UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

MESTRADO EM MATEMÁTICA

σ-COBERTURAS DE GRUPOS SOLÚVEIS FINITOS

Darlan Portela Veras

Fortaleza

2007

Darlan Portela Veras

σ-COBERTURAS DE GUPOS SOLÚVEIS FINITOS

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

Orientador: Prof. Dr. José Robério Rogério.

Fortaleza

2007

.

À minha terceira mãe, que está na casa de Deus, TIA LIDUÍNA.

Agradecimentos

A Deus, antes de tudo, por Ele ter colocado em minha vida, as pessoas certas, nas horas certas, e que levaram-me a concluir este mestrado.

Ao meu orientador, professor Robério, por sua paciência, compreensão e por mostrar-nos que a simplicidade é a grande virtude de um vencedor. Obrigado professor.

A todos os amigos verdadeiros que Deus colocou em minha vida. Cada um, à sua maneira, incentivou-me a jamais desistir. A todos os cachorros vermelhos, os amigos da Universidade, da Comunidade de São Vicente, o meu muito obrigado.

À minha irmã Mônica, meu cunhado Samuel e os sobrinhos Nathan e Letícia. Pela amizade, os divertimentos na Iparana e suas orações, muito obrigado MONQUINHA.

Ao meu irmão Cristiano, minha cunhada Milena e o primeiro bebê da família. Pelas brincadeiras, pela amizade e suas orações, muito obrigado TETÉ.

Ao meu irmão Flávio, minha cunhada Mara e a sobrinha Ana Beatriz. Pelo exemplo de fé e perseverança, e por suas orações, muito obrigado FLAVIM.

À minha esposa Michelle e o nosso primeiro filho, Marcus Vinícius . Pelo apoio incondicional nos momentos mais difíceis, por seu amor e por todas as orações, muito obrigado MIMI.

Ao meu pai, Seu Airton, minha vozinha Maria e as minhas três mães, Tia Etinha, Tia Liduína(que está na casa de Deus) e Dona Beta. Pela confiança irrestrita, pelas palavras que nunca sairão da minha cabeça - Você vai conseguir. Tenha fé! - Por todas as orações, muitíssimo obrigado ZÉ de AIRTON e MÃE ZUCA.

Ao CNPq, pelo apoio financeiro.

.

"Veja, não diga que a canção está perdida. Tenha fé em Deus, tenha fé na vida. Tente outra vez".

(Tente outra vez - Raul Seixas)

.

Resumo

Estuda-se as coberturas de grupos finitos por subgrupos próprios. Mostramos alguns resultados sobre coberturas de grupos solúveis por subgrupos maximais ordenados pelos índices (σ-coberturas). O resultado mais importante, relata que todo grupo solúvel finito admite uma σ-cobertura normal ou conjugada.

Sumário

Introdução

Para um grupo finito G, denotamos por $\sigma(G)$ o menor inteiro n tal que G pode ser escrito como a união de n subgrupos próprios. Neste caso, G é chamado de n-soma e a união dos subgrupos é uma cobertura de G. Em 1994, J. H. E. Cohn, divulga o seu trabalho sobre os grupos n-soma. Neste, ele apresenta, entre outras coisas, os $\sigma(G)$ de grupos nilpotentes e de grupos específicos. Em 1997, M. J. Tomkinsom apresenta um resultado valiosíssimo sobre grupos n-soma. Neste, o autor mostra que o $\sigma(G)$ de um grupo solúvel não-nilpotente finito, é igual a ordem de um fator principal específico, acrescentado de uma unidade.

Em 2005, os iranianos Alireza Jamali e Hamid Mousavi divulgam mais contribuições sobre os grupos n-soma. Em específico, os grupos solúveis. Eles definem a σ-cobertura de G como a união, ordenada pelos índices de forma não-decrescente, de subgrupos maximais. Estudam os índices dos maximais em G e mostram que todo grupo solúvel possui uma σ-cobertura de uma das duas formas: normal ou conjugada.

O nosso trabalho faz um resumo dos três artigos citados. Iniciamos o primeiro capítulo com os resultados que constituem a base da Álgebra Abstrata. Aqui, definimos os subgrupos característicos de G, bem como o normalizador e o centralizador de um subgrupo H em G. Enunciamos os teoremas mais famosos. Entre eles, o teorema de Sylow e os teoremas de isomorfismos. Na segunda seção, estudamos os grupos que possuem uma série subnormal

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$$

onde $\dfrac{G_i}{G_{i-1}}$ é abeliano para todo $i = 1, 2, ..., n$. Estamos falando dos grupos Solúveis.Veremos que todo fator principal de um grupo solúvel G tem ordem potência de um primo. Encerramos a seção definindo grupo supersolúvel e estudando alguns resultados sobre o mesmo. Por último, estudaremos os grupos Nilpotentes, isto é, os que possuem uma série central.

Também definiremos o subgrupo de Frattini $\Phi(G)$ de G que é a interseção de todos os maximais de G. Mostraremos que $\Phi(G)$ é nilpotente se G for finito. Finalizamos o capítulo caracterizando os grupos nilpotentes finitos.

O núcleo normal de um subgrupo H em G, denotado por H_G, é definido como a interseção de todos os conjugados de H em G. No capítulo 2 fazemos uma abordagem sobre os grupos finitos que possuem um subgrupo maximal M tal que $M_G = 1$. Esta é a definição de grupo Primitivo. Veremos com o teorema de Ore-Baer que se um grupo primitivo G tem um subgrupo normal minimal, então este é o único subgrupo normal minimal em G, é abeliano elementar, ele é seu próprio centralizador e este complementa o maximal, com núcleo trivial, em G. Como corolário, temos que dois subgrupos maximais conjugados de um grupo solúvel primitivo tem o mesmo núcleo normal em G.

Os grupos n-soma constituem o terceiro capítulo. Mostaremos que se $G = \bigcup_{l=1}^{n} H_l$, onde $n = \sigma(G)$ e cada H_l é um subgrupo próprio de G de índice i_l com $i_1 \leq i_2 \leq ... \leq i_n$, então $i_2 \leq n-1$. Mais ainda, se G é nilpotente e não-cíclico, então $\sigma(G) = p+1$, onde p é o menor primo tal que o p-subgrupo de Sylow de G é não-cíclico. Encerramos o capítulo com um teorema de muita importância para o nosso trabalho, que é o teorema de Tomkinson. Este, diz que se G é solúvel finito não-nilpotente e $\frac{H}{K}$ é um fator principal com ordem mínima entre os que tem mais de um complemento, então $\sigma(G) = |\frac{H}{K}| + 1$.

No último e mais importante capítulo, restringimos o nosso estudo aos grupos solúveis finitos. O resultado mais importante do nosso trabalho é o que diz que todo grupo solúvel finito com $\sigma(G) = n$ possui uma σ-cobertura onde ocorre uma das duas condições:

i) M_1 é normal de índice menor que $n-1$ e $M_2, ..., M_n$ são todos conjugados;

ii) Cada M_i é normal de índice n-1.

Uma σ-cobertura que satisfaz a condição **i)** é chamada σ-cobertura conjugada e a que satisfaz a condição **ii)** é uma σ-cobertura normal. Mostraremos que se G tem um subgrupo maximal não-normal de índice $\sigma(G) - 1$, então G tem uma σ-cobertura conjugada. Finalizamos o trabalho mostrando que se G é um grupo solúvel finito, então para qualquer subgrupo maximal não-normal M de índice $\sigma(G) - 1$, o grupo $\frac{M}{M_G}$ é cíclico em alguns casos.

Capítulo 1

Preliminares

Neste 1° capítulo do nosso trabalho falaremos sobre os "alicerces"da álgebra abstrata. Enunciaremos muitos resultados sem demonstrá-los, pois, vários deles são estudados em cursos de álgebra básica. Procuramos provar aqueles que possuem uma maior importância em nosso trabalho e aqueles que não são tão "comuns".

1.1 Resultados Básicos

A letra "G"para nós denotará sempre um grupo. Um subgrupo H de um grupo G será denotado por $H \leq G$. Se $H \neq G$, dizemos que H é um subgrupo próprio de G e denotamos por $H < G$. Escreveremos $|G|$ para denotarmos a ordem do grupo G e $|G : H|$ para denotarmos o índice do subgrupo H em G.

Em princípio, falaremos sobre grupos quaisquer. Mais na frente, restringiremos a grupos finitos, pois, estes estão no centro do nosso trabalho.

Vejamos alguns exemplos de grupos.

Exemplo 1 *a) Grupo simétrico de grau n.*

Seja $X = I_n$=$\{1, 2, ..., n\}$. *Chamamos de grupo simétrico (ou, grupo das permutações) de grau n, denotado por* S_n, *o grupo formado pelas aplicações bijetivas* $\varphi : X \to X$, *com* *a operação de composição de aplicações. Cada aplicação (permutação) é chamada de r-ciclo(r é o número de elementos envolvidos na permutção) e sempre pode ser escrita como um produto de 2-ciclos(transposições). Chamamos de permutação par, aquela que pode ser escrita por uma quantidade par de transposições. O subgrupo de S_n formado por todas as permutações pares é chamado de grupo alternado e é denotado por A_n. É fácil ver que $|S_n : A_n|$=2.*

b) Grupo Linear Geral.

Sejam F um corpo e $GL(n, F)$ o conjunto de todas as matrizes com entradas em F e com determinante diferente de zero. $GL(n, F)$ é um grupo com a operação de multiplicação de matrizes, chamado Grupo Linear Geral de grau n. Denotamos por $SL(n, F)$ o subgrupo de $GL(n, F)$ formado pelas matrizes com determinante 1.

c) Grupo das classes residuais módulo n.

Dado um inteiro positivo $n \geq 1$, denotamos por Z_n o grupo formado pelo conjunto $\{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, onde $\overline{r} = \{x \in Z | x \equiv r (mod\, n)\}$ para todo $0 \leq r \leq n-1$, e com a operação de adição $\overline{r}$+$\overline{s}$=$\overline{r+s}$. Z_n é um corpo se, e somente se, n for um número primo.

Nos exemplos acima, apenas em c) temos um grupo abeliano, isto é, seus elementos comutam. A ordem de um elemento $g \in G$ é o menor inteiro positivo n tal que g^n=1. Além disso, a ordem de todo elemento divide a ordem do grupo. O teorema que iremos enunciar a seguir relaciona a ordem de um grupo e as ordens de seus elementos.

Teorema 1.1 (Cauchy) *Se G é um grupo finito e p é um número primo dividindo a ordem de G, então G tem um elemento de ordem p.*

Um grupo abeliano G tal que cada elemento tem ordem p, onde p é primo, é dito p-abeliano elementar. Pelo teorema de Cauchy fica fácil perceber que todo grupo p-abeliano elementar tem ordem p^α, onde α é um inteiro positivo. Se a ordem de um grupo for potência de um primo p, dizemos que se trata de um p-grupo. Assim sendo, todo p-abeliano elementar é um p-grupo.

Temos vários teoremas que relacionam a ordem de G com a de seus subgrupos e os índices desses. Lembramos que um subgrupo H é normal em G se $H^g = \{g^{-1}hg | h \in H\} \subseteq H($ ou equivalentemente, $H^g = H)$ para todo $g \in G$. Denotamos, $H \trianglelefteq G$. Um exemplo trivial de subgrupo normal é dado pelo centro $Z(G) = \{g \in G | gh = hg$, para cada $h \in G\}$ de G. Claramente, G é abeliano se, e somente se, $G = Z(G)$.

Teorema 1.2 (Lagrange) *Sejam K e H subgrupos de G com $K \leq H \leq G$. Então $|G : K|$=$|G : H| \cdot |H : K|$.*

Lema 1.1 *Sejam H e K subgrupos de G. Então:*

a) $HK \leqslant G \Leftrightarrow HK = KH$.

b) Se $H \trianglelefteq G$, então $HK = KH$. Portanto, $HK \leqslant G$.

Teorema 1.3 (Do índice) *Sejam H e K subgrupos de G. Então:*

a) $|HK| \cdot |H \cap K| = |H| \cdot |K|$.

b) $|G : H \cap K| \leqslant |G : H|.|G : K|$. Ocorrendo a igualdade se $|G : H|$ e $|G : K|$ são primos entre si.

Dado um subconjunto S de um grupo G, o conjunto $\{a_1.a_2...a_n | n \in N, a_i \in S$ ou $a_i^{-1} \in S\}$ será denotado por $\langle S\rangle$. É fácil ver que $\langle S\rangle$ é um subgrupo de G. Mais ainda, $\langle S\rangle$ é o menor subgrupo de G que contém S (aqui, "menor" quer dizer que todo subgrupo de G que contém S contém $\langle S\rangle$). Se S for um conjunto unitário dizemos que $\langle S\rangle$ é um grupo cíclico. Um exemplo de grupo cíclico é dado pelo grupo Z_n, pois, $Z_n = \langle\overline{1}\rangle$. Se G tem ordem p, onde p é primo, então G é cíclico. De fato, todo elemento não-trivial $x \in G$ tem ordem p. Assim, $G = \langle x\rangle$, para todo $x \neq 1$ em G.

Proposição 1.1 *Sejam $G = \langle g\rangle$ e $H \leqslant G$.*

a) Se G é infinito, então $H = 1$ ou H é cíclico infinito.

b) Se $|G| = n$, então H é cíclico. Além disso, para cada divisor d de n existe um único subgrupo de G com ordem d, a saber, $\langle g^{\frac{n}{d}}\rangle$.

Sejam H e K subgrupos de G, definimos o grupo gerado por H e K por

$$\langle H, K\rangle = \langle H \cup K\rangle$$

Lema 1.2 *Sejam H, K_1 e K_2 subgrupos de G. Se $H \trianglelefteq K_1$ e $H \trianglelefteq K_2$, então $H \trianglelefteq \langle K_1, K_2\rangle$*

A proposição a seguir nos dá uma fácil e importante relação entre subgrupos de G.

Proposição 1.2 (Regra de Dedekind) *Sejam A, B e C subgrupos de G tal que $B \leqslant A$. Então,*

$$A \cap (BC) = B(A \cap C)$$

Prova: Veja que não sabemos se BC e $B(A \cap C)$ são subgrupos de G. Como $B \leqslant A$, $B \leqslant BC$, $A \cap C \leqslant A$ e $A \cap C \leqslant C \leqslant BC$, temos que $B(A \cap C) \leqslant A \cap (BC)$.

Seja $a \in A \cap (BC)$. Então, a = bc, para algum $b \in B$ e $c \in C$. Assim, $b^{-1}a = c \in A \cap C$, pois $B \leqslant A$. Logo, $a = bc \in B(A \cap C)$. Portanto, $A \cap (BC) \leqslant B(A \cap C)$. Segue o resultado.
■

Agora, definiremos e enunciaremos importantes resultados sobre homomorfismos de grupos. Lembramos que se $H \trianglelefteq G$, definimos o grupo quociente $\dfrac{G}{H}$ por

$$\frac{G}{H} = \{gH | g \in G\}$$

com a operação $g_1H.g_2H = g_1g_2H$.

Definição 1.1 (Homomorfismo de grupo) *Sejam G e G_1 grupos. Um homomorfismo φ de G para G_1 é uma aplicação $\varphi : G \to G_1$ tal que $\varphi(g.g_1) = \varphi(g).\varphi(g_1)$, para todo $g, g_1 \in G$.*

Chamamos a imagem inversa do elemento identidade 1_{G_1} de G_1, de núcleo do homomorfismo. Denotamos por $Ker(\varphi) = \varphi^{-1}(1_{G_1})$. Se φ é uma bijeção, dizemos que se trata de um isomorfismo. Neste caso, dizemos que G e G_1 são isomorfos e escrevemos $G \simeq G_1$.

Teorema 1.4 (Fundamental dos homomorfismos) .

Sejam G e G_1 grupos, $\varphi : G \to G_1$ um homomorfismo e $N = Ker(\varphi)$. A aplicação $\Psi : \dfrac{G}{N} \to \varphi(G) : gN \mapsto \varphi(g)$ é um isomorfismo. Logo, $\dfrac{G}{N} \simeq \varphi(G)$.

Corolário 1.1 (1° teorema do isomorfismo) *Sejam $H \leqslant G$ e $N \trianglelefteq G$. Então, $H \cap N \trianglelefteq H$, e vale $\dfrac{H}{H \cap N} \simeq \dfrac{HN}{N}$.*

Corolário 1.2 (2° teorema do isomorfismo) *Sejam N e H subgrupos normais de G, com $H \subseteq N$. Então $H \trianglelefteq N$, $\dfrac{N}{H} \trianglelefteq \dfrac{G}{H}$ e $\dfrac{G}{N} \simeq \dfrac{\frac{G}{H}}{\frac{N}{H}}$*

Discutiremos mais um resultado que deriva do teorema fundamental dos homomorfismos.

Corolário 1.3 *Sejam N e H subgrupos normais de G. Então, $H \cap N \trianglelefteq HN$ e*

$$\frac{HN}{H \cap N} \simeq \frac{H}{H \cap N} \times \frac{N}{H \cap N}$$

Em particular, se $H \cap N = 1$, então $HN \simeq H \times N$ e dizemos que $H \times N$ é o produto direto de H por N.

Prova: Temos que para todo $g \in G$, $H^g \subseteq H$ e $N^g \subseteq N$. Assim, dados $y = hn \in HN$ e $x \in H \cap N$, $x^y \in H \cap N$. Logo, $(H \cap N)^y \subseteq H \cap N$, $\forall y \in HN$, e então $H \cap N \trianglelefteq HN$. Agora, defina

$$\varphi : \frac{HN}{H \cap N} \to \frac{H}{H \cap N} \times \frac{N}{H \cap N} : hn(H \cap N) \mapsto (h(H \cap N), n(H \cap N))$$

Claramente φ é um homomorfismo sobrejetivo.

Temos que

$$Ker(\varphi) = \{hn(H \cap N) \in \frac{HN}{H \cap N} | (h(H \cap N), n(H \cap N)) = (H \cap N, H \cap N)\} = \{H \cap N\}$$

Como o núcleo de φ é a identidade do grupo $\dfrac{HN}{H \cap N}$, temos pelo teorema fundamental do homomorfismo, que $\dfrac{HN}{H \cap N} \simeq \dfrac{H}{H \cap N} \times \dfrac{N}{H \cap N}$. ■

Observação 1.1 *No enunciado do corolário acima vimos a definição de produto direto. Se H e K são subgrupos de G com $H \trianglelefteq G$, $K \ntrianglelefteq G$, $H \cap K = 1$ e $G = HK$, dizemos que G é o produto semi-direto de H por K e denotamos por $G = H \rtimes K$.*

Definição 1.2 (Grupo dos automorfismos) *Um isomorfismo de G em G é chamado de automorfismo. O grupo dos automorfismos de G é formado por todos os automorfismos de G com a operação de composição. Denotamos por $Aut(G)$.*

Definição 1.3 (Subgrupo característico) *Um subgrupo H de G é característico em G se para cada $\varphi \in Aut(G)$, $\varphi(H) \subseteq H$. Denotamos por $N \trianglelefteq_{car} G$.*

Um exemplo de subgrupo característico é dado por Z(G). De fato, dados $x \in Z(G)$, $\varphi \in Aut(G)$ e $g \in G$, temos

$$\varphi(x).g = \varphi(x).\varphi(\varphi^{-1}(g)) = \varphi(x.\varphi^{-1}(g)) = \varphi(\varphi^{-1}(g).x) = g.\varphi(x)$$

Assim, $\varphi(x) \in Z(G)$. Logo, $\varphi(Z(G)) \subseteq Z(G)$, para todo $\varphi \in Aut(G)$.

Lema 1.3 *Sejam H e K subgrupos de G*

i) Se $H \trianglelefteq_{car} G$, então $H \trianglelefteq G$.

ii) Se $H \trianglelefteq_{car} K \trianglelefteq G$, então, $H \trianglelefteq G$.

Prova:
i)Dado $g \in G$, é fácil ver que $\varphi : G \to G : x \mapsto g^{-1}xg$ é um automorfismo. Assim, se $h \in H$, temos

$$h^g = g^{-1}hg = \varphi(h) \in H$$

Logo $H^g \leqslant H$ e então $H \trianglelefteq G$.
ii) Seja $g \in G$. Como $K \trianglelefteq G$, temos que $\varphi_g : K \to K : k \mapsto g^{-1}kg$ é um automofismo de K. Como $H \trianglelefteq_{car} K$, temos que $\varphi_g(H) \subseteq H$. Assim, $H^g \subseteq H$ e portanto, $H \trianglelefteq G$. ■

O grupo aditivo Z_n também é um anel comutativo com identidade multiplicativa $\overline{1}$. O subanel das unidades de Z_n, denotado por $U(Z_n)$, é formado pelos elementos que possuem inverso multiplicativo em Z_n. Vimos que se n = p para p primo, então Z_p é corpo. Assim, $U(Z_p) = \{\overline{1}, \ldots, \overline{p-1}\}$.

Lema 1.4 *Seja p um primo. Então*

a) $Aut(Z_p) \simeq U(Z_p)$

b) $U(Z_p) \simeq C_{p-1}$, onde C_{p-1} denota um grupo cíclico de ordem p-1

Prova: $a)$ Sabemos que $U(Z_p) = \{\overline{1}, ..., \overline{p-1}\}$ é o conjunto dos geradores de Z_p. Defina a aplicação

$$\Psi : Aut(Z_p) \to U(Z_p) : \varphi \mapsto \varphi(\overline{1})$$

Como $\langle \overline{1} \rangle = Z_p$ e $\varphi \in Aut(Z_p)$, $\langle \varphi(\overline{1}) \rangle = Z_p$. Logo, $\varphi(\overline{1}) \in Z_p$. Assim, a aplicação está bem definida. Claramente é um homomorfismo e

$$Ker(\Psi) = \{\varphi \in Aut(Z_p)/\Psi(\varphi) = \varphi(\overline{1}) = \overline{1}\} = Id_{Z_p}$$

Logo, Ψ é injetiva.

Agora, sobre a sobrejeção. Dado $\overline{a} \in U(Z_p)$, defina $\varphi : Z_p \to Z_p : \overline{1} \mapsto \overline{a}$. Assim, $\varphi(\overline{r}) = r\overline{a}$. Claramente $\varphi \in Aut(Z_p)$. Então, $\Psi(\varphi) = \varphi(\overline{1}) = \overline{a}$. Portanto, Ψ é sobrejetiva. Segue o resultado.

$b)$ Mostraremos primeiro a seguinte afirmação.

AFIRMAÇÃO: Se G é um grupo abeliano finito e a é o elemento que possui a maior ordem em G, então a ordem de todo o elemento de G divide a ordem de a.

De fato, $o(a) = p_1^{\alpha_1}...p_r^{\alpha_r}$, onde $\alpha_i \geq 0$, $\forall\ i = 1, ..., r$. Dado $x \in G$, temos que $o(x) = p_1^{\beta_1}...p_k^{\beta_k}.p_{k+1}^{\beta_{k+1}}...p_r^{\beta_r}$, onde $0 < k < r$, $0 \leq \alpha_i \leq \beta_i$, $\forall\ 1 \leq i \leq k$ e $0 \leq \beta_j \leq \alpha_j$, $\forall\ k+1 \leq j \leq r$.

