, $|\langle\beta\rangle : K^2| = 2$ o que implica $|K : K^2| = |K : \langle\beta\rangle||\langle\beta\rangle : K^2| = 2.2 = 4$. Donde, $\left|\frac{H_{i+1}}{H_{i-1}} : \frac{\overline{H}_i}{H_{i-1}}\right| = |K : K^2| = 4$, e portanto, $|H_{i+1} : \overline{H}_i| = 4$.



CONCLUSÃO: Substitua H_i por $\overline{H}_i$ e acrescente, entre $\overline{H}_i$ e H_{i+1}, o subgrupo $\widetilde{H}_i$ para o qual $\frac{\widetilde{H}_i}{\overline{H}_i}$ é um subgrupo normal minimal de $\frac{H_{i+1}}{\overline{H}_i}$. ♦

A.3 Grupos Nilpotentes

Definição A.3 *Dizemos que um grupo G é nilpotente, se existe uma série central*

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G. \tag{A.4}$$

Isto é, $G_i \trianglelefteq G$ e $\frac{G_{i+1}}{G_i} \subseteq Z\left(\frac{G}{G_i}\right)$ (ou, equivalentemente, $[G_{i+1}, G] \subseteq G_i$).

Observe que todo grupo nilpotente é solúvel. Porém, a recíproca não é válida, por exemplo, o grupo S_3 é solúvel (pois $1 \lhd A_3 \lhd S_3$) e não é nilpotente, pois $Z(S_3)$ é trivial.

Proposição A.5 *Seja G um grupo nilpotente. Então:*

(i) todo subgrupo de G é nilpotente;

(ii) se $N \trianglelefteq G$, então $\frac{G}{N}$ é nilpotente;

(iii) se $N \trianglelefteq G$, com $N \subseteq Z(G)$ e $\frac{G}{N}$ nilpotente, então G é nilpotente.

Prova: (i) Sejam $H \leq G$ e $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ uma série central de G. Considere $H_i = G_i \cap H$. Como $G_i \trianglelefteq G$, segue que $H_i = G_i \cap H \trianglelefteq H$. Devemos mostrar que $[H_{i+1}, H] \leq H_i$. Com efeito, temos $[H_{i+1}, H] = [G_{i+1} \cap H, H] \leq [H, H] \leq H$ e $[H_{i+1}, H] = [G_{i+1} \cap H, H] \leq [G_{i+1}, H] \leq [G_{i+1}, G] \leq G_i$ o que implica $[H_{i+1}, H] \leq G_i \cap H = H_i$. Donde, H é nilpotente.

(ii) Seja $N \trianglelefteq G$. Considere $H_i = \frac{NG_i}{N}$. Logo, $H_i = \frac{NG_i}{N} \trianglelefteq \frac{G}{N}$. Além disso,

$$\begin{aligned}\left[H_{i+1}, \frac{G}{N}\right] &= \left[\frac{NG_{i+1}}{N}, \frac{G}{N}\right] = \frac{[NG_{i+1}, G]N}{N} = \\ &= \frac{[N, G][G_{i+1}, G]N}{N} \leq \frac{[G_{i+1}, G]N}{N} \leq \frac{NG_i}{N} = H_i.\end{aligned}$$

Logo, $\frac{G}{N}$ é nilpotente.

(iii) Seja $1 = \frac{N}{N} \leq \frac{N_1}{N} \leq \ldots \leq \frac{N_s}{N} = \frac{G}{N}$ uma série central de $\frac{G}{N}$. Como $\frac{N_i}{N} \trianglelefteq \frac{G}{N}$, temos que $N_i \trianglelefteq G$. Além disso,

$$\left[\frac{N_{i+1}}{N}, \frac{G}{N}\right] \leq \frac{N_i}{N} \iff \frac{[N_{i+1}, G]N}{N} \leq \frac{N_i}{N} \iff [N_{i+1}, G]N \leq N_i.$$

Do fato de $N \leq N_i$, segue que $[N_{i+1}, G] \leq N_i$. Desse modo, como $N \leq Z(G)$, temos que $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ é uma série central de G, e portanto, G é nilpotente. ♦

Exemplo 8 *Todo p-grupo é nilpotente, onde p é um número primo.*

Seja G um grupo com ordem igual a $|G| = p^n$. Como G é um p-grupo, $Z(G)$ é não-trivial. Logo, $\frac{G}{Z(G)}$ é nilpotente. Da Proposição A.5, item (iii), concluímos que G é nilpotente.

