

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

Luís Farias Maia

COBERTURAS DE GRUPOS

FORTALEZA

2011

Luís Farias Maia

COBERTURA DE GRUPOS

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.

Área de concentração: Matemática

Orientador: Prof. Dr. José Robério
Rogério

Fortaleza

2011

Maia, Luís Farias

M187c

Cobertura de Grupos / Luís Farias Maia – Fortaleza: 2011.
99f.

Orientador: Prof. Dr. José Robério Rogério.

Área de concentração: Matemática.

Dissertação(Mestrado) - Universidade Federal do Ceará,
Centro de Ciências, Departamento de Matemática, Fortaleza,
2011

1. Teoria dos Grupos. I. Rogério, José Robério (Orient.)

CDD 512.2

Esta folha será substituída pela ata.

*Aos meus pais, Valmir e Zuleide,
aos meus irmãos, Júnior e Leandro,
e à minha linda noiva, Hilda,
por estarem sempre ao meu lado.*

Agradecimentos

Agradeço primeiramente a Deus, porque a ele pertence toda primazia.

A todas as pessoas que entraram na minha vida e me inspiraram, comoveram e iluminaram com sua presença. Expresso minha gratidão às seguintes pessoas pelo enorme apoio e contribuição à minha jornada e a conclusão desta dissertação:

Ao Sr. Assis, pelas palavras de conforto nos momentos mais difíceis.

À Alessandra (Lelê), por me fazer acreditar nesse meu sonho.

Ao meu orientador, professor Robério Rogério, pelas palavras animadoras que me mantiveram confiante até o término deste trabalho, por suas lições que foram e serão relevantes durante toda minha vida acadêmica e por acreditar no meu esforço e no meu potencial.

Aos meus grandes amigos da Matemática: Joserlan Perote e Michel Pinho, pelos momentos que passamos juntos no Pici e no Itaperi.

À Kiara, pela digitação desta dissertação.

À minha família (meus queridos pais, Valmir e Zuleide, e meus irmãos, Junior e Leandro) e à minha amada noiva, Hilda, pelo apoio incondicional durante este período do mestrado. Sem vocês tudo seria absurdamente mais difícil.

Por fim, aos meus anjos da guarda por colocarem todas essas pessoas (e muitas outras que não citei) em minha vida. Sem vocês, nada disso seria possível.

“A Matemática, olhada corretamente, possui não apenas verdade, mas suprema beleza, uma beleza fria e austera, como aquela da escultura, sem apelo a qualquer parte de nossa natureza mais fraca, sem as encantadoras armadilhas da pintura ou da música, mas sublimemente pura, e capaz de uma rigorosa perfeição que somente a maior das artes pode exibir. ”

Bertrand A. W. Russel(1872 - 1970)

Filósofo e Matemático.

Resumo

Esta dissertação apresenta resultados sobre Coberturas de Grupos por Subgrupos Abelianos, Subgrupos de Sylow e Subgrupos Normais. O Teorema de Neumann é indispensável no estudo das Coberturas por Subgrupos. Apresentamos no Apêndice C uma prova elementar de um resultado muito importante nas Coberturas p-Sylow.

Abstract

The paper results on the Coverage Groups by Abelian Subgroups, Subgroups of Sylow and Normal Subgroups. Neumann's Theorem is essential in the story of Coverage by Subgroups. We present in Appendix C an elementary proof of a very important result in the Coverage p-Sylow.

Sumário

Introdução	11
1 Preliminares	16
1.1 Grupos e Subgrupos	16
1.2 Classes Laterais	19
1.3 Subgrupos Clássicos	22
1.4 Teoremas: dos Isomorfismos e da Correspondência	25
1.5 O Grupo Simétrico S_n	28
1.6 Representação Permutacional	30
1.7 Os Teoremas de Schur e Baer	32
1.8 Subgrupos de Sylow	34
1.9 Grupos Nilpotentes e Grupos Solúveis	36
2 Cobertura por Subgrupos	42
2.1 Cobertura por Três Subgrupos	43
2.2 O Teorema de Neumann	46
2.3 Características dos Grupos que possuem Coberturas por Subgrupos Próprios	47
2.4 Cobertura por Subgrupos Cíclicos	49

3	Coberturas p-Sylow	51
3.1	Coberturas Contendo Subgrupos de Sylow	52
3.2	O Grupo Simétrico	54
4	Cobertura por Subgrupos Abelianos	58
4.1	Caracterização das Coberturas por Abelianos	58
5	Cobertura por Subgrupos Normais	67
5.1	Caracterização dos Grupos que são cobertos por Subgrupos Normais	67
5.2	Cobertura por Subgrupos Verbais	82
	Apêndice A - O Teorema de Ramsey	87
	Apêndice B - O Teorema de Bertrand	89
	Apêndice C - Uma Prova Elementary	94
	Referências Bibliográficas	97

Introdução

No início da década de 50, o matemático italiano D. Greco publicou os primeiros trabalhos que tratavam de um problema aparentemente simples:

Quando podemos escrever um grupo como união de n subgrupos?

D. Greco procurou estudar os casos pequenos. Ele conseguiu uma caracterização para os grupos que podem ser cobertos por 2, 3 ou 4 subgrupos. Para o caso $n = 5$, sua caracterização foi apenas parcial, o que mostrava a dificuldade do problema. Percebeu-se ali que talvez esta não fosse a abordagem mais interessante e outras idéias começaram a surgir.

No ano de 1954, B. H. Neumann publicou dois artigos: “Groups covered by permutable subsets”, “Groups covered by finitely cosets” relacionados com o assunto. Ele estudou o problema da cobertura de um grupo, não só por subgrupos, mas também por classes laterais. Um dos resultados mais importantes obtidos por Neumann nos diz que se um grupo G pode ser coberto por uma quantidade finita de classes laterais(à direita):

$$G = X_1x_1 \cup X_2x_2 \cup \dots \cup X_nx_n \quad (1)$$

então pelo menos um dos subgrupos X_i deve ter índice finito em G , e as classes laterais dos subgrupos de índice infinito podem ser omitidas da cobertura.

Diremos que a cobertura (1) é irredundante quando nenhuma das classes lat-

erais puder ser omitida. Em outras palavras, quando:

$$X_i x_i \not\subseteq \bigcup_{j \neq i} X_j x_j.$$

O resultado de Neumann pode então ser reescrito como:

Teorema 0.1 (Neumann) *Se G admite uma cobertura irredundante por n classes laterais:*

$$G = X_1 x_1 \cup X_2 x_2 \cup \dots \cup X_n x_n$$

então o índice $\left| G : \bigcap_{i=1}^n X_i \right|$ é finito.

Este teorema se aplica ao caso particular onde as classes são subgrupos. R. Baer em “Groups covered by finitely many cosets” observou que quando os subgrupos eram abelianos, sua interseção estava contida no centro de G , o que nos permite concluir que $|G : Z(G)|$ é finito neste caso. Daí, por diante, vários trabalhos foram publicados relacionados a tal problema. Começou-se a estudar o problema de cobertura de grupos por subgrupos específicos, por exemplo, por subgrupos normais (M. A. BRADIE, R. F. CHAMBERLAIN e L. C. KAPPE), por subgrupos próprios (J. H. E. COHN), etc.

Este trabalho dissertativo, que aqui apresentamos é baseado nos seguintes artigos: [2], [5], [6], [7], [8]. Apresentamos agora um pouco da estrutura do texto, ou seja, dos capítulos e apêndices que compõem esse trabalho.

Esta dissertação é composta de cinco capítulos e três apêndices. Vamos falar um pouco agora da estrutura do texto, do que é feito em cada um dos cinco capítulos e dos três apêndices.

No capítulo 1 desenvolvemos todos os pré-requisitos que serão necessários no decorrer da leitura. As seis primeiras seções são tópicos elementares do currículo da Teoria dos Grupos. A seção 1.7 (os Teoremas de Schur e Baer) traz o principal teorema do Capítulo 1.

Teorema 0.2 (Schur) *Se $\frac{G}{Z(G)} \in \mathcal{F}$ então $G' \in \mathcal{F}$, onde \mathcal{F} representa a família de grupos finitos.*

Ainda no Capítulo 1, falamos sobre os FC-grupos, que são aqueles onde cada elemento possui um número finito de conjugados. Comentamos também sobre os Teoremas de Sylow e sobre os Grupos Nilpotentes e os Grupos Solúveis.

No Capítulo 2 daremos a definição de Cobertura de Grupos, faremos Proposições e Teoremas que terão grande utilidade no decorrer de todo o trabalho. Daremos a caracterização dos grupos que são cobertos por três subgrupos, com o seguinte:

Teorema 0.3 (Haber-Rosenfeld) *Um grupo G é a união de três subgrupos próprios se e só se o grupo de Klein for imagem homomórfica de G .*

Provamos também o Teorema de Neumann, que é indispensável no estudo das Coberturas de Grupos.

Teorema 0.4 (Neumann) *Suponhamos que o grupo G é coberto por n subgrupos, $G = \bigcup_{i=1}^n H_i$. Suponha que para certo $i \in \{1, 2, 3, \dots, n\}$ tenhamos $H_i \not\subseteq \bigcup_{j \neq i} H_j$, então $|G : H_i|$ é finito.*

Na última seção deste capítulo (2.4), caracterizamos os grupos que podem ser cobertos por Subgrupos Cíclicos:

Teorema 0.5 *Um grupo G admite cobertura finita por subgrupos cíclicos se, e somente se, G é finito ou $G = C_\infty$.*

O Capítulo 3 é baseado no artigo [7] sobre Coberturas p-Sylow. Daremos a caracterização de tais coberturas e estudaremos as Coberturas p-Sylow do Grupo S_n . O principal Teorema deste capítulo é:

Teorema 0.6 *Seja G um grupo finito não cíclico e p um primo que divide a ordem de G . G possui uma p -Sylow cobertura se, e somente se, existe um C_{pp} elemento em G .*

Para o estudo das Coberturas p -Sylow do grupo S_n , precisamos de resultados de Teoria dos Números, como o Postulado de Bertrand, que é um dos nossos Apêndices. Usamos um Lema muito importante, onde apresentaremos no Apêndice C deste trabalho uma prova elementar de nossa autoria.

Lema 0.7 *Se α é uma permutação de S_n , de modo que α é decomposta em exatamente a_i i -ciclos, $a_i \geq 0$, temos*

$$|C_{S_n}(\alpha)| = \prod (a_i!)^{a_i}$$

onde $n = a_1 + 2a_2 + 3a_3 + \dots + na_n$.

O Capítulo 4 trata das Coberturas por Subgrupos Abelianos e dos conjuntos de elementos dois a dois não comutantes. A seção 4.1 mostra como o problema da Cobertura por Subgrupos se relaciona com o problema de cotar o índice $|G : Z(G)|$ a partir do tamanho máximo de conjuntos com elementos dois a dois não comutantes. A última parte do Teorema 4.1 é dedicada ao problema proposto por Paul Erdős. Em janeiro de 1975, o famoso matemático Paul Erdős lançou a primeira pergunta no assunto.

Se um grupo G não admite conjunto infinito de elementos dois a dois não comutantes, existirá uma cota superior para quantidade de elementos desses conjuntos?

No mesmo ano, Neumann caracterizou os conjuntos mencionados por Erdős, publicando o seguinte teorema:

Teorema 0.8 (Neumann - 1976) *Um grupo G tem centro com índice finito se, e somente se, G não possui um conjunto infinito de elementos dois a dois não comutantes.*

No Capítulo 5 estudamos a Cobertura por Subgrupos Normais e por Subgrupos Verbais. Daremos a caracterização dos grupos que podem ser cobertos por uma quantidade finita de Subgrupos Normais, com o seguinte teorema:

Teorema 0.9 *Um grupo G possui uma cobertura finita não trivial por subgrupos normais se, e somente se, existe $N \triangleleft G$, tal que*

$$\frac{G}{N} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$$

para algum primo p .

O trabalho é, enfim, encerrado com três apêndices. No primeiro provamos o Teorema de Ramsey na sua versão infinita, usamos para provarmos o Teorema 2.2 de Neumann. No segundo apêndice, provamos o Postulado de Bertrand, onde foi muito importante nas coberturas p -Sylow para provarmos o Teorema 3.5. E por fim, no terceiro apêndice damos uma prova elementar do Lema 3.2.

Capítulo 1

Preliminares

Neste primeiro capítulo trataremos de vários conceitos básicos e fundamentais da teoria dos grupos. Abordaremos temas clássicos como subgrupos, normalidade, grupo simétrico, Teorema de Sylow e Teorema de Schur. Enunciaremos, porém, alguns resultados sem apresentar uma demonstração, tendo em vista que muitos dos resultados aqui apresentados são comumente estudados em cursos iniciais de Álgebra, por outro lado, deixaremos sempre referência para uma demonstração do resultado.

1.1 Grupos e Subgrupos

Definição 1.1 *Um conjunto G com uma operação*

$$\begin{aligned} G \times G &\rightarrow G \\ (a, b) &\rightarrow a \cdot b \end{aligned}$$

é um grupo se as condições seguintes são satisfeitas:

(i) *A operação é associativa, isto é,*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a, b, c \in G$$

(ii) Existe um elemento neutro, isto é,

$$\exists e \in G, \text{ tal que } e \cdot a = a \cdot e = a, \quad \forall a \in G$$

(iii) Todo elemento possui um elemento inverso, isto é,

$$\forall a \in G, \exists b \in G, \text{ tal que } a \cdot b = b \cdot a = e$$

O grupo é abeliano ou comutativo se:

(iv) A operação é comutativa, isto é,

$$a \cdot b = b \cdot a, \quad \forall a, b \in G$$

Observação 1.1

- 1) O elemento neutro é único.
- 2) O elemento inverso é único.

Definição 1.2 Seja G um grupo. Um subconjunto não vazio H de G é um subgrupo de G (denotamos por $H < G$) quando, com a operação de G , o conjunto H é um grupo, isto é, quando as condições são satisfeitas.

- i) $h_1 \cdot h_2 \in H, \forall h_1, h_2 \in H$.
- ii) $h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3, \forall h_1, h_2, h_3 \in H$.
- iii) $\exists e_H \in H, \text{ tal que } e_H \cdot h = h \cdot e_H = h, \forall h \in H$.
- iv) Para cada $h \in H$, existe $k \in H$, tal que $h \cdot k = k \cdot h = e_H$.

Observação 1.2

- 1) A condição (ii) é sempre satisfeita, pois a igualdade $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ é válida para todos os elementos de G .

2) O elemento neutro e_H de H é necessariamente igual ao elemento neutro e de G .

3) Dado $h \in H$, o inverso de h em H é necessariamente igual ao inverso de h em G .

Proposição 1.1 *Seja H um subconjunto não vazio do grupo G . Então H é um subgrupo de G se, e somente se, as duas condições são satisfeitas:*

$$i) h_1 \cdot h_2 \in H, \forall h_1, h_2 \in H$$

$$ii) h^{-1} \in H, \forall h \in H$$

Demonstração: Suponhamos que H seja um subgrupo de G . A condição i) é então claramente satisfeita. Agora, seja $h \in H$; sendo H um grupo, h possui um inverso em H ; mas tal inverso é necessariamente igual ao inverso de h em G , isto é, é necessariamente igual ao inverso de h em G ; logo $h^{-1} \in H$. Reciprocamente, suponhamos que as duas condições sejam satisfeitas. Então, a condição i) da Definição 1.2 é claramente satisfeita. A condição ii) é sempre satisfeita como já vimos. Para ver que iii) é satisfeita, basta ver que $e \in H$; isto de fato acontece, pois tomando $h \in H$, temos $h^{-1} \in H$ pela conclusão ii) e logo $e = h \cdot h^{-1} \in H$.

■

Proposição 1.2 *Seja G um grupo. Então:*

(i) *Se $\{H_\lambda; \lambda \in \Lambda\}$ é uma família de subgrupos G , então $I = \bigcap_{\lambda \in \Lambda} H_\lambda$ é subgrupo de G .*

(ii) *Se $H, K \leq G$, então $HK \leq G \Leftrightarrow HK = KH$.*

(iii) (*Lei Modular de Dedekind*) Sejam H, K, L subgrupos de um grupo G tal que $K \subseteq L$. Então

$$(HK) \cap L = (H \cap L)K, \quad (HK = \{hk; h \in H \text{ e } k \in K\}).$$

Demonstração: Veja [9], 1.3.2, 1.3.13 e 1.3.14.

1.2 Classes Laterais

Em nosso texto, G denotará um grupo, indicado multiplicativamente, com elemento neutro 1. Se H é um subgrupo de G , podemos definir em G a seguinte relação de equivalência:

$$x \sim y \Leftrightarrow y^{-1} \cdot x \in H.$$

Dessa forma a classe de equivalência contendo $x \in G$ será o subconjunto:

$$xH = \{xh; h \in H\}$$

que será chamada classe lateral à esquerda de H contendo x . Observe que duas classes laterais à esquerda são iguais ou disjuntas, e G é a união de todas elas. Um subconjunto $T \subset G$ é dito ser um transversal (à esquerda) quando G se escreve como a união disjunta:

$$G = \dot{\bigcup}_{t \in T} tH.$$

Observe que em um transversal T aparece um, e somente um, representante de cada classe. Assim, cada elemento de G poderá ser escrito de forma única como th , onde $t \in T$, e $h \in H$. De modo análogo, definimos a classe lateral à direita de H contendo x ;

$$Hx = \{hx; h \in H\}.$$

Esta é a classe de equivalência de $x \in G$ pela relação:

$$x \sim y \Leftrightarrow x \cdot y^{-1} \in H.$$

Um transversal (à direita) pode ser então definido como acima.

Denotaremos a cardinalidade de um conjunto X por $|X|$. Como definição, temos o seguinte:

- 1) $|X| = |Y|$ se existe uma bijeção $F : X \rightarrow Y$.
- 2) $|X| \leq |Y|$ se existe uma injeção $F : X \rightarrow Y$.
- 3) $|X| \cdot |Y| = |X \times Y|$.