Definamos $y = a^{p_1^{\alpha_1}...p_k^{\alpha_k}}$ e $z = x^{p_{k+1}^{\beta_{k+1}}...p_r^{\beta_r}}$. Assim, $o(y) = p_{k+1}^{\alpha_{k+1}}...p_r^{\alpha_r}$ e $o(z) = p_1^{\beta_1}...p_k^{\beta_k}$. Como $MDC(o(y), o(z)) = 1$, temos que

$$o(yz) = p_1^{\beta_1}...p_k^{\beta_k}p_{k+1}^{\alpha_{k+1}}...p_r^{\alpha_r} = MMC(o(a), o(x)) \geq o(a)$$

Mas, $o(a)$ é a maior ordem. Logo, $o(yz) = MMC(o(a), o(x)) = o(a)$. Portanto, $o(x)$ divide $o(a)$.**OK!**

Temos que $U(Z_p) = \{\overline{1}, ..., \overline{p-1}\}$. Seja a o elemento de maior ordem em $U(Z_p)$. Pela afirmação, $o(x)$ divide $o(a)$ para todo $x \in U(Z_p)$. Assim,

$$P(y) = y^{o(a)} - \overline{1} = (y - \overline{1})...(y - (\overline{p-1})).Q(x)$$

Logo, $p - 1 \leq o(a)$. Mas, $o(a)$ divide $|U(Z_p)| = p - 1$, isto é, $o(a) \leq p - 1$.

Portanto, $o(a) = p - 1$ e então, $U(Z_p) = \langle a \rangle$.$\blacksquare$

Agora, falaremos sobre ação de grupos em conjuntos.

Definição 1.4 (Ação de grupo em conjunto) *Sejam G um Grupo, X um conjunto e S_X o grupo formado por todas as bijeções de X em X, com a operação de composição de aplicações. Chamamos de ação de G sobre o conjunto X um homomorfismo $\varphi : G \to S_X$.*

Dado $x \in X$, definimos a órbita de x, denotamos por O_x, como sendo o conjunto $O_x = \{\varphi(g)x | g \in G\}$, e o estabilizador de x, denotado por E_x, como sendo o conjunto $E_x = \{g \in G | \varphi(g)(x) = x\}$. Facilmente prova-se que $E_x \leqslant G$. Além disso, temos a seguinte proposição.

Proposição 1.3 *Seja $\varphi : G \to S_X$ uma ação. Então, para qualquer $x \in X$, $|G : E_x| = |O_x|$.*

Exemplo 2 ***a)*** *Sejam G um grupo e $X = G$. Definimos a aplicação*

$$\varphi : G \to S_G : g \mapsto \varphi(g)(x) = gxg^{-1}$$

Claramente, φ é um homomorfismo. Assim, temos uma ação do grupo G sobre o conjunto G. Definimos o centralizador de um elemento x de G como sendo

$$C_G(x) = \{g \in G | g^{-1}xg = x\}$$

Dessa forma
$O_x = \{g^{-1}xg | g \in G\} = x^G$ e $E_x = \{g \in G | g^{-1}xg = x\} = C_G(x)$. Portanto, pela proposição anterior,

$$|x^G| = |O_x| = |G : E_x| = |G : C_G(x)|$$

b) *Sejam $H \leqslant G$ e $X = \{H^x | x \in G\}$. Defina o homomorfismo*

$$\varphi : G \to S_X : g \mapsto \varphi(g)(H^x) = H^{xg^{-1}}$$

Lembramos que o normalizador de um subgrupo H de G é definido por

$$N_G(H) = \{g \in G | H^g = H\}$$

Logo, como $H \in X$, temos

$$O_H = \{\varphi(g)(H) | g \in G\} = \{H^{g^{-1}} | g \in G\} = X$$

e

$$E_H = \{g \in G | \varphi(g)(H) = H\} = \{g \in H | H^{g^{-1}} = H\} = N_G(H)$$

portanto, pela proposição anterior,

$|\{H^x | x \in G\}| = |X| = |O_H| = |G : E_H| = |G : N_G(H)|$ *que divide* $|G : H|$*. Com isso, temos que o número de conjugados de um subgrupo* H *em* G *é o índice* $|G : N_G(H)|$.

c) *Sejam* $H \leqslant G$, $|G : H| = n$ *e* $X = \{xH | x \in G\}$*. Consideremos a aplicação*

$$\varphi : G \to S_X : g \mapsto \varphi(g)(xH) = gxH$$

É fácil mostrar que φ *é homomorfismo. Temos*

$g \in Nuc(\varphi) \Leftrightarrow \varphi(g)(xH) = Id_{S_X}(xH)$, $\forall x \in G \Leftrightarrow gxH = xH$, $\forall x \in G \Leftrightarrow x^{-1}gx \in H$, $\forall x \in G \Leftrightarrow Nuc(\varphi) = [Nuc(\varphi)]^x \subseteq H$, $\forall x \in G$.

Portanto, neste caso, $Nuc(\varphi) \leqslant H$.

Lema 1.5 *Se* G *é um p-grupo, então* $Z(G) \neq 1$.

Prova: Seja $|G| = p^\alpha$. Da ação do exemplo a) temos

$$G = 1 \cup x_1^G \cup ... \cup x_r^G$$

Logo,

$$\begin{aligned} p^\alpha = |G| &= 1 + |x_1^G| + ... + |x_r^G| \\ &= 1 + |G : C_G(x_1)| + ... + |G : C_G(x_r)| \\ &= 1 + p^{\alpha_1} + ... + p^{\alpha_r} \end{aligned}$$

se $\alpha_i \neq 0$, $\forall\ i = 1, ..., r$, então p divide 1. Absurdo. Portanto, $\alpha_i = 0$ para algum i. Assim $|x_i^G| = 1$, o que implica que $x_i^G = x_i$. Portanto, $1 \neq x_i \in Z(G)$.$\blacksquare$

Para encerrarmos esta primeira seção, enunciaremos o teorema de Sylow e faremos algumas aplicações do mesmo.

Teorema 1.5 (De Sylow) *Sejam p um número primo e G um grupo de ordem* $p^m.b$*, onde* $MDC(p, b) = 1$*. Se* Syl_pG *denota o conjunto dos p-subgrupos de Sylow de G, isto é, dos subgrupos de G com ordem* p^m*,então* *i) Para cada n, $0 \leq n \leq m$, existe um subgrupo H de G tal que $|H| = p^n$. Em particular, $Syl_pG \neq \phi$;*

ii) $|Syl_pG| \equiv 1(mod\, p)$;

iii) Todo subgrupo H de G com ordem p^n, onde $n \leq m$, está contido em um p-subgrupo de Sylow de G;

iv) Dados $S, P \in Syl_pG$, existe $x \in G$ tal que $P = S^x$, isto é, S e P são conjugados. Com isso, dado $P \in Syl_pG$, $|Sly_pG| = |\{P^x|x \in G\}| = |G : N_G(P)|$ divide $|G : P|$. Em particular, se $P \trianglelefteq G$, então $|Syl_pG| = |\{P\}| = 1$.

O teorema de Sylow possui várias aplicações. Vejamos algumas.

Lema 1.6 *Se G é um grupo não-abeliano de ordem 6, então $G \simeq S_3$.*

Prova: Temos que $|G| = 2.3$. Pelo teorema de Sylow, existe H e K subgrupo de G tais que $|H| = 2$ e $|K| = 3$. Como $|G : K| = \dfrac{|G|}{|K|} = 2$, $K \lhd G$. Suponhamos que $H \lhd G$. Assim, pelo lema 1.1, $G = HK$. Como $H \cap K = 1$, temos, pelo corolário 1.3, $G \simeq H \times K \cong Z_2 \times Z_3$. Logo, G é abeliano. O que é um absurdo. Portanto, $H \ntriangleleft G$. Seja $X = \{xH/x \in G\}$. Defina a ação

$$\varphi : G \to S_X : g \mapsto \varphi(g)(xH) = gxH$$

Vimos que $Nuc(\varphi) \leqslant H$. Como H é não-normal em G, $Nuc(\varphi) < H$. Portanto, $Nuc(\varphi) = 1$ e, com isso, $G \simeq S_X$. Veja que $S_X \simeq S_3$, pois, $|X| = 3$. Assim, $G \simeq S_3$.■

Proposição 1.4 (Argumento de Frattini) *Sejam G um grupo finito, $N \trianglelefteq G$ e $P \in Syl_pN$. Então, $N \cdot N_G(P) = G$.*

Prova: Como $N \lhd G$, $N \cdot N_G(P) \leqslant G$. Por outro lado, dado $g \in G$, temos que $P^g \subseteq N$, pois, $N \trianglelefteq G$. Como P e P^g tem a mesma ordem, $P^g \in Syl_pN$. Pelo teorema de Sylow, existe $x \in N$ tal que $P^g = P^x$. Logo, $P = P^{gx^{-1}}$. Portanto, $gx^{-1} \in N_G(P)$. Com isso, $g \in N_G(P) \cdot N$. Segue o resultado. ■

1.2 Grupos Solúveis

Inicialmente, lembramos que uma série subnormal de um grupo G é uma cadeia de subgrupos $(G_i)_{0\leq i\leq n}$ de G, tal que

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G,$$

onde $G_{i-1} \trianglelefteq G_i\ \forall\ i = 1, \ldots, n$.

Como o subgrupo de Klein $V = \{Id, (12)(34), (13)(24), (14)(23)\}$ é normal em A_4, temos que $1 \trianglelefteq V \trianglelefteq A_4$ é uma série subnormal de A_4.

Definição 1.5 *Seja G um grupo. Dizemos que G é solúvel se existe uma série subnormal $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$, com $\frac{G_i}{G_{i-1}}$ abeliano, $\forall\ 1 \leq i \leq n$.*

Exemplo 3 *A_4 é um grupo solúvel. De fato, $\left|\frac{A_4}{V}\right| = \frac{12}{4} = 3$. Pelo fato de que todo grupo de ordem p ou p^2, onde p é primo, ser abeliano, temos que $\frac{A_4}{V}$ e V são abelianos. Como vimos que $1 \trianglelefteq V \trianglelefteq A_4$ é uma série subnormal de A_4, temos o que queremos.*

A proposição que enunciaremos a seguir, relaciona um grupo solúvel com seus subgrupos.

Proposição 1.5 *Seja G um grupo solúvel.*

a) Se $H \leq G$, então H é solúvel.

b) Se $H \trianglelefteq G$, então $\frac{G}{H}$ é solúvel.

c) Seja $H \trianglelefteq G$. Se N e $\frac{G}{N}$ são solúveis, então G é solúvel.

Vejamos agora um importante subgrupo de G.

Definição 1.6 *Se H e K são dois subgrupos de G, definimos o subgrupo dos comutadores de H e K como sendo*

$$[H, K] = \langle h^{-1}k^{-1}hk \mid h \in H\ ,\ k \in K\rangle.$$

Chamamos de subgrupo dos comutadores(ou derivado) do grupo G, denotado por G', o grupo $G' = [G, G]$.

Observação:

1. Claramente se vê que, se $G' = 1$, então G é abeliano.

2. Se $N \trianglelefteq G$, então $[N, G] \leq N$. De fato, dados $x \in N$ e $g \in G$, temos $x^{-1}(g^{-1}xg) \in N \cdot N^g = N \cdot N = N$.

Proposição 1.6 $G' = \langle x^{-1}y^{-1}xy \,|\, x, y \in G \rangle$ *é um subgrupo normal de* G.

Prova: Seja $S = \{x^{-1}y^{-1}xy \,|\, x, y \in G\}$. Se $\alpha = x^{-1}y^{-1}xy \in S, \alpha^{-1} = y^{-1}x^{-1}yx \in S$. Assim, dado $\beta \in G'$, β se escreve como $\beta = a_1 \ldots a_n$ com $a_i \in S$. Dado $g \in G$, temos

$$g^{-1}\beta g = g^{-1}(a_1 \ldots a_n)g = g^{-1}a_1(gg^{-1}) \ldots (gg^{-1})a_n g = (g^{-1}a_1 g) \ldots (g^{-1}a_n g).$$

Queremos mostrar que $g^{-1}\beta g \in G'$. Para isto, basta mostrarmos que $g^{-1}ag \in S$ quando $a \in S$. Seja $a = x^{-1}y^{-1}xy$ um elemento de S. Assim,

$$\begin{aligned} g^{-1}ag &= g^{-1}(x^{-1}y^{-1}xy)g = (g^{-1}x^{-1}g)(g^{-1}y^{-1}g)(g^{-1}xg)(g^{-1}yg) = \\ &= (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \in S. \blacksquare \end{aligned}$$

Observação:

1. Mais geralmente, $[X, G] \trianglelefteq G$, $\forall\ X \leq G$.

2. $G' \underset{\text{car}}{\trianglelefteq} G$. De fato, dados $\beta \in G'$ e $\theta \in \operatorname{Aut}(G)$, temos que $\beta = a_1 \ldots a_n$, onde $a_i \in S$. Assim, $\theta(\beta) = \theta(a_1) \ldots \theta(a_n)$. Como $a_i \in S$, $a_i = x_i^{-1}y_i^{-1}x_i y_i$. Logo, $\theta(a_i) = [\theta(x_i)]^{-1}[\theta(y_i)]^{-1}\theta(x_i)\theta(y_i) \in S, \forall\ i = 1, \ldots, n$. Portanto, $\theta(\beta) \in G'$.

O subgrupo G' de G tem um importante papel nos grupos quocientes de G. É disso que trata a próxima proposição que enunciaremos.

Proposição 1.7 *Sejam* G *um grupo e* G' *seu subgrupo dos comutadores. Então:*

a) $\frac{G}{G'}$ *é abeliano;*

b) G' *é o menor subgrupo normal de* G *com essa propriedade, isto é, se* $H \trianglelefteq G$ *é tal que* $\frac{G}{N}$ *é abeliano, então* $G' \leq H$. *Em particular, se* G *é solúvel, então* $G' < G$.

Exemplo 4 *$S_4' = A_4$. Em particular, $\frac{S_4}{V}$ não é abeliano. Com efeito, é um fato conhecido que os subgrupo normais de S_4 são 1, V, A_4 e S_4. Temos que $(123)(234) = (12)(34) \neq (13)(24) = (234)(123)$. O que mostra que S_4 não é abeliano. Assim, $(S_4)' \neq 1$. Como $\left|\frac{S_4}{A_4}\right| = 2$, $\frac{S_4}{A_4}$ é abeliano e, pela proposição anterior, $S_4' \leq A_4$. Assim, $S_4' \neq A_4$. Ou seja, $S_4' = K$ ou $S_4' = A_4$. Mas, veja que, dados $\alpha = (124)$ e $\beta = (23)$, elementos de S_4, temos $\alpha^{-1}\beta^{-1}\alpha\beta = (142)(23)(124)(23) = (132) \notin K$. Então, $S_4' \neq K$ e, portanto, $S_4' = A_4$.*

Vimos na proposição 1.6, que $G' \trianglelefteq G$. Assim sendo, podemos definir os seguintes subgrupos normais em G:

$$G^{(2)} = [G', G'], \ldots, G^{(n)} = [G^{(n-1)}, G^{(n-1)}].$$

Claramente, temos que $G^0 = G \trianglerighteq G' \trianglerighteq G^{(2)} \trianglerighteq \ldots \trianglerighteq G^{(n)} \trianglerighteq \ldots$. Veja que $\frac{G^{(n-1)}}{G^{(n)}}$ é abeliano, para todo inteiro positivo. É fácil ver que G é solúvel se, e somente se, existe um inteiro positivo tal que $G^{(n)} = 1$. O menor inteiro positivo com essa propriedade é chamado de comprimento derivado de G.

Definição 1.7 *Dizemos que um subgrupo normal $1 \neq L$ de G é normal minimal de G, se não existe um subgrupo normal K de G tal que $1 \neq K < L$.*

Definição 1.8 *Sejam H e K dois subgrupos normais de G, com $H < K$. Dizemos que $\frac{K}{H}$ é um fator principal de G quando $\frac{K}{H}$ é um subgrupo normal minimal de $\frac{G}{H}$.*

Existe um resultado mais geral sobre fatores principais de grupos solúveis. Mas, preferimos restringir este resultado para grupos finitos, pois, estes são os que atendem ao nosso interesse. Isto, é o que discutiremos neste próximo resultado.

Proposição 1.8 *Seja G um grupo solúvel finito. Se $\frac{H}{K}$ é um fator principal de G, então existe um primo p e um inteiro positivo n tal que $\left|\frac{H}{K}\right| = p^n$.*

Prova: Para facilitar a notação, seja N um fator principal de G. Temos que $N' \trianglelefteq_{\text{car}} N \trianglelefteq G$. Assim, pelo lema 1.3, $N' \trianglelefteq G$. Como N é normal minimal de G, $N = 1$ ou $N' = N$. Como G é solúvel, N é solúvel e, então $N' \neq N$. Portanto, $N' = 1$, o que implica que N é abeliano.

Seja p um primo divisor de $|N|$. Definamos $N[p] = \{x \in N \mid o(x) = p\}$.

AFIRMAÇÃO: $N[p] \trianglelefteq_{\text{car}} N$.

De fato, dado $1 \neq x \in N[p]$ e $\varphi \in \operatorname{Aut}(N)$, $[\varphi(x)]^p = \varphi(x^p) = \varphi(1) = 1$. Assim, $o(\varphi(x))$ divide p. Como $1 \neq x$, $\varphi(x) \neq 1$. Logo, $o(\varphi(x)) = p$. Portanto, $\varphi(x) \in N[p]$.

Temos que $N[p] \trianglelefteq_{\text{car}} N \trianglelefteq G$. Logo, $N[p] \trianglelefteq G$. Portanto, $N[p] = 1$ ou $N[p] = N$. Pelo teorema de Cauchy, existe $1 \neq x \in N$ tal que $o(x) = p$. Assim, $N = N[p]$ e, então N é p-abeliano elementar. O que implica que $|N| = p^n$, para algum inteiro positivo n.■

Definição 1.9 *Dizemos que um subgrupo próprio M de um grupo G é maximal em G, se para todo subgrupo H de G com $M \leq H$, tivermos que, ou $H = M$ ou $M = G$. Denotamos M maximal em G por $M \lessdot G$.*

Em S_3, temos que $H_1 = \{Id, (12)\}, H_2 = \{Id, (13)\}, H_4 = \{Id, (23)\}$ e $H_4 = \{Id, (123), (132)\} = A_3$ são exemplos de subgrupos maximais de S_3. De fato, $|S_3 : H_i| = 3$, para $i = 1, 2, 3$; e $|S_3 : A_3| = 2$. Logo, não existe subgrupo próprio de S_3 que contenha H_i, $\forall\ i = 1, \ldots, 4$, propriamente. Mais geralmente, todo subgrupo H de um grupo G de índice primo é maximal. Como sabemos, o único subgrupo próprio que é normal em S_3 é A_3. Assim, H_1, H_2 e H_3 não são normais em S_3, apesar de seus índices em S_3 serem primos. Veremos, a seguir, que a recíproca é verdadeira.

Proposição 1.9 *Seja M um subgrupo maximal de um grupo G. Se $M \trianglelefteq G$, então $|G : M| = p$, para algum primo p.*

Prova: Como $M \trianglelefteq G$, então $M \lessdot G$ equivale a dizer que $\frac{G}{M}$ não possui subgrupo próprio. Mas, pelo teorema de Sylow, isto só irá ocorrer se, e somente se, $\left|\frac{G}{M}\right| = p$, para algum primo p.

Lema 1.7 *Seja G um grupo finito e p um divisor de $|G|$. Se cada subgrupo maximal de G com índice primo com p é normal, então G tem um p-subgrupo de Sylow normal.*

Prova: Seja $P \in Syl_p(G)$. Temos que $N_G(P) = G$ ou $P \leq N_G(P) \leq M \lessdot G$.

Se $G = N_G(P)$, então P é normal em G.

Se $N_G(P) \neq G$, então $N_G(P)$ está contido em um subgrupo maximal M de G. Como $|G : P|$ não é divisível por p, então $|G : M|$ não é divisível por p. Assim, por hipótese,

$M \trianglelefteq G$. Como $|G : M|$ não é divisível por p, temos que $P \in Syl_p(M)$. Logo, pelo argumento de Frattini, $G = M \cdot N_G(P)$. Mas $N_G(P) \leq M$, então $G = M$, absurdo.

Portanto, $N_G(P) = G$ e, então, $P \trianglelefteq G$. ■

Lema 1.8 *Seja G um grupo. Suponha que $G = HA$, onde H é um subgrupo próprio e A é um subgrupo normal abeliano de G. Então H é maximal em G se, e somente se, $\frac{A}{A\cap H}$ é um fator principal de G. Também, $|G : H| = |A : A \cap H|$.*

Prova: Pelo 1^o teorema dos isomorfismos, $A \cap H \trianglelefteq H$. Como A é abeliano, $A \cap H \trianglelefteq A$. Assim, $A \cap H \trianglelefteq G$, pois $G = HA$.

($\Rightarrow$) Suponha que $1 \neq H \lessdot G$. Seja $\frac{K}{A\cap H} \trianglelefteq \frac{G}{A\cap H}$ tal que $\frac{K}{A\cap H} \leq \frac{A}{A\cap H}$. Como $H \lessdot G$, $KH = H$ ou $KH = G$.

Se $H = HK$, então $K \leq A \cap H \leq K$. Logo, $K = A \cap H$.

Se $HK = G$, então $A = A \cap G = A \cap (KH) = (A \cap H)K = K$.

Portanto, $\frac{A}{A\cap H}$ é um subgrupo normal minimal de $\frac{G}{A\cap H}$.

($\Leftarrow$) Suponha que $\frac{A}{A\cap H}$ é um subgrupo normal minimal de $\frac{G}{A\cap H}$. Seja $H \leq L \leq G$. Como $G = HA$, $G = LA$. Pelo teorema citado acima $L \cap A \trianglelefteq L$. Logo, $L \cap A \trianglelefteq G$. Portanto, $\frac{L\cap A}{A\cap H} \trianglelefteq \frac{G}{A\cap H}$. Como $L \cap A \leq A$, temos que $L \cap A = H \cap A$ ou $L \cap A = A$.

Se $A \cap L = A \cap H$, então $L = L \cap G = L \cap (HA) = (L \cap A)H = (H \cap A)H = H$.

Se $L \cap A = A$, então $A \leq L$. Logo, $G = AL = L$.

Portanto, $H \lessdot G$.

Para o que resta, temos que $|G : A| = |H : A \cap H|$. Pelo teorema de Lagrange, $|G : A||A : A \cap H| = |G : A \cap H| = |G : H||H : A \cap H|$.

Portanto, $|G : H| = |A : A \cap H|$. ■

Teorema 1.6 *Seja G um grupo solúvel finito. Se M é um subgrupo maximal de G, então $|G : M| = p^n$, onde p é um primo e n é um inteiro positivo.*

Prova: Como G é solúvel, existe um inteiro positivo n tal que $G^{(n)} = 1$. Seja $k \leq n$ o maior inteiro positivo tal que $A = G^{(k)} \not\leq M$. Temos assim, que $A' = G^{(k+1)} \leq M$ e $\frac{M}{A'}$ é um subgrupo maximal de G. Como $\frac{A}{A'} \not\leq \frac{M}{A'}$, $\frac{G}{A'} = \frac{A}{A'}\frac{M}{A'}$. Sabemos que $\bar{A} = \frac{A}{A'}$ é abeliano e $\bar{M} = \frac{M}{A'} \lessdot \frac{G}{A'} = \bar{G}$. Pelo lema 1.8, $\frac{\bar{A}}{\bar{A}\cap\bar{M}}$ é um fator principal de $\bar{G}$. Além disso,

$|\bar{G} : \bar{M}| = |\bar{A} : \bar{A} \cap \bar{M}|$. Como $\bar{G}$ é solúvel finito, temos pela proposição 1.8, que existe um primo p e um inteiro positivo n tal que

$$|G : M| = |\bar{G} : \bar{M}| = |\bar{A} : \bar{A} \cap \bar{M}| = p^n.\blacksquare$$

Para encerrarmos esta seção, falaremos um pouco sobre grupos supersolúveis.

Definição 1.10 *Um grupo G é supersolúvel se existe uma série normal, isto é, uma cadeia de subgrupos normais em G*

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

tais que $\frac{G_i}{G_{i-1}}$ é cíclico $\forall\ i = 1, \ldots, n$.