Proposição A.6 *Sejam G um grupo nilpotente e $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ uma série central. Então:*

(i) $\gamma_i(G) \subseteq G_{n-i+1}$, para todo $i \geq 1$;

(ii) $G_i \subseteq Z_i(G)$, para todo $i \geq 0$.

Em particular, $\gamma_n(G) = 1$ e $Z_n(G) = G$. Em outras palavras, G é nilpotente se, e somente se, existe $n \in \mathbb{N}$ tal que $\gamma_n(G) = 1$ e $Z_n(G) = G$.

Prova: Provaremos por indução sobre i.

(i) Se $i = 1$, temos $\gamma_1(G) = G = G_n$. Suponha, por indução, que $\gamma_i(G) = G_{n-i+1}$. Como $[G_{n-i+1}, G] \subseteq G_{n-i}$, obtemos $\gamma_{i+1}(G) = [\gamma_i(G), G] \subseteq [G_{n-i+1}, G] \subseteq G_{n-i}$.

(ii) Se $i = 0$, então $G_0 = 1 = Z_0(G)$. Suponha, por indução, que $G_i \subseteq Z_i(G)$. Temos $[G_{i+1}, G] \subseteq G_i$ implicando, por indução, que $[G_{i+1}, G] \subseteq Z_i(G)$. Daí

$$[G_{i+1}Z_i(G), G] = [G_{i+1}, G][Z_i(G), G] \leq G_iZ_i(G) = Z_i(G).$$

Donde, $\frac{G_{i+1}Z_i(G)}{Z_i(G)} \leq Z\left(\frac{G}{Z_i(G)}\right) = \frac{Z_{i+1}(G)}{Z_i(G)}$ o que acarreta $G_{i+1}Z_i(G) \subseteq Z_{i+1}(G)$, e portanto, $G_{i+1} \subseteq Z_{i+1}(G)$. ♦

Proposição A.7 *Se G é nilpotente e N é um subgrupo normal, não-trivial, de G. Então $Z(G) \cap N$ é não-trivial.*

Prova: Como G é nilpotente, existe n inteiro tal que $Z_n(G) = G$. Seja i o menor inteiro para o qual $Z_i(G) \cap N \neq 1$. Sabemos que $[Z_i(G), G] \leq Z_{i-1}(G)$ e que $[N, G] \leq N$ (pois $N \trianglelefteq G$). Daí, $[Z_i(G) \cap N, G] \leq Z_{i-1}(G) \cap N = 1$ o que implica $Z_i(G) \cap N \subseteq Z(G)$. Donde, concluímos que $Z(G) \cap N$ é não-trivial. ♦

Teorema A.3 (Caracterização dos Grupos Nilpotentes Finitos) *Seja G um grupo finito. São equivalentes:*

(i) G nilpotente;

(ii) todo subgrupo de G é subnormal;

(iii) se $H < G$, então $H < N_G(H)$;

(iv) G é o produto direto de seus subgrupos de Sylow.

Em particular, todo subgrupo maximal de um grupo nilpotente G é normal em G.

Prova: $(i) \Rightarrow (ii)$: Sejam $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ uma série central de G e $H \leq G$. Afirmamos que $HG_i \trianglelefteq HG_{i+1}$. De fato, $(HG_i)^{HG_{i+1}} = H^{G_{i+1}}G_i$. Sejam $h \in H$ e $x \in G_{i+1}$. Daí, $[h, x] = h^{-1}x^{-1}hx = h^{-1}h^x \in G_i$ o que implica $h^x \in HG_i$. Donde, $(HG_i)^{HG_{i+1}} \subseteq HG_i$, o que prova a afirmação.

$(ii) \Rightarrow (iii)$: Seja H um subgrupo próprio de G. Por hipótese, temos H subnormal, isto é, $H \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$. Logo, $H \subsetneq H_1 \subseteq N_G(H)$.

$(iii) \Rightarrow (iv)$: Seja $P \in Syl_p(G)$ e $H = N_G(P)$. Logo, $N_G(H) = H$. Do item (iii), concluímos que $H = G$. Donde, $N_G(P) = H = G$, e portanto, P é normal em G. Desse modo, G é o produto direto de seus subgrupos de Sylow.