Proposição 1.3 Se $A_i; i \in I$ são conjuntos disjuntos com $|A_i| = |A|$, então:

$$\left| \dot{\bigcup}_{i \in I} A_i \right| = |I| \cdot |A|$$

Demonstração: Para ver isso denote por $F_i : A \rightarrow A_i$ uma bijeção e defina $\phi : I \times A \rightarrow \dot{\bigcup}_{i \in I} A_i$ por $\phi(i, a) = F_i(a)$. É fácil ver que ϕ é bijetiva.

■

Todas as classes laterais de H têm a mesma cardinalidade de H em virtude da bijeção $h \rightarrow hx$ de H em xH . Definamos o índice de H em G como sendo a cardinalidade do conjunto das classes laterais à esquerda (ou à direita) de H em G , o qual denotaremos por $|G : H|$.

Proposição 1.4 (Lagrange) Se $H \leq G$, temos

$$|G| = |G : H| \cdot |H|.$$

Demonstração: Segue diretamente da Proposição 1.2, já que

$$G = \dot{\bigcup}_{t \in T} tH$$

e $|G : H| = |T|$, onde T é um transversal.



Proposição 1.5 *Sejam $H \leq K \leq G$, então:*

$$|G : H| = |G : K| \cdot |K : H|.$$

Demonstração: Sejam T um transversal de K em G , e U um transversal de H em K . Temos

$$G = \dot{\bigcup}_{t \in T} Kt \quad ; \quad K = \dot{\bigcup}_{u \in U} Hu.$$

Afirmamos que $G = \dot{\bigcup}_{(u,t) \in U \times T} Hut$, o que demonstra a Proposição. Para ver isso, tome $g \in G$ qualquer, daí,

$$g = kt \Rightarrow g = hut \Rightarrow G = \dot{\bigcup}_{(u,t) \in U \times T} Hut \quad (\text{Ainda não sabemos se são disjuntos}).$$

Porém, se

$$Hut \cap Hu_1t_1 \neq \emptyset \Rightarrow ut = hu_1t_1 \Rightarrow t = kt_1 \Rightarrow t = t_1 \Rightarrow u = u_1.$$



Proposição 1.6 *Se $H, K \leq G$, então:*

$$|G : H \cap K| \leq |G : H| \cdot |G : K|.$$

Demonstração: Denotemos por $(G : H)$ o conjunto das classes laterais de H em G . Montemos uma função que será injetiva,

$$F : (G : H \cap K) \rightarrow (G : H) \times (G : K)$$

dada por $(H \cap K)g \mapsto (Hg, Kg)$. Vejamos que F é bem definida, ou seja, que independe do representante da classe:

$$\begin{aligned} (H \cap K)g = (H \cap K)g_1 &\Rightarrow gg_1^{-1} \in H \cap K \\ &\Rightarrow gg_1^{-1} \in H; gg_1^{-1} \in K \\ &= Hg = Hg_1; Kg = Kg_1 \end{aligned}$$

Agora vejamos a sua injetividade:

$$\begin{aligned}(Hg, Kg) = (Hg_1, Kg_1) &\Rightarrow gg_1^{-1} \in H; gg_1^{-1} \in K \\ &\Rightarrow gg_1^{-1} \in H \cap K \\ &\Rightarrow (H \cap K)g = (H \cap K)g_1\end{aligned}$$

■

Apresentemos um resultado que será muito importante em nosso trabalho.

Corolário 1.1 (Poincaré) *Se A_1, A_2, \dots, A_n são subgrupos de G com índice finito, então $\bigcap_{i=1}^n A_i$ tem índice finito em G .*

Demonstração: Segue da Proposição anterior que:

$$\left| G : \bigcap_{i=1}^n A_i \right| \leq \prod_{i=1}^n |G : A_i| < \infty.$$

■

1.3 Subgrupos Clássicos

Esta é uma seção especial para consolidarmos a notação a ser usada no texto.

Vejamos as definições:

- Se $x \in G$ definimos a ordem de x , indicada por $o(x)$ como sendo o menor natural tal que $x^{o(x)} = 1$ (Caso não exista tal natural, diremos que x tem ordem infinita).
- Se $x, g \in G$ o conjugado de x por g será $x^g = g^{-1}xg$.
- Se $x \in G$, a classe de conjugação de x é o subconjunto:

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

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

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

Quando $N^x = N, \forall x \in G$ diremos que N é normal em G e denotaremos por $N \trianglelefteq G$.

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

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

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

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

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

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

- Se $H \leq G$, definimos o normalizador de H em G como sendo o subgrupo

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

Note que $H \trianglelefteq N_G(H) \leq G$.

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

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

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

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

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

Lembrando que se $X \subset G$, o subgrupo gerado por X será:

$$\langle X \rangle = \{x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \dots \cdot x_n^{\alpha_n}; x_i \in X; \alpha_i = \pm 1\}.$$

Observe ainda que $G' \trianglelefteq G$.

- Se $H, K \subset G$ definimos $[H, K] = \langle [h, k]; h \in H, k \in K \rangle$. Note que $G' = [G, G]$.
- Um grupo K é dito ser de torção quando $o(x) < \infty, \forall x \in K$.
- Um grupo G é cíclico quando ele pode ser gerado por um elemento, isto é, quando $G = \langle g \rangle$, para algum $g \in G$.

Se $N \trianglelefteq G$, o conjunto das classes de N à direita (ou à esquerda) é um grupo com a operação $Nx \cdot Ny = Nxy$. Tal grupo é chamado grupo quociente de G por N e denotado por G/N . A proposição seguinte caracteriza os grupos quocientes abelianos.

Proposição 1.7 *Se $N \trianglelefteq G$, então G/N é abeliano $\Leftrightarrow G' \leq N$*

Demonstração:

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

$$N = N(a^{-1}b^{-1}ab) = (Na^{-1})(Nb^{-1})(Na)(Nb) = (Na)^{-1}(Nb)^{-1}(Na)(Nb)$$

$$\Rightarrow (Nb)(Na) = (Na)(Nb) \Rightarrow G/N \text{ é abeliano.}$$

(\Rightarrow) Suponhamos G/N abeliano:

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

■

Proposição 1.8 *Seja G um grupo e seja $Z(G)$ seu centro. Se $G/Z(G)$ é cíclico, então $Z(G) = G$.*

Demonstração: Seja \bar{z} um gerador do grupo $G/Z(G)$. Então, $\forall g \in G, \exists i$ tal que $\bar{g} = \bar{z}^i$. Logo $g = z^i \cdot h$ com $h \in Z(G)$. Se $g_1 := z^{i_1} \cdot h_1$ e $g_2 := z^{i_2} \cdot h_2$ são dois elementos quaisquer de G , temos:

$$g_1 g_2 = z^{i_1} \cdot h_1 \cdot z^{i_2} \cdot h_2 = z^{i_1+i_2} \cdot h_1 \cdot h_2 = z^{i_2} \cdot h_2 \cdot z^{i_1} \cdot h_1 = g_2 g_1,$$

pois h_1 e h_2 comutam com qualquer elemento de G . Isto mostra que o grupo G é abeliano, isto é, $G = Z(G)$.

■

1.4 Teoremas: dos Isomorfismos e da Correspondência

Definição 1.3 *Sejam G e G_1 grupos. A aplicação $\varphi : G \rightarrow G_1$ que satisfaz $\varphi(xy) = \varphi(x)\varphi(y), \forall x, y \in G$ é chamada um homomorfismo entre os grupos G e G_1 .*

Ao conjunto $\{g \in G; \varphi(g) = 1_{G_1}\}$ chamaremos de núcleo do homomorfismo e denotamos por $\text{Ker}\varphi$. Denotamos ainda $\varphi(G)$ por $\text{Im}\varphi$. Facilmente podemos verificar que $\text{Ker}\varphi$ é um subgrupo normal de G e $\text{Im}\varphi$ é um subgrupo de G_1 . Se φ for bijeção, então, esta é dita ser um isomorfismo. Neste caso, $\text{Ker}\varphi = \{1_{G_1}\}$, G e G_1 são ditos isomorfos e escrevemos:

$$G \simeq G_1.$$

Se além disso tivermos $G = G_1$, então φ é dito ser um automorfismo de G . O conjunto de todos os automorfismos de G é, na realidade, um grupo com a operação de composição de funções. Denotamos este grupo por $\text{Aut}G$.

Teorema 1.1 (1º Teorema do Isomorfismo) *Seja $\varphi : G \rightarrow G_1$ um homomorfismo de grupos. Então*

$$\frac{G}{\text{Ker}\varphi} \simeq \text{Im}(\varphi).$$

Em particular, se φ é sobrejetiva, então

$$\frac{G}{\text{Ker}\varphi} \simeq G_1.$$

Demonstração: Veja [9], 1.4.3.

Teorema 1.2 (2º Teorema do Isomorfismo) *Sejam H e N subgrupos de G tal que $N \trianglelefteq G$. Então:*

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

Demonstração: Veja [9], 1.4.4.

Teorema 1.3 (3º Teorema do Isomorfismo) *Sejam H, K subgrupos normais em G , tais que $K \leq H$, então:*

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

Demonstração: Veja [9], 1.4.5.

Teorema 1.4 (da Correspondência) *Seja $\varphi : G \rightarrow G_1$ um homomorfismo sobrejetor com núcleo $N = \text{Ker}\varphi$. Sejam $H_1 = \{\text{subgrupos de } G \text{ que contém } N\}$ e $H_2 = \{\text{subgrupos de } G'\}$. Então a aplicação dada por $H \mapsto \varphi(H)$ é uma bijeção de H_1 sobre H_2 . Além disso, para $H \in H_1$, $H \trianglelefteq G \Leftrightarrow \varphi(H) \trianglelefteq G'$*

Demonstração: Pelas Propriedades de Homomorfismos, sabemos que $\varphi(H) \leq G'$ para todo $H \leq G$, e se $H' \in H'_1$, então $H = \varphi^{-1}(H') \trianglelefteq G$. Como $N = \varphi^{-1}(\{0\}) \subseteq \varphi^{-1}(H') = H$ vem que $H \in H_1$. Além disso, como φ é sobre, temos $\varphi(H) = H'$. Sejam $H, L \in H_1$, e suponhamos que $\varphi(H) = \varphi(L)$. Temos

$$\begin{aligned} x \in H &\Leftrightarrow \varphi(x) \in \varphi(H) = \varphi(L) \\ &\Leftrightarrow \exists y \in L, \quad \text{tal que } \varphi(y) = \varphi(x) \\ &\Leftrightarrow \varphi(xy^{-1}) = 1 \\ &\Leftrightarrow xy^{-1} \in N \subseteq L \\ &\Rightarrow x \in Ly \subseteq L. \end{aligned}$$

Com isso fica provado que $H \subseteq L$. De modo análogo, tem-se $L \subseteq H$. Portanto, $\varphi : H_1 \rightarrow H'_1 : H \mapsto \varphi(H)$ é um bijeção.

Se $H \trianglelefteq G$, tem-se

$$\varphi(x)\varphi(H)\varphi^{-1}(x) = \varphi(x)\varphi(H)\varphi(x^{-1}) = \varphi(xHx^{-1}) = \varphi(H)$$

isto é, $\varphi(H) \trianglelefteq G'$; na outra direção, se $\varphi(H) \trianglelefteq G'$, então para todo $x \in G$, $\varphi(xHx^{-1}) = \varphi(x)\varphi(H)\varphi^{-1}(x) = \varphi(H)$. Logo, $xHx^{-1} \subseteq \varphi^{-1}(\varphi(H))$. Se $y \in \varphi^{-1}(\varphi(H))$, tem-se $\varphi(y) = \varphi(z), \exists z \in H$. Segue-se daí que $yz^{-1} \in N \subseteq H$ e, portanto, $y = (yz^{-1})z \in H$. Provamos assim que $\varphi^{-1}(\varphi(H)) \subseteq H$.

Como, de um modo geral para conjuntos, $H \subseteq \varphi^{-1}(\varphi(H))$, concluímos que $\varphi(xHx^{-1}) = \varphi(H)$. Como $N \subseteq H$ e $N \trianglelefteq G$, vem $N = xHx^{-1} \subseteq xHx^{-1}$. Finalmente, como φ é uma bijeção, segue-se que $xHx^{-1} = H$, para cada $x \in G$.

■

Corolário 1.2 *Seja $N \trianglelefteq G$. Dado um subconjunto \overline{H} de $\frac{G}{N}$, existe um único subgrupo H de G tal que $\overline{H} = \frac{H}{N}$. Além disso, $H \trianglelefteq G$ se, e somente se, $\frac{H}{N} \trianglelefteq \frac{G}{N}$*

Demonstração: Veja [1], 3.29.

■

1.5 O Grupo Simétrico S_n

Uma permutação $\alpha \in S_n$ é chamada ciclo, mais especificamente um k -ciclo, $2 \leq k \leq n$, se existem $i_1, i_2, \dots, i_k \in I_n = \{1, 2, 3, \dots, n\}$, distintos, tais que $\alpha(j) = j$, para todo $j \notin \{i_1, i_2, \dots, i_k\}$, e $\alpha(i_l) = i_{l+1}$, para $l = 1, 2, \dots, k - 1$ e $\alpha(i_k) = i_1$.

Usaremos a notação abreviada $\alpha = (i_1 i_2 \dots i_k)$, onde $\{i_1, i_2, \dots, i_k\}$ é chamado o conjunto suporte de α . Denotaremos por (1) ou mais geralmente por (a) , $a \in I_n$, a permutação identidade. Para $k = 2$ e 3 , diremos que α é uma transposição e tríciclo, respectivamente. Dois ciclos são ditos disjuntos se os seus respectivos conjuntos suporte são disjuntos.

Proposição 1.9 *Se dois ciclos α e β são disjuntos, então eles comutam, entre si, isto é, $\alpha\beta = \beta\alpha$.*

Demonstração: Supondo os ciclos $\alpha = (i_1, i_2, \dots, i_k)$ e $\beta = (j_1, j_2, \dots, j_m)$ disjuntos, temos

$$I_n = \{i_1, i_2, \dots, i_k\} \dot{\cup} \{j_1, j_2, \dots, j_m\} \cup J \quad (\text{União Disjunta}).$$

Para cada $i \in I_n$ temos:

1º) $i \notin \{i_1, i_2, \dots, i_k\} \cup \{j_1, j_2, \dots, j_m\}$. Assim,

$$\alpha\beta(i) = \alpha(\beta(i)) = \alpha(i) = i = \beta(i) = \beta(\alpha(i)) = \beta\alpha(i).$$

2º) $i \in \{i_1, i_2, \dots, i_k\}$. Neste caso, temos:

$$\alpha(\beta(i)) = \alpha(i) = \beta(\alpha(i)) = \beta\alpha(i),$$

pois $\alpha(i) = i_p$ não é elemento do conjunto de β .

■

Proposição 1.10 *Toda permutação $(1) \neq \alpha \in S_n$ é um produto de ciclos disjuntos, e tal decomposição é única, a menos da ordem dos fatores.*

Demonstração: Veja [1], 2.4

■

Proposição 1.11 (Regra de Jordan) *Sejam $\alpha = (a_1 a_2 \dots a_r)$ um r -ciclo e $\beta \in S_n$. Então $\beta\alpha\beta^{-1} = (\beta(a_1)\beta(a_2)\dots\beta(a_r))$.*

Demonstração: Façamos $\theta = \beta\alpha\beta^{-1}$ e $\delta = (\beta(a_1)\beta(a_2)\dots\beta(a_r))$. Seja $a \in I_n$.

Se $a \notin \{\beta(a_1), \beta(a_2), \dots, \beta(a_r)\}$, então $\delta(a) = a$. Portanto

$$a \neq \beta(a_i) \Leftrightarrow \beta^{-1}(a) \neq a_i, \quad \forall i = 1, 2, 3, \dots, r.$$

Assim $\beta^{-1}(a) \in \{a_1, a_2, \dots, a_r\}$ e portanto,

$$\theta(a) = \beta\alpha\beta^{-1}(a) = \beta\beta^{-1}(a) = a = \delta(a).$$

Se $a \in \{\beta(a_1), \beta(a_2), \dots, \beta(a_r)\}$ então $a = \beta(a_i)$ para algum $i \in \{1, 2, \dots, r\}$.

Agora temos dois casos:

1º) $i < r \Rightarrow \theta(a) = \beta\alpha\beta^{-1}(\beta(a_i)) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = \delta(\beta(a_i)) = \delta(a)$.

2º) $i = r \Rightarrow \theta(a) = (\beta\alpha\beta^{-1})(\beta(a_k)) = \beta(\alpha(a_k)) = \delta(a)$.

Em suma: $\theta(a) = \delta(a), \forall a \in I_n$, isto é, $\theta = \delta$.

■

1.6 Representação Permutacional

Se X é um conjunto qualquer, denotaremos por S_X o conjunto de todas as funções $F : X \rightarrow X$ bijetoras. É tarefa fácil verificar que S_X com a operação de composição de funções é um grupo. Quando $|X| = n < \infty$, o grupo $S_X = S_n$ será o grupo das permutações de n símbolos.

Definição 1.4 *Uma representação de permutações (ou ação) de um grupo G sobre um conjunto X é um homomorfismo $\varphi : G \rightarrow S_X$.*

A imagem do elemento $g \in G$ será denotada por $\varphi(g)$. No estudo de uma ação, destacam-se os seguintes conjuntos:

- Se $x \in X$, definiremos o estabilizador de x como sendo o subconjunto G_x de G :

$$G_x = \{g \in G; \varphi(g)(x) = x\}.$$

- Se $x \in X$, definimos a órbita de x como sendo o subconjunto Gx de X dado por:

$$Gx = \{\varphi(g)(x); g \in G\}.$$

- Se $g \in G$, o conjunto dos pontos fixos de $\varphi(g)$ será denotado por X_g , ou seja:

$$X_g = \{x \in X; \varphi(g)(x) = x\}.$$

Podemos definir a seguinte relação de equivalência em X :

$$x \sim y \Leftrightarrow y = \varphi(g)(x), \quad \text{para algum } g \in G.$$

Verificamos isto a seguir:

- (i) $x \sim x$ pois $x = \varphi(1)(x)$.

(ii) Se $x \sim y$ então $y = \varphi(g)(x)$. Daí $x = \varphi(g^{-1})(y) \Rightarrow y \sim x$.