Em particular, todo grupo supersolúvel é solúvel. Mas, por exemplo, A_4 é solúvel, mas não é supersolúvel. De fato, a única série normal de A_4 é $1 \trianglelefteq V \trianglelefteq A_4$. No entanto, V não é cíclico, com isso, A_4 não é supersolúvel.

Assim como nos solúveis, todo subgrupo H de um supersolúvel G é supersolúvel. Mas, se $N \trianglelefteq G$ e $\frac{G}{N}$ são supersolúveis, não implica que G é supersolúvel. De fato, como vimos acima, A_4 não é supersolúvel, mas o grupo de Klein V e $\frac{A_4}{V}$ são supersolúveis, pois $|V| = 2^2$ e $\left|\frac{A_4}{V}\right| = 3$.

Veremos que todo subgrupo maximal de um grupo supersolúvel tem índice primo. Este, é o conteúdo do próximo teorema.

Teorema 1.7 *Seja G supersolúvel. Então, todo fator principal tem ordem prima e todo subgrupo maximal tem índice primo em G.*

Prova: Para facilitar a notação, seja N um fator principal de G. Como G é supersolúvel, temos

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

com $G_i \trianglelefteq G$ e $\frac{G_i}{G_{i-1}}$ cíclico $\forall\ i = 1, \ldots, n$.

Seja r o menor inteiro positivo tal que $G_r \cap N \neq 1$. Logo, $G_{r-1} \cap N = 1$. Como $G_r \cap N \trianglelefteq G$ e $G_r \cap N \leq N$, temos que $G_r \cap N = N$. Assim, $N \leq G_r$. Logo,

$$N = \frac{N}{N \cap G_{r-1}} \simeq \frac{NG_{r-1}}{G_{r-1}} \leq \frac{G_r G_{r-1}}{G_{r-1}} = \frac{G_r}{G_{r-1}}.$$

Portanto, N é cíclico. Assim, todo subgrupo próprio de N é normal característico em N e, assim, normal em G. Mas, N é um subgrupo normal minimal de G, então $|N| = p$ para algum primo p.

Seja M um subgrupo maximal de G. Como G também é solúvel, provaremos por indução sobre o comprimento derivado k de G. Assumiremos que todo grupo com comprimento derivado menor que k satisfaz o que queremos. Veremos dois casos:

1º caso: $G^{(k-1)} \leq M$.

Temos que $\frac{M}{G^{(k-1)}} \lessdot \frac{G}{G^{(k-1)}}$. Como o comprimento derivado de $\frac{G}{G^{(k-1)}}$ é menor que k, temos que $\left|\frac{G}{G^{(k-1)}} : \frac{M}{G^{(k-1)}}\right| = p$ para algum primo p.

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

2º caso: $G^{(k-1)} \nleq M$.

Aqui, $MG^{(k-1)} = G$. Logo, $|G : M| = |G^{(k-1)} : G^{(k-1)} \cap M|$. Como $G^{(k-1)}$ tem comprimento derivado menor que k e $G^{(k-1)} \cap M$ é maximal em $G^{(k-1)}$, temos que $|G : M| = p$ para algum primo p. ■

1.3 Grupos Nilpotentes

Definição 1.11 *Um grupo G é dito nilpotente se tem uma série central, isto é, uma série normal*

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

tal que $\frac{G_i}{G_{i-1}}$ está contido no centro de $\frac{G}{G_{i-1}}$ para todo $i = 1, \ldots, n$.

Lema 1.9 *Dados H, K subgrupos normais de G, temos que $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$ se, e somente se, $[H, G] \leq K$.*

Prova: Se $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$, então $\forall\ h \in H$ e $g \in G$, $hgK = (hK)(gK) = (gK)(hK) = ghK$. Daí, $h^{-1}g^{-1}hg = (gh)^{-1}hg \in K$. Logo, $[H, G] \leq K$.

Agora, suponha que $[H, G] \leq K$. Assim, $\forall\ h \in H$ e $g \in G$, $h^{-1}g^{-1}hg = (gh)^{-1}hg \in K$. Logo, $(hK)(gK) = hgK = ghK = (gK)(hK)$. Portanto, $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$.■

Dado um primo p, todo p-grupo finito é um exemplo de um grupo nilpotente. Isto é o conteúdo da nossa próxima proposição.

Proposição 1.10 *Seja p um primo e n um inteiro positivo. Se $|G| = p^n$, então G é nilpotente.*

Prova: Provemos por indução sobre $|G|$. Pelo lema, $Z(G) \neq 1$. Assim, $\left|\frac{G}{Z(G)}\right| < |G|$ e, por hipótese de indução, $\frac{G}{Z(G)}$ é nilpotente. Seja

$$\bar{1} = \frac{Z(G)}{Z(G)} \trianglelefteq \frac{G_1}{Z(G)} \trianglelefteq \ldots \trianglelefteq \frac{G_n}{Z(G)} = \frac{G}{Z(G)}$$

uma série central de $\frac{G}{Z(G)}$. Pelo 2^o teorema dos isomorfismos, temos

$$\frac{G_{i+1}}{G_i} \simeq \frac{\frac{G_{i+1}}{Z(G)}}{\frac{G_i}{Z(G)}} \leq Z\left(\frac{\frac{G}{Z(G)}}{\frac{G_i}{Z(G)}}\right) \simeq Z\left(\frac{G}{G_i}\right) \quad \forall\, i = 0, 1, \ldots, n-1.$$

Portanto, $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ é uma série central de G e, então G é nilpotente.■

Observação 1.2 *Note que na demonstração da proposição 1.10, provamos que se $\frac{G}{Z(G)}$ é nilpotente, então G é nilpotente.*

Vamos agora definir o subgrupo de Frattini de um grupo G. Veremos que se G é nilpotente, então esse subgrupo é nilpotente.

Definição 1.12 *O subgrupo de Frattini de um grupo G é definido como a interseção de todos os subgrupos maximais de G. Denotamos por $\Phi(G)$.*

Claramente, $\Phi(G)$ é um subgrupo característico de G. Quando G é um grupo finito, temos resultados bem interessantes sobre o seu subgrupo de Frattini.

Um elemento $g \in G$ é dito não-gerador de G, se $G = \langle X, g\rangle$, $\forall\ X \subseteq G$, tivermos $G = \langle X\rangle$. Mostraremos que o conjunto dos não-geradores coincide com o subgrupo de Frattini.

Proposição 1.11 *Seja G um grupo finito. Então $\Phi(G) = \{g \in G \,|\, g$ é não-gerador de $G\}$.*

Prova: Seja g um não-gerador de G. Se $g \notin \Phi(G)$, então existe um subgrupo maximal M tal que $g \notin M$. Assim, $\langle M, g\rangle = G$. Por definição, $M = G$, absurdo. Logo, $g \in \Phi(G)$.

Agora, sejam $g \in \Phi(G)$ e $X \subseteq G$ tal que $\langle X, g\rangle = G$. Suponha que $G \neq \langle X\rangle$. Assim, podemos encontrar um subgrupo M maximal dentre os subgrupos $H \leq G$ tais que $\langle X\rangle \leq H$ e $g \notin H$. A existência desse elemento maximal é garantida pelo Lema de Zorn.

Afirmamos que $M \lessdot G$. De fato, seja $K \leqslant G$ tal que $M < K \leqslant G$. Como $\langle X \rangle \leqslant M$, $\langle X \rangle < K$. Pela maximalidade de M, temos que $g \in K$. Logo, $G = \langle X, g \rangle \leq K$. Portanto, $G = K$, e então $M \lessdot G$.

Portanto, como $g \notin M$, $g \notin \Phi(G)$, absurdo. Logo, g é não-gerador.■

Proposição 1.12 *Seja G um grupo finito.*

a) Se $N \trianglelefteq G, H \leq G$ e $N \leq \Phi(H)$, então $N \leq \Phi(G)$.

b) Se $N \trianglelefteq G$, então $\Phi(N) \leq \Phi(G)$.

c) Se $N \trianglelefteq G$, então $\Phi\left(\frac{G}{N}\right) \geq \frac{\Phi(G)N}{N}$. Se $N \leq \Phi(G)$, ocorre a igualdade.

Prova: a) Suponhamos que $N \nleq \Phi(G)$. Assim, existe $M \lessdot G$ tal que $N \nleq M$. Logo, $G = MN$. Então

$$H = H \cap G = H \cap (MN) = (H \cap M)N = \langle H \cap M, N \rangle.$$

Como $N \leq \Phi(H)$, pela proposição 1.11, $H = \langle H \cap M \rangle = H \cap M$. Logo, $H \leq M$ e, então $N \leq M$, absurdo. Portanto, $N \leq \Phi(G)$.

b) Temos que $\Phi(N) \underset{\text{car}}{\lhd} N \trianglelefteq G$. Assim, $\Phi(N) \trianglelefteq G$. Pelo item a), $\Phi(N) \leq \Phi(G)$.

c) Seja $\frac{M}{N} \lessdot \frac{G}{N}$. Assim, $M \lessdot G$ e, então $\Phi(G) \leq M$. Logo,

$$\frac{\Phi(G)N}{N} \leq \frac{MN}{N} = \frac{M}{N} \Rightarrow \frac{\Phi(G)N}{N} \leq \Phi\left(\frac{G}{N}\right)$$

Agora, suponha que $N \leq \Phi(G)$. Temos então que $\frac{\Phi(G)}{N} = \frac{\Phi(G)N}{N} \leq \Phi\left(\frac{G}{N}\right)$. Assim, $\Phi\left(\frac{G}{N}\right) = \frac{H}{N}$ para algum $H \leq G$.

Seja $M \lessdot G$. Então, $\frac{M}{N} \lessdot \frac{G}{N}$. Logo, $\frac{H}{N} = \Phi\left(\frac{G}{N}\right) \leq \frac{M}{N}$. Assim, $H \leq M$. Portanto, $H \leq \Phi(G)$. Segue o resultado.■

Caracterizaremos os grupos nilpotentes finitos.

Teorema 1.8 (Caracterização dos Grupos Nilpotentes Finitos) *Seja G um grupo finito. Então, as seguintes afirmações são equivalentes:*

i) G é nilpotente.

ii) *Todo subgrupo de G é subnormal em G, isto é, existe uma série subnormal de H para G.*

iii) *Para todo $H < G$, temos $H < N_G(H)$.*

iv) *Todo subgrupo maximal de G é normal em G.*

v) *$G' \leq \Phi(G)$.*

vi) *Todo subgrupo de Sylow de G é normal em G.*

vii) *G é o produto direto de grupos de ordens potência de primo.*

Prova: $i) \Rightarrow ii)$: Para isto, definiremos a série central superior de G. $Z_0(G) = 1, Z_1(G) = Z(G)$ e $\frac{Z_i(G)}{Z_{i-1}(G)} = Z\left(\frac{G}{Z_{i-1}(G)}\right)$ $\forall\, i \geq 1$. Veja que $1 = Z_0(G) \leq Z_1(G) \leq \ldots \leq Z_n(G) \leq \ldots$.

É fácil ver que se G é nilpotente, existe n tal que $G = Z_n(G)$. Temos também que $Z_i(G) \trianglelefteq_{\text{car}} G$, $\forall\, i = 1, \ldots, n$. Assim, $H = HZ_0(G) \leq HZ_1(G) \leq \ldots \leq HZ_n(G) = G$. Devemos mostrar que $HZ_{i-1}(G) \trianglelefteq HZ_i(G)$, $\forall\, i = 1, \ldots, n$. Como o centro de um grupo G está contido no normalizador de qualquer subgrupo H em G, temos

$$\frac{Z_i(G)}{Z_{i-1}(G)} \leq N_{\frac{G}{Z_{i-1}(G)}}\left(\frac{HZ_{i-1}(G)}{Z_{i-1}(G)}\right) \;,\ \forall\, i = 1, \ldots, n.$$

Então

$$\frac{HZ_{i-1}(G)}{Z_{i-1}(G)} \trianglelefteq \frac{Z_i(G)}{Z_{i-1}(G)}\frac{HZ_{i-1}(G)}{Z_{i-1}(G)} = \frac{Z_i(G)H}{Z_{i-1}(G)}.$$

Portanto, $HZ_{i-1}(G) \trianglelefteq HZ_i(G)$, $\forall\, i = 1, \ldots, n$.

$ii) \Rightarrow iii)$: Seja $H < G$. Por (ii), existe uma série subnormal de H para G. Seja $H = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = G$ tal série. Como $H \ntrianglelefteq G$ e $n > 1$, $H \triangleleft H_1 \leq N_G(H)$. Portanto, $H \triangleleft N_G(H)$.

$iii) \Rightarrow iv)$: Seja M um subgrupo maximal de G. Como $M < N_G(M) \leq G$, pela maximalidade de M, $N_G(M) = G$. Assim, $M \trianglelefteq G$.

$iv) \Rightarrow v)$: Seja M um subgrupo maximal de G. Por $iv)$, $M \trianglelefteq G$. Logo, $\left|\frac{G}{M}\right| = p$, para algum primo p. Assim, $\frac{G}{M}$ é cíclico e, portanto abeliano. O que implica que $G' \leq M$. Como isto acontece para todo maximal, $G' \leq \Phi(G)$.

$v) \Rightarrow iv)$: Seja M um subgrupo maximal de G. Então $v)$ implica que $G' \leq M$. Então $\frac{M}{G'}$ é um subgrupo do grupo abeliano $\frac{G}{G'}$. Assim, $\frac{M}{G'} \trianglelefteq \frac{G}{G'}$. Portanto, $M \trianglelefteq G$.

$iv) \Rightarrow vi)$: Seja P um p-subgrupo de Sylow de G. Suponha que $N_G(P) < G$. Então existe um subgrupo maximal M de G que contém $N_G(P)$. Como $P \leq M < G$, P é um p-subgrupo de Sylow de M. Por iv), $M \triangleleft G$. Assim, pelo Argumento de Frattini $G = M.N_G(P) = M$. Absurdo. Logo, $N_G(P) = G$ e então $P \trianglelefteq G$

$vi) \Rightarrow vii)$: Sejam $p_1, p_2, \ldots, p_s$ os divisores primos de $|G|$. Seja P_i um p_i-subgrupo de Sylow de G. Por $vi)$, $P_i \trianglelefteq G$, $\forall\, i = 1, \ldots, s$. Como $P_i \cap P_j = 1$, $\forall\, i \neq j$, temos que $G = P_1 \times \ldots \times P_s$.

$vii) \Rightarrow i)$: Por $vii)$, $G = P_1 \times \ldots \times P_s$, onde $|P_i| = p_i^{\alpha_i}$, onde p_i é primo e α_i é inteiro positivo para cada $i = 1, \ldots, s$. Pela proposição 1.10, P_i é nilpotente $\forall\, i = 1, \ldots, s$.
<u>AFIRMAÇÃO:</u> Se $G = H \times K$ e H,K são subgrupos nilpotentes, então G é nilpotente.

De fato, H e K possuem séries centrais

$$1 = H_0 \leq H_1 \leq \ldots \leq H_n = G \quad e \quad 1 = K_0 \leq K_1 \leq \ldots \leq K_m = G,$$

respectivamente. Inserindo repetições de termos se necessário, podemos assumir que $n = m$. É fácil provar que

$$1 = H_0 \times K_0 \trianglelefteq H_1 \times K_1 \trianglelefteq \ldots \trianglelefteq H_n \times = G.$$

E, também que, para cada $i = 1, \ldots, n$,

$$[H_i \times K_i, G] = [H_i, H] \times [K_i, K] \leq H_{i-1} \times K_{i-1}.$$

Logo, G é nilpotente.

Assim, interando $s-1$ vezes a afirmação, temos $G = P_1 \times \ldots \times P_s$ nilpotente.$\blacksquare$

Para encerrarmos esta seção, mostraremos, entre outras coisas, que o subgrupo de Frattini de G finito é nilpotente.

Teorema 1.9 *Seja H um grupo finito tal que $\Phi(G) \leq H \trianglelefteq G$ e $\frac{H}{\Phi(G)}$ é nilpotente. Então H é nilpotente.*

Prova: Sejam p um primo que divide $|H|$ e $P \in Syl_p(H)$.

<u>AFIRMAÇÃO:</u> $\frac{\Phi(G)P}{\Phi(G)} \in Syl_p\left(\frac{H}{\Phi(G)}\right)$.

De fato, $\frac{\Phi(G)P}{\Phi(G)} \simeq \frac{P}{\Phi(G)\cap P}$. Como $|P| = p^{\alpha}$, temos que $\left|\frac{\Phi(G)P}{\Phi(G)}\right| = p^{\beta}$, com $\beta \leq \alpha$. Como p não divide $|H : P|$, temos que p não divide $|H : \Phi(G)P|$. Logo, p não divide $\left|\frac{H}{\Phi(G)} : \frac{\Phi(G)P}{\Phi(G)}\right| = |H : \Phi(G)P|$. Portanto, $\frac{\Phi(G)P}{\Phi(G)} \in Syl_p\left(\frac{H}{\Phi(G)}\right)$.

Seja $N = \Phi(G)P$. Como $\frac{H}{\Phi(G)}$ é nilpotente, $\frac{N}{\Phi(G)} \underset{\text{car}}{\lhd} \frac{H}{\Phi(G)} \trianglelefteq \frac{G}{\Phi(G)}$. Logo, $\frac{N}{\Phi(G)} \trianglelefteq \frac{G}{\Phi(G)}$ e, então $N \trianglelefteq G$. Como $P \leq N \leq H$, $P \in Syl_p(N)$.

Assim, pelo Argumento de Frattini, $G = NN_G(P)$. Com isso,

$$G = NN_G(P) = \Phi(G)PN_G(P) = \Phi(G)N_G(P) = \langle \Phi(G), N_G(P)\rangle = N_G(P).$$

Portanto, $P \trianglelefteq G$. Isso ocorre para todo p-subgrupo de Sylow de G. Assim, G é nilpotente.■

Corolário 1.4 *Seja G um grupo finito. Então:*

i) $\Phi(G)$ é nilpotente.

ii) Se $\frac{G}{\Phi(G)}$ é nilpotente, então G é nilpotente.

Prova: *i*) Basta fazer $H = \Phi(G)$ no teorema anterior.

ii) Basta fazer $H = G$ no teorema anterior.■

Capítulo 2

Grupos Primitivos

Os grupos primitivos assumem um papel importantíssimo em nosso trabalho. Neste capítulo pretendemos apresentar uma quantidade suficiente de resultados sobre este grupos, a fim de aplicá-los mais adiante.

2.1 Definições e Resultados

Definição 2.1 *Seja H um subgrupo de G. Chamamos de núcleo normal de H em G, denotamos por H_G, o subgrupo normal de G dado por $H_G = \bigcap_{g \in G} H^g$.*

Verifica-se facilmente, que H_G é o maior subgrupo normal de G que está contido em H. "Maior"aqui, está no sentido de que qualquer outro subgrupo normal K de G que está contido em H, está contido em H_G.

Definição 2.2 *Dizemos que um grupo finito é primitivo se existe um subgrupo maximal M de G, tal que $M_G = 1$.*

Exemplo 5 *S_4 é um grupo primitivo. De fato, $M = \{Id, (12), (13), (23), (123), (132)\}$ é um subgrupo maximal de S_4. Com efeito, se M não fosse maximal, existiria um subgrupo de H de S_4 com índice 2 em G, tal que $M < H$. Mas, o único subgrupo maximal de S_4 com índice 2 é A_4. E, claramente $M \nleq A_4$. Portanto, M é maximal em S_4. Como $M_{S_4} \trianglelefteq S_4$ e $V \nleq M$, pois, o grupo de Klein V tem 4 elementos e, assim, $|V| \nmid |M|$, temos $M_{S_4} = 1$.*

Proposição 2.1 *Sejam G um grupo finito e p um primo. Então G possui um único maior p-subgrupo normal, que é denotado por $O_p(G)$ e chamado de p-radical de G. (Aqui, $O_p(G)$ é "maior"no sentido de qualquer outro p-subgrupo normal de G está contido em $O_p(G)$.)*

Prova: Entre todos os p-subgrupos normais de G, escolhamos K que possui a maior ordem (possivelmente $K = 1$). Seja H um p-subgrupo normal de G. Assim, $HK \trianglelefteq G$ e pelo 1^o teorema dos isomorfismos, $\left|\frac{HK}{K}\right| = \left|\frac{H}{H\cap K}\right|$. Como H é um p-grupo, $\frac{H}{H\cap K}$ é p-grupo e, portanto $\frac{HK}{K}$ é p-grupo. Mais ainda, $|HK| = \frac{|HK||K|}{|K|} = \left|\frac{HK}{K}\right| |K|$. Logo, HK é um p-subgrupo normal de G. Temos que $K \leq HK$. Mas, pela escolha de K chegamos que $K = HK$ e, portanto $H \leq K$. Assim, $K = O_p(G)$.$\blacksquare$

Note que se P é um p-subgrupo de Sylow normal em G, então $O_p(G) = P$. Veremos na próxima seção a importância do subgrupo p-radical de um grupo primitivo G.

Mostraremos que se M é um subgrupo maximal de G, então $\frac{G}{M_G}$ é um grupo primitivo.

Proposição 2.2 *Sejam N,M subgrupos de G. Se $N \trianglelefteq G$ e $N \leq M$, então $\left(\frac{M}{N}\right)_{\frac{G}{N}} = \frac{M_G N}{N}$.*

Prova: Dado $g \in G$, temos

$$\begin{aligned} \left(\frac{M}{N}\right)^{gN} &= g^{-1}N\left(\frac{M}{N}\right)gN = \{g^{-1}N(mN)gN \,|\, m \in M\} \\ &= \{(g^{-1}mg)N \,|\, m \in M\} = \frac{M^g N}{N}. \end{aligned}$$

Logo,

$$\left(\frac{M}{N}\right)_{\frac{G}{N}} = \bigcap_{g\in G}\left(\frac{M}{N}\right)^{gN} = \bigcap_{g\in G}\left(\frac{M^g N}{N}\right) = \frac{\left(\bigcap_{g\in G} M^g\right)N}{N} = \frac{M_G N}{N}.\blacksquare$$

Corolário 2.1 *Se M é um subgrupo maximal de um grupo finito G, então $\frac{G}{M_G}$ é primitivo.*

Prova: Usando a notação da proposição anterior, faça $N = M_G$ e $M = M$. Assim,

$$\left(\frac{M}{M_G}\right)_{\frac{G}{M_G}} = \frac{M_G M_G}{M_G} = \frac{M_G}{M_G} = 1.$$

Como $\frac{M}{M_G} \lessdot \frac{G}{M_G}$, $\frac{G}{M_G}$ é primitivo.$\blacksquare$

2.2 O Teorema de Ore-Baer

Definição 2.3 *Seja $H \leq G$. Dizemos que M é um complemento de H em G se $G = MH$ e $M \cap H = 1$.*

Teorema 2.1 (Ore-Baer) *Seja G um grupo primitivo finito e p um primo. Suponha que $O_p(G) \neq 1$. Seja $L = O_p(G), |L| = p^n$ e M um subgrupo maximal de G tal que $M_G = 1$. Então,*

a) L é p-abeliano elementar;

b) M é um complemento de L em G, isto é, $G = ML$ e $M \cap L = 1$. Em particular, $|G : M| = p^n$;

c) L é normal minimal de G, e

d) $C_G(L) = \{g \in G \,|\, l^g = l \; \forall \, l \in L\} = L$; então L é o único subgrupo normal minimal de G.

Suponha ainda que existe um primo q tal que $O_q(M) \neq 1$. Então,

e) $p^n \equiv 1 \,(mod\, p)$. Em particular, $q \neq p$, e

f) Qualquer complemento de L em G é conjugado a M.