$(iv) \Rightarrow (i)$: Seja $G = P_1 \times \ldots \times P_r$, onde $P_i \in Syl_{p_i}(G)$. Como cada P_i é nilpotente, temos $\gamma_{n_i}(P_i) = 1$. Considere $n = \max\{n_1, \ldots, n_r\}$. Daí,

$$\gamma_n(G) = \gamma_n(P_1 \times \ldots \times P_r) = \gamma_n(P_1) \times \ldots \times \gamma_n(P_r) = 1.$$

Portanto, G é nilpotente. ♦

Proposição A.8 *Seja G um grupo finito. Então $\Phi(G)$ é um grupo nilpotente.*

Prova: Seja $P \in Syl_p(\Phi(G))$. Como $\Phi(G) \trianglelefteq G$, pelo Argumento Frattini, segue que $G = \Phi(G)N_G(P) \Rightarrow G = N_G(P)$. Donde, P é normal em G, e em particular, $P \trianglelefteq \Phi(G)$. Do Teorema A.3, concluímos que $\Phi(G)$ é nilpotente. ♦

Proposição A.9 *G é um grupo nilpotente se, e somente se, $\frac{G}{\Phi(G)}$ é um grupo nilpotente.*

Prova: Se G é um grupo nilpotente, da Proposição A.5, item (ii), concluímos que $\frac{G}{\Phi(G)}$ é um grupo nilpotente. Reciprocamente, suponha que $\frac{G}{\Phi(G)}$ é nilpotente. Seja $P \in Syl_p(G)$. Logo, $\frac{P\Phi(G)}{\Phi(G)} \in Syl_p\left(\frac{G}{\Phi(G)}\right)$ o que implica $\frac{P\Phi(G)}{\Phi(G)} \trianglelefteq \frac{G}{\Phi(G)}$. Donde, $P\Phi(G) \trianglelefteq G$. Por outro lado, temos $P \in Syl_p(P\Phi(G))$ implicando que $P \overset{\trianglelefteq}{\text{car}} P\Phi(G)$, e portanto, P é normal em G. Desse modo, G é o produto diretos de seus subgrupos de Sylow, isto é, G é nilpotente. ♦

Proposição A.10 *Seja G um grupo solúvel finito. Se todo fator principal de G é Frattini ou central, então G é nilpotente.*

Prova: Provemos por indução sobre a ordem $|G|$.

Seja N um subgrupo normal minimal de G. Por hipótese, $N \subseteq Z(G)$ ou $N \subseteq \Phi(G)$. Considere $\frac{\overline{H}}{\overline{K}}$ um fator principal de $\frac{G}{N}$. Temos que $\overline{H} = \frac{H}{N}$ e $\overline{K} = \frac{K}{N}$. Além disso, $\overline{H} = \frac{H}{N} \trianglelefteq \frac{G}{N}$ e $\overline{K} = \frac{K}{N} \trianglelefteq \frac{G}{N}$ o que implica $H \trianglelefteq G$ e $K \trianglelefteq G$. Por outro lado,

$$\frac{\overline{H}}{\overline{K}} = \frac{\frac{H}{N}}{\frac{K}{N}} \simeq \frac{H}{K} \quad \text{e} \quad \frac{\frac{G}{N}}{\frac{K}{N}} \simeq \frac{G}{K},$$

ou seja, $\frac{H}{K}$ é um fator principal de G. Desse modo, concluímos que todo fator principal de $\frac{G}{N}$ é Frattini ou central. Logo, por indução, temos que $\frac{G}{N}$ é nilpotente.

Se $N \subseteq \Phi(G)$, temos $\frac{G}{\Phi(G)} \simeq \frac{\frac{G}{N}}{\frac{\Phi(G)}{N}}$ o que implica, pela Proposição A.5, item (ii), que $\frac{G}{\Phi(G)}$ é nilpotente. Da Proposição A.9, obtemos que G é nilpotente.

Se $N \subseteq Z(G)$, temos $\frac{G}{Z(G)} \simeq \frac{\frac{G}{N}}{\frac{Z(G)}{N}}$ acarretando, pela Proposição A.5, itens (ii) e (iii), que G é nilpotente. ♦

Proposição A.11 *Se G é um grupo nilpotente finito, então existe um subgrupo normal minimal de G com ordem p, para todo primo p que divide $|G|$.*

Prova: Seja $P \in Syl_p(G)$. Sendo G é nilpotente, temos $P \trianglelefteq G$. Considere $x \in Z(P)$, com $o(x) = p$ e $N = \langle x \rangle$. Como $[P, Q] = 1$ para todo $Q \in Syl_q(G)$, com $q \neq p$ e $[N, P] = 1$ (pois $N \subseteq Z(P)$), concluímos que $N \leq Z(G)$, e portanto, $N \trianglelefteq G$. Do fato de $|N| = p$, obtemos que N é um subgrupo normal minimal de G. ♦