(iii) Se $x \sim y$ e $y \sim z$, então $y = \varphi(g_1)(x)$ e $z = \varphi(g_2)(y)$. Daí obtemos:

$$z = \varphi(g_1)(\varphi(g_2)(x)) = \varphi(g_1g_2)(x) \Rightarrow x \sim z.$$

Veja ainda que a classe de equivalência do elemento x é o conjunto

$$\bar{x} = \{\varphi(g)(x); g \in G\} = Gx \quad (\text{Órbita de } X).$$

Teorema 1.5 *Seja $\varphi : G \rightarrow S_X$ uma ação de grupo G em um conjunto X . Então:*

(i) $G_x \leq G$

(ii) $|Gx| = |G : G_x|$

Demonstração :

(i) Como $\varphi(1)(x) = x, \forall x \in X$, temos que $1 \in G_x$. Daí, $G_x \neq \emptyset$. Dados $g_1, g_2 \in G_x$, temos: $\varphi(g_1)(x) = x$ e $\varphi(g_2)(x) = x$.

Assim,

$$\varphi(g_1g_2^{-1})(x) = \varphi(g_1)(\varphi(g_2^{-1})(x)) = \varphi(g_1)(x) = x.$$

Portanto, $g_1g_2^{-1} \in G_x$.

Como g_1 e g_2 foram tomados arbitrariamente em G_x , o resultado segue.

(ii) Definamos a função Ψ por:

$$\begin{aligned} \{gG_x; g \in G\} & \xrightarrow{\Psi} Gx \\ gG_x & \mapsto \varphi(g)(x) \end{aligned}$$

Vamos provar que esta função está bem definida, ou seja, que independe do elemento da classe, e que é uma bijeção.

- Ψ está bem definida: Se $gG_x = hG_x \Rightarrow g = hz; z \in G_x$. Daí teremos:

$$\varphi(g)(x) = \varphi(hz)(x) = \varphi(h)(\varphi(z)(x)) = \varphi(h)(x)$$

- Ψ é injetiva: Suponha que $\varphi(g)(x) = \varphi(h)(x)$. Com isso teremos:

$$\varphi(h^{-1})(\varphi(g)(x)) = x \Rightarrow \varphi(h^{-1}g)(x) = x \Rightarrow h^{-1}g \in G_x \Rightarrow gG_x = hG_x.$$

- Obviamente Ψ é sobrejetiva.

Concluimos portanto que Ψ é uma bijeção, logo $|G : G_x| = |Gx|$.

■

Teorema 1.6 *Seja G um grupo. Então para cada $x \in G$, $|G : C_G(x)| = |x^G|$.*

Demonstração: Definamos φ agora por:

$$\begin{aligned} \varphi & : G \rightarrow S_G \\ g & \mapsto \varphi(g) : x \rightarrow gxg^{-1} \end{aligned}$$

Dessa forma φ será uma representação de permutações. Vejamos quem é Gx nessa ação:

$$Gx = \{gxg^{-1}; g \in G\} = \{x^{g^{-1}}; g \in G\} = x^G.$$

Além disso: $G_x = \{g \in G; x^{g^{-1}} = x, \forall x \in G\} = C_G(x)$. E pelo Teorema 1.5, segue o resultado.

■

1.7 Os Teoremas de Schur e Baer

Enunciaremos dois Teoremas que serão importantíssimos no nosso trabalho.

Teorema 1.7 (Schur) *Se $\frac{G}{Z(G)}$ é finito então G' é finito. Mais ainda, se $\left| \frac{G}{Z(G)} \right| = n$, então $x^n = 1, \forall x \in G'$, em outras palavras $o(x) | n, \forall x \in G'$.*

Demonstração: Veja [9], 10.1.4.

Definição 1.5 Diremos que um grupo G é *FC-grupo* (do inglês: *FC* = “*Finite Conjugate*”) se x^G é finito para qualquer $x \in G$. Sobre a classe de conjugação x^G , lembramos que:

$$|x^G| = |G : C_G(x)|.$$

Note ainda que $C_G(\langle x^G \rangle) = C_G(x^G)$. Além disso $\langle x^G \rangle \trianglelefteq G$, o que implica que $C_G(x^G) \trianglelefteq G$, já que o centralizador de um subgrupo normal é normal.

Proposição 1.12 Se G é um *FC-grupo* se, e somente se, $\frac{G}{C_G(x^G)}$ for finito para qualquer $x \in G$.

Demonstração:

(\Rightarrow) Suponhamos que G é um *FC-grupo*. Faça $x^G = \{x_1, x_2, \dots, x_n\}$. Daí:

$$|x^G| = |x_i^G| = |G : C_G(x_i)| = |G : C_G(x)| = n.$$

Usando Poincaré, concluímos que

$$|G : C_G(x^G)| = \left| G : \bigcap_{i=1}^n C_G(x_i) \right| < \infty.$$

Ou melhor: $\frac{G}{C_G(x^G)}$ é finito.

(\Leftarrow) Veja que para qualquer $x \in G$, $C_G(x^G) \leq C_G(x) \leq G$. Daí teremos:

$$|x^G| = |G : C_G(x)| \leq |G : C_G(x^G)| < \infty$$

e portanto G será um *FC-grupo*. ■

Teorema 1.8 (Baer) Se G é um *FC-grupo*, então $\frac{G}{Z(G)}$ é de torção.

Demonstração: Tome $x \in G$ e faça $C = C_G(x)$, temos:

$$|x^G| = |G : C| = n.$$

Seja $\{t_1, t_2, \dots, t_n\}$ um transversal de C em G , daí

$$G = \dot{\bigcup}_{i=1}^n Ct_i.$$

Logo, $G = \langle C, t_1, t_2, \dots, t_n \rangle$. Considerando agora $H = \bigcap_{i=1}^n C_G(t_i^G)$. Observe que H tem índice finito em G , pelo Teorema de Poincaré, já que G é um FC -grupo. Além disso, como vimos no início desta seção, cada $C_G(t_i^G) \trianglelefteq G$, e daí $H \trianglelefteq G$ pois é a interção de normais. Em outras palavras $\frac{G}{H}$ é finito.

Existirá então um natural m , tal que:

$$(xH)^m = H \Rightarrow x^m \in H \Rightarrow x^m t_i = t_i x^m, \quad i = 1, 2, \dots, n.$$

E ainda:

$$x^m c = c x^m, \quad \forall c \in C.$$

Portanto,

$$x^m \in Z(G) \Rightarrow o(xZ(G)) \leq m.$$

■

1.8 Subgrupos de Sylow

Teorema 1.9 (1º Teorema de Sylow) *Sejam p um número primo e G um grupo de ordem $p^m \cdot b$ com $(p, b) = 1$. Então, para cada n , $0 \leq n \leq m$, existe um subgrupo H de G tal que $|H| = p^n$.*

Demonstração: Ver [9].

Corolário 1.3 (Generalização do Lema de Cauchy) *Sejam G um grupo finito e p um número primo que divide $|G|$. Então existe um elemento $x \in G$ de ordem p .*

Definição 1.6 *Sejam G um grupo finito, p um primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que têm ordem p^m são chamados de p -subgrupos de Sylow de G .*

Teorema 1.10 (2º Teorema de Sylow) *Seja um grupo finito e p um primo tal que $|G| = p^m \cdot b$, com $\text{mdc}(p, b) = 1$, então:*

- 1) *Todo p -subgrupo de G está contido em um subgrupo de ordem p^m .*
- 2) *Todos os p -subgrupos de Sylow são conjugados.*

Demonstração: Veja [9], 1.6.16.

Teorema 1.11 (3º Teorema de Sylow) *Seja G um grupo finito e p um número primo, tal que $|G| = p^m \cdot b$, com $\text{mdc}(p, b) = 1$, então:*

- 1) *Se S é um p -subgrupo de Sylow, temos $n_p = (G : N_G(S))$, onde n_p é o número de p -subgrupos de Sylow de G .*
- 2) *n_p divide b e $n_p \equiv 1 \pmod{p}$*

Demonstração: Veja [9], 1.6.16.

O Teorema de Sylow possui inúmeras aplicações. Mostraremos, nesse momento algumas delas. Consideremos em cada umas delas G um grupo finito.

Corolário 1.4 *Um p -subgrupo de Sylow de um grupo G é único se, e somente se, for normal em G .*

Demonstração:

(\Rightarrow) Seja P o único p -subgrupo de Sylow de G . Ora, $\forall g \in G$, temos $|P^g| = |P|$, logo $P^g = P$, donde $P \trianglelefteq G$.

(\Leftarrow) Sejam P e P_1 p -subgrupos de Sylow onde $P \trianglelefteq G$. Pelo 2º Teorema de Sylow, $\exists g \in G$ tal que $P_1 = P^g$, como $P \trianglelefteq G$, segue-se que $P_1 = P$. Logo $n_p = 1$.

■

Corolário 1.5 *Seja P um p -subgrupo de Sylow e $|G : P| = q$, onde q é o menor primo que divide $|G|$, então $P \trianglelefteq G$.*

Demonstração: Pelo 3º Teorema de Sylow, temos:

$$n_p \equiv 1 \pmod{p} \quad \text{e} \quad n_p \text{ divide } q.$$

Logo, $n_p = 1 + kp$, onde $k \in \mathbb{N}$, mas $n_p \leq q \leq p$. Logo $k = 0$ e $n_p = 1$ e pelo Corolário anterior $P \trianglelefteq G$.

■

1.9 Grupos Nilpotentes e Grupos Solúveis

Nesta seção, faremos alguns resultados, utilizados neste trabalho, sobre grupos nilpotentes e solúveis.

Definição 1.7 (Grupo Solúvel) *Um grupo G é dito solúvel, se existe uma série subnormal*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_n = G$$

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

Proposição 1.13 *Se G um grupo, temos:*

- (i) Se G é solúvel, então todo subgrupo de G é solúvel.
- (ii) Se G é solúvel e se $N \triangleleft G$, então o grupo $\frac{G}{N}$ é solúvel.
- (iii) Se $N \triangleleft G$, com N e $\frac{G}{N}$ solúveis, então G é solúvel.

Demonstração:

(i) Como G é solúvel, existe uma série subnormal

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_n = G$$

onde os grupos quocientes $\frac{G_{i+1}}{G_i}$ são abelianos. Seja H um subgrupo de G , e considere $H_i = G_i \cap H$. Seja $h \in H_{i+1} = G_{i+1} \cap H$, daí

$$H_i^h = (G_i \cap H)^h = G_i^h \cap H^h = G_i \cap H$$

o que implica $H_i \trianglelefteq H_{i+1}$, além disso

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

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

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

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

Portanto, $\frac{\frac{G_{i+1} N}{N}}{\frac{G_i N}{N}}$ é abeliano.

Logo,

$$I = N \trianglelefteq \frac{G_1 N}{N} \trianglelefteq \dots \trianglelefteq \frac{G_n N}{N} = \frac{G}{N}$$

é uma série subnormal de $\frac{G}{N}$, portanto $\frac{G}{N}$ é solúvel.

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

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

e

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

Porém, $\frac{\frac{H_{i+1}}{N}}{\frac{H_i}{N}} \simeq \frac{H_{i+1}}{H_i}$, portanto,

$$1 \leq N_0 \trianglelefteq N_1 \trianglelefteq \dots \triangleright N_r = N \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_r = G$$

é uma série subnormal, ou seja G é solúvel.

■

Proposição 1.14 *Sejam G um grupo solúvel e $1 \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ uma série subnormal onde todos os grupos quocientes $\frac{G_{i+1}}{G_i}$ são abelianos. Então $G^{(i)} \subseteq G_{n-i}$ para todo i .*

Demonstração: Provaremos por indução sobre i .

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

Por outro lado, $G^{(i)} \subseteq G_{n-i}$ (Hipótese Indutiva), isto implica, $G^{(i+1)} \subseteq G'_{n-i}$ donde $G^{(i+1)} \subseteq G_{n-i+1}$.

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

■

Corolário 1.6 *G é um grupo solúvel se, e somente se, existe $n \in \mathbb{N}$, tal que $G^{(n)} = 1$.*

Define-se o n -ésimo centro de G indutivamente tomando $Z_1 = Z_1(G) = Z(G)$ o centro de G . Pelo Teorema da Correspondência, existe um único subgrupo normal $Z_2 = Z_2(G)$ de G correspondente ao centro $Z\left(\frac{G}{Z_1}\right)$, isto é, $\frac{Z_2}{Z_1} = Z\left(\frac{G}{Z_1}\right)$. Para $n \geq 2$, define-se $Z_n(G)$ pela igualdade:

$$\frac{Z_n(G)}{Z_{n-1}} = Z\left(\frac{G}{Z_{n-1}}\right).$$

Fazendo $Z_0(G) = \{1\}$, temos então $Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \dots$, chamada a série central crescente de G .

Segue imediatamente da definição que:

$$Z_n(G) = \{x \in G; xyx^{-1}y^{-1} \in Z_{n-1}(G); \text{ para todo } y \in G\}.$$

Assim, $Z'_n \subseteq Z_{n-1}$ para cada $n \geq 1$.

Definição 1.8 Um grupo G é dito nilpotente se $Z_n(G) = G$, para algum $n \geq 1$. O menor desses n é chamado a classe de nilpotência de G .

Em particular, todo grupo abeliano é nilpotente de classe 1. Também, todo grupo nilpotente é solúvel, pois a série central termina em $Z_n = G$, e cada fator $\frac{Z_n}{Z_{n-1}} = Z\left(\frac{G}{Z_{n-1}}\right)$ é abeliano. A recíproca dessa afirmação é falsa. Por exemplo, S_3 é solúvel, mas $Z_1(S_3) = Z_2(S_3) = \dots = \{1\}$. Logo, S_3 não é nilpotente.

Proposição 1.15 Todo p -grupo finito é nilpotente.

Demonstração: Já vimos que $Z_1 = Z(G) = p^{a_1}$, $a_1 > 0$. Se $Z_1 \neq G$, temos

$$\frac{Z_2}{Z_1} = Z\left(\frac{G}{Z_1}\right) = p^{a_2}$$

com $a_2 \geq 1$. Prosseguindo com esse processo, obtemos a sequência crescente de números inteiros

$$1 < |Z_1| = p^{a_1} < |Z_2| = p^{a_1+a_2} < \dots$$

Logo, existe $n \geq 1$ tal que $Z_n(G) = G$.



Proposição 1.16 *Um grupo G é nilpotente se, e somente se, G tem uma série normal*

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_m = G$$

tal que $\frac{G_i}{G_{i-1}} \leq Z\left(\frac{G}{G_{i-1}}\right)$ para $i = 1, 2, 3, \dots, m$.

Demonstração: Se G é nilpotente, então a série central crescente

$$\{1\} = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \dots \trianglelefteq Z_n(G) = G$$

tem fatores abelianos pois $\frac{Z_i(G)}{Z_{i-1}(G)} \leq Z\left(\frac{G}{Z_{i-1}(G)}\right)$. Na outra direção, partindo de uma série normal como no enunciado, então $G_1 \leq Z(G)$, e $\frac{G_2}{G_1} \leq Z\left(\frac{G}{G_1}\right)$. Logo, para todos $x \in G_2$, $y \in G$ tem-se $xyx^{-1}y^{-1} \in G_1 \leq Z(G)$, isto é, $G_2 \leq Z_2(G)$, pois $Z_2(G)$ é o único subgrupo de G tal que $\frac{Z_2(G)}{Z_1(G)} = Z\left(\frac{G}{Z_1(G)}\right)$. Repetimos o processo, obtemos $G_i \leq Z_i(G)$, $i = 1, 2, \dots, m$.

Portanto, $Z_m(G) = G$, e G é nilpotente.



Proposição 1.17 *Seja G um grupo nilpotente. Então:*

(i) *Todo subgrupo de G é nilpotente.*

(ii) *Se $N \trianglelefteq G$, então $\frac{G}{N}$ é nilpotente.*

Demonstração:

(i) Consideremos $H \leq G$ e $1 = G_0 \leq G_1 \leq \dots \leq G_n = G$ uma série central de G . Fazamos $H_i = H \cap G_i$. Logo, como $G_i \trianglelefteq G$, segue-se que $H_i = H \cap G_i \trianglelefteq H$. É suficiente mostrar que a série

$$1 = H_0 \leq H_1 \leq \dots \leq H_n = H$$

é central, ou ainda, que $[H_{i+1}, H_i] \leq H_i, \forall i$. Ora,

$$[H_{i+1}, H] \leq [H \cap G_{i+1}, H] \leq [H, H] \leq H$$

e também,

$$[H_{i+1}, H] \leq [H \cap G_{i+1}, H] \leq [G_{i+1}, G] \leq G_i.$$

Logo,

$$[H_{i+1}, H] \leq H \cap G_i = H_i.$$

Donde, H é nilpotente.

(ii) Seja $N \trianglelefteq G$ e considere $N_i = \frac{G_i N}{N}$. Logo, $N_i \trianglelefteq \frac{G}{N}$ e além disso,

$$\left[N_{i+1}, \frac{G}{N} \right] = \left[\frac{G_{i+1} N}{N}, \frac{G}{N} \right] \leq \frac{[G_{i+1} N, G] N}{N} = \frac{[G_{i+1}, G][N, G] N}{N} \leq \frac{[G_{i+1}, G] N}{N} \leq \frac{G_i N}{N} = N.$$

Portanto, $\frac{G}{N}$ é nilpotente.

■

Capítulo 2

Cobertura por Subgrupos

Neste capítulo, daremos as definições sobre coberturas de grupos, faremos proposições e teoremas que terão grande utilidade no decorrer de todo o trabalho. Daremos a caracterização dos grupos que são cobertos por três subgrupos e dos grupos que são cobertos por subgrupos cíclicos.

Definição 2.1 Dizemos que um grupo G admite uma cobertura finita por subgrupos, se:

$$G = \bigcup_{i=1}^n H_i$$

onde $H_i \leq G$. Dizemos que a cobertura é não trivial, se $H_i < G$, para $i \in \{1, 2, 3, \dots, n\}$. Da mesma forma, diremos que uma cobertura é irredundante, quando nenhum dos subgrupos puder ser omitido.