Prova: *a*) Temos que $|L| = p^n$. Como $L \trianglelefteq G$, $\Phi(L) \leq \Phi(G)$. Como $\Phi(G) \leq M$ e $\Phi(G) \trianglelefteq G$, temos que $\Phi(G) = 1$, pois $M_G = 1$. Assim, $\Phi(L) = 1$. Como L é p-grupo, L é nilpotente. Logo, $L' \leq \Phi(L) = 1$ e, então L é abeliano. Sejam $N \lessdot L$ e $g \in L$. Como L é abeliano, $N \trianglelefteq L$ e então $\left|\frac{L}{N}\right| = p$. Assim, $g^p N = (gN)^p = N$. O que implica que $g^p \in N$. Isto ocorre para todo maximal de L. Assim, $g^p \in \Phi(L)$. Portanto, $g^p = 1$.

b) Como $M_G = 1$, $1 \neq L \nleq M$. Assim, $G = ML$. Pelo 1^o teorema dos isomorfismos $M \cap L \trianglelefteq M$. Como L é abeliano, pelo item *a*), $M \cap L \trianglelefteq L$. Logo, $M \cap L \trianglelefteq ML = G$. Mas, $M_G = 1$. Portanto, $M \cap L = 1$. Em particular, pelo mesmo teorema citado $|G : M| = |L| = p^n$.

c) Seja $K \trianglelefteq G$ tal que $1 \neq K \leq L$. Temos que $K \cap M \leq L \cap M = 1$. Assim, $KM = G$ e $K \cap M = 1$. Pelo teorema dos isomorfismos, $|K| = |G : M| = |L|$. Então, $K = L$ e portanto, L é normal minimal.

d) Como L é abeliano, $L \leq C_G(L)$. Assim, por Dedekind,

$$C_G(L) = G \cap C_G(L) = ML \cap C_G(L) = L(M \cap C_G(L)). \tag{2.1}$$

Mas, veja que $C_G(L)M = G$. Daí, temos que $C_G(L) \cap M \trianglelefteq M$. E pelo fato que $C_G(L) \cap M \trianglelefteq C_G(L)$, temos que $C_G(L) \cap M \trianglelefteq G$. Portanto, $C_G(L) \cap M = 1$, pois $M_G = 1$.

Dessa forma, de 2.1 temos que $C_G(L) = L$. Ademais, seja N um subgrupo normal minimal de G e $N \neq L$. Então, $[N, L] \leq N \cap L \trianglelefteq G$ e $N \cap L \neq N$. Assim, $N \cap L = 1$ e, portanto $[N, L] = 1$. Dessa forma, $N \leq C_G(L) = L$. Logo, $N = L$, absurdo.

e) Seja $Q = O_q(M) \neq 1$, com $|Q| = q^m$. Como $Q \trianglelefteq M$ e $L \trianglelefteq G = ML$, temos $Q^M = Q$ e $L^G = L^{LM} = L^M = L$. Assim,

$$\begin{aligned} (LQ)^M &= L^M Q^M = LQ \;\Rightarrow\; M \leq N_G(LQ) \\ (LQ)^L &= L \cdot Q^L. \end{aligned} \tag{2.2}$$

Veja que $Q^L \leq QL$. De fato, dados $x \in L$ e $q \in Q$, temos $q^x = x^{-1}qx = x^{-1}x'q' \in LQ$ (pois, $LQ = QL$). Logo, $Q^L \leq LQ$. Assim, por (2.2), $(LQ)^L \leq LLQ = LQ$ e, então, $L \leq N_G(LQ)$. Portanto, $LQ \trianglelefteq LM = G$.

Temos que $L \cap Q \leq L \cap M = 1$. Assim, $L \cap Q = 1$ e então

$$|LQ| = \frac{|L||Q|}{|L \cap Q|} = |L||Q| = p^n q^m.$$

Se $p = q$, então LQ seria um p-subgrupo normal de G com $|LQ| > |L|$, absurdo. Logo, $p \neq q$. Temos que $Q \in Syl_q(LQ)$. Como $1 \neq Q \trianglelefteq M$ e $M_G = 1$, $Q \ntrianglelefteq G$. Logo, $N_G(Q) = M$, pela maximalidade de M. Por Dedekind,

$$N_{LQ}(Q) = LQ \cap N_G(Q) = LQ \cap M = Q(L \cap M) = Q.$$

Portanto, pelo teorema de Sylow,

$$|L| = |LQ : Q| = |LQ : N_{LQ}(Q)| = |Syl_q(LQ)| \equiv 1 \,(mod\, q).$$

Portanto, $p^n \equiv 1\,(mod\,q)$.

$f)$ Sejam M^* um complemento de L em G e $Q^* = O_q(M^*)$. O homomorfismo natural $f : G \to \frac{G}{L} : g \mapsto gL$ aplica bijetivamente Q em $\frac{QL}{L}$ e Q^* em $\frac{Q^*L}{L}$. De fato,

$$Nuc\, f|_Q = \{g \in Q \mid gL = L\} = Q \cap L = 1 \quad e \quad \left|\frac{QL}{L}\right| = \frac{|Q||L|}{|L|} = |Q|.$$

Logo, $f|_Q : Q \to \frac{QL}{L}$ é um isomorfismo. O mesmo argumento serve para $f|_{Q^*} : Q^* \to \frac{Q^*L}{L}$ é um isomorfismo.

Como M é um complemento de L em G, a restrição de f a M é um isomorfismo de M para $\frac{G}{L}$. De fato,

$$Nuc\, f|_M = \{g \in M \mid gL = L\} = M \cap L = 1 \quad e \quad |M| = \left|\frac{G}{L}\right|.$$

Logo, $f|_M : M \to \frac{G}{L}$ é um isomorfismo.

Portanto, f aplica $Q = O_q(M)$ sobre $O_q\left(\frac{G}{L}\right)$ e, então, pelo que vimos acima,

$$\frac{QL}{L} = O_q\left(\frac{G}{L}\right) = \frac{Q^*L}{L}.$$

Assim, $QL = Q^*L$. Por $e)$, $p \neq q$ e então, Q e Q^* são q-subgrupos de Sylow de QL. Portanto, pelo teorema de Sylow, existe $x \in QL$ tal que $Q^* = Q^x$. Vimos em $e)$ que $M = N_G(Q)$. Como $Q^* \trianglelefteq M^*$, $M^* \leq N_G(Q^*) = N_G(Q^x) = [N_G(Q)]^x = M^x$. Como M e M^* são complementos de L em G, temos que $|M^*| = \left|\frac{G}{L}\right| = |M| = |M^x|$ e, portanto $M^* = M^x$.$\blacksquare$

Observação 2.1 *Se G é um grupo solúvel finito não-trivial, então existe um primo p tal que $O_p(G) \neq 1$. De fato, existe $1 \neq H \trianglelefteq G$. Assim, existe $1 \neq N \leq H$ que é normal minimal em G. Em particular N é um fator principal de G. Logo, pela proposição 1.8, existem um primo p e um inteiro positivo n, tal que $|N| = p^n$ e, então $1 \neq N \leq O_p(G)$.*

Assim sendo, se G é um grupo solúvel primitivo e não-trivial, as afirmações de $a)$ e $d)$ ocorrem. Em particular, existe um único primo p tal que $O_p(G) \neq 1$. Como M também é solúvel, existe um primo q tal que $O_q(M) \neq 1$ e então as afirmações $e)$ e $f)$ também ocorrem.

Corolário 2.2 *Sejam G um grupo solúvel finito não-trivial e M, M^* subgrupos maximais de G. Então, M e M^* são subgrupos conjugados de G se, e somente se, $M_G = M^*_G$.*

Prova: Suponhamos que $N = M_G = M^*_G$. Temos que $\frac{G}{N}$ é um subgrupo solúvel primitivo não-trivial. Pela observação 2.1, existe um primo p tal que $\frac{L}{N} = O_p\left(\frac{G}{N}\right) \neq 1$ e então todas as afirmações do teorema 2.1 ocorrem.

Pelo teorema, $\frac{M}{N}$ e $\frac{M^*}{N}$ são complementos de $\frac{L}{N}$ em $\frac{G}{N}$ e então, existe $g = xN \in \frac{G}{N}$ tal que $\left(\frac{M}{N}\right)^g = \frac{M^*}{N}$. Assim, dado $m \in M$, temos

$$(mN)^g = (mN)^{xN} = x^{-1}N(mN)xN = x^{-1}mxN = m^xN \in \frac{M^x}{N}.$$

Logo, $\frac{M^*}{N} = \left(\frac{M}{N}\right)^g \leq \frac{M^x}{N}$ e portanto, $M^* = M^x$ para algum $x \in G$.

Agora, sejam M e M^* subgrupos conjugados de G. Isto é, existe $g \in G$ tal que $M^* = M^g$. Seja N um conjugado a M^*. Assim, existe $x \in G$ tal que $N^x = M^* = M^g$. Logo, $N^{xg^{-1}} = M$ e então, N é conjugado a M. Portanto, todo conjugado a M é conjugado a M^* e vice-versa. Logo,

$$M_G = \bigcap_{g\in G} M^g = \bigcap_{h\in G} (M^*)^h = M^*_G. \blacksquare$$

Para encerrarmos o capítulo, faremos algumas aplicações do teorema de Ore-Baer.

Lema 2.1 *Sejam L e M subgrupos maximais distintos de um grupo solúvel finito G. Então quaisquer duas das afirmações são equivalentes:*

a) L é conjugado a M em G;

b) $LM \neq G$;

c) LM não é um subgrupo de G.

Prova: $a) \Rightarrow b)$: Existe $g \in G$ tal que $M = L^g \neq L$. Suponha que $LM = G$. Então $g = lm$, onde $l \in L$ e $m \in M$. Assim, $M = L^{lm} = L^m$ e, então $M = M^{m^{-1}} = L$, absurdo.

$b) \Rightarrow c)$: Se LM for um subgrupo de G, então, como $L \lessdot G$ e $M \leq L$, $ML = G$, absurdo.

$c) \Rightarrow a)$: Suponha que L e M não são conjugados em G. Seja $K = L_G$ e $R = M_G$. Pelo corolário de Ore-Baer, $K \neq R$, pois, L e M não são conjugados. Sem perda de generalidade, podemos supor que $K \nleq R$. Logo, $K \nleq M$ e, portanto, $LM \geq KM = G$. Portanto, $LM = G$, absurdo.$\blacksquare$

Definição 2.4 *Seja $\frac{H}{K}$ um fator principal de G. Diz-se que $\frac{H}{K}$ é de Frattini se $\frac{H}{K} \leq \Phi\left(\frac{G}{K}\right)$.*

Lema 2.2 *Sejam $\frac{H}{K}$ um fator principal abeliano de um grupo finito G. Então:*

a) Se $\frac{H}{K}$ não é de Frattini, então $\frac{H}{K}$ possui complemento.

b) Se $\frac{H}{K}$ possui complemento $\frac{M}{K}$, então M é um subgrupo maximal de G.

Prova: *a*) Por hipótese, $\frac{H}{K} \nleq \Phi\left(\frac{G}{K}\right)$. Assim, $\frac{H}{K} \nleq \frac{M}{K}$ para algum $\frac{M}{K}$ maximal de $\frac{G}{K}$. Logo, $HM = G$. Pelo teorema dos isomorfismos $\frac{G}{H} \simeq \frac{M}{H\cap M}$. Como $\frac{H\cap M}{K} \leq \frac{H}{K}$, $K = H \cap M$ ou $H \cap M = H$. Se $H \cap M = H$, então $H \leq M$, absurdo. Portanto, $H \cap M = K$ e, então $\frac{M}{K}$ complementa $\frac{H}{K}$ em $\frac{G}{K}$.

b) Seja $\frac{M}{K}$ um complemento de $\frac{H}{K}$ em $\frac{G}{K}$, e $M \leq L \lessdot G$. Como $H \nleq L$, o argumento da parte *a*) mostra que $\frac{L}{K}$ complementa $\frac{H}{K}$ em $\frac{G}{K}$. Então $|G : L| = \left|\frac{H}{K}\right| = |G : M|$, e portanto $M = L$.■

Do lema 2.2, item *b*), temos que se $\frac{H}{K}$ é de Frattini, então $\frac{H}{K}$ não possui complemento.

Teorema 2.2 *Sejam L e M subgrupos maximais não-conjugados de um grupo solúvel finito G. Se $M_G \nleq L_G$, então $M \cap L$ é um subgrupo maximal de L.*

Prova: Sejam $R = M_G$ e $\frac{S}{R}$ o único subgrupo normal minimal do grupo solúvel primitivo $\frac{G}{R}$. Se $R \leq L$, então $R \leq L_G$. Mas, por hipótese, $R \nleq L_G$. Logo, $R \nleq L$ e, assim $LR = G$. Por Dedekind, $S = S \cap G = S \cap LR = (S \cap L)R$. Pelo teorema dos isomorfismos,

$$\frac{S}{R} = \frac{(S\cap L)R}{R} \simeq \frac{S\cap L}{R\cap S\cap L} = \frac{S\cap L}{R\cap L}$$

e, portanto, $\frac{S\cap L}{R\cap L}$ é um fator principal de L. Mostraremos que $\frac{M\cap L}{R\cap L}$ é um complemento de $\frac{S\cap L}{R\cap L}$ em $\frac{G}{R\cap L}$, e assim, pelo lema 2.2, item *b*), temos que $M \cap L \lessdot G$.

Como $S\cap L \leq L$ e $L\cap M \leq L$, $(S\cap L)(L\cap M) \leq L$. Assim, $|L : L\cap M| \geq |(S\cap L)(M\cap L) : L \cap M|$. Pelo teorema dos isomorfismos

$$\begin{aligned} |(S\cap L)(M\cap L) : L\cap M| &= |S\cap L : (S\cap L)\cap(M\cap L)| = \\ &= |S\cap L : R\cap M| = |S : R| = |G : M|. \end{aligned}$$

Pelo lema 2.1, $G = LM$. Logo, $|G : M| = |LM : M| = |L : L\cap M|$. Assim, $|L : L\cap M| = |(S\cap L)(M\cap L) : L\cap M|$ e, então $L = (S\cap L)(M\cap L)$.

Portanto, concluímos o teorema.■

Corolário 2.3 *Sejam L e M subgrupos maximais não-conjugados de um grupo solúvel finito G. Então, $L \cap M$ é maximal em L ou M.*

Prova: Como L e M são não-conjugados, $L_G \neq M_G$. Assim, ou $L_G \nleq M_G$ ou $M_G \nleq L_G$. Daí, do teorema 2.2, $L \cap M \lessdot M$ ou $L \cap M \lessdot L$.■

Capítulo 3

Grupos n-soma

A nossa conversa agora é com a cobertura de grupos por subgrupos próprios. Chamaremos de $\sigma(G)$ o menor número natural tal que G pode ser coberto por $\sigma(G)$ subgrupos próprios. Toda a primeira seção é parte do paper de J. H. E. Cohn, sobre grupos n-soma. Encerramos o capítulo com um resultado fundamental para o nosso trabalho, o teorema de Tomkinson.

3.1 Definições e Resultados

Definição 3.1 *Seja G um grupo finito. Denotamos por $\sigma(G)$ o menor inteiro positivo tal que G é a união de $\sigma(G)$ subgrupos próprios. Neste caso, dizemos que G é um grupo σ-soma, onde $\sigma = \sigma(G)$. E, que a união dos σ subgrupos é uma cobertura de G.*

Sejam M e N subgrupos próprios de G tais que $G = M \cup N$. Como M e N são próprios, existem $m \in M \backslash N$ e $n \in N \backslash M$. Mas, $mn \in G = M \cup N$. Logo, $mn \in M$ ou $mn \in N$. Se $mn \in M$, então $mn = x \in M$ e portanto, $n = m^{-1}x \in M$, absurdo. Se supusermos que $mn \in N$ chegaremos ao mesmo absurdo. Portanto, podemos concluir que não existe grupo 2-soma e então, $\sigma(G) \geq 3$.

Exemplo 6 *O grupo $G = S_3$ é um grupo 4-soma. De fato, os subgrupos próprios não-triviais são: $H_1 = \{Id, (12)\}, H_2 = \{Id, (13)\}, H_3 = \{Id, (23)\}$ e $H_4 = \{Id, (123), (132)\}$.*

Logo, $S_3 = H_1 \cup H_2 \cup H_3 \cup H_4$. Se retirarmos um subgrupo, a união deixa de ser igual a S_3. Assim, $\sigma(S_3) = 4$.

Observação 3.1 *(i) Convencionamos que $\sigma(G) = \infty$, quando G for um grupo cíclico finito. Faremos isto pelo fato de que todo subgrupo de G que contém o gerador é igual a G e, com isso G não pode se igual a união de subgrupos próprios.*

(ii) Todo subgrupo próprio de um grupo finito não-cíclico G está contido em um subgrupo maximal de G. Assim, a cobertura pode ser formada apenas por subgrupos maximais.

No que segue, escrevemos $G = \bigcup_{r=1}^{n} H_r$, onde H_r é subgrupo próprio de G com $i_r = |G : H_r| \leq |G : H_{r+1}|$ para cada $r = 1, \ldots, n-1$.

Teorema 3.1 *Seja $G = \bigcup_{r=1}^{n} H_r$. Então $|G| \leq \sum_{r=2}^{n} |H_r|$, e a igualdade ocorre se, e somente se;*

(i) $H_1 H_r = G$, $\forall\, r \neq 1$ e

(ii) $H_r \cap H_s \subseteq H_1$, $\forall\, r \neq s$.

Prova: Sabemos que a quantidade de elementos de H_r que não são elementos de H_1 é dada por $|H_r| - |H_1 \cap H_r|$. Mas, como $|H_1 H_r| \leq |G|$, $\forall\, r$, temos:

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

Logo,

$$\begin{aligned} |G| &\leq |H_1| + \sum_{r=2}^{n} (|H_r| - |H_1 \cap H_r|) && (3.1) \\ &\leq |H_1| + \sum_{r=2}^{n} |H_r| \left(1 - \frac{|H_1|}{|G|}\right) && (3.2) \\ \Rightarrow \quad |G| &\leq |H_1| + \left(1 - \frac{|H_1|}{|G|}\right) \sum_{r=2}^{n} |H_r| \,. && (3.3) \end{aligned}$$

Dividindo $|G|$ nos dois membros, temos:

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

Como $\frac{|H_1|}{|G|} < 1$, $\left(\frac{|H_1|}{|G|} - 1\right) < 0$ e, portanto $1 - \frac{1}{|G|}\sum_{r=2}^{n}|H_r| \leq 0$. Assim, $|G| \leq \sum_{r=2}^{n}|H_r|$.

Suponha que $|G| = \sum_{r=2}^{n}|H_r|$. Dessa forma, temos:

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

Primeiramente, vamos supor, por absurdo, que $H_1H_k \neq G$ para algum $k \neq 1$. Assim, da desigualdade 3.1, temos:

$$\begin{aligned}
|G| &\leq |H_1| + \sum_{r=2}^{n}\left(1 - \frac{|H_1|}{|H_1H_r|}\right)|H_r| = \\
&= |H_1| + \sum_{\substack{r=2\\ r\neq k}}^{n}\left(1 - \frac{|H_1|}{|G|}\right)|H_r| + \left(1 - \frac{|H_1|}{|H_1H_k|}\right)|H_k| < \\
&< |H_1| + \left(1 - \frac{|H_1|}{|G|}\right)\sum_{\substack{r=2\\ r\neq k}}^{n}|H_r| + \left(1 - \frac{|H_1|}{|G|}\right)|H_k| = \\
&= |H_1| + \left(1 - \frac{|H_1|}{|G|}\right)\sum_{r=2}^{n}|H_r| = |G| \quad \text{(Absurdo!)}
\end{aligned}$$

Portanto, $H_1H_r = G$, $\forall\, r \neq 1$.

Mostraremos agora que $H_r \cap H_s \subseteq H_1$, $\forall\, r \neq s$. Para isto, consideremos $K_i = H_i - H_i \cap H_1$.
AFIRMAÇÃO: $H_i \cap H_j \subseteq H_1 \Leftrightarrow K_i \cap K_j = \varnothing$, $\forall\, i, j \in \{1, \ldots, n\}$ e $i \neq j$.

De fato, para cada $x \in H_i \cap H_j$, temos que $x \in H_1$. Como $K_i \cap K_j$ é formado pelos elementos de $H_i \cap H_j$ que não pertencem a H_1, temos que $K_i \cap K_j = \varnothing$. Reciprocamente, se não existe $y \in K_i \cap K_j$, então não existe y que pertença a $H_i \cap H_j$ e não esteja contido em H_1. Assim, para cada $y \in H_i \cap H_j$, temos que $y \in H_1$. Logo, $H_i \cap H_j \subseteq H_1$, o que prova a afirmação.

Assim, precisamos mostrar que $K_i \cap K_j = \varnothing$, $\forall\, i, j \in \{1, \ldots, n\}$ e $i \neq j$. Se supusermos, por absurdo, que $K_i \cap K_j \neq \varnothing$, para algum i e j, teremos

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

Portanto, $H_r \cap H_s \subseteq H_1$, $\forall\, r \neq s$.

Agora, suponhamos que $H_1 H_r = G$, $\forall\, r \neq 1$ e $H_r \cap H_s \subseteq H_1$, $\forall\, r \neq s$. Se supusermos, por absurdo, que $|G| < \sum_{r=2}^{n} |H_r|$, então

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

Absurdo. Logo, concluímos o teorema.■

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

Prova: Pelo teorema anterior, como $i_2 \leq i_r$, $\forall\, r \geq 2$, temos

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

Logo, $i_2 \leq n - 1$, quando $\sigma(G) = n$.■

O próximo resultado, em parte, generaliza o primeiro.

Teorema 3.2 *Se $\sigma(G) = n$ e $G = \left(\bigcup_{r=1}^{m} H_r\right) \cup \left(\bigcup_{r=m+1}^{n} K_r\right)$, onde cada subgrupo é maximal em G, $H_r \lhd G$ $\forall\, r = 1, \ldots, m$ e $|H_r| \neq |H_s|$, $\forall\, r \neq s$, então $|G| \leq \sum_{r=m+1}^{n} |K_r|$.*

Prova: Seja $|G : H_r| = p_r$ para todo $r = 1, \ldots, m$. Pela proposição 1.9, $p_1, \ldots, p_m$ são todos primos. Por hipótese, $p_1, \ldots, p_m$ são distintos dois a dois. Logo, pelo teorema 1.3

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

Seja $D = \bigcup_{r=1}^{m} H_r$. Assim

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

Como $H_r \lhd G$, $\forall\, r = 1, \ldots, m$ e todos da cobertura de G são maximais, $G = H_r K_s$. Logo,

$$|H_r \cap K_s| = \frac{|H_r||K_s|}{|H_r K_s|} = \frac{|H_r||K_s|}{|G|} = \frac{|K_s|}{p_r}.$$

Assim, $|H_r \cap K_s| = \frac{|K_s|}{p_r}$ $\forall\, r = 1, \ldots, m$ e $s = m+1, \ldots, n$. Mais ainda, $|H_r \cap H_t \cap K_s| \Big| \frac{|K_s|}{p_r}$ e $|H_r \cap H_t \cap K_s| \Big| \frac{|K_s|}{p_t}$. Temos que $|K_s| = p_r a = p_t b$. Como p_r e p_s são distintos, $p_r \mid b$ e $p_t \mid a$. O que implica que $|K_s| = |H_r \cap H_t \cap K_s|.p_r p_t c$. Assim, $|H_r \cap H_t \cap K_s| \Big| \frac{|K_s|}{p_r p_t}$. Por outro lado,

$$\begin{aligned}
|H_r \cap H_t \cap K_s| &= \frac{|K_s||H_r \cap H_t|}{|K_s(H_r \cap H_t)|} \\
&= \frac{|K_s||G|}{p_r p_t |K_s(H_r \cap H_t)|} \\
&\ge \frac{|K_s||G|}{p_r p_t |G|} = \frac{|K_s|}{p_r p_t}
\end{aligned}$$

Portanto, $|H_r \cap H_t \cap K_s| = \frac{|K_s|}{p_r p_t}$, $\forall\, r, t = 1, \ldots, m$ e $\forall\, s = m+1, \ldots, n$.

Seja k_r o número de elementos de K_r que não pertencem a D. Assim,

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

Logo,

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

Donde,

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

Observação 3.2 *Do teorema anterior, temos*

$$|G| \le \sum_{r=m+1}^{n} |K_r| \quad \Rightarrow \quad 1 \le \sum_{r=m+1}^{n} \frac{|K_r|}{|G|} = \sum_{r=m+1}^{n} \frac{1}{i_r}.$$

Como $i_{m+1} \le i_r$, $\forall\, r = m+1, \ldots, n$, *temos que* $\frac{1}{i_r} \le \frac{1}{i_{m+1}}$. *Assim,*

$$1 \le \sum_{r=m+1}^{n} \frac{1}{i_r} \le \sum_{r=m+1}^{n} \frac{1}{i_{m+1}} = \frac{n-m}{i_{m+1}}.$$

Portanto, $i_{m+1} \le n - m$.

Mostraremos algumas relações de $\sigma(G)$ com σ de subgrupos de G.

Lema 3.1 *Se $N \lhd G$, então $\sigma(G) \leq \sigma\left(\frac{G}{N}\right)$.*

Prova: Seja $\frac{G}{N} = \frac{M_1}{N} \cup \ldots \cup \frac{M_m}{N}$ uma cobertura de $\frac{G}{N}$, onde $m = \sigma\left(\frac{G}{N}\right)$. Dado $g \in G$, $gN \in \frac{G}{N}$. Logo, $gN \in \frac{M_i}{N}$ para algum $i = 1, \ldots, m$. Assim $g \in M_i$. Logo, $G \subseteq M_1 \cup \ldots \cup M_m$. Como todos os M_i's são subgrupos de G, temos que $G = M_1 \cup \ldots \cup M_m$. Portanto, $\sigma(G) \leq \sigma\left(\frac{G}{N}\right)$.■

Corolário 3.2 $\sigma(H \times K) \leq min\{\sigma(H), \sigma(K)\}$.

Prova: Seja $G = H \times K$. Sabemos que podemos identificar H com $H \times \{1\}$ e K com $\{1\} \times K$. Assim, $H \lhd G$ e $K \lhd G$, $G = HK$ e $H \cap K = 1$. Logo, pelo lema 3.1

$$\begin{aligned} &\sigma(H \times K) \leq \sigma\left(\frac{H \times K}{K}\right) = \sigma(H) \\ e \qquad &\sigma(H \times K) \leq \sigma\left(\frac{H \times K}{H}\right) = \sigma(K). \end{aligned}$$

Portanto, $\sigma(G) = \sigma(H \times K) \leq min\{\sigma(H), \sigma(K)\}$.■

Dessa forma, dado um grupo n-soma podemos construir outros grupos n-soma.

Definição 3.2 *Um grupo finito G é dito n-soma primitivo se $\sigma(G) = n$ e G não tem um subgrupo normal N tal que $\sigma(G) = \sigma\left(\frac{G}{N}\right)$.*

Observação 3.3 *Se G é um grupo n-soma primitivo, então $\Phi(G) = 1$. De fato, seja $G = M_1 \cup \ldots \cup M_n$ uma cobertura de G por subgrupos maximais. Como $\Phi(G) \leq M_i$, $\forall\, i = 1, \ldots, n$, temos que*

$$\frac{G}{\Phi(G)} = \frac{M_1}{\Phi(G)} \cup \ldots \cup \frac{M_n}{\Phi(G)}.$$

Assim, $\sigma\left(\frac{G}{\Phi(G)}\right) \leq n$. Logo, $\sigma(G) = \sigma\left(\frac{G}{\Phi(G)}\right)$. Como G é n-soma primitivo, $\Phi(G) = 1$.

Para nós C_p sempre denotará um grupo cíclico de ordem p.

Lema 3.2 *$C_p \times C_p$ é um grupo $(p+1)$-soma primitivo, onde p é primo.*

Prova: Sabemos que $|C_p \times C_p| = p^2$. Assim, todo subgrupo próprio tem índice p. Logo, pelo corolário 3.1, $\sigma(C_p \times C_p) \geq p+1$. Por outro lado, sejam $\langle a \rangle$ e $\langle b \rangle$ dois grupos cíclicos de ordem p. Assim,

$$C_p \times C_p = \langle a \rangle \times \langle b \rangle \simeq \{a^i b^j \,|\, 0 \leq i, j \leq p-1\}.$$

Consideremos $H_i = \langle ab^i \rangle$ e $H = \langle b \rangle$. Logo, $C_p \times C_p = H_0 \cup H_1 \cup \ldots \cup H_{p-1} \cup H$. O que implica que $\sigma(C_p \times C_p) \leq p+1$. Portanto, $\sigma(C_p \times C_p) = p+1$.

Como $C_p \times C_p$ é abeliano de ordem p^2, temos que todo subgrupo próprio e não-trivial de $C_p \times C_p$ é normal e tem índice p. Assim, o grupo quociente de $C_p \times C_p$ por um subgrupo próprio é cíclico. Portanto, $C_p \times C_p$ é $(p+1)$-soma primitivo.■

No próximo teorema, mostraremos que $C_p \times C_p$ não é apenas um grupo $(p+1)$-soma primitivo, mas o único com essa propriedade.

Teorema 3.3 *Se G é um p-grupo não-cíclico, então $\sigma(G) = p+1$, e G é um $(p+1)$-soma primitivo se, e somente se, $G = C_p \times C_p$.*

Prova: Seja $|G| = p^k$. Como todo subgrupo próprio tem índice potência de p, temos pelo corolário 3.1, $\sigma(G) \geq p^\alpha + 1 \geq p+1$.

Se supusermos que G é abeliano, então G é o produto direto de dois p-subgrupos. Logo, existe subgrupo K de G tal que $\frac{G}{K} \simeq C_p \times C_p$. Portanto, $\sigma(G) \leq \sigma\left(\frac{G}{K}\right) = p+1$ e, então $\sigma(G) = p+1$. Mas, se G não for abeliano, mostraremos por indução sobre k, que $\sigma(G) \leq p+1$.

- $k = 2$:

  Como G é não-cíclico, $G \simeq C_p \times C_p$. Assim, $\sigma(G) = p+1$, pelo lema anterior.

- Hipótese de Indução: O resultado vale para todo grupo com ordem menor que p^k, onde $k \geq 3$.

  Como G é não-abeliano, $1 \neq Z(G) \neq G$. Como $\frac{G}{Z(G)}$ não é cíclico (de fato, se $\frac{G}{Z(G)}$ é cíclico, então G é abeliano) temos, por hipótese, que $\sigma\left(\frac{G}{Z(G)}\right) \leq p+1$. Assim, $\sigma(G) \leq \sigma\left(\frac{G}{Z(G)}\right) \leq p+1$. Portanto, $\sigma(G) = \sigma\left(\frac{G}{Z(G)}\right) = p+1$.

  Ademais, se G for $(p+1)$-soma primitivo, então $G = Z(G)$, pois, $Z(G) \neq 1$ e $\sigma(G) = \sigma\left(\frac{G}{Z(G)}\right)$. Assim, G é abeliano e pelo o que vimos anteriormente existe um subgrupo

K de G tal que $\frac{G}{K} \simeq C_p \times C_p$. Assim, $\sigma\left(\frac{G}{K}\right) = p + 1 = \sigma(G)$. Logo, $K = 1$ e, então $G \simeq C_p \times C_p$.$\blacksquare$

Para desenvolvermos o próximo lema, precisamos do argumento da seguinte proposição.

Proposição 3.1 *Seja $G = H \times K$, onde $mdc(|H|, |K|) = 1$, e $S \leq G$. Então $S = (H \cap S) \times (K \cap S)$. Se $M \lessdot G$, então $M = H \times L$, onde $L \lessdot K$, ou $M = L \times K$, onde $L \lessdot H$.*

Prova: Como $|G| = |H||K|$, temos que $|G : H| = \frac{|G|}{|H|} = |K|$ e $|G : K| = |H|$. Assim, $mdc(|G : H|, |G : K|) = 1$. Logo,

$$\frac{|G|}{|H \cap K|} = |G : H \cap K| = |G : H||G : K| = \frac{|G|}{|H|}\frac{|G|}{|K|}.$$

O que implica que $|G| = \frac{|H||K|}{|H \cap K|} = |HK|$ e, então $G = HK$. Assim, podemos supor que $G = HK$, com $H \lhd G, K \lhd G$ e $H \cap K = 1$. Como $mdc(|G : H|, |G : K|) = 1$, temos que $mdc(|S : S \cap H|, |S : S \cap K|) = 1$ e, então, pelo argumento acima, $S = (S \cap H)(S \cap K)$. Logo, $S = (S \cap H) \times (S \cap K)$.

Agora, seja $M \lessdot G$. Vimos que $M = (H \cap M) \times (K \cap M)$. Temos que $M \leq HM \leq G$ e $M \leq KM \leq G$. Assim,

(i) $M = HM$ ou $HM = G$ e

(ii) $M = KM$ ou $KM = G$.

Seja $HM = G$. Como $\frac{G}{H} \simeq K$ e $\frac{HM}{H} \simeq M \cap K$, temos que $K = M \cap K$. O que implica que $K \leq M$. Assim, $M = (H \cap M) \times K$.

AFIRMAÇÃO: $H \cap M \lessdot H$.

Seja $H \cap M \leq S \leq H$. Veja que $M = (H \cap M)K \leq SK \leq G$. Assim, $M = SK$ ou $SK = G$. Se $M = SK$, então $S = S \cap SK = S \cap M \leq H \cap M$. Logo, $S = H \cap M$. Por outro lado, se $SK = G$, então $H = H \cap SK = (H \cap K)S = S$, o que prova a afirmação.

O outro caso é análogo. Logo, segue a proposição.$\blacksquare$

Lema 3.3 *Sejam H e K dois grupos finitos. Se $mdc(|H|, |K|) = 1$, então $\sigma(H \times K) = min\{\sigma(H), \sigma(K)\}$.*

Prova: É fácil ver que $G = H \times K$ é cíclico se, e somente se, ambos os grupos H e K são cíclicos. Neste caso, tudo certo.

Suponhamos que G não é cíclico e que $\sigma(G) = n$. Da proposição 3.1 qualquer subgrupo de G é da forma $X \times Y$, onde $X \leq H$ e $Y \leq K$, e para qualquer subgrupo maximal de G, ou $X = H$ e $Y \lessdot K$, ou $Y = K$ e $X \lessdot H$. Assim, uma cobertura de G por maximais é da forma

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

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

Nosso objetivo é mostrar que $p = 0$ ou $q = 0$. Para isto, suponhamos que $q \neq 0$. Assim, $G_1 \neq G$, isto é, existe $(h_1, k) \in G$ tal que $(h_1, k) \notin G_1$. Mas, como $G_1 = \bigcup_{r=1}^{p} H \times Y_r$, temos que $(h, k) \notin G_1$, $\forall\, h \in H$. Assim, $(h, k) \in G_2$, $\forall\, h \in H$. Logo, $(h, k) \in G_2$, $\forall\, (h, k) \in G$. Portanto, $G = G_2$ e, então $p = 0$. Como $p = 0$, temos que

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

Portanto, $H = \bigcup_{s=1}^{q} X_s$ e, então $\sigma(H) \leq n$. Da mesma forma, se $q = 0$, então $\sigma(K) \leq n$. Assim, $min\{\sigma(H), \sigma(K)\} \leq n = \sigma(G)$. Portanto, pelo corolário 3.2, $\sigma(G) = min\{\sigma(H), \sigma(K)\}$.■

Veremos a seguir um importante resultado sobre cobertura de grupos nilpotentes.

Teorema 3.4 *Se G é um grupo nilpotente finito não-cíclico, então $\sigma(G) = p + 1$, onde p é o menor primo tal que o p-subgrupo de Sylow de G é não-cíclico. Ademais, o único grupo $(p + 1)$-soma primitivo e nilpotente é $C_p \times C_p$.*

Prova: Seja $|G| = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Do teorema de caracterização dos grupos nilpotentes finitos, temos que $G = P_1 \times \ldots \times P_r$, onde P_i é p_i-subgrupo de Sylow de G para cada $i = 1, \ldots, r$. Como os primos $p_1, \ldots, p_r$ são, dois a dois, distintos temos, pelo teorema anterior, que $\sigma(G) = min\{\sigma(P_1), \ldots, \sigma(P_r)\}$. Como G é não-cíclico, existe P_i que é não-cíclico. Seja p_i o menor primo tal que P_i é não cíclico. Como P_i é p_i-grupo, temos, pelo teorema 3.3, que $\sigma(P_i) = p_i + 1$. Portanto, $\sigma(G) = \sigma(P_i) = p_i + 1$.

Pelo mesmo teorema citado, $C_p \times C_p$ é o único grupo $(p+1)$-soma primitivo e nilpotente, pois, $|C_p \times C_p| = p^2$.■

Lema 3.4 *Sejam $G = \bigcup_{r=1}^{n} H_r$, onde $\sigma(G) = n$, e L um subgrupo de todos os H_r's, com exceção, possivelmente, de um dos H_r's. Então $L \leq H_r$, $\forall\, r = 1, \ldots, n$.*

Prova: Suponhamos que $L \leq H_r$, $\forall\, r = 1, \ldots, k-1, k+1, \ldots, n$ e $L \nleq H_k$. Tomemos $a \in H_k$ tal que $a \notin H_r$, $\forall\, r \neq k$.

AFIRMAÇÃO: $aL \cap H_r = \varnothing$, $\forall\, r \neq k$.

De fato, se existe $x_r \in aL \cap H_r$, então $x_r \in aL$ e $x_r \in H_r$. Assim, existe $y \in L$ tal que $x_r = ay$. Assim, $a = x_r y^{-1} \in H_r L = H_r$, absurdo.

Como $G = \bigcup_{r=1}^{n} H_k$, $aL \leq H_k$. Portanto, $L \leq H_k$.■

Para encerrarmos a seção, discutiremos um resultado sobre grupos n-soma primitivos.

Teorema 3.5 *Seja G um grupo n-soma primitivo, então ou $G \simeq C_p \times C_p$ ou, $Z(G)$ é um subgrupo trivial.*

Prova: Se supusermos G abeliano, então G será nilpotente. Logo, pelo teorema 3.4, $G \simeq C_p \times C_p$. Por outro lado, se supusermos que G não é abeliano, mostraremos que $Z(G) = 1$. Para isto, suponha, por absurdo, que $Z(G) \neq 1$. Assim, existe um primo p tal que $p \mid |Z(G)|$. Pelo teorema de Cauchy, existe $u \in Z(G)$ tal que $o(u) = p$. Sejam $U = \langle u \rangle$ e $G = \bigcup_{r=1}^{n} H_r$, onde todos os H_r's são maximais em G. Como G é n-soma primitivo e $U \lhd G$, temos que $\sigma(G) < \sigma\left(\frac{G}{U}\right)$. Assim, U não está contido em todos os H_r's. Pelo lema 3.4, U não está contido em, no mínimo, dois maximais. Sejam H e K maximais da cobertura tal que $U \nleq H$ e $U \nleq K$. Dessa forma, $U \cap H = 1 = U \cap K$. Como $H \lessdot G$, $G = HU$ e, então

$$G = \bigcup_{i=0}^{p-1} Hu^i. \tag{3.4}$$

Além disso, $H^G = H^{HU} = (H^H)^U = H^U = H$, pois $U \leq Z(G)$. Logo, $H \lhd G$ e então, $\frac{G}{H} \simeq U \simeq C_p$.

Analogamente, $K \lhd G$ e $\frac{G}{K} \simeq U \simeq C_p$. Assim, $\sigma(G) < \sigma(H)$ e $\sigma(G) < \sigma(K)$. Como H e K são normais e maximais de G, temos que $G = HK$ e $X = H \cap K \lhd G$. Assim, $\left|\frac{H}{X}\right| = \left|\frac{G}{K}\right| = p$ e então $\left|\frac{G}{X}\right| = \left|\frac{G}{H}\right| \left|\frac{H}{X}\right| = p^2$. Dessa forma, $X \neq 1$. De fato, se $X = 1$, então $|G| = p^2$. Assim, G seria abeliano, o que é absurdo.

De $\frac{H}{X} \simeq C_p$, temos $\frac{H}{X} = \langle vX \rangle$, onde $v \notin X$ e $v^p \in X$. Daí,

$$H = \bigcup_{j=0}^{p-1} Xv^j = X\langle v \rangle, \text{ onde } v \notin X \text{ e } v^p \in X. \tag{3.5}$$

Substituindo (3.5) em (3.4), temos

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

Mas, para cada $0 < j \leq p-1$ e $0 < i \leq p-1$ existe um único $0 < k \leq p-1$ tal que $ik \equiv j \,(mod\, p)$. Assim, podemos reescrever $Xu^i v^j = Xu^i v^{ik} = X(uv^k)^i$, pois $u \in Z(G)$. E então

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

Para cada $k = 0, \ldots, p-1$, definiremos

$$B_k = \bigcup_{i=0}^{p-1} X(uv^k)^i = X\langle uv^k \rangle \leq G.$$

AFIRMAÇÃO: $|G : B_k| = p$, $\forall\, k = 0, \ldots, p-1$.

Temos que $X \leq B_k \leq G$. Como $|G : X| = p^2$, temos que $|B_k : X| = 1, p$ ou p^2.

Se $|B_k : X| = 1$, então $X = B_k = X\langle uv^k \rangle$. Assim, $\langle uv^k \rangle \leq X$. Daí, $uv^k = x \in X \Rightarrow u = xv^{-k} \in XH = H \Rightarrow u \in H \cap U = 1$, absurdo.

Se $|B_k : X| = p^2$, então $G = B_k = X\langle uv^k\rangle$. Assim, $H \leq X\langle uv^k\rangle$. Daí, $h = x(uv^k)^i$, onde $h \in H, x \in X$ e $0 \leq i \leq p-1 \Rightarrow\ h = xu^iv^{ki}\ \Rightarrow\ u^i = x^{-1}hv^{-ki} \in XH = H\ \Rightarrow\ u^i \in H \cap U = 1\ \Rightarrow\ i = 0$.

Logo, para todo $h \in H$, $h = x(uv^k)^0 = x \in X$. Assim, $H \leq X \leq H$ e com isso, $X = H$, absurdo, pois $\left|\frac{H}{X}\right| = p$.

Portanto, $|B_k : X| = p$ e com isso, $|G : B_k| = p$, $\forall\, k = 0, \ldots, p-1$, o que prova a afirmação.

Dessa forma, $B_k \lessdot G$ para todo $k = 0, \ldots, p-1$. Como $G = H \cup \left(\bigcup_{k=0}^{p-1} B_k\right)$, temos que $\sigma(G) \leq p+1$.

AFIRMAÇÃO: $U \nleq B_k$ para $0 < k \leq p-1$.

De fato, se $\langle u\rangle \leq B_k$, então teríamos $u = x(uv^k)^r$, para algum $0 < r \leq p-1$. Assim, $u = xu^rv^{kr} = xu^rv^j \overset{u\in Z(G)}{\Rightarrow} u^{r-1} = x^{-1}v^{-j}\,(0 < j \leq p-1)$. Daí, $u^{r-1} \in H \cap U = 1$. Assim, $r = 1$ e $u = xuv^k \Rightarrow 1 = xv^k \Rightarrow v^k = x^{-1} \in X$. Absurdo, pois,$0 \leq k \leq p-1$.

Dessa forma, $U \cap B_k = 1$, $\forall\, k = 1, \ldots, p-1$. Também temos $G = B_kU$, pois $B_k \lessdot G$. Assim,

$$B_k^G = B_k^{B_kU} = (B_k^{B_k})^U = B_k^U = B_k,\ \text{pois } U \leq Z(G).$$

Com isso, $B_k \lhd G$ e então $\sigma(G) < \sigma\left(\frac{G}{U}\right) = \sigma(B_k)$.

Veja que

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

Se $H_r \cap B_k \neq B_k$, $\forall\, k = 1, \ldots, n$, então $\sigma(B_k) \leq n$. Mas, $\sigma(B_k) > \sigma(G) = n$. Logo, $H_r \cap B_k = B_k$ para algum $r = 1, \ldots, n$. Assim, $B_k \leq H_r$. Mas, $B_k \lessdot G$ e assim, $B_k = H_r$. Portanto, para cada $k = 1, \ldots, p-1$, existe $r_k = 1, \ldots, n$ tal que $B_k = H_{r_k}$. Assim, na representação $G = \bigcup_{r=1}^{n} H_r$ existem, no mínimo, p maximais, a saber, $H, B_1, \ldots, B_{p-1}$ e U não está contido em nenhum deles. Dessa forma $\sigma(G) \geq p+1$ e, então $\sigma(G) = p+1$.

Mas, veja que

$$\frac{G}{X} \simeq \frac{H}{X} \times \frac{K}{X} \simeq C_p \times C_p.$$

Logo, $\sigma\left(\frac{G}{X}\right) = p+1 = \sigma(G)$, absurdo, pois, $X \neq 1$ e G é n-soma primitivo. Portanto, $Z(G) = 1$.■

3.2 O Teorema de Tomkinson

Para chegarmos ao teorema principal desta seção, vamos discutir alguns lemas que serão utilizados na discussão do nosso resultado.

Lema 3.5 *Se o fator principal $\frac{H}{K}$ de um grupo finito G é abeliano e tem um único complemento, então $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$. Ademais, existe um primo q tal que $\left|\frac{H}{K}\right| = q$.*

Prova: Seja $\frac{L}{K}$ o único complemento de $\frac{H}{K}$ em G. Assim sendo, não existem conjugados a $\frac{L}{K}$ em G e, por isso, $\frac{L}{K} \lhd \frac{G}{K}$. Como $\frac{H}{K} \lhd \frac{G}{K}$, temos que $\frac{G}{K} \simeq \frac{L}{K} \times \frac{H}{K}$. Nestas condições, os elementos de $\frac{L}{K}$ comutam com os elementos de $\frac{H}{K}$. Como $\frac{H}{K}$ é abeliano, $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$. Com isso, todo subgrupo próprio de $\frac{H}{K}$ é normal em $\frac{G}{K}$. Mas, $\frac{H}{K}$ é normal minimal de $\frac{G}{K}$ e assim, $\frac{H}{K}$ não possui subgrupo próprio. Portanto, $\left|\frac{H}{K}\right| = q$, para algum primo q.■

Proposição 3.2 *Se G é um grupo solúvel finito tal que todo fator principal tem um único complemento ou é de Frattini, então G é nilpotente.*

Prova: Seja N um normal minimal de G. Do argumento da proposição 1.8, N é abeliano. Por hipótese, N é de Frattini ou possui um único complemento. Neste último caso, temos, pelo lema anterior, que $N \leq Z(G)$.

Vamos provar por indução sobre a ordem de G. Suponhamos que todo grupo satisfazendo as hipóteses da proposição e com ordem menor que $|G|$ é nilpotente. Assim, $\frac{G}{N}$ é nilpotente.

1^o caso: $N \leq Z(G)$.

Neste caso, $\frac{G}{Z(G)} \simeq \frac{\frac{G}{N}}{\frac{Z(G)}{N}}$ é nilpotente. Pela observação 1.2, G é nilpotente.

2^o caso: $N \leq \Phi(G)$.