Proposição 2.1 Um grupo G não admite cobertura irredundante por dois subgrupos.

Demonstração: Suponha que $G = H \cup K$ com $K < G$ e $H < G$. Veja que não podemos ter $H \leq K$ ou $K \leq H$, logo devem existir elementos $h \in H - K$ e $k \in K - H$. Encontramos uma contradição quando analisamos o elemento hk ,

pois, se $hk \in H \Rightarrow k \in H$ o que não pode, e se $hk \in K \Rightarrow h \in K$ o que também não pode, mas $hk \in G = H \cup K$, contradição. ■

Lema 2.1 Se $G = \bigcup_{i=1}^n X_i$ é uma cobertura irredundante por subgrupos, então para cada i , X_i contém $\bigcap_{j \neq i} X_j$

Demonstração: A mesma idéia da Proposição anterior. ■

Agora, veremos os grupos que são cobertos por três subgrupos, e daremos a caracterização destas coberturas.

2.1 Cobertura por Três Subgrupos

Teorema 2.2 (Haber-Rosenfeld) Um grupo G é a união de três subgrupos próprios se, e só se, o grupo de Klein for imagem homomórfica de G .

Demonstração: Obviamente o grupo de Klein $K = \{1, a, b, ab\}$ pode ser coberto por três subgrupos próprios, a saber: $\{1, a\}$, $\{1, b\}$, $\{1, ab\}$.

(\Leftarrow) Suponha que exista um homomorfismo sobrejetor $\phi : G \rightarrow K$. Temos então a seguinte cobertura irredundante de G por três subgrupos:

$$G = \phi^{-1}(\{1, a\}) \cup \phi^{-1}(\{1, b\}) \cup \phi^{-1}(\{1, ab\})$$

(\Rightarrow) Suponhamos que o grupo G admita uma cobertura por três subgrupos próprios $G = A \cup B \cup C$. Segue, da Proposição 2.1, que esta cobertura deve ser irredundante.

Definiremos $A_1 = A - (B \cup C)$, $B_1 = B - (A \cup C)$ e $C_1 = C - (A \cup B)$. Sabemos então que devem existir elementos $a \in A_1$, $b \in B_1$ e $c \in C_1$. Pelo Lema 2.1, temos que:

$$(B \cap C) \subset A \quad ; \quad (A \cap C) \subset B \quad ; \quad (A \cap B) \subset C.$$

Segue, portanto, que:

$$H = A \cap B \cap C = A \cap B = A \cap C = B \cap C.$$

Concluimos que:

$$G = A_1 \dot{\cup} B_1 \dot{\cup} C_1 \dot{\cup} H$$

Vamos continuar nossa demonstração através de pequenos fatos.

Fato 2.1 Se $x \in A_1$, então $x^{-1} \in A_1$.

Demonstração: $x \in A_1 \Rightarrow x \in A \Rightarrow x^{-1} \in A$. Note agora que caso $x^{-1} \in H$, deveríamos ter $x \in H$ (pois H é subgrupo), o que não ocorre. Segue então que $x^{-1} \notin H \Rightarrow x^{-1} \in A_1$. O resultado análogo vale para B_1 e C_1 .

Fato 2.2 Se $x \in A_1$ e $y \in B_1$, temos $xy \in C_1$

Demonstração: Observe que xy não pode estar em A , pois nesse caso $y \in A$. Analogamente, $xy \notin B$. A única opção, portanto, é $xy \in C_1$. Vale o resultado análogo se trocarmos a ordem de A_1, B_1, C_1 .

Fato 2.3 Se $x, y \in A_1$, então $xy \in H$.

Demonstração: Tome $b \in B_1$. Observe que $(xy) = (xb)(b^{-1}y)$. Pelos Fatos 2.1 e 2.2, $xb \in C_1$ e $b^{-1}y \in C_1$, logo $xy \in C$. Analogamente, $xy \in B$ e desde o princípio $xy \in A$. Portanto, $xy \in H$.

Fato 2.4 Se $x \in A_1$, $h \in H$, então $hx \in A_1$.

Demonstração: Observe que hx não pode estar em B , pois nesse caso $x \in B$, o que é absurdo. Analogamente, $hx \notin C$, donde concluímos que $hx \in A_1$.

Fato 2.5 H é subgrupo normal de G .

Demonstração: Tome elementos $h \in H$ e $x \in G$. Se $x \in H$ temos $h^x \in H$. Se $x \in A_1$, pelo Fato 2.1, $x^{-1} \in A_1$, pelo Fato 2.4, $hx \in A_1$. Finalmente, pelo Fato 2.3, $h^x = x^{-1}(hx) \in H$. E daí, $H \triangleleft G$.

Fato 2.6 A_1, B_1, C_1 são classes laterais de H .

Demonstração: Tome $a \in A_1$, provaremos que $A_1 = Ha$. Pelo Fato 2.4, $Ha \subset A_1$. Tome agora $x \in A_1$, veja que:

$$x = (xa^{-1})a.$$

Pelos Fatos 2.1 e 2.3, $xa^{-1} \in H$, donde segue que $A_1 = Ha$. De modo análogo $B_1 = Hb$ e $C_1 = Hc$.

Para concluirmos a demonstração do Teorema, observemos que no grupo $\frac{G}{H}$ temos, pelos Fatos 2.2 e 2.3.

$$(Ha) \cdot (Ha) = Ha^2 = H \quad ; \quad (Hb) \cdot (Hb) = H \quad ; \quad (Hc) \cdot (Hc) = H$$

$$(Ha) \cdot (Hb) = Hc \quad ; \quad (Hb) \cdot (Hc) = Ha \quad ; \quad (Hc) \cdot (Ha) = Hb$$

então, $\frac{G}{H}$ é o grupo de Klein.

Tome então $\phi : G \rightarrow \frac{G}{H}$ como sendo a projeção.

■

Corolário 2.1 Se G é um grupo coberto por três subgrupos, estes são normais em G .

2.2 O Teorema de Neumann

O Teorema que provaremos agora, é de grande utilidade no estudo da teoria das coberturas de grupos. Em 1954 Neumann provou o seguinte:

Teorema 2.3 (Neumann) *Suponhamos que o grupo G é coberto por n subgrupos $G = \bigcup_{i=1}^n H_i$. Suponha que para certo $i \in \{1, 2, \dots, n\}$ tenhamos $H_i \not\subseteq \bigcup_{j \neq i} H_j$, então $|G : H_i|$ é finito.*

Demonstração: Podemos supor, sem perda de generalidade, que $i = 1$, daí $H_1 \not\subseteq \bigcup_{i=2}^n H_i$. Suponhamos que $|G : H_1|$ seja infinito, daí consideremos $S = \{x_1, x_2, x_3, \dots\}$ o transversal de H_1 em G . Observemos que se $a < b$, $a, b \in \{1, 2, 3, \dots\}$ teremos que $x_a x_b^{-1} \notin H_1$, caso contrário, teríamos $x_a \in H_1 x_b$ e conseqüentemente $H_1 x_a = H_1 x_b$, o que não é verdade, visto que $S = \{x_1, x_2, x_3, \dots\}$ é um transversal de H_1 em G .

Podemos escrever $G = H_1 \cdot g^{-1}$, onde $g \in \bigcup_{j=2}^n H_j$, como $G = \bigcup_{i=1}^n H_i$, temos então que:

$$G = \left(\bigcup_{i=1}^n H_i \right) g^{-1} = H_1 \bigcup_{j=2}^n (H_j g^{-1}).$$

Assim, dados $a, b \in \mathbb{N}^*$, com $a < b$, existe $m(a, b)$ o menor inteiro, que depende de a e b , tal que $x_a x_b^{-1} \in H_m g^{-1}$, $m = m(a, b)$. Observe que, para todos $a, b \in \mathbb{N}^*$, $m(a, b) \in \{2, 3, \dots, n\}$.

Definamos $\Delta_m = \{(x_a, x_b); x_a x_b^{-1} \in H_m g^{-1}, m = m(a, b)\}$. Observe que podemos escrever $[S]^2 = \bigcup \Delta_m$, com $2 \leq m \leq n$. Usando o Teorema de Ramsey, existe $T \subset S$ infinito, $T = \{x_{a_1}, x_{a_2}, x_{a_3}, \dots\}$ tal que $[T]^2 \subset \Delta_k$ para algum $k \in \{2, 3, \dots, n\}$.

Sendo $a < b < c$ tais que: $x_a, x_b, x_c \in T$, deste modo:

$$x_a x_b^{-1} \in H_k g^{-1} \quad ; \quad x_a x_c^{-1} \in H_k g^{-1} \quad ; \quad x_b x_c^{-1} \in H_k g^{-1}$$

e assim, $g^{-1}x_b x_a^{-1}, g^{-1}x_c x_a^{-1}, g^{-1}x_c x_b^{-1} \in H_k$.

Afirmamos que $g^{-1} \in H_k$.

De fato, consideremos o produto, dos três elementos

$$\begin{aligned} (g^{-1}x_b x_a^{-1}) \cdot (g^{-1}x_c x_a^{-1})^{-1} \cdot (g^{-1}x_c x_b^{-1}) &= (g^{-1}x_b x_a^{-1}) \cdot (x_a x_c^{-1} g) \cdot (g^{-1}x_c x_b^{-1}) \\ &= (g^{-1}x_b x_a^{-1} x_a) \cdot (x_c^{-1} g g^{-1}) \cdot (x_c x_b^{-1}) \\ &= (g^{-1}x_b) \cdot (x_c^{-1} x_c x_b^{-1}) = g^{-1} \in H_k. \end{aligned}$$

Como H_k é subgrupo, teremos $g \in H_k$, o que não é verdade. Portanto, $|G : H_1|$ é finito. ■

Corolário 2.2 (Neumann) *Seja $G = \bigcup_{i=1}^n H_i$ uma cobertura por subgrupos. Podemos retirar desta cobertura os subgrupos H_i , tais que $|G : H_i|$ é infinito.*

Demonstração: Seja H_i um subgrupo, tal que $|G : H_i|$ seja infinito. Pelo Teorema de Neumann devemos ter $H_i \subset \bigcup_{j \neq i} H_j$, daí $G = \bigcup_{i=1}^n H_i = \bigcup_{j \neq i} H_j$. ■

2.3 Características dos Grupos que possuem Coberturas por Subgrupos Próprios

Proposição 2.2 *Um grupo G admite cobertura não trivial se, e somente se, G é não cíclico.*

Demonstração:

(\Leftarrow) Se G é não cíclico, então $G = \bigcup_{a \in G} \langle a \rangle$, com $\langle a \rangle < G$, e assim G admite cobertura não trivial por subgrupos.

(\Rightarrow) Se G é cíclico, digamos $G = \langle a \rangle$, então se um subgrupo de G , possui o elemento a , este será igual a G , logo G não possui cobertura não trivial. ■

Agora veremos uma condição necessária e suficiente, para que um grupo G admita cobertura finita por subgrupos próprios.

Teorema 2.4 *Seja G um grupo. G admite cobertura finita e não trivial por subgrupos se, e somente se, existe $N \triangleleft G$, com $\frac{G}{N}$ não cíclico e finito.*

Demonstração: Digamos que exista $N \triangleleft G$, tal que $\frac{G}{N}$ seja finito e não cíclico. Usando a Proposição anterior, temos que $\frac{G}{N}$ admite cobertura não trivial e finita, devido ao fato que $\frac{G}{N}$ é finito. Observemos que todo subgrupo de $\frac{G}{N}$ é da forma $\frac{H}{N}$, onde $N \triangleleft H$, $H < G$. Donde $\frac{G}{N} = \bigcup_{i=1}^n \left(\frac{H_i}{N} \right)$ e portanto, $G = \bigcup_{i=1}^n H_i$, isto é, G admite cobertura finita e não trivial.

Suponhamos agora que $G = \bigcup_{i=1}^n H_i$, $H_i < G$. Pelo Teorema de Neumann, podemos supor que $|G : H_i|$ é finito, para $i \in \{1, 2, 3, \dots, n\}$. Definamos $B = \bigcap_{i=1}^n H_i$ e usando Poincaré, temos que $|G : B|$ é finito. Definamos a seguinte ação:

$$\begin{aligned} \varphi : G &\rightarrow S_X = \{F : X \rightarrow X, F \text{ bijetiva}\} \\ g &\mapsto \varphi(g)(xH) = gxH \end{aligned}$$

onde $X = \{xB, x \in G\}$.

Sendo $N = \text{Nuc}\varphi$, sabemos que $N \triangleleft G$ e $N \leq B$. Usando o Teorema dos Isomorfismos, temos $\frac{G}{N} \approx S_X$, como S_X é finito, pois $|X| = |G : B|$, então $\frac{G}{N}$ é finito. Falta provarmos que $\frac{G}{N}$ é não cíclico. Como $N \leq B \leq H_i$, podemos escrever: $\frac{G}{N} = \bigcup_{i=1}^n \left(\frac{H_i}{N} \right)$, assim $\frac{G}{N}$ admite uma cobertura finita e não trivial e pela Proposição anterior $\frac{G}{N}$ é não cíclico. ■

2.4 Cobertura por Subgrupos Cíclicos

Começaremos nesta seção com uma aplicação do Teorema de Schur, que será muito importante para a caracterização dos grupos que admitem cobertura finita por subgrupos cíclicos.

Proposição 2.3 (Federov) *Se um grupo infinito G tem a propriedade de:*

$$1 \neq H \leq G \Rightarrow |G : H| < \infty$$

então $G = C_\infty$ (Cíclico de ordem infinita)

Demonstração: Tome $1 \neq x \in G$. Como $1 \neq \langle x \rangle \leq G$, temos por hipótese $|G : \langle x \rangle|$ é finito, digamos $|G : \langle x \rangle| = n$. Seja $T = \{t_1, t_2, \dots, t_n\}$ um transversal de $\langle x \rangle$ em G com $t_i \neq 1, \forall i$. Então, $G = \bigcup_{i=1}^n \langle x \rangle t_i = \langle x, t_1, t_2, \dots, t_n \rangle$. Como $\langle x \rangle \subset C_G(x)$ teremos $|G : C_G(x)| \leq |G : \langle x \rangle| = n$. Analogamente, para todo $t_i \in \{t_1, t_2, \dots, t_n\}$ temos $1 \neq \langle t_i \rangle \leq G$ e do mesmo modo, $\langle t_i \rangle \subset C_G(t_i)$ teremos $|G : C_G(t_i)| \leq |G : \langle t_i \rangle| < \infty, \forall i$.

Agora, sendo $Z(G) = \bigcap_{y \in \{x, t_i\}} C_G(y)$, usando Poincaré, teremos $|G : Z(G)| < \infty$. Usando o Teorema de Schur, temos que: G' é finito, e supondo $|G : Z(G)| = m$ teremos que $x^m = 1, \forall x \in G'$. Provaremos que $G' = 1$, de fato, se existisse $1 \neq g \in G'$, com $o(g) < \infty$, teríamos: $|G| = |G : \langle g \rangle| \cdot |\langle g \rangle| < \infty$, o que não é verdade, logo $G' = 1$, e assim G é abeliano.

Então, pelo Teorema Fundamental dos Grupos Abelianos Finitamente Gerados:

$$G = C_\infty \times C_\infty \times \dots \times C_\infty.$$

Se houvesse mais de uma cópia, a primeira seria um subgrupo de índice infinito, o que não pode ocorrer. Logo:

$$G = C_\infty.$$



Teorema 2.5 *Um grupo G admite cobertura finita por subgrupos cíclicos se, e somente se, G é finito ou $G = C_\infty$.*

Demonstração:

(\Rightarrow) Suponhamos que:

$$G = \langle x_1 \rangle \cup \langle x_2 \rangle \cup \dots \cup \langle x_n \rangle$$

seja uma cobertura irredundante de G por subgrupos cíclicos. Pelo Teorema de Neumann, $|G : \langle x_i \rangle|$ é finito para $i \in \{1, 2, 3, \dots, n\}$. Seja $1 \neq H \leq G$, tomemos um elemento $1 \neq g \in H$. Daí $g \in \langle x_i \rangle$ para algum i , isso implica que:

$$|\langle x_i \rangle : \langle g \rangle| \text{ é finito.}$$

E portanto:

$$|G : H| \leq |G : \langle g \rangle| = |G : \langle x_i \rangle| \cdot |\langle x_i \rangle : \langle g \rangle| < \infty.$$

Aplicando o resultado de Federov concluímos que o G é finito, ou $G = C_\infty$.

(\Leftarrow) Se G é finito, digamos $G = \{x_1, x_2, \dots, x_n\}$, então:

$$G \subseteq \bigcup_{i=1}^n \langle x_i \rangle \subseteq G.$$

Caso $G = C_\infty$, o grupo é a própria cobertura.



Capítulo 3

Coberturas p -Sylow

Neste capítulo, estudaremos coberturas nas quais existe algum subgrupo de Sylow. Daremos a caracterização de tais coberturas e estudaremos as coberturas p -Sylow do grupo S_n .

Definição 3.1 *Seja G um grupo finito e p um número primo. Uma p -Sylow cobertura de G , é uma cobertura irredudante de G , que contém de algum p -Sylow subgrupo.*

Exemplo 3.1 *No Grupo Simétrico S_3 , a família $\{A_3, \langle(1, 2)\rangle, \langle(1, 3)\rangle, \langle(2, 3)\rangle\}$ é cobertura de S_3 que possui subgrupos de Sylow. O grupo $G = S_3 \times \mathbb{Z}_2$ não possui 3-Sylow cobertura, mas possui uma 2-Sylow cobertura, como veremos mais adiante.*

Definição 3.2 *Seja G um grupo finito e p um número primo, um p -elemento de G , é um elemento que possui a ordem uma potência de p . Um p -elemento de G é chamado um C_{pp} -elemento se o seu centralizador em G é um p -subgrupo, isto é, um subgrupo cuja ordem é um potência de p .*

3.1 Coberturas Contendo Subgrupos de Sylow

Nesta seção damos uma caracterização para coberturas p -Sylow onde p é um primo que divide a ordem do grupo G .