Assim, pela proposição 1.12, $\Phi\left(\frac{G}{N}\right) = \frac{\Phi(G)}{N}$. Logo,

$$\frac{G}{\Phi(G)} \simeq \frac{\frac{G}{N}}{\frac{\Phi(G)}{N}} = \frac{\frac{G}{N}}{\Phi\left(\frac{G}{N}\right)} \text{ é nilpotente.}$$

Pelo teorema 1.9, G é nilpotente.■

Observação 3.4 *Da proposição 3.2, temos que se G é não-nilpotente, então existe fator principal de G que possui mais de um complemento em G.*

Lema 3.6 *Sejam G um grupo solúvel primitivo não-cíclico. Se o único subgrupo normal minimal N de G é tal que $\frac{G}{N}$ é cíclico, então $\sigma(G) = |N| + 1$.*

Prova: Seja M um subgrupo maximal de G tal que $M_G = 1$. Assim, $MN = G$ e $M \cap N = 1$. Sabemos que todos os $|G : N_G(M)| = |G : M| = |N|$ subgrupos maximais conjugados a M complementam N. Pelo corolário 2.2, esses maximais têm núcleo normal trivial. Todos são cíclicos, pois, $M_i \simeq \frac{G}{N}$.

Seja $G = X_1 \cup \ldots \cup X_n$, onde $\sigma(G) = n$. Temos que

$$\langle x_i \rangle = M_i = M_i \cap G = M_i \cap \left(\bigcup_{j=1}^{n} X_j \right) = \bigcup_{j=1}^{n} (M_i \cap X_j), \ \forall\, i = 1, \ldots, |N|.$$

Logo, $x_i \in M_i \cap X_j$ para algum $j = 1, \ldots, n$. Assim, $M_i \leq X_j$. Portanto, $M_i = X_j$ para algum $j = 1, \ldots, n$ e, então $|N| \leq n$. Veja que dado$x \in N$, $1 \neq x \notin M_i$, $\forall\, i = 1, \ldots, |N|$. Logo, $N \nleq M_1 \cup \ldots \cup M_{|N|}$. Portanto, $M_1 \cup \ldots \cup M_{|N|} \neq G$ e, assim $|N| + 1 \leq \sigma(G)$.

Agora, mostraremos que $\sigma(G) \leq |N| + 1$. Como M_i e M_j são cíclicos, $M_i \cap M_j$ é normal em ambos. Assim, $M_i \cap M_j \lhd \langle M_i, M_j \rangle = G$. Como M_i possui núcleo normal trivial em G, $M_i \cap M_j = 1$, $\forall\, i, j$. Sendo $m = |N|$, temos

$$\begin{aligned}
|M_1 \cup \ldots \cup M_m| &= |\{1\} \cup (M_1 - \{1\}) \cup \ldots \cup (M_m - \{1\})| = 1 + m(|M| - 1) \\
&= 1 + |N| \left(\frac{|G|}{|N|} - 1 \right) = 1 + |G| - |N| = |G| - (|N| - 1). \\
\therefore \quad |G| &= |M_1 \cup \ldots \cup M_m| + |N| - 1.
\end{aligned}$$

Mas,

$$\begin{aligned}
|M_1 \cup \ldots \cup M_m \cup N| &= |(M_1 \cup \ldots \cup M_m) \cup (N - \{1\})| = \\
&= |M_1 \cup \ldots \cup M_m| + |N| - 1 = |G|.
\end{aligned}$$

Portanto, $\sigma(G) \leq |N| + 1$.$\blacksquare$

O último resultado antes do teorema principal é dado a Wolfgang Gaschütz. O leitor mais interessado no assunto poderá encontrar a demonstração no paper intitulado "*Existenz und Konjugiertsein von Untergruppen, die in endlichen auflösbaren Gruppen durch gewisse Indexschranken definiert sind*", publicado em 1977.

Teorema 3.6 (Gaschütz) *Seja G um grupo solúvel primitivo finito e L o único subgrupo normal minimal de G. Então, todo fator principal de G distinto de L tem ordem menor que a ordem de L.*

Teorema 3.7 (Tomkinson) *Sejam G um grupo solúvel finito e não-nilpotente e $\frac{H}{K}$ um fator principal de G com ordem mínima entre os que possuem mais que um complemento em G. Então $\sigma(G) = \left|\frac{H}{K}\right| + 1$.*

Prova: Veja que a existência de $\frac{H}{K}$ é garantida pela observação 3.4. Como G é solúvel finito, pela proposição 1.8, existe um primo p e um inteiro positivo a tal que $|\frac{H}{K}| = p^a$. Mostraremos, primeiramente, que $\sigma(G) \leq p^a + 1$.

Escolhamos um fator principal $\frac{V}{W}$ de G com a seguintes propriedades:

(i) $\frac{V}{W}$ tem mais de um complemento em G.

(ii) $\left|\frac{V}{W}\right| = p^a$.

(iii) $\frac{G}{V}$ tem ordem mínima com as propriedades anteriores.

Assim sendo, se $\frac{S}{T}$ é um fator principal de G com complemento, $\left|\frac{S}{T}\right| \leq p^a$ e $S > V$, então $\frac{S}{T}$ possui um único complemento em G. Como $\frac{S}{T}$ é abeliano, pois, G é solúvel, temos, pelo lema 3.5, que $\frac{S}{T} \leq Z\left(\frac{G}{T}\right)$ e $\left|\frac{S}{T}\right| = q$, para algum primo q.

Seja M um complemento de $\frac{V}{W}$ em G. Assim, $\frac{G}{W} \simeq \frac{V}{W} \rtimes \frac{M}{W}$. Logo, M é um subgrupo maximal de G. Seja $Y = M_G$. Temos que $\frac{G}{Y}$ é um grupo primitivo e seja $\frac{X}{Y}$ o único normal minimal de $\frac{G}{Y}$. Como $W \leq M$ e $W \lhd G$, temos que $W \leq Y$.

AFIRMAÇÃO 1: $X = YV$ e $Y \cap V = W$.

De fato, $\frac{YV}{Y} \lhd \frac{G}{Y}$. Assim, $X \leq YV$. Por Dedekind,

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

Temos que $W \leq Y \cap V$. Assim, $\frac{Y \cap V}{W} \lhd \frac{G}{W}$ e $Y \cap V \leq V$. Logo, $Y \cap V = W$ ou $Y \cap V = V$. Se $Y \cap V = V$, então $V \leq Y$. Assim, pelo que vimos acima, $Y = YV = X$, absurdo. Portanto, $W = Y \cap V$.

Assim sendo, $\frac{X}{Y} = \frac{YV}{Y} \simeq \frac{V}{Y \cap V} = \frac{V}{W}$. Logo, $\left|\frac{X}{Y}\right| = p^a$. Se $X > V$, então, pelo que vimos acima, $\frac{X}{Y} \leq Z\left(\frac{G}{Y}\right)$ e $\left|\frac{X}{Y}\right| = p$.

AFIRMAÇÃO 2: $\frac{V}{W} \leq Z\left(\frac{G}{W}\right)$.

Com efeito, temos que $X = YV$ e $[X, G] \leq Y$. Assim,

$$[X, G] \leq Y \Rightarrow [YV, G] \leq Y \Rightarrow [Y, G][V, G] \leq Y.$$

Como $Y \lhd G$, temos que $[Y, G] \leq Y$ e, portanto, $[V, G] \leq Y$. Por outro lado, $V \lhd G$ e assim $[V, G] \leq V$. Portanto, $[V, G] \leq Y \cap V = W$.

Sejam $\frac{M_1}{W}$ e $\frac{M_2}{W}$ complementos de $\frac{V}{W}$ em G. Como $\frac{V}{W} \leq Z\left(\frac{G}{W}\right)$, temos

$$\left(\frac{M_i}{W}\right)^{\frac{G}{W}} = \left(\frac{M_i}{W}\right)^{\frac{M_i}{W}\frac{V}{W}} = \left(\frac{M_i}{W}\right)^{\frac{V}{W}} = \frac{M_i}{W}, \quad \forall\, i = 1, 2.$$

Portanto, $\frac{M_i}{W} \lhd \frac{G}{W}$, $\forall\, i = 1, 2$.

Assim, $\frac{G}{W} = \frac{M_i}{W} \times \frac{V}{W}$, com $\left|\frac{G}{W} : \frac{M_i}{W}\right| = \left|\frac{V}{W}\right| = p$, $\forall\, i = 1, 2$. Pelo epimorfismo $\varphi : G \to \frac{G}{M_1} \times \frac{G}{M_2} : g \mapsto (gM_1, gM_2)$, temos que $Nuc = (\varphi)\{g \in G \,|\, (gM_1, gM_2) = ((M_1, M_2))\} = M_1 \cap M_2$. Portanto,

$$\frac{G}{M_1 \cap M_2} \simeq \frac{G}{M_1} \times \frac{G}{M_2} \simeq C_p \times C_p \Rightarrow \sigma(G) \leq \sigma\left(\frac{G}{M_1 \cap M_2}\right) = p + 1.$$

Agora, suponhamos que $X = V$. Logo, $Y = W$, $\frac{G}{W}$ é primitivo e $\frac{V}{W}$ é o único normal minimal de $\frac{G}{W}$. Pelo teorema de Gaschütz, todo fator principal de $\frac{G}{W}$, distinto de $\frac{V}{W}$, tem ordem menor que $\frac{V}{W}$. Como todo fator principal de $\frac{G}{V}$ é também fator principal de $\frac{G}{W}$, temos que cada um deles tem ordem menor que $\left|\frac{V}{W}\right| = p^a$.

AFIRMAÇÃO 3: Todo fator principal de $\frac{G}{V}$, a menos de isomorfismo, é um fator principal de G.

De fato, seja $\frac{\frac{K}{V}}{\frac{H}{V}}$ um fator principal de $\frac{G}{V}$. Assim, $\frac{K}{H} \simeq \frac{\frac{K}{V}}{\frac{H}{V}}$ é normal minimal de $\frac{\frac{G}{V}}{\frac{H}{V}} \simeq \frac{G}{H}$.

Portanto, pelaminimalidade de $\left|\frac{G}{V}\right|$, temos que cada fator principal de $\frac{G}{V}$ tem um único ou não tem complemento. Assim, pela proposição 3.2, $\frac{G}{V}$ é nilpotente.

AFIRMAÇÃO 4: Se G é nilpotente finito, então para todo primo q que divide $|G|$, existe um fator principal de G com ordem q.

De fato, seja $|G| = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Pelo Teorema de Caracterização dos Nilpotentes Finitos, $G = P_1 \times \ldots \times P_r$, onde $P_i \in Syl_{p_i}(G)$, $\forall\, i = 1, \ldots, r$. Seja $1 \neq x \in Z(P_i)$ tal que $o(x) = p_i$. Assim, $N = \langle x \rangle$ é um subgrupo de G de ordem p_i. Como $N \leq Z(P_i)$, temos que $[N, P_i] = 1$. Além disso, Como $N \cap P_j = 1$ e $P_j \lhd G$, $\forall\, j \neq i$, temos $[N, P_j] = 1$, $\forall\, j \neq i$. Logo,

$N^G = N^{P_1 \dots P_r} = (N^{P_1})^{P_2 \dots P_r} = N^{P_2 \dots P_r} = \dots = N^{P_r} = N$. Então, $N \lhd G$ e, portanto, N é normal minimal com ordem p_i. O mesmo ocorre para todo primo p_i. Assim, segue a afirmação.

Portanto, pela afirmação acima, todo primo q que divide $\left|\frac{G}{V}\right|$ é menor que $p^a = \left|\frac{V}{W}\right|$.

Se $\frac{G}{V}$ não for cíclico, então, pelo teorema 3.4, $\sigma(G) \leq \sigma\left(\frac{G}{V}\right) = q + 1 \leq p^a + 1$, onde q é o menor primo tal que o q-subgrupo de Sylow de $\frac{G}{V}$ é não-cíclico.

Se $\frac{G}{V}$ for cíclico, então $\frac{\frac{G}{W}}{\frac{V}{W}} \simeq \frac{G}{V}$ é cíclico. Assim, pelo lema 3.6, $\sigma(G) \leq \sigma\left(\frac{G}{W}\right) = \left|\frac{V}{W}\right| + 1 = p^a + 1$. Portanto, chegamos que $\sigma(G) \leq p^a + 1$.

Agora, mostraremos que $\sigma(G) \geq p^a + 1$.

Seja $N \lhd G$ e maximal com a propriedade $\sigma(G) = \sigma\frac{G}{N}$. Logo, se $\frac{K}{N}$ é um subgrupo normal minimal de $\frac{G}{N}$, então $\sigma(G) \neq \sigma\left(\frac{G}{K}\right)$. Assim, ou $\frac{G}{K}$ é cíclico ou $\sigma(G) < \sigma\left(\frac{G}{K}\right)$.

Seja $G = X_1 \cup \dots \cup X_n$, onde $\sigma(G) = n$, $X_i \lessdot G$ e $N \leq X_i$, $\forall\, i = 1, \dots, n$.

AFIRMAÇÃO 5: $K \nleq X_i$ para algum i.

De fato, se $K \leq X_i$, $\forall\, i = 1, \dots, n$. Então $\frac{G}{K} = \frac{X_1}{K} \cup \dots \cup \frac{X_n}{K}$. Se $\frac{G}{K}$ não for cíclico, $\sigma\left(\frac{G}{K}\right) \leq \sigma(G) < \sigma\left(\frac{G}{K}\right)$, absurdo. Se $\frac{G}{K}$ for cíclico, $G = X_i$ para algum i, absurdo.

Portanto, $\frac{K}{N}$ possui complemento em G. Pelo lema 3.4, $\frac{K}{N}$ possui mais de um complemento em G. Dividiremos a nossa demonstração em dois casos.

1^o caso: $\frac{K}{N}$ tem um complemento normal.

Seja $\frac{M}{N}$ um complemento normal de $\frac{K}{N}$ em G. Logo, $\frac{G}{N} \simeq \frac{K}{N} \times \frac{M}{N}$. Então, $[K, M] \leq N$ e portanto, $[G, K] = [KM, K] = [K, K][M, K] \leq N$. Assim, $\frac{K}{N} \leq Z\left(\frac{G}{N}\right)$. O que implica que todos os outros complementos de $\frac{K}{N}$ são normais em G. Como $M \lessdot G$ e $M \lhd G$, temos que $\left|\frac{G}{M}\right| = q$, para algum primo q. Logo, $\left|\frac{K}{N}\right| = q$.

Dado $1 \neq \frac{H}{N} \lhd \frac{G}{N}$. Temos que

$$\sigma\left(\frac{\frac{G}{N}}{\frac{H}{N}}\right) = \sigma\left(\frac{G}{H}\right) > \sigma(G) = \sigma\left(\frac{G}{N}\right).$$

Logo, $\frac{G}{N}$ é n-soma primitivo. Como $Z\left(\frac{G}{N}\right) \neq 1$, pelo teorema 3.5, $\frac{G}{N} \simeq C_q \times C_q$. Assim, $\sigma(G) = \sigma\left(\frac{G}{N}\right) = q + 1$. Como $\frac{K}{N}$ é um fator principal de G e tem mais de um complemento, temos que $q \geq p^a$. Portanto, $\sigma(G) \geq p^a + 1$.

2^o caso: Todos os complementos de $\frac{K}{N}$ são não-normais.

Seja M um complemento de $\frac{K}{N}$ em G. Como $M \lessdot G$ e não-normal, temos que $\frac{K}{N}$ tem, no mínimo, $k = \left|\frac{G}{N} : \frac{M}{N}\right| = |G : M|$ complementos em G. Sejam $M_1, \ldots, M_k$ esses complementos.

Seja $G = X_1 \cup \ldots \cup X_n$, onde $n = \sigma(G), X_j \lessdot G$ e $N \leq X_j$, $\forall\, j = 1, \ldots, n$.

$$M_i = M_i \cap G = M_i \cap \left(\bigcup_{j=1}^{n} X_j\right) = \bigcup_{j=1}^{n}(M_i \cap X_j), \quad \text{para cada } i = 1, \ldots, k.$$

Como $\frac{M_i}{N} \simeq \frac{G}{K}$, temos que ou $\sigma\left(\frac{M_i}{N}\right) = \sigma\left(\frac{G}{K}\right) > \sigma(G)$ ou $\frac{M_i}{N}$ é cíclico.

(a) $\sigma\left(\frac{M_i}{N}\right) > \sigma(G)$.

Como $N < M_i$ para cada $i = 1, \ldots, k$, temos

$$\frac{M_i}{N} = \frac{M_i \cap X_1}{N} \cup \ldots \cup \frac{M_i \cap X_n}{N}. \tag{3.6}$$

Logo, $\sigma\left(\frac{M_i}{N}\right) \leq \sigma(G) < \sigma\left(\frac{M_i}{N}\right)$, absurdo. Com isso, existe $j \in \{1, \ldots, n\}$ tal que $\frac{M_i}{N} = \frac{M_i \cap X_j}{N}$, isto é, $M_i = M_i \cap X_j$. Assim, $M_i \leq X_j$. Pela maximalidade de ambos, $M_i = X_j$. Portanto, $\left|\frac{K}{N}\right| = \left|\frac{G}{N} : \frac{M}{N}\right| = k < \sigma(G)$. Por hipótese, $p^a \leq \left|\frac{K}{N}\right|$. Logo, $p^a + 1 \leq \left|\frac{K}{N}\right| + 1 = k + 1 \leq \sigma(G) \Rightarrow p^a + 1 \leq \sigma(G)$.

(b) $\frac{M_i}{N}$ cíclico.

Devido à equação 3.6, existe $j \in \{1, \ldots, n\}$ tal que $M_i = M_i \cap X_j$. Segue o mesmo argumento do item (a). Portanto, $\sigma(G) \geq p^a + 1.$■

Capítulo 4

σ-Coberturas de grupos solúveis finitos

Finalmente chegamos ao principal capítulo do nosso trabalho. Definiremos uma σ-cobertura de um grupo finito e mostraremos que todo grupo solúvel finito possui uma σ-cobertura conjugada ou normal, que iremos definir. Para finalizar o capítulo, estudaremos com mais rigor as σ-coberturas conjugadas.

4.1 σ-Cobertura de um grupo finito

Nesta seção, assumiremos que G é um grupo solúvel finito com $\sigma(G) = n$. Assim, $G = \bigcup_{i=1}^{n} M_i$, onde M_i é maximal em G para cada $i = 1, \ldots, n$. Nosso objetivo será de calcular os índices de M_i em G.

Lema 4.1 *Sejam G um grupo solúvel primitivo finito e L o (único)subgrupo normal minimal de G. Então, $\sigma(G) \leq |L| + 1$.*

Prova: Mostraremos que L possui mais de um complemento e usaremos o teorema de Tomkinson para concluir o lema.

Seja $M \lessdot G$ tal que $M_G = 1$. Como G é solúvel, pela observação 2.1, M é complemento de L em G. De $M_G = 1$, temos que $M \ntrianglelefteq G$. Assim, existe $g \in G$ tal que $M^g \neq M$. Daí, $G = ML \Rightarrow G^g = (ML)^g = M^g L^g \overset{L \trianglelefteq G}{\Rightarrow} G = M^g L$. Como L é normal minimal de G,

$L \cap M^g = 1$ ou $L \cap M^g = L$. Se $L \cap M^g = L$, então $L \leq M^g$. Assim, $L = L^{g^{-1}} \leq (M^g)^{g^{-1}} = M$, absurdo. Logo, $L \cap M^g = 1$ e então M^g é outro complemento de L em G. Assim, L é um fator principal de G com mais de um complemento. Como existe $M \lessdot G$ tal que $M \ntrianglelefteq G$, temos que G é não-nilpotente. Portanto, pelo teorema de Tomkinson, $\sigma(G) \leq |L| + 1$.■

Teorema 4.1 *Sejam G um grupo solúvel finito e p um divisor primo de $|G|$. Se G tem no mínimo dois subgrupos maximais de índice p^n, então $\sigma(G) \leq p^n + 1$.*

Prova: Suponhamos que G possui dois subgrupos maximais normais distintos M e N de mesmo índice p em G. Assim, $G = MN$ e $M \cap N \lhd G$. Do isomorfismo, $\frac{G}{M\cap N} \simeq \frac{G}{M} \times \frac{G}{N}$, temos que $\frac{G}{M\cap N} \simeq C_p \times C_p$. Logo, $\sigma(G) \leq \sigma\left(\frac{G}{M\cap N}\right) = p + 1$, pelo lema 3.2.

Agora, suponhamos que G tem um subgrupo maximal não-normal M de índice p^n. Seja $C = M_G$. Sabemos que $\frac{G}{C}$ é um grupo primitivo. Sendo $\frac{L}{C}$ o (único)subgrupo normal minimal de $\frac{G}{C}$, temos que $\frac{G}{C} \simeq \frac{L}{C} \rtimes \frac{M}{C}$. Assim,

$$\left|\frac{L}{C}\right| = \left|\frac{G}{C} : \frac{M}{C}\right| = |G : M| = p^n.$$

Portanto, pelo lema 4.1, $\sigma(G) \leq \sigma\left(\frac{G}{C}\right) \leq \left|\frac{L}{C}\right| + 1 = p^n + 1$, o que conclui o teorema.■

Corolário 4.1 *Seja G um grupo solúvel finito com $\sigma(G) = n$. Se $m < n - 1$, então G tem no máximo um subgrupo maximal de índice m.*

Prova: Como G é solúvel, $m = q^k$, onde q é primo e k é inteiro positivo. Se G tem no mínimo dois subgrupos maximais de índice q^k, então, pelo teorema 4.1, $\sigma(G) - 1 \leq q^k$. Mas, por hipótese, $q^k < n - 1$, absurdo.

Portanto, G tem no máximo um subgrupo maximal de índice m.■

Definição 4.1 *Sejam G um grupo finito com $\sigma(G) = n$ e $M_1, \ldots, M_n$ subgrupos maximais de G com $|G : M_k| = i_k$, $k = 1, \ldots, n$. A n-upla $(M_1, \ldots, M_n)$ é chamada de σ-cobertura de G, se $G = \bigcup_{k=1}^n M_k$ e $i_1 \leq i_2 \leq \ldots \leq i_n$.*

Lema 4.2 *Sejam G um grupo solúvel finito com $\sigma(G) = n$ e $(M_1 \ldots, M_n)$ uma σ-cobertura de G. Então:*

(i) O único índice que pode ser menor que n-1 é i_1 e, portanto, $i_2 = n-1$.

(ii) Se $i_1 < n-1$, então $M_i \ntriangleleft G$ para todo $i \geq 2$.

Prova: (i) Do corolário 3.1 e da definição de σ-cobertura, temos que $i_1 \leq i_2 \leq n-1$. Seja l o maior número tal que $i_l < n-1$. Pelo corolário 4.1, M_k é o único maximal com índice i_k para cada $1 \leq k \leq l$. Dessa forma, $M_1 \ldots, M_l$ são todos distintos e normais em G. Logo, pela observação 3.2, $n-1 \leq i_{l+1} \leq n-l$. Portanto, $l \leq 1$. Além disso, $i_2 = n-1$.

(ii) Suponha que $M_k \triangleleft G$ para algum $k \in \{2, \ldots, n\}$. Como $i_1 < n-1$ e $i_k \geq n-1$, temos que M_1 e M_k têm ordens diferentes.

Suponhamos que $i_k = n-1$. Assim, podemos reordenar os maximais de tal forma que $(M_1, M_k, M_2, \ldots, M_{k-1}, M_{k+1}, \ldots, M_n)$ seja uma σ-cobertura de G. Pela observação 3.2,

$$1 \leq \sum_{\substack{r=2 \\ r\neq k}}^{n} \frac{1}{i_r} \leq \sum_{\substack{r=2 \\ r\neq k}}^{n} \frac{1}{i_2} = \frac{n-2}{i_2}.$$

Daí, $n-1 = i_2 \leq n-2$, absurdo.