Teorema 3.1 *Seja G um grupo finito não cíclico e p um primo, tal que p divide $|G|$. G possui uma p -Sylow cobertura se, e somente se, existe um C_{pp} elemento em G .*

Demonstração: Suponhamos primeiramente que G possui uma p -Sylow cobertura, isto é, existe um P subgrupo de Sylow que faz parte da cobertura irredundante de G . Se para cada $a \in P$, a não é um C_{pp} elemento, então existe $x_a \in C_G(a) = \{g \in G; ag = ga\}$, tal que $o(x_a) = q$, q primo diferente de p , pois se a não é um C_{pp} elemento, então $|C_G(a)|$ não é uma potência de p , por Cauchy, existe $x_a \in C_G(a)$, com ordem q , q primo diferente de p . Veja que $a \cdot x_a$ pertence a algum componente da cobertura irredundante p -Sylow de G . Afirmamos que $a \cdot x_a \notin P$, de fato: Se $a \cdot x_a \in P$, teríamos $(a \cdot x_a)^{p^n} = 1$, para algum natural n , visto que P é um p -Sylow subgrupo. Como $x_a \in C_G(a)$, temos que:

$$(a \cdot x_a)^{p^n} = 1 \Rightarrow a^{p^n} \cdot (x_a)^{p^n} = 1 \Rightarrow (x_a)^{p^n} = 1,$$

Como a ordem de x_a é q , teremos que q divide p^n o que não é verdade. Logo $a \cdot x_a \notin P$.

Como $a \cdot x_a \in G$, e como G é coberto por uma cobertura irredundante, então $a \cdot x_a \in H$, para algum elemento da cobertura. Sabemos que $\text{mdc}(q, p^n) = 1$, por Bezout, existem inteiros k e l tais que:

$$k \cdot q + l \cdot p^n = 1.$$

Como $a \cdot x_a \in H$, então $(a \cdot x_a)^q \in H$ mas, $(a \cdot x_a)^q = a^q \cdot x_a^q = a^q \in H$, observe que:

$$a^1 = a^{kq} \cdot a^{l \cdot p^n} = (a^q)^k \cdot (a^{p^n})^l = (a^q)^k \in H.$$

Deste modo, cada elemento $a \in P$, estaria em outra componente da cobertura irredundante, o que é um absurdo. Assim, deve existir $a \in P$ tal que a é um C_{pp} elemento, o que prova a primeira parte.

Agora suponhamos que exista $a \in G$, tal que a é um C_{pp} elemento. Suponhamos por contradição que G não possui p -Sylow cobertura. Seja A_1 um p -subgrupo de Sylow de G que contém o elemento a . Agora construiremos uma cobertura de G do seguinte modo: Primeiro consideremos $\mathcal{A} = \{A_1\}$ e vamos adicionar a \mathcal{A} outros p -subgrupos de Sylow um a um até eles cobrirem todos os p -elementos de G . Agora para todos os outros primos $q \neq p$ que dividem a ordem de G , façamos o mesmo procedimento. Desse modo obtemos $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ que é uma cobertura irredundante para os elementos de G cuja ordem é uma potência de um primo. Definamos o seguinte conjunto $\mathcal{B} = \{\langle g \rangle, g \in G - \bigcup_{i=1}^n A_i\}$. Ordenemos \mathcal{B} pela inclusão, para cada cadeia de \mathcal{B} escolhamos o elemento maximal e adicionamos esses elementos maximais a $\mathcal{A} = \{A_1, A_2, \dots, A_n, B_1, B_2, \dots, B_m\}$. Agora \mathcal{A} é uma cobertura para G . Ou seja $G = \left(\bigcup_{i=1}^n A_i\right) \cup \left(\bigcup_{i=1}^m B_i\right)$. Como estamos supondo que G não tem p -Sylow cobertura, todos os subgrupos A_1, A_2, \dots, A_n podem ser omitidos. Em particular $A_1 \subset \bigcup_{i=1}^m B_i$. Como $a \in A_1$, existe $j \in \{1, 2, \dots, m\}$ tal que $a \in B_j = \langle g \rangle$, para algum $g \in G - \bigcup_{i=1}^n A_i$. Assim $a = g^\alpha$, para algum $\alpha \in \mathbb{Z} - \{0\}$. Deste modo $B_j \subset C_G(a)$, donde teremos $|B_j| = p^\alpha$ para algum k natural não nulo o que não é verdade. ■

3.2 O Grupo Simétrico

Nesta seção estudaremos as coberturas p -Sylow nos grupos simétricos, e determinemos quais grupos simétricos possuem p -Sylow cobertura para cada primo p , p dividindo a ordem do grupo.

Lema 3.2 *Se α é uma permutação de S_n , de modo que α é decomposta em exatamente a_i i -ciclos, $a_i \geq 0$, temos:*

$$|C_{S_n}(\alpha)| = \prod (a_i!) i^{a_i},$$

onde $n = a_1 + 2a_2 + 3a_3 + \dots + na_n$.

Demonstração: Veja o Apêndice C. ■

Corolário 3.1 *Para cada $n \geq 3$, o grupo simétrico S_n possui um C_{2^k} elemento. Em particular, $\alpha \in S_n$ é um C_{2^k} elemento, se e somente se, α é um produto de 2^k -ciclos com $k \in \mathbb{N}$.*

Demonstração: Podemos provar facilmente que todo natural n pode ser escrito da forma:

$$n = 2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_k},$$

com $\alpha_1, \alpha_2, \dots, \alpha_k$ distintos dois a dois.

Tomemos $\alpha \in S_n$, com a seguinte estrutura cíclica

$$\alpha = \underbrace{(\dots\dots)}_{2^{\alpha_1}} \underbrace{(\dots\dots)}_{2^{\alpha_2}} \dots \underbrace{(\dots\dots)}_{2^{\alpha_k}}$$

Escrevendo, $n = a_1 + 2a_2 + 3a_3 + 4a_4 + \dots + na_n$, veja que $o(\alpha) = 2^{\alpha_1}$. Só falta provar que $|C_{S_n}(\alpha)|$ é uma potência de 2. Observe que $a_i = 0$ ou 1,

$a_i = 1 \Leftrightarrow i$ é potência de 2 e usando o Lema acima, $|C_{S_n}(\alpha)| = \prod (a_i!)^{a_i}$ vemos que $|C_{S_n}(\alpha)|$ é uma potência de 2, logo α é um C_{22} -elemento.

Em particular, se α é um C_{22} elemento, então temos que: $o(\alpha)$ é uma potência de 2 e $|C_{S_n}(\alpha)| = \prod (a_i!)^{a_i}$ é um potência de 2 onde $n = a_1 + 2a_2 + 3a_3 + \dots + na_n$.

Sendo $|C_{S_n}(\alpha)|$ uma potência de 2, devemos ter que todos os a_i , $a_i \leq 2$ e os i devem ser potências de 2, $a_i = 0$, para i não potência de 2, o que prova o resultado. ■

Corolário 3.2 *Para cada $n \geq 3$, o grupo simétrico S_n possui uma 2-SyLOW cobertura.*

Teorema 3.3 *Seja G o grupo simétrico S_n para $n \geq 3$ e seja $p \leq n$ um primo ímpar. G possui um C_{pp} elemento se, e somente se, 0 e 1 são os únicos dígitos que aparecem na representação de n na base p .*

Demonstração: Suponhamos que G possui um C_{pp} elemento, digamos $\alpha \in S_n$ é C_{pp} isto é, $o(\alpha) = p^\lambda$ e $|C_{S_n}(\alpha)| = \prod (a_i!)^{a_i}$, onde $n = a_1 + 2a_2 + 3a_3 + \dots + na_n$.

Para que $|C_{S_n}(\alpha)|$ seja potência de p , primo ímpar, $a_i = 0$ ou 1 e i deve ser potência de p . Então escrevemos n da forma

$$n = a_1 + p^{\alpha_1} + p^{\alpha_2} + \dots + p^{\alpha_k}$$

ou seja, 0 e 1 são os únicos dígitos que aparecem na representação de n na base p .

Suponhamos agora, que 0 e 1 são os únicos dígitos na representação de n na base p . Isto é,

$$n = p^{\alpha_k} + p^{\alpha_{k-1}} + \dots + p^{\alpha_2} + p^{\alpha_1} + r$$

onde $r = 0$ ou 1.

Tomemos $\alpha \in S_n$, com a seguinte estrutura cíclica

$$\alpha = \underbrace{(\dots\dots)}_{p^{\alpha_k}} \underbrace{(\dots\dots)}_{p^{\alpha_{k-1}}} \dots \underbrace{(\dots\dots)}_{p^{\alpha_1}} \underbrace{(\dots\dots)}_{p^{\alpha_0}}.$$

Observe que $o(\alpha) = p^{\alpha_k}$, α_k é o máximo dos α_i . Escrevendo

$$n = a_1 + 2a_2 + 3a_3 + \dots + na_n,$$

teremos que $a_i = 0$ ou 1, e $a_i = 0$, se i não é potência de p .

Daí, $|C_{S_n}(\alpha)| = \prod (a_i!)^{a_i}$ será potência de p .

Assim, G tem um C_{pp} elemento. ■

Corolário 3.3 *Seja G o grupo simétrico S_n , $n \geq 3$ e p um primo ímpar que divide $|G|$. G possui uma p -Sylow cobertura se, e somente se, 0 e 1 são os únicos dígitos que aparecem na representação de n na base p .*

Lema 3.4 *Para cada número inteiro $n \geq 7$, existe um número primo $p \geq 3$, tal que: $p + 4 \leq n < 3p$.*

Demonstração: Provaremos por indução sobre n e usaremos o Teorema de Bertrand, que provaremos no Apêndice B.

Para $n = 7$, basta tomarmos $p = 3$. Suponhamos que para $n > 7$ exista um primo p , tal que: $p + 4 \leq n < 3p$. Agora, provaremos que para $n + 1$ existe um primo q , tal que: $q + 4 \leq n + 1 < 3q$. Para isto, consideremos dois casos:

1º Caso) $n + 1 < 3p$, daí temos a seguinte situação:

$$p + 4 \leq n < n + 1 < 3p,$$

então, basta tomar $p = q$.

2º Caso) $n + 1 = 3p$, pelo Teorema de Bertrand, existe um primo q_1 , tal que: $p < q_1 < 2p$, daí temos a seguinte situação:

$$q_1 + 4 \leq 2p + 3 \leq 3p = n + 1 < 3q_1,$$

então, basta tomar o primo $q = q_1$, o que conclui a demonstração. ■

Teorema 3.5 *Os grupos S_3 e S_4 são os únicos grupos simétricos que possuem p -Sylow cobertura para cada primo $p \leq n$.*

Demonstração: É fácil ver que S_3 e S_4 possuem 2-Sylow cobertura e 3-Sylow cobertura. Veremos agora que S_5, S_6, S_7 e S_8 não possuem 3-Sylow cobertura, basta notar que:

$$5 = (12)_3, \quad 6 = (20)_3, \quad 7 = (21)_3, \quad 8 = (22)_3 \quad \text{e} \quad 9 = (22)_3.$$

Suponhamos $n > 9$. Pelo Lema 3.4 existe p primo, $p > 3$, tal que:

$$p < p + 4 \leq n < 3p < p^2.$$

Assim, quando formos escrever n na base p , os dígitos não podem ser somente 0 e 1. De fato, como $n < p^2$, $(n)_p$ não pode ter mais que dois algarismos, e os possíveis números serão $(11)_p = p + 1$ ou $(10)_p = p$ e como $n \geq p + 4$, S_n não possui p -Sylow cobertura. ■

Capítulo 4

Cobertura por Subgrupos Abelianos

Aqui veremos o grupo G sendo coberto por n grupos abelianos A_i :

$$G = A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n.$$

Vamos também investigar o problema do número máximo de elementos dois a dois não-comutantes que um grupo G pode ter, e mostrar como este se relaciona aos problemas de cobertura.

4.1 Caracterização das Coberturas por Abelianos

Teorema 4.1 *Seja G um grupo, são equivalentes:*

(i) $|G : Z(G)|$ é finito.

(ii) $G = \bigcup_{i=1}^n A_i$, A_i abelianos, $A_i \leq G$.

(iii) G tem somente um número finito de subgrupos abelianos maximais.

(iv) Todo abeliano maximal tem índice finito.

(v) Para todo subconjunto $S \subseteq G$, tal que: $xy \neq yx$, para todos $x, y \in S$, temos que S é finito.

Demonstração:

(i) \Rightarrow (ii) Digamos que $|G : Z(G)|$ seja finito. Consideremos o transversal $T = \{x_1, x_2, \dots, x_n\}$ de $Z(G)$ em G . Podemos escrever:

$$G = \bigcup_{i=1}^n x_i Z(G) \subseteq \bigcup_{i=1}^n \langle x_i \rangle Z(G) = \bigcup_{i=1}^n A_i \subseteq G$$

onde $A_i = \langle x_i \rangle Z(G)$, observe que para cada i , A_i é abeliano e subgrupo de G . Logo $G = \bigcup_{i=1}^n A_i$, A_i abeliano, $A_i \leq G$.

(ii) \Rightarrow (i) Agora digamos que $G = \bigcup_{i=1}^n A_i$, com A_i abeliano e $A_i < G$. Podemos assumir que esta cobertura é irredundante, e por Neumann $|G : A_i| < \infty$.

Definamos $N = \bigcap A_i$, usando Poincaré, temos que $|G : N|$ é finito.

Afirmamos que $N \subseteq Z(G)$. De fato, tome $x \in N$ e $g \in G = \bigcup_{i=1}^n A_i$ então $g \in A_i$ para algum i . Como $N = \bigcap A_i$, temos que $x, g \in A_i$ para o mesmo i , logo, $xg = gx$ e assim $x \in Z(G)$, o que prova $N \subseteq Z(G)$.

Portanto, $|G : Z(G)|$ é finito.

Agora, provaremos a implicação (i) \Rightarrow (iv). Antes, provaremos que todo $x \in G$ está contido em algum subgrupo abeliano maximal de G . Então, para cada $x \in G$ definamos:

$$S = \{A < G, A \text{ é abeliano com } x \in A\}.$$

Veja que $\langle x \rangle \in S$. Assim, S é não vazio. Seja $T \subset S$, T totalmente ordenado. Consideremos $A_0 = \bigcup_{A \in T} A$, é fácil perceber que A_0 é subgrupo abeliano de G , com $x \in A_0$ e para todo $B \in T$, temos que $B < A_0$, assim A_0 é majorante de T . Usando o Lema de Zorn, existe um elemento maximal em S , ou seja, para cada $x \in G$, existe A abeliano maximal com $x \in A$.

Agora, provaremos $(i) \Rightarrow (iv)$. Seja M abeliano maximal, então $Z(G)M$ é subgrupo, visto que $Z(G) \triangleleft G$ e assim $Z(G)M$ é abeliano. Observe que $M \leq Z(G)M$, como M é abeliano maximal, temos que $Z(G)M = M$, o que implica $Z(G) \leq M$. Como $|G : Z(G)|$ é finito, então $|G : M|$ também o é.

$(i) \Rightarrow (iii)$ Seja M abeliano maximal, vimos anteriormente que $Z(G)M$ é abeliano e $Z(G) \leq M = Z(G)M$, daí $Z(G) \triangleleft M$. Então $\frac{M}{Z(G)} \leq \frac{G}{Z(G)}$, como $\frac{G}{Z(G)}$ é finito, segue que só podemos ter uma quantidade finita de subgrupos abelianos maximais M .

$(iii) \Rightarrow (ii)$ Sejam M_1, M_2, \dots, M_n todos os abelianos maximais de G . Para cada $x \in G$, existe $i \in \{1, 2, \dots, n\}$ tal que $x \in M_i$, daí $G \subseteq \bigcup_{i=1}^n M_i \subseteq G$, portanto

$$G = \bigcup_{i=1}^n M_i, M_i \text{ abeliano.}$$

$(iv) \Rightarrow (i)$ Sabemos que para cada $x \in G$, existe M abeliano maximal com $x \in M$, assim $M \subseteq C_G(x)$, como $|G : M|$ é finito, temos que $|G : C_G(x)|$ é finito para cada $x \in G$. Tomemos M abeliano maximal, como $|G : M|$ é finito, consideremos $T = \{t_1, t_2, \dots, t_n\}$ o transversal de M em G , daí $G = \bigcup_{i=1}^m Mt_i$. Podemos dizer que $G = \langle M, t_1, t_2, \dots, t_n \rangle$. Podemos facilmente concluir que

$$Z(G) = C_G(M) \cap C_G(t_1) \cap \dots \cap C_G(t_n),$$

usando Poincaré, temos:

$$|G : Z(G)| \leq |G : C_G(M)| \cdot |G : C_G(t_1)| \cdot \dots \cdot |G : C_G(t_n)|,$$

como todos são finitos, temos que $|G : Z(G)|$ é finito.

Observação: Como M é abeliano, $M \subset C_G(M)$, e assim $|G : C_G(M)|$ é finito.

$(i) \Rightarrow (iv)$ Digamos que $|G : Z(G)| = n$, consideremos $T = \{t_1, t_2, \dots, t_n\}$ um transversal de $Z(G)$ em G , então podemos escrever $G = \bigcup_{i=1}^n t_i Z(G)$. Agora,

usaremos um princípio de contagem, conhecido como Princípio das Gavetas. Qualquer conjunto com mais de n elementos em G , deve ter dois elementos na mesma componente na cobertura, isto é, existe $i \in \{1, 2, \dots, n\}$ tal que:

$$a, b \in t_i Z(G).$$

Deste modo, existem $g_1, g_2 \in Z(G)$, com $a = t_i g_1, b = t_i g_2$, veja que:

$$b^{-1} = g_2^{-1} \cdot t_i^{-1} \quad \text{e} \quad b^{-1}a = g_2^{-1} \cdot t_i^{-1} \cdot t_i \cdot g_1 = g_2^{-1} \cdot g_1 \in Z(G)$$

e portanto $[a, b] = 1$. Deste modo, se $S \subset G$, tal que $xy \neq yx$, para todos $x, y \in S$, S deve ter menos que $n + 1$ elementos, ou seja, S é finito.

Para demonstrarmos a implicação $(v) \Rightarrow (i)$ usaremos vários Lemas e resultados como o Teorema de Ramsey.

Em 1975, o famoso matemático Paul Erdős, em um encontro da Australian Mathematical Society, propôs a implicação $(v) \Rightarrow (i)$. No mesmo ano, B. H. Neumann resolveu o problema. Vamos aqui reconstruir sua demonstração.

Lema 4.2 *Seja G um grupo. Suponha que para todo $S \subset G$, tal que $xy \neq yx$ para todos $x, y \in S$, tenhamos que S é finito. Então, para todo $x \in G$, x^G é finito.*

Demonstração: Suponhamos que exista $g \in G$, tal que g^G seja infinito, isto é, g possui infinitos conjugados. Consideremos $T \subset G$ um conjunto infinito, tal que:

$$\text{Se } x, y \in T, x \neq y \Rightarrow g^x \neq g^y.$$

Agora usaremos Ramsey, para isto, consideremos $[T]^2 = \{(x, y); x, y \in T\}$. Podemos escrever $[T]^2$ da seguinte maneira:

$$[T]^2 = \{(x, y); xy = yx; x, y \in T\} \cup \{(x, y); xy \neq yx; x, y \in T\}.$$

Por Ramsey, existe $L \subset T$ infinito, tal que:

1º) $[L]^2 \subset \{(x, y); xy \neq yx; x, y \in T\}$, neste caso, existiria $L \subset S$ infinito, tal que $xy \neq yx$, para todos $x, y \in L$, o que contraria a hipótese.

ou

2º) $[L]^2 \subset \{(x, y); xy = yx; x, y \in T\}$. Assim, existe $L \subset G$ infinito, tal que: se $x, y \in L, xy = yx$. Definamos o conjunto $gL = \{gx, x \in L\}$. Tomando $x, y \in L, x \neq y$, é fácil notar que $[gx, gy] \neq 1$. Como $gL \subset G$ e para todos $a, b \in gL, a \neq b, ab \neq ba$, temos novamente uma contradição.

Assim, para todo $x \in G, x^G$ deve ser finito.

■

Lema 4.3 *Seja G um grupo, tal que para todo $x \in G, x^G$ é finito, e A um subgrupo abeliano de G com $|G : A|$ finito. Então, $|G : Z(G)|$ é finito.*

Demonstração: Consideremos $T = \{t_1, t_2, \dots, t_n\}$ um transversal de A em G , assim podemos escrever, $G = \bigcup_{i=1}^n t_i A$.

Afirmção 4.1 $Z(G) = C_G(A) \cap C_G(T)$

Sabemos que $C_G(A) = \{g \in G; gx = xg, \forall x \in A\} = \bigcap_{x \in A} C_G(x)$ e

$$C_G(T) = \{g \in G; gt = tg, \forall t \in T\} = \bigcap_{t \in T} C_G(t).$$

Que $Z(G) \subset C_G(A) \cap C_G(T)$ é de fácil verificação, provemos a outra inclusão.

Tomemos $x \in C_G(A) \cap C_G(T)$, então por definição, x comuta com todo elemento de A e com todo elemento de T . Seja y qualquer, $y \in G$ então $y = t_i \cdot a, t_i \in \{t_1, t_2, \dots, t_n\}$ e $a \in A$. Veja que:

$$xy = x(t_i a) = (xt_i)a = (t_i x)a = t_i(xa) = t_i(ax) = (t_i a)x = yx.$$

O que prova $Z(G) = C_G(A) \cap C_G(T)$.

Sabemos do Capítulo 1, que $|G : C_G(x)| = |x^G|$. Agora, como T é finito, então:

$$|G : T| = |G : \bigcap_{t \in T} C_G(t)| \leq |G : C_G(t_1)| \cdot |G : C_G(t_2)| \cdot \dots \cdot |G : C_G(t_n)|.$$

Assim, $|G : T|$ é finito. Sendo A abeliano, temos:

$$A \leq C_G(A) \Rightarrow |G : C_G(A)| \leq |G : A|$$

que é finito.

Como $Z(G) = C_G(A) \cap C_G(T)$, então:

$$|G : Z(G)| \leq |G : C_G(A)| \cdot |G : C_G(T)|$$

e portanto, $|G : Z(G)|$ é finito. ■

Corolário 4.1 *Se G é um grupo, tal que para todo $x \in G$, x^G é finito, $|G : Z(G)|$ é infinito e possui um subgrupo H , com $|G : H|$ finito, então H não é abeliano.*

Lema 4.4 *Seja G um grupo, tal que para todo $x \in G$, x^G é finito, $|G : Z(G)|$ é infinito. Assuma que G contém duas sequências finitas de n elementos*

$$(a_1, a_2, \dots, a_n) \quad e \quad (b_1, b_2, \dots, b_n)$$

satisfazendo:

- i) Se $i \neq j$, $[a_i, a_j] = 1$.
- ii) Para todo i , $[a_i, b_i] \neq 1$,
- iii) Se $i \neq j$, $[a_i, b_j] = 1$.
- iv) Para todo i, j , $[b_i, b_j] = 1$

Então, G conterá outros dois elementos a_{n+1} e b_{n+1} tais que (i), (ii), (iii), (iv) continuarão valendo para as sequências:

$$(a_1, a_2, \dots, a_n, a_{n+1}) \quad \text{e} \quad (b_1, b_2, \dots, b_n, b_{n+1})$$

de tamanho $n + 1$.

Demonstração: Definamos

$$A = C_G(\{a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n\}) = \left(\bigcap_{i=1}^n C_G(a_i) \right) \cap \left(\bigcap_{i=1}^n C_G(b_i) \right)$$

Usando o Corolário acima, como A tem índice finito, então A não é abeliano. Assim, podemos escolher dois elementos a e b pertencentes a A que não comutam.

Definimos:

$$a_{n+1} = ab_1b_2 \dots b_n \quad \text{e} \quad b_{n+1} = b$$

teremos, então, para $1 \leq i \leq n$;

$$(i')[a_i, a_{n+1}] = [a_i, b_i] \neq 1$$

Provaremos o caso quando $i = 1$, os outros são análogos, visto que a e todos os b_j , à exceção de b_i , comutam com a_i . Vejamos para $i = 1$.

$$\begin{aligned} [a_1, ab_1b_2 \dots b_n] &= a_1^{-1} \cdot b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_1^{-1} \cdot a^{-1} \cdot a_1ab_1b_2 \dots b_n \\ &= a_1^{-1} \cdot b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_1^{-1} \cdot a^{-1} \cdot aa_1b_1b_2 \dots b_n \\ &= a_1^{-1} \cdot b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_1^{-1} \cdot b_2^{-1}b_2a_1b_1 \dots b_n \\ &\quad \vdots \\ &= a_1^{-1} \cdot b_1^{-1}a_1b_1 = [a_1, b_1] \neq 1. \end{aligned}$$

$$(ii')[a_{n+1}, b_i] = [a_i, b_{n+1}] = 1$$

Provaremos o caso quando $i = 1$, os outros são análogos, visto que a e todos b_j comutam com b_i e a_i comuta com b .

$$\begin{aligned}
[ab_1b_2 \dots b_n, b_1] &= (ab_1b_2 \dots b_n)^{-1} \cdot b_1^{-1} \cdot (ab_1b_2 \dots b_n) \cdot b_1 \\
&= b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_2^{-1} \cdot b_1^{-1} \cdot a^{-1} \cdot b_1^{-1} \cdot a \cdot b_1b_2 \dots b_n \cdot b_1 \\
&= b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_2^{-1} \cdot b_1^{-1} \cdot b_1^{-1} \cdot a^{-1} \cdot a \cdot b_1b_2 \dots b_n \cdot b_1 \\
&= b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_2^{-1} \cdot b_1^{-1} \cdot b_1^{-1} \cdot b_1b_2 \dots b_n \cdot b_1 \\
&= b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_2^{-1} \cdot b_1^{-1} \cdot b_2 \dots b_n \cdot b_1 \\
&\quad \vdots \\
&= b_1^{-1} \cdot b_1 = 1.
\end{aligned}$$

$$(iii')[a_{n+1}, b_{n+1}] = [a, b] \neq 1.$$

De fato, como todos os b_j comutam com b , mas a e b não comutam.

$$\begin{aligned}
[ab_1b_2 \dots b_n, b] &= b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_1^{-1} \cdot a^{-1} \cdot b_1^{-1} \cdot a \cdot b_1b_2 \dots b_n \cdot b \\
&= b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_1^{-1} \cdot b_1 \cdot a^{-1} \cdot b^{-1} \cdot a \cdot bb_2 \dots b_n \\
&= b_n^{-1} \cdot b_{n-1}^{-1} \cdot \dots \cdot b_2^{-1} \cdot a^{-1} \cdot b^{-1} \cdot abb_2b_3 \dots b_n \\
&\quad \vdots \\
&= a_1^{-1} \cdot b_1^{-1} \cdot a \cdot b \neq 1.
\end{aligned}$$

$$(iv')[b_i, b_{n+1}] = 1.$$

Pois $b_{n+1} = b$, e b comuta com todo b_i .

Note que as condições acima garantem automaticamente que $a_{n+1} \neq a_1, a_2, \dots, a_n$ e que $b_{n+1} \neq b_1, b_2, \dots, b_n$. O Lema fica então provado. ■

Agora, provaremos a implicação $(v) \Rightarrow (i)$.

Suponhamos para todo subconjunto $S \subset G$, tal que: $xy \neq yx$ para todos $x, y \in S$, temos que S é finito. Pelo Lema 4.2, temos que para todo $x \in G$, x^G é

finito. Digamos que $|G : Z(G)|$ não é finito, daí G não é abeliano. Tomemos a_1 e b_1 elementos de G que não comutam, e usando o Lema 4.4, contruímos recursivamente uma sequência infinita (a_1, a_2, \dots, a_n) de elementos que não comutam dois a dois. O que contraria a hipótese.

Portanto, $|G : Z(G)|$ é finito.



Capítulo 5

Cobertura por Subgrupos Normais

Aqui, veremos o grupo G sendo coberto por n subgrupos normais A_i :

$$G = A_1 \cup A_2 \cup \dots \cup A_n.$$

Vamos também estudar coberturas por subgrupos verbais. Daremos a caracterização dos grupos que podem ser cobertos por subgrupos normais.

5.1 Caracterização dos Grupos que são cobertos por Subgrupos Normais

Para os resultados que vamos demonstrar sobre coberturas por subgrupos normais, vamos precisar de alguns resultados preliminares, que vamos demonstrar a partir de agora.

Lema 5.1 *Seja G nilpotente. Então, existe $N \triangleleft G$, com $\frac{G}{N}$ não cíclico e finito se e somente se, existe $H \triangleleft G$, tal que $\frac{\frac{G}{H}}{\frac{G'}{H}}$ é finito e não cíclico.*

Demonstração: Se existe $H \triangleleft G$, tal que $\frac{G}{\frac{G'}{H}}$, seja finito e não cíclico basta tomar $N = H$, pois usando o Teorema dos Isomorfismos temos que:

$$\frac{\frac{G}{\frac{G'}{H}}}{\frac{G'}{G}} \simeq \frac{G}{H}.$$

Agora, suponhamos a existência de $N \triangleleft G$, tal que $\frac{G}{N}$ seja não cíclico e finito. Como G é nilpotente, temos que $\frac{G}{N}$ também o é. Agora, usaremos resultados sobre grupos nilpotentes. Sendo $\frac{G}{N}$ nilpotente, existe $n \in \mathbb{N}$ tal que $Z_n\left(\frac{G}{N}\right) = \frac{G}{N}$, ou seja, temos a série central

$$1 = Z_0 \subset Z_1\left(\frac{G}{N}\right) \subset Z_2\left(\frac{G}{N}\right) \subset \dots \subset Z_n\left(\frac{G}{N}\right) = \frac{G}{N}$$

onde

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

Também, temos pela construção da série que $Z_i\left(\frac{G}{N}\right) \triangleleft \frac{G}{N}$.

Pelo Teorema da Correspondência, podemos definir $\frac{\bar{Z}_i}{N} = Z_i\left(\frac{G}{N}\right)$ para $i \in \{1, 2, \dots, n\}$ com $\bar{Z}_i \triangleleft G$, $N \triangleleft \bar{Z}_i$.

Agora, usando os fatos acima, teremos:

$$\frac{Z_n\left(\frac{G}{N}\right)}{Z_{n-1}\left(\frac{G}{N}\right)} = Z\left(\frac{\frac{G}{N}}{Z_{n-1}\left(\frac{G}{N}\right)}\right) = \frac{\frac{G}{N}}{Z_{n-1}\left(\frac{G}{N}\right)} = \frac{\frac{G}{N}}{\frac{\bar{Z}_{n-1}}{N}} \simeq \frac{G}{\bar{Z}_{n-1}},$$

que é abeliano.

Que $\frac{G}{\overline{Z}_{n-1}}$ é finito, não há nada o que fazer, pois $\frac{G}{N}$ é finito. Mostraremos agora que $\frac{G}{\overline{Z}_{n-1}}$ é não cíclico.

Suponhamos por contradição que $\frac{G}{\overline{Z}_{n-1}}$ seja cíclico. Observemos que:

$$\frac{\frac{G}{N}}{\frac{\overline{Z}_{n-2}}{N}} = \frac{\frac{G}{N}}{\frac{\overline{Z}_{n-2}}{N}} = \frac{G}{\overline{Z}_{n-1}} \approx \frac{G}{\overline{Z}_{n-1}}$$

Mas daí, teremos que:

$$\frac{\frac{G}{N}}{\frac{\overline{Z}_{n-2}}{N}} = Z \left(\frac{\frac{G}{N}}{Z_{n-2} \left(\frac{G}{N} \right)} \right) = \frac{\overline{Z}_{n-1}}{N},$$

donde teremos:

$$\frac{G}{N} = \frac{\overline{Z}_{n-1}}{N} = Z_{n-1} \left(\frac{G}{N} \right)$$

o que não é verdade.

Portanto, $\frac{G}{\overline{Z}_{n-1}}$ é finito, abeliano e não cíclico. Assim, $G' \subset \overline{Z}_{n-1}$ e teremos:

$$\frac{\frac{G}{G'}}{\frac{\overline{Z}_{n-1}}{G'}} \approx \frac{G}{\overline{Z}_{n-1}}$$

não é cíclico e finito.

Basta tomar $H = \overline{Z}_{n-1}$.

■

Lema 5.2 *Seja $G = H \times M$ um grupo, onde H é um grupo não abeliano simples. Então, dado $N \triangleleft G$, temos $N = H \times S$ ou $N = 1 \times S$ com $S \triangleleft M$.*

Demonstração: Podemos escrever:

$$G = \{(a, b); a \in H, b \in M\}$$

identificamos

$$H = H \times 1 = \{(a, 1); a \in H\} \quad \text{e} \quad M = 1 \times M = \{(1, b); b \in M\}.$$

Deste modo, é fácil perceber que $H, M \triangleleft G$. Mostraremos o caso em que $H \triangleleft G$.

De fato, que $H < G$ é óbvio e:

$$(h, 1)^g = g^{-1}(h, 1)g = (a^{-1}, b^{-1})(h, 1)(a, b) = (a^{-1}ha, 1) \in H.$$

Portanto, $H \triangleleft G$.

Consideremos agora um subgrupo normal $N, N \triangleleft G$. Como $H, N \triangleleft G$, teremos

$$i) [H, N] \subset H \cap N \subset N$$

$$ii) [H, N] \triangleleft H$$

Demonstração:

(i) Por definição $[H, N] = \langle [a, b]; ; a \in H, b \in N \rangle$ e $[a, b] = a^{-1}b^{-1}ab$. Como $H, N \triangleleft G$, então temos:

$$a^{-1}b^{-1}a \in N \Rightarrow a^{-1}b^{-1}ab \in N, b^{-1}ab \in H \Rightarrow a^{-1}b^{-1}ab \in H$$

o que prova (i).

(ii) Devemos provar que $[H, N]^h \subseteq [H, N], \forall h \in H$. Provaremos que $[a, b]^h \in [H, N]$ para todos $a \in H, b \in N$ e $h \in H$. Então vejamos:

$$[a, b]^h = \underbrace{h^{-1}a^{-1}h}_{l^{-1}} \underbrace{h^{-1}b^{-1}h}_{k^{-1}} \underbrace{h^{-1}ah}_{l} \underbrace{h^{-1}bh}_{k},$$

note que se $l^{-1} = h^{-1}a^{-1}h$ e $k^{-1} = h^{-1}b^{-1}h$, então, $l \in H$ e $k \in N$, daí $[a, b]^h = l^{-1}k^{-1}lk = [l, k] \in [H, N]$ o que prova (ii).

Agora, vamos considerar o conjunto S da seguinte forma:

$$S = \{m \in M; \exists h \in H, \text{ com } (h, m) \in N\}.$$

É fácil ver que S é subgrupo de M . Notemos que $N \subseteq H \times S$, pela construção de S .

Tomemos agora $(h, m) \in H \times S$, afirmamos que existem $k, k' \in H$ com $(k, m) \in N$ e $k \cdot k' = h$. De fato, como $m \in S$, existe $k \in H$, com $(k, m) \in N$, escolhamos $k' = k^{-1} \cdot h$ (tal escolha é possível). Como H é um grupo não abeliano simples e provamos que $[H, N] \triangleleft H$, então temos dois casos possíveis para $[H, N]$. 1º Caso) $[H, N] = H$. Como $H = H \times 1 = [H, N] \subset H \cap N \subseteq N$, sabemos que $N \subset H \times S$, provaremos que $H \times S \subseteq N$ e conseqüentemente $N = H \times S$.

Dado $(x, y) \in H \times S$, como $y \in S$, existem $x_1, x_2 \in H$, com $x_1 \cdot x_2 = x$ e $(x_1, y) \in N$. Note que $(x_2, 1) \in H \subset N$, daí:

$$(x, y) = (x_1, y) \cdot (x_2, 1) = (x_1, x_2, y) \in N$$

E assim, $N = H \times S$.