Agora, suponhamos que $i_k > n-1$. Do corolário 3.1, temos

$$1 \leq \sum_{r=2}^{n} \frac{1}{i_r} \leq \frac{n-1}{i_2} = \frac{n-1}{n-1} = 1 \quad \Rightarrow \quad \sum_{r=2}^{n} \frac{1}{i_r} = 1.$$

Como $i_k > n-1$, temos

$$1 = \sum_{r=2}^{k-1} \frac{1}{i_r} + \sum_{r=k}^{n} \frac{1}{i_r} \leq \sum_{r=2}^{k-1} \frac{1}{i_2} + \sum_{r=k}^{n} \frac{1}{i_k} = \frac{k-2}{n-1} + \frac{n-k+1}{i_k}.$$

Assim,

$$\begin{aligned} & (n-1)i_k \leq i_k(k-2) + (n-k+1)(n-1) \\ \Rightarrow \quad & i_k(n-1-k+2) \leq (n-k+1)(n-1) \quad \Rightarrow \quad i_k \leq n-1, \end{aligned}$$

absurdo, pois $n-1 < i_k$. Portanto, $M_k \ntriangleleft G$, $\forall\, k = 2, \ldots, n$.■

Teorema 4.2 *Sejam G um grupo solúvel finito com $\sigma(G) = n$ e $(M_1, \ldots, M_n)$ uma σ-cobertura de G. Então $i_1 \leq n-1$ e $i_2 = i_3 = \ldots = i_n = n-1$.*

Prova: Do lema 4.2, temos $i_1 \leq i_2 = n-1$. Suponha que existe $k(2 \leq k \leq n-1)$ tal que $i_k < i_{k+1}$. Do corolário 3.1, temos

$$1 \leq \sum_{r=2}^{n} \frac{1}{i_r} \leq \frac{n-1}{i_2} = \frac{n-1}{n-1} = 1 \quad \Rightarrow \quad \sum_{r=2}^{n} \frac{1}{i_r} = 1.$$

Ora,

$$1 = \sum_{r=2}^{k} \frac{1}{i_r} + \sum_{r=k+1}^{n} \frac{1}{i_r} \leq \frac{k-1}{n-1} + \frac{n-k}{i_{k+1}}.$$

Daí,

$$\begin{aligned} & (k-1)i_{k+1} + (n-k)(n-1) \geq (n-1)i_{k+1} \\ \Rightarrow \quad & (n-1)(n-k) \geq i_{k+1}(n-1-k+1) \\ \Rightarrow \quad & (n-1)(n-k) \geq i_{k+1}(n-k) \quad \Rightarrow \quad i_{k+1} \leq n-1 \leq i_k, \end{aligned}$$

absurdo, pois $i_k < i_{k+1}$. Portanto, $i_2 = \ldots = i_n = n-1$.■

Veja que do teorema 4.2, se G é solúvel finito não-cíclico, então existe um maximal cujo índice em G é $\sigma(G)-1$. Logo, existe um primo p e um inteiro positivo α tal que $\sigma(G) = 1+p^{\alpha}$. Assim, por exemplo, não existe grupo solúvel finito G com $\sigma(G) = 7$. De fato, não existe primo p e inteiro α tal que $1 + p^{\alpha} = 7$.

Veremos, a seguir, que dado uma σ-cobertura $(M_1, \ldots, M_n)$ de G para sabermos algo sobre $M_2, \ldots, M_n$, basta conhecermos o índice de M_1 em G.

Proposição 4.1 *Sejam G um grupo solúvel finito com $\sigma(G) = n$ e $(M_1, \ldots, M_n)$ uma σ-cobertura de G.*

(i) Se $i_1 < n-1$, então $M_2, \ldots, M_n$ são todos conjugados em G.

(ii) Se $i_1 = n-1$ e $M_i \lhd G$ para algum $i \in \{1, \ldots, n\}$, então $M_i \lhd G$ para todo $i = 1, \ldots, n$.

Prova: (i) Pelo corolário 4.1, M_1 é o único maximal em G com índice i_1. Logo, $M_1 \lhd G$. Pelo item (ii) do lema 4.2, $M_i \ntriangleleft G$ para todo $i = 2, \ldots, n$. Vamos mostrar que $M_2, \ldots, M_n$ são todos conjugados em G.

Suponhamos, por absurdo, que existem $i \neq j$ tal que M_i e M_j não são conjugados. Pelo corolário 2.3, $M_i \cap M_j$ é um subgrupo maximal de M_i ou M_j. Suponhamos que $M_i \cap M_j \lessdot M_i$.

Do teorema 4.2, temos que $i_2 = \ldots = i_n = n-1$. Daí,

$$\sum_{r=2}^{n} |M_k| = \sum_{r=2}^{n} \frac{|G|}{|G:M_k|} = |G| \sum_{r=2}^{n} \frac{1}{n-1} = \frac{|G|(n-1)}{(n-1)} = |G|.$$

Logo, pelo teorema 3.1, $M_i \cap M_j \leq M_1$. Com isso, $M_i \cap M_j \leq M_1 \cap M_i \leq M_i$. Pela maximalidade de $M_i \cap M_j$ em M_i, temos que $M_i \cap M_j = M_i \cap M_1$ ou $M_i \cap M_1 = M_i$. Se $M_i \cap M_1 = M_i$, então $M_i \leq M_1$ e com isso, $M_i = M_1$, o que é absurdo. Portanto, $M_i \cap M_j = M_i \cap M_1$. Como $M_1 \lhd G$ e $M_i \nleq M_1$, $G = M_1 M_i$. Assim, pelo 1^o teorema dos isomorfismos, $M_i \cap M_j = M_i \cap M_1 \lhd M_i$. Dessa forma, $|M_i : M_i \cap M_j| = p$, para algum primo p. Como M_i e M_j têm a mesma ordem, $|M_j : M_i \cap M_j| = p$ e então, $M_i \cap M_j \lessdot M_j$. Assim, da mesma forma, $M_i \cap M_j \lhd M_j$. Logo, $M_i \cap M_j \lhd \langle M_i, M_j \rangle = G$. Pela maximalidade de $M_i \cap M_j$ em M_i e M_j, temos que $(M_i)_G = (M_j)_G = M_i \cap M_j$, o que é absurdo pelo corolário 2.2.

Portanto, $M_2, \ldots, M_n$ são todos conjugados em G.

(ii) Por hipótese, $i_1 = i_2 = \ldots = n-1$ e $M_i \lhd G$ para algum $i \in \{1, \ldots, n\}$. Como os índices são iguais, podemos reordenar os subgrupos maximais de forma que $(M_i, M_1, ..., M_{i-1}, M_{i+1}, ..., M_n)$ seja uma σ-cobertura. Logo, podemos supor, sem perda de generalidade, que $M_1 \lhd G$, e com isso, que existe um primo p tal que $n-1 = p$. Do argumento do item anterior, temos $|G| = \sum_{k=2}^{n} |M_k|$. Assim, pelo teorema 3.1, $M_w \cap M_k \leq M_1, \forall\, w \neq k (w, k \in \{1, \ldots, n\})$ e $M_k M_1 = G, \forall\, k \neq 1$. Em particular, $M_2 \cap M_k \leq M_1, \forall\, k \neq 2$ e com isso, $M_2 \cap M_k \leq M_1 \cap M_2$ e $M_2 \cap M_k \leq M_1 \cap M_k, \forall\, k \neq 2$. Por outro lado,

$$|M_2 \cap M_k| = \frac{|M_2||M_k|}{|M_2 M_k|} \geq \frac{|M_2||M_k|}{|G|} = \frac{|M_2||M_1|}{|M_1 M_2|} = |M_1 \cap M_2|.$$

Com isso, $M_1 \cap M_2 = M_k \cap M_2, \forall\, k \neq 2$. Também temos,

$$|M_2 \cap M_k| = \frac{|M_2||M_k|}{|M_2 M_k|} \geq \frac{|M_2||M_k|}{|G|} = \frac{|M_1||M_k|}{|M_1 M_k|} = |M_1 \cap M_k|, \quad \forall\, k \neq 1.$$

Portanto, $M_2 \cap M_k = M_1 \cap M_k, \forall\, k \notin \{1, 2\}$. Dessa forma, $M_1 \cap M_2 = M_1 \cap M_k \lhd M_k, \forall\, k \neq 1$, e assim, $M_1 \cap M_2 \lhd \langle M_2, M_k \rangle = G$. Como $|M_1 : M_1 \cap M_2| = |M_1 M_2 : M_2| = |G : M_2| = p$, temos que $\frac{G}{M_1 \cap M_2}$ é um grupo de ordem p^2. Logo, $\frac{G}{M_1 \cap M_2}$ é abeliano e assim,

$$\frac{M_k}{M_1 \cap M_k} = \frac{M_k}{M_1 \cap M_2} \lhd \frac{G}{M_1 \cap M_2}, \quad \forall\, k \neq 1.$$

Portanto, $M_k \lhd G, \forall\, k \neq 1$. Como $M_1 \lhd G$, concluímos o item (ii).$\blacksquare$

Observação 4.1 *Da proposição* 4.1*, temos que se* G *é solúvel finito com* $\sigma(G) = n$ *e* $i_1 < n-1$*, então* $n \geq 4$*. De fato, como* $1 < i_1 < n-1$*, temos que* $n-1 \geq 3$*. Logo,* $n \geq 4$*.*

Agora, iremos estudar o teorema mais importante do nosso trabalho. Veremos que em todo grupo solúvel finito com $\sigma(G) = n$, existe uma σ-cobertura com um "rosto"bem interessante.

Teorema 4.3 *Seja* G *um grupo solúvel finito com* $\sigma(G) = n$*. Então existe uma* σ*-cobertura* $(M_1, \ldots, M_n)$ *de* G *tal que uma das seguintes afirmações ocorre:*

(i) $i_1 < n-1$ *e* $M_2, \ldots, M_n$ *são conjugados.*

(ii) $i_k = n-1$ *e* $M_k \lhd G$ *para todo* $k = 1, \ldots, n$*.*

Prova: Pela proposição anterior, basta provarmos o teorema quando G possui σ-cobertura $(M_1, \ldots, M_n)$ com $i_k = n-1$ e $M_k \ntriangleleft G$ $\forall\, k = 1, \ldots, n$. Assim, $|G| = \sum_{j=1}^{n-1} |M_{k_j}|$, onde $M_{k_j} \in \{M_1, \ldots, M_n\}$ e $M_{k_j} \neq M_{k_i}$ $\forall\, i \neq j$. Logo, pelo teorema 3.1, $G = M_iM_j$ $\forall\, i \neq j$. Com isso, pelo lema 2.1, M_i e M_j não são conjugados para $i \neq j$.

Seja $\mathcal{M}$ o conjunto de todos os subgrupos maximais não-normais de índice $n-1$ em G. Seja $M \in \mathcal{M}$ tal que M_G tem a maior ordem dentre os núcleos normais dos elementos de $\mathcal{M}$. Se $C = M_G$, temos que $\frac{G}{C}$ é um grupo primitivo. Seja $\frac{L}{C}$ o único normal minimal de $\frac{G}{C}$. Daí, pelo lema 4.1,

$$n = \sigma(G) \leq \sigma\left(\frac{G}{C}\right) \leq \left|\frac{L}{C}\right| + 1. \tag{4.1}$$

Pelo teorema de Ore-Baer, $\frac{M}{C}$ é um complemento de $\frac{L}{C}$ em $\frac{G}{C}$. Assim,

$$\left|\frac{L}{C}\right| = \left|\frac{G}{C} : \frac{M}{C}\right| = |G : M| = n-1.$$

De (4.1), temos que $n \leq \sigma\left(\frac{G}{C}\right) \leq \left|\frac{L}{C}\right| + 1 = n-1+1 = n$. Logo, $\sigma\left(\frac{G}{C}\right) = n = \sigma(G)$. Seja $\left(\frac{M_1^*}{C}, \ldots, \frac{M_n^*}{C}\right)$ uma σ-cobertura de $\frac{G}{C}$. Com isso, $(M_1^*, \ldots, M_n^*)$ é uma σ-cobertura de G. Sabemos que $|G : M_k^*| = n-1$, $\forall\, k \geq 2$. Se $|G : M_1^*| < n-1$, então pela proposição 4.1, $(M_1^*, \ldots, M_n^*)$ é uma σ-cobertura satisfazendo (i).

Para encerrar, precisamos mostrar que $M_k^* \lhd G$, $\forall\, k = 1, \ldots, n$ quando $|G : M_1^*| = n-1$. Pela proposição 4.1, basta mostrar que $M_k^* \lhd G$ para algum $1 \leq k \leq n$. Suponha, por absurdo, que $M_k^* \ntrianglelefteq G\ \forall\, k = 1, \ldots, n$. Como $C \leq M_k^*$ e $C \lhd G$, temos que $C \leq (M_k^*)_G$, $\forall\, k = 1, \ldots, n$. Assim, pela maximalidade de C em $\mathcal{M}$, temos $C = (M_k^*)_G$, $\forall\, k = 1, \ldots, n$. Logo, pelo corolário 2.2, M é conjugado a todos os M_k's. Isto não pode ocorrer, pois, M tem exatamente $|G : N_G(M)| = |G : M| = n - 1$ conjugados em G. Portanto, $(M_1^*, \ldots, M_n^*)$ satisfaz (ii) se $|G : M_1| = n - 1$.■

Do teorema temos a seguinte definição.

Definição 4.2 *Qualquer σ-cobertura que satisfaz a condição (i) do teorema é chamada de σ-cobertura conjugada, e que satisfaz a condição (ii) é chamada de σ-cobertura normal.*

4.2 Coberturas Conjugadas

Vimos que um subgrupo maximal e normal M de um grupo finito G tem índice primo em G. Assim, se $\sigma(G) - 1$ não for primo, então G não possui σ-cobertura normal. A seguir, encontraremos algumas condições para que G não possua uma σ-cobertura normal.

Proposição 4.2 *Seja G um grupo solúvel, não-nilpotente e n-soma primitivo. Então:*

(i) G não tem σ-cobertura normal e

(ii) G é primitivo.

Prova: (i) Suponha, por absurdo, que $(M_1, \ldots, M_n)$ é uma σ-cobertura normal de G. Por definição, $M_j \lhd G$ para cada $j = 1, \ldots, n$ e $i_1 = \ldots = i_n = n - 1 = p$, para algum primo p. Assim,

$$\frac{M_2}{M_1 \cap M_2} \simeq \frac{M_1 M_2}{M_1} = \frac{G}{M_1} \simeq C_p.$$

Analogamente, $\frac{M_1}{M_1 \cap M_2} \simeq C_p$. Como $\frac{G}{M_1 \cap M_2} \simeq \frac{M_1}{M_1 \cap M_2} \times \frac{M_2}{M_1 \cap M_2}$, temos que $\frac{G}{M_1 \cap M_2} \simeq C_p \times C_p$. Portanto, pelo lema 3.2, $\sigma\left(\frac{G}{M_1 \cap M_2}\right) = p + 1 = n = \sigma(G)$. Mas, G é n-soma primitivo e, com isso, $M_1 \cap M_2 = 1$. Logo, $G \simeq C_p \times C_p$ e portanto, $|G| = p^2$, o que é absurdo, pois G é não-nilpotente.

Dessa forma, G não possui σ-cobertura normal.

(ii) Seja $(M_1, \ldots, M_n)$ uma σ-cobertura de G. Por (i), a σ-cobertura não é normal. Assim, existe $M \in \{M_2, \ldots, M_n\}$ que não é normal em G. Seja $C = M_G$. Mostraremos que $C = 1$.

Seja $\frac{L}{C}$ o único subgrupo normal minimal do grupo primitivo $\frac{G}{C}$. Pelo lema 4.1, $\sigma(G) \leq \sigma\left(\frac{G}{C}\right) \leq \left|\frac{L}{C}\right| + 1$. No entanto, como $\frac{M}{C}$ é complemento de $\frac{L}{C}$ em $\frac{G}{C}$, temos

$$\left|\frac{L}{C}\right| = \left|\frac{G}{C} : \frac{M}{C}\right| = |G : M| = n - 1.$$

Daí, $\sigma(G) \leq \sigma\left(\frac{G}{C}\right) \leq n - 1 + 1 = n$. Logo, $\sigma\left(\frac{G}{C}\right) = n$. Mas, como G é n-soma primitivo, segue que $C = 1$.

Portanto, G é primitivo.■

Observação 4.2 (i) *A recíproca da proposição não é verdadeira. Por exemplo, S_4 é um grupo solúvel, primitivo com $\sigma(S_4) = 4$ e não admite uma σ-cobertura normal, mas não é um grupo 4-soma primitivo.*

De fato, no exemplo 3 vimos que A_4 é solúvel. Como $A_4 \trianglelefteq S_4$ e $\frac{S_4}{A_4}$ é solúvel, pois, é abeliano, temos do item c) da proposição 1.5, que S_4 é solúvel. Do exemplo 5, temos que S_4 é primitivo.

Seja V o subgrupo de Klein de A_4. Do exemplo 4, temos que $\frac{S_4}{V}$ não é abeliano. Como $|\frac{S_4}{V}| = \frac{24}{4} = 6$, temos, do lema 1.6, que $\frac{S_4}{V} \simeq S_3$.É fácil ver que

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

Assim $\sigma(S_3) \leq 4$. Como $|A_3| = 3$, temos que $1 \leqslant A_3 \leqslant S_3$ é uma série subnormal de S_3 com os grupos quocientes abelianos. Logo, S_3 é solúvel. Assim, do teorema 4.3 o grupo possui uma cobertura normal ou conjugada. Como S_3 possui um único subgrupo normal, o grupo só admite uma cobertura conjugada $(M_1, ..., M_n)$, onde $n = \sigma(S_3)$. Assim, $|G : M_1| < n - 1$. Logo, da observação 4.1 $\sigma(S_3) \geq 4$. Portanto, $\sigma(S_3) = 4$ e então $\sigma(\frac{S_4}{V}) = 4$.

Do lema 3.1, $\sigma(S_4) \leq \sigma(\frac{S_4}{V}) = 4$. Temos que os únicos subgrupos normais próprios de S_4 são V e A_4. Assim, S_4 não admite uma σ-cobertura normal, e pelo mesmo argumento acima $\sigma(S_4) \geq 4$. Portanto, $\sigma(S_4) = 4$ e S_4 não é um 4-soma primitivo.

(ii) *A recíproca da proposição é verdadeira quando assumimos que G é um grupo supersolúvel. De fato, seja G um grupo supersolúvel, primitivo, com $\sigma(G) = n$. Se L é o* *único subgrupo normal minimal de G, então $|L| = p$ para algum primo p, pois, L é um fator principal de G. Seja M o subgrupo maximal de G com $M_G = 1$ e que complementa L em G.*

Definamos o homomorfismo

$$\begin{aligned} \varphi : M &\rightarrow Aut(L) \\ g &\mapsto \varphi(g)(x) = gxg^{-1}. \end{aligned}$$

Claramente, $Nuc(\varphi) = \{g \in M \,|\, g^{-1}xg = x\,,\, \forall\, x \in L\} = C_M(L)$. No entanto, pelo teorema de Ore-Baer, $C_M(L) = M \cap C_G(L) = M \cap L = 1$. Logo, pelo teorema fundamental do homomorfismo, $M \lesssim Aut(L)$. Como $L \simeq \mathbb{Z}_p$, temos que $Aut(L) \simeq \mathbb{Z}_{p-1}$. Assim, M é cíclico e sua ordem divide $p - 1$.

Se $1 \neq N$ é um subgrupo normal em G, então $L \leq N$. De fato, se $L \nleq N$, então N é ou contém, propriamente, um normal minimal em G, o que é absurdo, pela unicidade de L. Assim, $N \nleq M$ e com isso, $G = MN$. Logo, $\frac{G}{N} \simeq \frac{M}{M \cap N}$. Como M é cíclico, $\frac{M}{M\cap N}$ é cíclico e portanto, $\frac{G}{N}$ é cíclico. Assim, $\sigma\left(\frac{G}{N}\right) = \infty$ e com isso, G é n-soma primitivo. Como G é primitivo, existe maximal que não é normal. Portanto, G é não-nilpotente.

Proposição 4.3 *Seja G um grupo solúvel finito. Se G tem um subgrupo maximal não-normal de índice $\sigma(G) - 1$, então G tem uma σ-cobertura conjugada.*

Prova: Seja $\sigma(G) = n$. Pelo teorema 4.3, G possui uma σ-cobertura normal ou conjugada. Seja $(M_1, \ldots, M_n)$ uma σ-cobertura normal de G. Por definição, $M_k \lhd G$ e $|G : M_k| = n-1 = p$, onde p é primo, para cada $k = 1, \ldots, n$.

Seja M o subgrupo maximal e não-normal de G com índice $n - 1 = p$. Sejam $C = M_G$ e $\frac{L}{C}$ o único normal minimal do grupo primitivo $\frac{G}{C}$. Como $\frac{M}{C}$ é um complemento de $\frac{L}{C}$ em $\frac{G}{C}$, temos

$$\left|\frac{L}{C}\right| = \left|\frac{G}{C} : \frac{M}{C}\right| = |G : M| = n - 1 = p.$$

Assim, pelo mesmo argumento do item ii) da observação 4.2, $\frac{M}{C}$ é cíclico e sua ordem divide $p-1 = n-2$. Pelo lema 4.1, $n = \sigma(G) \leq \sigma\left(\frac{G}{C}\right) \leq \left|\frac{L}{C}\right| + 1 = n-1+1 = n$. Logo, $\sigma\left(\frac{G}{C}\right) = n$.

AFIRMAÇÃO: $\frac{G}{C}$ não possui subgrupo maximal normal com índice $n - 1$.

De fato, suponha, por absurdo, que $\frac{K}{C}$ é um subgrupo maximal normal de $\frac{G}{C}$ com índice $n-1=p$. Como $\frac{M}{C} \ntrianglelefteq \frac{G}{C}$, temos que $\frac{G}{C} = \frac{M}{C}\frac{K}{C}$ e com isso,

$$\frac{G}{K} \simeq \frac{\frac{G}{C}}{\frac{K}{C}} \simeq \frac{\frac{M}{C}}{\frac{M}{C} \cap \frac{K}{C}} \quad \Rightarrow \quad \left| \frac{\frac{M}{C}}{\frac{M}{C} \cap \frac{K}{C}} \right| = p.$$

Isto implica que $\left|\frac{M}{C}\right|$ é divisível por p, absurdo, pois $\left|\frac{M}{C}\right| \leq p-1$.

Da afirmação e como $\sigma\left(\frac{G}{C}\right) = n$, temos que $\frac{G}{C}$ não possui uma σ-cobertura normal. Assim, pelo teorema 4.3, $\frac{G}{C}$ admite uma σ-cobertura conjugada $\left(\frac{M_1^*}{C}, \ldots, \frac{M_n^*}{C}\right)$. Portanto, $(M_1^*, \ldots, M_n^*)$ é uma σ-cobertura conjugada de G.

Além disso, como $\left|\frac{G}{C} : \frac{M_k^*}{C}\right| = n-1 = p$, temos que $\frac{L}{C} \nleq \frac{M_k^*}{C}$ para todo $k = 2, \ldots, n$. Com efeito, se $\frac{L}{C} \leq \frac{M_k^*}{C}$ para algum $k \in \{2, \ldots, n\}$, então $\left|\frac{G}{C} : \frac{L}{C}\right| = \left|\frac{G}{C} : \frac{M_k^*}{C}\right| . \left|\frac{M_k^*}{C} : \frac{L}{C}\right|$ é divisível por p. Mas, isto não ocorre, pois $\left|\frac{G}{C} : \frac{L}{C}\right| = \left|\frac{M}{C}\right| \leq p-1$. Mais ainda, $M_k^* \cap L = C$ e então $\frac{M_k^*}{C}$ complementa $\frac{L}{C}$ em $\frac{G}{C}$ para cada $k = 2, \ldots, n$.