Afirmamos que $S \triangleleft M$. Já sabemos que S é subgrupo de M , vamos provar que $S^g \subset S$, para todo $g \in G$. Identifiquemos $S = 1 \times S$, observemos que:

$$S^g = g^{-1}Sg = (a, b)^{-1}(1, s)(a, b) = (a^{-1}, b^{-1})(1, s)(a, b) = (1, b^{-1}sb),$$

para concluir basta provar que $b^{-1}sb \in S$. Como $N = H \times S$ e $N \triangleleft G$, então $N^g \subset N = H \times S$. Agora, tomando $g = (a, b)$ e $(h, s) \in H \times S = N$, temos:

$$(h, s)^g = (a^{-1}, b^{-1})(h, s)(a, b) = (a^{-1}ha, b^{-1}sb)$$

e daí, $b^{-1}sb \in S$, donde $S \triangleleft M$.

2º Caso) Suponhamos que $[H, N] = 1$, neste caso provaremos que $N = 1 \times S$ com $S \triangleleft M$. Dizer que $[H, N] = 1$, quer dizer que $ab = ba$, para todos $a \in H$

e $b \in N$. Como H é subgrupo simples não abeliano, então é fácil observar que $Z(H) = \{1\}$. Provamos anteriormente que $N \subset H \times S$, assim, dado $l \in N \Rightarrow l \in H \times S$, isto é, $l = (h, s)$. Tomemos um elemento qualquer da forma $(b, 1) \in H$, veja que:

$$(h, s) \cdot (b, 1) = (h \cdot b, s) = (b, 1) \cdot (h, s) = (bh, s) \Rightarrow hb = bh,$$

para todo $b \in H$, como $Z(H) = 1$, então $h = 1$, daí se $l = (h, s) \in N$ então $l = (1, s)$ e deste modo provamos que $N \subseteq 1 \times S$. Agora, dado $l \in 1 \times S$ teremos $l = (1, s)$ com $s \in S$, pela definição de S , existe $h \in H$ com $(h, s) \in N$. Como $N \subseteq 1 \times S$, teremos que $h = 1$ e portanto, $N = 1 \times S$. De maneira análoga provamos que $S \triangleleft G$, o que prova o Lema. ■

Definição 5.1 *Seja G um grupo. Dizemos que G é PNS se, para todo $K \triangleleft G$, $K \neq 1, G$, existe $H_k \triangleleft G$ com $H_k \neq G$ tal que $K \cdot H_k = G$.*

Por vacuidade, se G é grupo simples então G é PNS, pois para não ser PNS é preciso existir $N \triangleleft G$, $N \neq 1$, $N \neq G$ tal que N não tem suplemento próprio em G , isto é, não existe $K < G$; $KN = G$. Mas, G sendo simples, não existe $N \triangleleft G$, $N \neq 1, G$. Portanto, G simples é PNS.

Lema 5.3 *Seja $G = H \times M$ um grupo PNS. Então H e M são PNS.*

Demonstração: Provaremos apenas que M é um grupo PNS. Tomemos K um subgrupo normal próprio de M , isto é, $K \triangleleft M$. É fácil observar que $K \neq G$, provaremos que $K \triangleleft G$.

De fato, identifiquemos $K = 1 \times K$ e devemos provar que $K^g \subseteq K$, para todo $g \in G$, basta provar que $k^g \in K$, para todo $k \in K$, e todo $g \in G$. Tomemos $(1, k) \in K$ e $(h, m) \in G$. Observemos que:

$$(1, k)^{(h, m)} = (h^{-1}, m^{-1})(1, k)(h, m) = (h^{-1}h, m^{-1}km) = (1, m^{-1}km) \in K,$$

pois, $K \triangleleft M$, $m^{-1}km \in K$, para todo $m \in M$.

Agora, usando o fato de que G é PNS e $K \triangleleft G$, $K \neq 1$, G , existe $L \triangleleft G$, $L \neq G$.

De modo que $KL = G$. Usando Dedekind, temos:

$$K(L \cap M) = KL \cap M = G \cap M = M,$$

agora verifiquemos que $L \cap M \neq M$. Se $L \cap M = M$, teríamos $K(L \cap M) = KM = M$ e $L \cap M = M \Rightarrow M \subset L$, assim teremos $K \subset M \subset L$, daí teríamos $KL = L = G$ o que não é verdade, logo $L \cap M \neq M$. Também, $L \cap M \neq 1$, pois se $L \cap M = 1$, teríamos $M = K(L \cap M) = K$, o que é falso.

Deste modo, $K(L \cap M) = M$, com $K, L \cap M \neq M$, $K \triangleleft M$, para vermos que $L \cap M \triangleleft M$ é de fácil verificação. Portanto, M é PNS.

■

Lema 5.4 *Seja G um grupo finito. G é PNS se, e somente se, G é um produto direto de grupos simples.*

Demonstração: Suponha que G é PNS. Se G é simples, então G é um produto de um fator simples. Podemos supor G não simples.

Provaremos o resultado sobre indução em $|G|$.

Passo Indutivo: Suponha que todo grupo de ordem menor que $|G|$ sendo PNS é o produto direto de grupos simples.

Seja H um subgrupo normal minimal (Esta escolha é possível visto que G é finito e não simples). Como G é PNS, então existe $M \triangleleft G$, $M \neq G$ com $G = HM$, como H é minimal e $H \cap M \triangleleft G$, teremos $H \cap M = \{1\}$. Então podemos supor, sem perda de generalidade, que $G = H \times M$, sendo H minimal, então H é simples. Usando agora o Lema 5.3, temos que M é PNS e $|M| < |G|$ e pela hipótese indutiva temos que M é o produto direto de grupos simples, e assim, G é o produto direto de grupos simples. O que prova o resultado da primeira parte.

Observação: Dentre todos os subgrupos normais de G com ordem diferente de 1, escolhemos H com a menor ordem.

Agora, vamos supor que G é o produto direto de grupos simples e provaremos que G é PNS. Para isto, consideremos dois casos:

1º) Caso: G não é abeliano.

Estamos supondo $G = H_1 \times H_2 \times \dots \times H_n$ onde H_i são simples. É claro que existe H_i simples, com $|H_i|$ um número composto, caso contrário, teríamos que $|H_i|$ seria primo para todo $i \in \{1, 2, \dots, n\}$, mas assim, teríamos G abeliano, o que não é verdade. Então, podemos supor sem perda de generalidade que $|H_1|$ é um número composto.

Podemos então escrever $G = H_1 \times M$, onde $M = H_2 \times H_3 \times \dots \times H_n$. Provaremos o resultado, sobre indução em n , isto é, o número de fatores simples do produto.

Passo Indutivo: Suponhamos que todo grupo T , tal que T é o produto direto de k grupos simples, $1 < k < n$, então T é PNS.

Podemos assumir que G é não simples, pois se G é simples então G é PNS trivial. Tomemos então $N \triangleleft G$ com $N \neq 1, G$. Por hipótese indutiva, M é PNS. Podemos escolher $N \neq H_1, M$. Como $G = H_1 \times M$ e $|H_1|$ é composto, H_1 é simples então H_1 não é abeliano. Usando o Lema 5.2, temos que $N = H_1 \times S$ ou $N = 1 \times S$ onde $S \triangleleft M$, da maneira que N foi escolhido temos que $S \neq M$ e $S \neq 1$. Como M é PNS, existe $T \neq 1, M$ com $T \triangleleft M$ tal que $M = ST$, donde obtemos que: $G = N(1 \times T)$ ou $G = N(H \times T)$ com $1 \times T \triangleleft G$ e $H \times T \triangleleft G$, o que conclui que G é PNS.

2º) Caso: G é abeliano.

Sendo G abeliano, então cada grupo do produto direto é abeliano e como cada grupo deste é simples, temos a seguinte:

Afirmção: Se L é um grupo abeliano simples, então $|L|$ é um número primo.

De fato, se $|L| = a \cdot b$ com $a, b \in \mathbb{N}$ e $1 < a \leq b$. Seja p um primo que divide a , daí existe $g \in L$ com $o(g) = p$, assim o subgrupo $\langle g \rangle$ cíclico é normal em L e $\langle g \rangle \neq 1, L$, mas $|L|$ é um grupo simples. Assim, $|L|$ é um número primo.

Como $G = H_1 \times H_2 \times \dots \times H_n$, com H_i abeliano e simples, então para cada $i \in \{1, 2, 3, \dots, n\}$ existe p_i primo, com $H_i \simeq \mathbb{Z}_{p_i}$. Então, podemos supor, sem perda de generalidade, que $G = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_n}$. Provaremos agora que G é PNS. Seja $H \triangleleft G$, com $H \neq 0, G$, então existe $v = \{a_1, a_2, \dots, a_n\} \in H$ com algum $a_i \neq 0$, podemos supor $a_1 \neq 0$. Consideremos o conjunto:

$$M = \{(0, m_2, m_3, \dots, m_n); m_i \in \mathbb{Z}_{p_i}, i = 2, 3, \dots, n\}$$

é fácil ver que M é um subgrupo de G , sendo G abeliano então $M \triangleleft G$. É claro que $H + M \subset G$. Provaremos a outra inclusão e por consequência $G = H + M$. Tomemos $w = (b_1, b_2, \dots, b_n) \in G$, isto é, $b_i \in \mathbb{Z}_{p_i}, i = 1, 2, \dots, n$. Sempre é possível encontrar um natural k , tal que $ka_i \equiv b_1 \pmod{p_1}$, basta usar fatos simples sobre congruência modular. Definimos agora $l = w - kv$, note que $l \in M$ e daí, $w = kv + l \in H + M$, isto é $G = H + M$, isto é, G é PNS. ■

Agora, estamos preparados para estudar as coberturas por subgrupos normais.

Teorema 5.5 *Um grupo G possui uma cobertura finita não trivial por subgrupos normais se, e somente se, existe $N \triangleleft G$, tal que:*

$$\frac{G}{N} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$$

para algum primo p .

Demonstração: Digamos que existe $N \triangleleft G$, com $\frac{G}{N} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ para algum primo p . Seja $G_1 = \mathbb{Z}_p \times \mathbb{Z}_p$, observemos que G_1 é abeliano e se $x \neq 1, x \in G_1$, então $o(x) = p$.

Assim, G_1 possui a seguinte cobertura por subgrupos normais próprios:

$$G_1 = \bigcup_{1 \neq a \in G_1} \langle a \rangle.$$

Como $\frac{G}{N} \simeq G_1$, então $\frac{G}{N}$ possui uma cobertura por subgrupos normais próprios, como todo subgrupo de $\frac{G}{N}$ é da forma $\frac{H}{N}$, com $N \triangleleft H$ e $H < G$, sendo a cobertura por subgrupos normais, teremos que:

$$\frac{G}{N} = \bigcup_{i=1}^n \left(\frac{H_i}{N} \right)$$

onde $N \triangleleft H_i$, $H_i \triangleleft G$, $H_i \neq 1, G$.

Donde obtemos $G = \bigcup_{i=1}^n H_i$, $H_i \triangleleft G$, $H_i \neq 1, G$.

Agora, suponhamos que $G = \bigcup_{i=1}^n N_i$ com $N_i \triangleleft G$, $N_i \neq G$. Consideremos

$N = \bigcap_{i=1}^n N_i$ temos que $N \triangleleft G$, devido ao fato que $N_i \triangleleft G$, para $i = 1, 2, \dots, n$. Podemos assumir, sem perda de generalidade, que N_1, N_2, \dots, N_n cobrem G irredudantemente, e usando o Teorema de Neumann, teremos que $|G : N_i|$ é finito para $i = 1, 2, \dots, n$. Agora, usando Poincaré, teremos que $|G : N|$ é finito, pois

$$|G : N| \leq |G : N_1| \cdot |G : N_2| \cdot \dots \cdot |G : N_n| < \infty.$$

Deste modo, $\frac{G}{N}$ é finito e possui cobertura finita por subgrupos normais próprios,

$$\frac{G}{N} = \bigcup_{i=1}^n \left(\frac{N_i}{N} \right).$$

Queremos provar que existe $M \triangleleft G$, com $\frac{G}{M} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ para algum primo p . Basta então mostrarmos que existe $\frac{M}{N} \triangleleft \frac{G}{N}$ com:

$$\frac{G}{M} \simeq \frac{\frac{G}{N}}{\frac{M}{N}} \simeq \mathbb{Z}_p \times \mathbb{Z}_p,$$

para algum primo p .

Para isto, precisaremos do seguinte:

Lema 5.6 *Seja G_1 um grupo finito tal que $G_1 = \bigcup_{i=1}^m W_i$ com $W_i \triangleleft G_1, W_i \neq G_1$. Então, existe $M \triangleleft G_1$ com $\frac{G_1}{M} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$, para algum primo p .*

Prova do Lema Provaremos por absurdo. Suponhamos que existe G_1 um grupo finito de ordem mínima tal que $G_1 = \bigcup_{i=1}^m W_i, W_i \triangleleft G_1, W_i \neq G_1$ e não existe $M \triangleleft G_1$, tal que $\frac{G_1}{M} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ para qualquer primo p .

Agora, vamos demonstrar que G_1 é PNS. Tomemos $K \triangleleft G$ com $K \neq 1, G_1$ como $G_1 = \bigcup_{i=1}^m W_i$, então $\frac{G_1}{K} = \bigcup_{i=1}^m \left(\frac{W_i K}{K} \right)$, como $\frac{G_1}{K}$ é finito e possui cobertura por subgrupos normais e $\left| \frac{G_1}{K} \right| < |G_1|$, assim deve existir $i \in \{1, 2, \dots, m\}$ com:

$$\frac{G_1}{K} = \frac{W_i K}{K}.$$

Podemos supor, sem perda de generalidade, que $i = 1$, assim teremos: $G_1 = W_1 K$, ou seja, G_1 é PNS. Como G_1 é finito, usando o Lema 5.4, obtemos que $G_1 = L_1 \times L_2 \times \dots \times L_n$ com L_i simples. Temos dois casos a analisar:

i) G_1 é abeliano.

Neste caso, cada L_i é abeliano simples, então $|L_i|$ é um número primo. Dividamos em dois casos:

a) Digamos que todos os primos são distintos, ou seja $|L_i| = p_i$ e $p_i \neq p_j, \forall i \neq j$. E usando o Teorema dos Isomorfismos e o Teorema Fundamental dos Grupos Abelianos Finitamente Gerados, teremos:

$$G_1 \simeq \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_n} \simeq \mathbb{Z}_{p_1 \cdot p_2 \cdot \dots \cdot p_n}$$

mas $\mathbb{Z}_{p_1 \cdot p_2 \cdot \dots \cdot p_n}$ é cíclico, mas sabemos do Capítulo 2, que os grupos cíclicos não possuem cobertura não trivial. Então, existem pelo menos dois primos iguais,

digamos, sem perda de generalidade, $p_1 = p_2$, assim temos o caso:

b) $G_1 = L_1 \times L_2 \times \dots \times L_n$, tomemos $M = L_3 \times L_4 \times \dots \times L_n$, veja que $M \triangleleft G_1$.

Consideremos $K_1 = L_1 \times L_2$, do mesmo modo temos também que $K_1 \triangleleft G$. Usando o Teorema dos Isomorfismos, temos $\frac{G_1}{M} \simeq K_1$. Como $K_1 = L_1 \times L_2$ e $L_1, L_2 \simeq \mathbb{Z}_{p_1}$ teremos:

$$\frac{G_1}{M} \simeq K_1 = L_1 \times L_2 \simeq \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1},$$

mas isto contraria a hipótese.

Portanto, G_1 não pode ser abeliano.

ii) G_1 não é abeliano.

Como $G_1 = L_1 \times L_2 \times \dots \times L_n$, onde os L_i são simples, então deve existir $i \in \{1, 2, \dots, n\}$ tal que $|L_i|$ é um número composto. Podemos assumir que $|L_1|$ é um número composto, e escrevemos:

$$G_1 = L_1 \times M, \text{ onde } M = L_2 \times L_3 \times \dots \times L_n.$$

Temos que $|M| < |G_1|$, consideremos o conjunto $J = \cup S_i$ onde $S_i \triangleleft M$, $S_i \neq M$. Pela minimalidade de G_1 , existe $m \in M$, com $m \notin J$. Consideremos o elemento $(h, m) \in G_1 = L_1 \times M$, com $h \neq 1$. Como G_1 possui uma cobertura por subgrupos normais próprios, existe $N \triangleleft G_1$, com $N \neq 1, G_1$, tal que $(h, m) \in N$. Aplicando o Lema 5.2, visto que $G = L_1 \times M$ e L_1 é simples com $|L_1|$ um número composto, então L_1 não é abeliano. Então, pelo Lema 5.2, temos que: $N = 1 \times S$ ou $N = L_1 \times S$, com $S \triangleleft M$, como $(h, m) \in N$, $h \neq 1$ teremos que $N = L_1 \times S$, $m \notin J$, então, $S = M$ e daí $N = L_1 \times M = G_1$ o que é uma contradição e o Lema 5.6 está demonstrado. ■

Corolário 5.1 *Seja G um grupo nilpotente. Então, G admite cobertura finita não trivial se, e somente se, G possui uma cobertura não trivial finita por subgrupos normais.*

Demonstração: Suponhamos que G admite cobertura não trivial finita. Pelo Teorema 2.4, temos que existe $N \triangleleft G$, com $\frac{G}{N}$ não cíclico e finito. Agora, usando o Lema 5.1, obtemos a existência de $H \triangleleft G$, tal que $\frac{\frac{G}{H}}{\frac{G'}{H}}$ é finito e não cíclico. Novamente, usando o Teorema 2.4, teremos que $\frac{G}{G'}$ admite uma cobertura finita e não trivial. Como $\frac{G}{G'}$ é abeliano, então todo subgrupo é normal, daí

$$\frac{G}{G'} = \bigcup_{i=1}^n \left(\frac{H_i}{G'} \right)$$

onde $\frac{H_i}{G'} \triangleleft \frac{G}{G'}$, $\frac{H_i}{G'} \neq \frac{G}{G'}$.

Deste modo, $G = \bigcup_{i=1}^n H_i$, onde $H_i \triangleleft G$, $H_i \neq G$.

■

Definição 5.2 Um grupo G_1 é dito perfeito, quando é igual ao seu derivado, isto é, $G_1 = G_1'$.