Portanto, pelo teorema de Ore-Baer, $\frac{M_k^*}{C}$ é conjugado a $\frac{M}{C}$ em $\frac{G}{C}$. Assim, M_k^* é conjugado a M para cada $k = 2, \ldots, n$.■

No que segue, impomos algumas condições sobre um subgrupo maximal não-normal M de um grupo solúvel finito G, para que G tenha uma σ-cobertura conjugada consistindo de todos os conjugados de M.

Definição 4.3 *Um grupo finito G é dito p-nilpotente se todo p-subgrupo de Sylow de G possui um complemento normal em G.*

Teorema 4.4 *Seja G um grupo solúvel finito com $\sigma(G) = p^n + 1$, para algum primo p. Se G tem um subgrupo maximal não-normal M de índice p^n, tal que $\frac{M}{M_G}$ é p-nilpotente ou tem sua ordem não divisível por p, então G tem uma σ-cobertura conjugada consistindo de todos os conjugados de M.*

Prova: Sejam $C = M_G, \bar{M} = \frac{M}{C}, \bar{G} = \frac{G}{C}$ e $\bar{L} = \frac{L}{C}$ o único normal minimal do grupo solúvel primitivo $\bar{G}$. Por Ore-Baer, $\bar{M}$ complementa $\bar{L}$ em $\bar{G}$. Daí,

$$|\bar{L}| = |\bar{G} : \bar{M}| = |G : M| = p^n = \sigma(G) - 1.$$

Pelo lema 4.1, $\sigma(G) \leq \sigma(\bar{G}) \leq |\bar{L}| + 1 = \sigma(G) - 1 + 1 = \sigma(G)$. Logo, $\sigma(G) = \sigma(\bar{G}) = p^n + 1$. Pela proposição anterior, $\bar{G}$ possui uma σ-cobertura conjugada $(\bar{M}_1, \ldots, \bar{M}_\sigma)$. Logo,

$(M_1, \ldots, M_\sigma)$ é um σ-cobertura conjugada de G. Precisamos mostrar que $M_2, \ldots, M_\sigma$ são conjugados de M em G. Para isto, mostraremos que nenhum subgrupo maximal não-normal com índice potência de p em $\bar{G}$ pode conter $\bar{L}$ e com isso, tais subgrupos maximais são conjugados de $\bar{M}$ em $\bar{G}$.

Se $|\bar{M}|$ não é divisível por p, então $\frac{\bar{G}}{\bar{L}} \simeq \bar{M}$ é um grupo cuja ordem não é divisível por p. Assim, não existe subgrupo com índice potência de p em $\bar{G}$ que contenha $\bar{L}$.

Se $\bar{M}$ é p-nilpotente, então, por definição, $\bar{M} = \bar{N}\bar{P}$, onde $\bar{P}$ é um p-subgrupo de Sylow de $\bar{M}$ e $\bar{N}$ é o complemento normal de $\bar{P}$ em $\bar{M}$.

AFIRMAÇÃO: $\bar{P}$ é cíclico.

De fato, se $n = 1$, então $|\bar{L}| = p$. Assim, pelo argumento do item ii) da observação 4.2, $\bar{M}$ é cíclico e com isso, $\bar{P}$ e cíclico. Se supusermos $n > 1$, basta observarmos:

$$p^n + 1 = \sigma(G) \leq \sigma(\bar{G}) \leq \sigma\left(\frac{\bar{G}}{\bar{L}}\right) = \sigma(\bar{M}) \leq \sigma\left(\frac{\bar{M}}{\bar{N}}\right) = \sigma(\bar{P}).$$

Se $\bar{P}$ não for cíclico, pelo teorema 3.3, $\sigma(\bar{P}) = p + 1$. Logo, $p^n + 1 \leq p + 1$, absurdo, pois, $n > 1$. Portanto, $\bar{P}$ é cíclico.

Seja $\bar{H}$ um subgrupo maximal de índice $p^\alpha (\alpha \geq 1)$ em $\bar{G}$ que contém $\bar{L}$. Como $\frac{\bar{G}}{\bar{L}} \simeq \bar{M}$ e $\frac{\bar{H}}{\bar{L}} \leq \frac{\bar{G}}{\bar{L}}$, existe $\bar{K}$ maximal de índice p^α em $\bar{M}$ tal que $\frac{\bar{H}}{\bar{L}} \simeq \bar{K}$. Se $\bar{N} \nleq \bar{K}$, então $\bar{N}\bar{K} = \bar{M}$ e assim, $\frac{\bar{M}}{\bar{N}} \simeq \frac{\bar{K}}{\bar{N} \cap \bar{K}}$. Daí, $|\bar{N} : \bar{N} \cap \bar{K}| = |\bar{M} : \bar{K}| = p^\alpha$, absurdo, pois, $|\bar{N}| = |\bar{N} : \bar{N} \cap \bar{K}||\bar{N} \cap \bar{K}|$ não é divisível por p. Dessa forma, $\bar{N} \leq \bar{K}$ e assim, $\frac{\bar{K}}{\bar{N}} \leq \frac{\bar{M}}{\bar{N}}$. Como $\frac{\bar{M}}{\bar{N}} \simeq \bar{P}$ e $\bar{P}$ é cíclico, temos que $\frac{\bar{M}}{\bar{N}}$ é cíclico e então $\frac{\bar{K}}{\bar{N}} \lhd \frac{\bar{M}}{\bar{N}}$. Daí, $\bar{K} \lhd \bar{M} \Rightarrow \frac{\bar{H}}{\bar{L}} \lhd \frac{\bar{G}}{\bar{L}} \Rightarrow \bar{H} \lhd \bar{G}$.

Concluímos assim, que nenhum subgrupo maximal não-normal com índice potência de p em $\bar{G}$ contém $\bar{L}$. Com isso, todo subgrupo maximal $\bar{J}$ com índice potência de p em $\bar{G}$ complementa $\bar{L}$ em $\bar{G}$. Portanto, por Ore-Baer, $\bar{J}$ é conjugado a $\bar{M}$ em $\bar{G}$. Como $\bar{M}_2, \ldots, \bar{M}_\sigma$ são maximais com índice $\sigma(g) - 1 = p^n$ em $\bar{G}$, temos que todos são conjugados a $\bar{M}$. Portanto, $M_2, \ldots, M_\sigma$ são conjugados a M.■

Lema 4.3 *Seja G um grupo solúvel finito com $\sigma(G) = p^n + 1$ para algum primo p. Se M é um subgrupo maximal p-nilpotente com núcleo normal trivial, então, ou G tem uma σ-cobertura normal, ou qualquer σ-cobertura conjugada de G possui todos os conjugados de M. No último caso, qualquer p-subgrupo de Sylow de M é cíclico.*

Prova: Seja L o único subgrupo normal minimal do grupo primitivo G. Assim, pelo lema 4.1, $p^n + 1 = \sigma(G) \leq |L| + 1$. Se $|L| = p^n$, então, como M complementa L em G, $|G : M| = |L| = p^n$. Usando a notação do argumento do teorema 4.4, $C = 1$. Assim, toda σ-cobertura conjugada de G é também de $\frac{G}{C}$. E, pelo argumento citado, se $\left(\frac{M_1}{C}, \ldots, \frac{M_\sigma}{C}\right)$ é uma σ-cobertura conjugada de $\frac{G}{C}$, então $(M_1, \ldots, M_\sigma)$ é uma σ-cobertura conjugada de G que contém os conjugados de M. Além disso, todo p-subgrupo de Sylow P de M é cíclico.

Quando tivermos $p^n < |L|$, mostraremos que todo subgrupo maximal com índice $m \leq \sigma(G) - 1 = p^n$ em G é normal em G.

Seja $H \lessdot G$ tal que $|G : H| = m \leq p^n = \sigma(G) - 1$. Se $m < p^n$, então, pelo corolário 4.1, $H \lhd G$. Se $m = p^n$, então $L \leq H$. De fato, se supusermos que $L \nleq H$, teremos que $G = LH$ e, pela minimalidade de L, $L \cap H = 1$. Logo, $|L| = |G : H| = p^n$, o que é absurdo. Dessa forma, $\frac{H}{L}$ é um subgrupo maximal de $\frac{G}{L}$. Como M é p-nilpotente, $M = PN$, onde P é um p-subgrupo de Sylow de M e N é o complemento normal de P em M. De $\frac{G}{L} \simeq M$, temos que existe $K \lessdot M$ tal que $\frac{H}{L} \simeq K$. Temos que $N \leq K$. De fato, se $N \nleq K$, então $M = NK$ e, portanto, $|N : N \cap M| = |M : K| = p^n$. Mas, como $|N| = |N : N \cap M||N \cap M|$ não é divisível por p, isto não pode ocorrer. De $\frac{M}{N} \simeq P$, temos que $\frac{M}{N}$ é nilpotente, pois, P é um p-grupo. Daí,

$$\frac{K}{N} \lhd \frac{M}{N} \quad \Rightarrow \quad K \lhd M \quad \Rightarrow \quad \frac{H}{L} \lhd \frac{G}{L} \quad \Rightarrow \quad H \lhd G.$$

Com isso, G não admite uma σ-cobertura conjugada quando $p^n < |L|$. Portanto, neste caso, G possui uma σ-cobertura normal.■

Corolário 4.2 *Se um grupo solúvel finito G tem um subgrupo maximal M nilpotente com núcleo normal trivial, então, ou*

(i) G tem uma σ-cobertura normal e $\sigma(G) = p + 1$, onde p é o menor primo tal que o p-subgrupo de Sylow de M é não-cíclico, ou

(ii) G tem uma σ-cobertura conjugada consistindo de todos os conjugados de M, e M é cíclico. Neste caso, qualquer subgrupo maximal não-normal de G é conjugado a M.

Prova: Do lema anterior, G tem uma σ-cobertura normal ou uma σ-cobertura conjugada consistindo de todos os conjugados de M. No último caso, como M é nilpotente, temos que

M é p-nilpotente para cada primo p divisor de $|M|$ e assim, todo p-subgrupo de Sylow de M é cíclico. Portanto, M é cíclico.

Seja $H \lessdot G$ tal que $H \ntriangleleft G$. Temos que $L \nleq H$. De fato, se $L \leq H$, então $\frac{H}{L} \lessdot \frac{G}{L}$. Como $\frac{G}{L} \simeq M$, temos que $\frac{G}{L}$ é nilpotente. Portanto, $\frac{H}{L} \lhd \frac{G}{L} \Rightarrow H \lhd G$, absurdo. Logo, $G = LH$ e, pela minimalidade de L, $L \cap H = 1$. Com isso, por Ore-Baer, H é conjugado a M em G.

Agora, suponha que G possui uma σ-cobertura normal $(M_1, \dots, M_\sigma)$. Assim, $|G : M_i| = p = \sigma(G) - 1$ para algum primo p. Como $M_i \lhd G$, $L \leq M_i$, $\forall\, i = 1, \dots, \sigma$. Daí,

$$\frac{G}{L} = \frac{M_1}{L} \cup \ldots \cup \frac{M_\sigma}{L} \quad \Rightarrow \quad \sigma\left(\frac{G}{L}\right) \leq \sigma(G) \leq \sigma\left(\frac{G}{L}\right).$$

Portanto, $\sigma\left(\frac{G}{L}\right) = \sigma(G)$ e como $M \simeq \frac{G}{L}$, $\sigma(M) = \sigma\left(\frac{G}{L}\right) = \sigma(G)$. Do teorema 3.4, $\sigma(G) = \sigma(M) = p+1$, onde p é o menor primo tal que o p-subgrupo de Sylow de M é não-cíclico. $\blacksquare$

Corolário 4.3 *Suponha que um grupo solúvel finito G tem um subgrupo maximal M abeliano não-normal. Se G tem uma σ-cobertura conjugada, então a cobertura contém todos os conjugados de M e $\frac{M}{M_G}$ é cíclico. Também, qualquer subgrupo maximal não-normal é conjugado a M.*

Prova: Seja $(M_1, \dots, M_\sigma)$ uma σ-cobertura conjugada de G, isto é, $|G : M_1| < \sigma(G) - 1$ e $M_2, \dots, M_\sigma$ são todos conjugados, com $|G : M_k| = \sigma - 1$, para todo $k = 2, \dots, \sigma$.

AFIRMAÇÃO: $M_G = Z(G)$.

De fato, se $Z(G) \nleq M$, então $G = MZ(G)$, pois $M \lessdot G$. Assim, $M^G = M^{MZ(G)} = (M^M)^{Z(G)} = M^{Z(G)} = M$. Logo, $M \lhd G$, absurdo. E com isso, $Z(G) \leq M$. Portanto, $Z(G) \leq M_G$.

Por outro lado, como $M \ntriangleleft G$, existe $g \in G$ tal que $M \neq M^g$. Assim, $G = \langle M, M^g \rangle$. Seja $x \in M_G = \bigcap_{z \in G} M^z$. Assim, $x \in M \cap M^g$. Seja $y \in G = \langle M, M^g \rangle$. Daí, $y = x_1 \dots x_r$, onde $x_i \in M \cup M^g$, para todo $i = 1, \dots, r$. Daí, como M e M^g são abelianos, temos

$$xy = xx_1 \dots x_r = x_1 x x_2 \dots x_r = \ldots = x_1 \dots x_r x = yx.$$

Portanto, $x \in Z(G)$ e então, $M_G \leq Z(G)$. Dessa forma, $M_G = Z(G)$.

No argumento da afirmação vimos que como $M_2, \dots, M_\sigma$ não são normais, temos que $Z(G) \leq M_k$, para todo $k = 2, \dots, \sigma$. Do lema 3.4, $Z(G) \leq M_1$. Logo,

$$\frac{G}{Z(G)} = \frac{M_1}{Z(G)} \cup \ldots \cup \frac{M_\sigma}{Z(G)}$$

é uma σ-cobertura conjugada do grupo primitivo $\frac{G}{Z(G)} = \frac{G}{M_G}$. Como $\frac{M}{Z(G)} \lessdot \frac{G}{Z(G)}$, $\frac{M}{Z(G)} \ntrianglelefteq \frac{G}{Z(G)}$ e $\frac{M}{Z(G)}$ é nilpotente, temos, pelo lema 4.3, que $\frac{M_2}{Z(G)}, \ldots, \frac{M_\sigma}{Z(G)}$ são conjugados a $\frac{M}{Z(G)}$. Daí, $M_2, \ldots, M_\sigma$ são conjugados a M. Do argumento de 4.2, $\frac{M}{Z(G)}$ é cíclico e qualquer subgrupo maximal não-normal de G é conjugado a M.■

Observação 4.3 *No corolário* 4.3*, se na* σ*-cobertura conjugada* $(M_1, \ldots, M_\sigma)$ *tivermos* M_1 *abeliano, então*

$$\frac{G}{Z(G)} \simeq E_{\sigma-1} \rtimes \mathbb{Z}_q,$$

onde $E_{\sigma-1}$ *é um grupo abeliano elementar de ordem* $\sigma - 1$*, e* q *é um número primo menor que* $\sigma - 1$*.*

De fato, vimos que $Z(G) \leq M_1$ e $Z(G) = M_G \leq M$. Pelo 1^o teorema dos isomorfismos, $M \cap M_1 \lhd M$. Como M_1 é abeliano, temos que $M \cap M_1 \lhd M_1$. Logo, $M \cap M_1 \lhd MM_1 = G$ e então $M \cap M_1 \leq M_G = Z(G) \leq M \cap M_1$. Assim, $M \cap M_1 = Z(G)$. Dessa forma,

$$\frac{G}{Z(G)} \simeq \frac{M_1}{Z(G)} \rtimes \frac{M}{Z(G)}.$$

Note que

$$\left|\frac{M}{Z(G)}\right| = \left|\frac{G}{Z(G)} : \frac{M_1}{Z(G)}\right| = |G : M_1| = q,$$

onde q é um primo menor que $\sigma - 1$.

AFIRMAÇÃO: $\frac{M_1}{Z(G)}$ é um subgrupo normal minimal de $\frac{G}{Z(G)}$ e, portanto $\frac{M_1}{Z(G)}$ é p-abeliano elementar de ordem $p^n = \sigma(G) - 1$.

Com efeito,

$$\left|\frac{M_1}{Z(G)}\right| = \left|\frac{G}{Z(G)} : \frac{M}{Z(G)}\right| = |G : M| = \sigma - 1 = p^n$$

para algum primo p.

Agora, se $\frac{H}{Z(G)} \trianglelefteq \frac{G}{Z(G)}$ e $\frac{H}{Z(G)} \leqslant \frac{M_1}{Z(G)}$, então $M \leqslant HM \leqslant G$ e assim, $HM = M$ ou $HM = G$.

Se $HM = M$, então $H \leq M \cap M_1 = Z(G)$. Assim, $H = Z(G)$.

Se $HM = G$, então $M_1 = G \cap M_1 = HM \cap M_1 = H(M \cap M_1) = HZ(G) = H$. Assim, $M_1 = H$.

Portanto, $\frac{M_1}{Z(G)}$ é normal minimal em $\frac{G}{Z(G)}$. E portanto, abeliano elementar.

Assim sendo, concluímos que $\frac{G}{Z(G)} \simeq E_{\sigma-1} \rtimes \mathbb{Z}_q$.

Além disso, se N é um subgrupo maximal abeliano normal em G, então $Z(G) = N \cap M \lessdot M$. De fato, como $N \lessdot G$, temos que $G = MN$. Pelo teorema dos isomorfismos, $N \cap M \lhd M$ e $\frac{M}{M \cap N} \simeq \frac{G}{N} \simeq C_p$, para algum primo p. Como N é abeliano, $M \cap N \lhd N$. Daí, $M \cap N \lhd MN = G \Rightarrow M \cap N \leq M_G \leq M$. Como $M \cap N \lessdot M$ e $M \neq M_G$, temos que $M \cap N = M_G = Z(G)$.

Nos resultados anteriores, vimos que se M é um subgrupo maximal não-normal com índice $\sigma(G) - 1$ tendo propriedades especiais, então $\frac{M}{M_G}$ é cíclico. Para encerrarmos o nosso trabalho, faremos algumas generalizações desse fato.

Proposição 4.4 *Seja G um grupo solúvel finito com $\sigma(G) = p^n + 1$, onde p é primo. Se M é um subgrupo maximal não-normal de índice p^n em G, então $\frac{M}{M_G}$ é cíclico quando uma das seguintes condições ocorre:*

(i) $n = 1$;

(ii) Qualquer subgrupo maximal de M com índice primo com p é normal em M;

Prova: (i) Sejam $\bar{G} = \frac{G}{M_G}$, $\bar{M} = \frac{M}{M_G}$ e $\bar{L} = \frac{L}{M_G}$ o único normal minimal do grupo primitivo $\bar{G}$. Por Ore-Baer, $\bar{M}$ complementa $\bar{L}$ em $\bar{G}$. Definamos o homomorfismo

$$\begin{aligned} \varphi : \bar{M} &\rightarrow \mathrm{Aut}(\bar{L}) \\ g &\mapsto \varphi(g)(x) = g^{-1}xg. \end{aligned}$$

Temos que $Nuc(\varphi) = \{g \in \bar{M} \,|\, g^{-1}xg = x\,, \forall\, x \in \bar{L}\} = C_{\bar{M}}(\bar{L})$. Também por Ore-Baer, $C_{\bar{M}}(\bar{L}) = \bar{M} \cap C_{\bar{G}}(\bar{L}) = \bar{M} \cap \bar{L} = \bar{1}$. Assim, $\bar{M} \lesssim \mathrm{Aut}(\bar{L})$. Como $|\bar{L}| = |\bar{G} : \bar{M}| = p$, temos que $\bar{L} \simeq \mathbb{Z}_p$. Logo, $\mathrm{Aut}(\bar{L}) \simeq \mathrm{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$. Portanto, $\bar{M}$ é cíclico.

(ii) Suponhamos que p divide $\left|\frac{M}{C}\right|$, onde $C = M_G$. Sabemos que se $\frac{H}{C} \lessdot \frac{M}{C}$, então $H \lessdot M$. Assim, por hipótese, todo maximal de $\frac{M}{C}$ com índice primo com p é normal em $\frac{M}{C}$. Logo, pelo lema 1.7 , $\bar{M} = \frac{M}{C}$ tem um p-subgrupo de Sylow normal. Seja $\bar{P} = \frac{P}{C} \in Syl_p(\bar{M})$ tal que $\bar{P} \lhd \bar{M}$. Seja $\bar{L}$ o único subgrupo normal minimal do grupo primitivo $\bar{G} = \frac{G}{C}$.

AFIRMAÇÃO: $\bar{L}\bar{P} \lhd \bar{G}$.

De fato, $(\bar{L}\bar{P})^{\bar{G}} = (\bar{L})^{\bar{G}}(\bar{P})^{\bar{G}} = \bar{L}(\bar{P})^{\bar{L}\bar{M}} = \bar{L}(\bar{P}^{\bar{M}})^{\bar{L}} = \bar{L}(\bar{P})^{\bar{L}}$. Seja $x \in \bar{P}$ e $y \in \bar{L}$. Assim, $z = x^y = y^{-1}xy \in \bar{P}^{\bar{L}}$. Daí, $z = y^{-1}xy = xx^{-1}y^{-1}xy = x[x,y]$. Como $\bar{L} \lhd \bar{G}$, temos que $[\bar{L},\bar{G}] \leq \bar{L}$. Assim, $z = x[x,y] \in \bar{P}\bar{L}$. Portanto, $(\bar{L}\bar{P})^{\bar{G}} = \bar{L}\bar{P}^{\bar{L}} \leq \bar{L}(\bar{L}\bar{P}) = \bar{L}\bar{P}$ e então $\bar{L}\bar{P} \lhd \bar{G}$.

Como $O_p(\bar{G}) = \bar{L}$ e $\bar{L}\bar{P}$ é um p-subgrupo normal de $\bar{G}$, temos $\bar{L}\bar{P} \leq \bar{L} \leq \bar{L}\bar{P}$. Assim, $\bar{L} = \bar{L}\bar{P}$ e portanto $\bar{P} \leq \bar{L} \cap \bar{M} = \bar{1}$. Com isso, $\bar{P} = \bar{1}$, absurdo. Logo, p não divide $\left|\frac{M}{C}\right|$.

Neste caso, todo subgrupo maximal de $\frac{M}{C}$ tem índice primo com p. Portanto, por hipótese, todo maximal é normal em $\frac{M}{C}$. Daí, $\frac{M}{C}$ é nilpotente.

Como todas as hipóteses do corolário 4.2 são satisfeitas, temos que ocorre (i) ou (ii) do corolário. Como vimos que p não divide $\left|\frac{M}{C}\right|$, então (i) não pode ocorrer. Dessa forma, ocorre (ii) e, portanto, $\frac{M}{M_G}$ é cíclico.■

Referências Bibliográficas

[**1**] BASTOS, Gervásio Gurgel.**Notas de Álgebra**. Fortaleza: Premius, 2002.

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

[**3**] DOERK, Klaus; HAWKES, Trevor.**Finite Soluble Groups**. Berlin; New York: Walter de Gruyter, 1992. 891 p.

[**4**] GARCIA, Arnaldo; LEQUAIN, Yves.**Elementos de Álgebra**. Rio de Janeiro: IMPA,2002. 326 p.(Projeto Euclides)

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

[**6**] JAMALI, Alireza; MOUSAVI, Hamid.**A Note on the σ-covers of Finite Soluble Groups**. Algebra Colloquium, Singapore, v. 12, p.691-697, 2005.

[**7**] ROBINSON, Derek Jonh Scott.**A Course in the Theory of Groups** - 2ª ed. New York: Springer-Verlag, 1996. 499 p. (Graduate texts in mathematics, 80)

[**8**] ROSE, JOHN S.,**A COURSE ON GROUP THEORY**. New York: Dover, 1978. 310 p.

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