Corolário 5.2 Todo subgrupo normal perfeito de um grupo G está contido em todo membro de uma cobertura irredundante de G por subgrupos normais próprios.

Demonstração: Seja M um subgrupo normal perfeito de G , então $M \triangleleft G$ e $M = M'$. Para cada $x \in G$, definamos $M_x = \langle M, x \rangle$. Sabemos que $\langle M, x \rangle$ é o menor subgrupo que contém M e x , e como M é normal, $M \cdot \langle x \rangle$ é um subgrupo, é fácil ver então que:

$$M_x = \langle M, x \rangle = M \cdot \langle x \rangle.$$

Agora, usando o Teorema dos Isomorfismos, obtemos:

$$\frac{M_x}{M} \simeq \frac{\langle x \rangle}{\langle x \rangle \cap M}.$$

Daí $\frac{M_x}{M}$ é cíclico. Como $\frac{M_x}{M'_x}$ é abeliano e $\frac{M_x}{M}$ também o é, temos que: $M'_x \subset M$, como $M_x = M\langle x \rangle$, então $M \subset M_x \Rightarrow M' \subset M'_x \subset M$, como $M = M'$ temos que $M'_x = M$.

Agora, observemos que M_x não possui cobertura por subgrupos normais próprios. De fato, se M_x possuísse tal cobertura, deveríamos ter pelo Teorema 5.5, que existiria $M_1 \triangleleft M_x$, de modo que:

$$\frac{M_x}{M_1} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$$

para algum primo p .

Como $\frac{M_x}{M_1} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ é abeliano, então $M'_x \subset M_1$. Mas $M'_x = M$. Logo, $M \leq M_1$ e $\frac{M_x}{M_1} \simeq \frac{M_x}{\frac{M}{M_1}}$ que é cíclico, pois

$$\frac{M_x}{M} = \frac{M\langle x \rangle}{M} \simeq \frac{\langle x \rangle}{M \cap \langle x \rangle},$$

o que é um absurdo, pois $\frac{M_x}{M_1} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

Sejam N_1, N_2, \dots, N_n subgrupos normais próprios de G , tais que $G = \bigcup_{i=1}^n N_i$ é cobertura irredundante. Tomemos H um subgrupo qualquer de G , notemos que:

$$H = H \cap G = H \cap \left(\bigcup_{i=1}^n N_i \right) = \bigcup_{i=1}^n (N_i \cap H),$$

note que $N_i \cap H \triangleleft H$. Isto quer dizer que toda cobertura por subgrupos normais de G , induz uma cobertura por subgrupos normais a qualquer subgrupo de G .

Então, $M_x = \bigcup_{i=1}^n (M_x \cap N_i)$ com $M_x \cap N_i \triangleleft M_x$. Como sabemos que a cobertura de M_x por subgrupos normais deve ser trivial, deve existir pelo menos um $k \in \{1, 2, 3, \dots, n\}$ de modo que $M_x = M_x \cap N_k$, isto quer dizer que $M_x \subset N_k$. Como $M \subset M_x$, teremos $M \subset N_k$. O objetivo é mostrar que $M \subset N_i$, para

todo $i \in \{1, 2, 3, \dots, n\}$. Digamos que exista $j \neq i, j \in \{1, 2, \dots, n\}$ tal que $M \not\subseteq N_j$, então para todo $x \in G$, teremos $M_x \not\subseteq N_j$.

Mas, daí, como $G = \bigcup_{x \in G} M_x \subseteq \bigcup_{i \neq j} N_i$, teremos um absurdo, visto que a cobertura é irredundante.

Portanto, $M \subset N_i, \forall i \in \{1, 2, \dots, n\}$.

■

Corolário 5.3 *Seja $G = \bigcup_{i=1}^n N_i$ onde N_1, N_2, \dots, N_n formam uma cobertura irredundante por subgrupos normais próprios. Então, $\frac{G}{D}$ é finito e solúvel onde*

$$D = \bigcap_{i=1}^n N_i$$

Demonstração: Como a cobertura é irredundante, e usando o Teorema de Neumann, temos que $|G : N_i|$ é finito para $i = 1, 2, \dots, n$. Agora usando Poincaré, concluímos que $|G : D|$ é finito. Como $N_i \triangleleft G$, temos que $D \triangleleft G$, e assim $H = \frac{G}{D}$ é finito, falta mostrarmos que é solúvel.

Consideremos a sequência de subgrupos de H

$$\dots \triangleleft H^{(3)} \dots \triangleleft H^{(2)} \dots \triangleleft H' \triangleleft$$

Observemos que cada $H^{(n)}$ é subgrupo de H e $H^{n+1} = (H^{(n)})'$. Como H é finito, existe um natural $k \in \mathbb{N}$, tal que: $H^k = H^{k+1}$. Isto quer dizer que H^k é subgrupo normal perfeito de H . Veja que:

$$H = \bigcup_{i=1}^n \left(\frac{N_i}{D} \right),$$

com $\frac{N_1}{D}, \frac{N_2}{D}, \dots, \frac{N_n}{D}$ formando uma cobertura irredundante de H por subgrupos normais próprios. Usando o Corolário 5.2, teremos que:

$$H^k \subset \frac{N_i}{D},$$

para $i = 1, 2, 3, \dots, n$, então

$$H^k \subset \bigcap_{i=1}^n \left(\frac{N_i}{D} \right) = 1,$$

isto é, $H^k = 1$, ou seja, H é solúvel o que prova o corolário.

■

5.2 Cobertura por Subgrupos Verbais

Antes de enunciarmos o Teorema desta seção, vamos fazer alguns comentários sobre subgrupos verbais.

Definição 5.3 *Seja A um conjunto enumerável, $A = \{x_1, x_2, x_3, \dots\}$ onde os x_i são as letras do alfabeto A . Uma palavra reduzida de A é uma expressão da forma*

$$w = x_{i_1}^{\alpha_1} \cdot x_{i_2}^{\alpha_2} \cdot \dots \cdot x_{i_n}^{\alpha_n}$$

onde $x_{ij} \neq x_{ik}$ para $j \neq k + 1$ ou $k \neq j + 1$, $\alpha_i \in \mathbb{Z}$.

Para cada letra x_i do alfabeto A e $\alpha_1, \alpha_2 \in \mathbb{Z}$, definimos $x_1^{\alpha_1 + \alpha_2} = x_1^{\alpha_1} \cdot x_1^{\alpha_2}$. Então, as palavras reduzidas do alfabeto A , geram um grupo, este grupo será denotado por $F[A]$, o grupo livre gerado pelo alfabeto A .

Definição 5.4 *Seja $A = \{x_1, x_2, x_3, \dots\}$ enumerável infinito. Consideremos o grupo $F[A]$, tomemos uma palavra $w \in F[A]$, $w = x_{i_1}^{\alpha_1} \cdot x_{i_2}^{\alpha_2} \cdot \dots \cdot x_{i_n}^{\alpha_n}$. Definimos o valor da palavra w nos elementos g_1, g_2, \dots, g_n de um grupo G , como sendo:*

$$w(g_1, g_2, \dots, g_n) = g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_n^{\alpha_n}.$$

Definição 5.5 *Seja W um subconjunto não vazio de $F[A]$. Definimos o subgrupo verbal de G , determinado por W , como sendo:*

$$W(G) = \langle w(g_1, g_2, \dots); w \in W, g_i \in G \rangle$$

isto é, o grupo gerado pelos valores das w de W em G .

Exemplo 5.1 *Se $W = \{x_1^{-1} \cdot x_2^{-1} \cdot x_1 \cdot x_2\} \subset F[A]$, $W(G) = G'$ (Grupo Derivado). Do mesmo modo, se $W = \{x_1^n\}$ então $W(G) = G^n = \langle g^n, g \in G \rangle$.*

Provaremos duas Proposições, referentes aos subgrupos verbais.

Proposição 5.1 *O grupo verbal $W(G)$ é normal em G , para qualquer $W \subset F[A]$.*

Demonstração: Para mostrarmos esta propriedade, basta ver que: $a^{-1}ka \in W(G)$, $\forall a \in G$ e $k \in W(G)$. Mostraremos que esta propriedade vale para os geradores de $W(G)$, e assim vale para todos os elementos de $W(G)$.

Tomemos w uma palavra de W , $w = x_{i_1}^{\alpha_1} \cdot x_{i_2}^{\alpha_2} \cdot \dots \cdot x_{i_n}^{\alpha_n}$, daí $w(g_1, g_2, \dots, g_n) = g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_n^{\alpha_n}$. Agora, para todo $a \in G$, observemos que:

$$\begin{aligned} a^{-1}w(g_1, g_2, \dots, g_n)a &= a^{-1} \cdot g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_n^{\alpha_n} \cdot a \\ &= a^{-1} \cdot g_1^{\alpha_1} \cdot a \cdot a^{-1} \cdot g_2^{\alpha_2} \cdot a \cdot a^{-1} \cdot g_3^{\alpha_3} \cdot a \cdot a^{-1} \cdot \dots \cdot a \cdot a^{-1} \cdot g_n^{\alpha_n} \cdot a \\ &= (a^{-1}g_1a)^{\alpha_1} \cdot (a^{-1}g_2a)^{\alpha_2} \cdot \dots \cdot (a^{-1}g_na)^{\alpha_n} \\ &= w(a^{-1}g_1a, a^{-1}g_2a, \dots, a^{-1}g_na) \in W(G). \end{aligned}$$

Intercalamos aa^{-1} entre os elementos $g_1^{\alpha_1} \cdot g_2^{\alpha_2} \cdot \dots \cdot g_n^{\alpha_n}$. Daí, temos que $W(G) \triangleleft G$. ■

Proposição 5.2 *Sejam A e B grupos. Então $W(A \times B) = W(A) \times W(B)$, para qualquer $W \subset F[A]$.*

Demonstração: Pela definição, temos:

$$W(A \times B) = \langle w((a_1, b_1), (a_2, b_2), \dots); w \in W, (a_i, b_i) \in A \times B \rangle$$

Tomemos uma palavra w de W , $w = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$, assim

$$\begin{aligned} w((a_1, b_1), (a_2, b_2), \dots, (a_n, b_n)) &= (a_1, b_1)^{\alpha_1} \cdot (a_2, b_2)^{\alpha_2} \cdot \dots \cdot (a_n, b_n)^{\alpha_n} \\ &= (a_1^{\alpha_1}, b_1^{\alpha_1}) \cdot (a_2^{\alpha_2}, b_2^{\alpha_2}) \cdot \dots \cdot (a_n^{\alpha_n}, b_n^{\alpha_n}) \\ &= (a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \dots \cdot a_n^{\alpha_n}, b_1^{\alpha_1} \cdot b_2^{\alpha_2} \cdot \dots \cdot b_n^{\alpha_n}) \\ &= (w(a_1, a_2, \dots, a_n), w(b_1, b_2, \dots, b_n)) \in W(A) \times W(B). \end{aligned}$$

Mostramos que todo gerador de $W(A \times B)$ está contido em $W(A) \times W(B)$ e assim, $W(A \times B) \subset W(A) \times W(B)$, a outra inclusão é análoga.

Assim, $W(A \times B) = W(A) \times W(B)$.

■

Agora, vamos enunciar e provar o seguinte:

Teorema 5.7 *Toda cobertura finita de um grupo consistindo somente de subgrupos verbais é trivial.*

Demonstração: O Teorema pede para provar o seguinte fato: Seja G um grupo. Se pudermos escrever $G = \bigcup_{i=1}^n W_i(G)$ onde $W_i(G)$ são subgrupos verbais de G , então, existe $i \in \{1, 2, \dots, n\}$ tal que $W_i(G) = G$.

Dividiremos a demonstração em dois casos: caso G finito e caso G infinito. Vamos provar sempre por contradição.

1º Caso) Vamos assumir por contradição que exista um grupo H de menor ordem, de modo que $H = \bigcup_{i=1}^n W_i(H)$, onde os $W_i(H)$ são subgrupos verbais próprios de H .

Agora, provemos que H é PNS. De fato, tome $K \triangleleft H, K \neq 1, H$. Usando argumentos similares aos das Proposições anteriores, concluímos que:

$$\frac{H}{K} = \bigcup_{i=1}^n W_i \left(\frac{H}{K} \right).$$

Como $\left| \frac{H}{K} \right| < |H|$, deve existir $i \in \{1, 2, \dots, n\}$ de modo que $\frac{H}{K} = W_i \left(\frac{H}{K} \right)$, também com fatos simples, podemos concluir que $W_i \left(\frac{H}{K} \right) = \frac{W_i(H)K}{K}$, logo $\frac{H}{K} = \frac{W_i(H)K}{K}$. Donde, $H = W_i(H)K$, isto é, H é PNS.

Como H é finito e usando o Lema 5.4, H pode ser escrito da seguinte forma: $H = H_1 \times H_2 \times \dots \times H_m$, onde os H_i são simples. Deste modo, para qualquer subgrupo verbal $W(H)$ de H , pela Proposição anterior, teremos que:

$$W(H) = W(H_1) \times W(H_2) \times \dots \times W(H_m).$$

Como os H_i são simples e $W(H_i) \triangleleft H$, então $W(H_i) = 1$ ou H_i . Sabendo que $H = H_1 \times H_2 \times \dots \times H_m$ e $H = \bigcup_{i=1}^n W_i(H)$, e supondo que a cobertura é por subgrupos próprios, então, para cada $i \in \{1, 2, 3, \dots, n\}$, deve existir $j \in \{1, 2, 3, \dots, m\}$ tal que: $W_i(H_{j_i}) = 1$.

Mas, daí se $h = (h_1, h_2, \dots, h_m)$ onde $h_i \neq 1$, para $i \in \{1, 2, 3, \dots, m\}$ teremos que $h \notin W_i(H)$, para todo $i \in \{1, 2, 3, \dots, n\}$ contradizendo a hipótese de $\bigcup_{i=1}^n W_i(H)$ ser cobertura para H .

Assim, se G é um grupo finito e admite cobertura por subgrupos verbais, esta deve ser trivial.

2º Caso) G infinito.

Agora suponhamos $G = \bigcup_{i=1}^n W_i(G)$, onde os $W_i(G)$ subgrupos verbais próprios de G . Pelo Teorema 2.3 podemos assumir que $|G : W_i(G)|$ é finito para $i \in \{1, 2, 3, \dots, n\}$. Definamos $N = \bigcap_{i=1}^n W_i(G)$, como $W_i(G) \triangleleft G$, temos que $N \triangleleft G$,

e assim

$$\frac{G}{N} = \bigcup_{i=1}^n \frac{W_i(G)}{N}.$$

Usando argumento análogo aos das Proposições anteriores, concluímos que

$$\frac{W_i(G)}{N} = W_i\left(\frac{G}{N}\right)$$

e assim, $\frac{G}{N} = \bigcup_{i=1}^n W_i\left(\frac{G}{N}\right)$. Como $\frac{G}{N}$ é finito, pelo 1º caso tal cobertura deve ser trivial, daí $W_i\left(\frac{G}{N}\right) = \frac{G}{N}$ para algum i .

Como $N \leq W_i(G)$, segue que $W_i\left(\frac{G}{N}\right) = \frac{W_i(G)}{N}$ e portanto $W_i(G) = G$.

■

Apêndice A - O Teorema de Ramsey

Em bons livros de introdução às idéias combinatórias, podemos encontrar o Teorema de Ramsey em sua versão finita. No nosso caso, na demonstração do Teorema de Neumann no Capítulo 2, usamos o Teorema de Ramsey, porém em sua versão infinita. Faço agora a prova deste Teorema, antes precisamos de algumas definições.

Definição 5.6 *Dado j inteiro positivo, definimos $I_j = \{1, 2, 3, \dots, j\}$.*

Definição 5.7 *Dado um conjunto A e um inteiro positivo m , denotamos por $[A]^m$ o conjunto dos subconjuntos de m elementos de A , ou seja,*

$$[A]^m = \{B \subset A; |B| = m\}.$$

Teorema 5.8 (Ramsey - versão infinita) *Sejam m, k inteiros positivos e A um conjunto infinito. Para qualquer função $F : [A]^m \rightarrow I_k$, existem $j \in I_k$ e um conjunto infinito $B \subset A$ tal que:*

$$F([B]^m) = \{F(x); x \in [B]^m\} = \{j\}.$$

Demonstração: Vamos provar o resultado por indução em m . Para $m = 1$ o resultado segue do fato de que se X é infinito e C é finito, então para toda função $f := X \rightarrow C$ existe $c \in C$ tal que $f^{-1}(c) = \{x \in X; f(x) = c\}$ é infinito.

Seja agora $m \geq 2$ e $F : [A]^m \rightarrow I_k$, onde A é infinito. Fixamos $x_0 \in A$, e definimos $A_0 = A - \{x_0\}$ e $g : [A_0]^{m-1} \rightarrow I_k$ por $g(C) := F(C \cup \{x_0\})$,

onde C é um subconjunto de $m - 1$ elementos de A_0 . Pela hipótese de indução, existe um conjunto infinito $B_0 \subset A_0$ e $j_0 \in I_k$ tal que $g_0([B_0]^{m-1}) = \{j_0\}$. A partir daí, repetimos o processo recursivamente: Dado $n \geq 0$, fixamos $x_{n+1} \in B_n$ e definimos $A_{n+1} = B_n - \{x_{n+1}\}$ e $g_{n+1} := [A_{n+1}]^{m-1} \rightarrow I_k$ por $g_{n+1}(C) = F(C \cup \{x_{n+1}\})$ para $C \subset A_{n+1}$ com $m - 1$ elementos. Pela hipótese de indução, existe $B_{n+1} \subset A_{n+1}$ infinito e $j_{n+1} \in I_k$ tal que $g([B_{n+1}]^{m-1}) = \{j_{n+1}\}$.

Podemos agora tomar $D = \{x_0, x_1, x_2, \dots\}$, que é infinito, e definir $h : D \rightarrow I_k$ por $h(x_r) = j_r$. Como I_k é finito, existe $j \in I_k$ tal que $h^{-1}(j) = \{x \in D; h(x) = j\}$ é infinito. Afirmamos que $B = h^{-1}(j)$ satisfaz a condição do enunciado. De fato, dado um subconjunto $X = \{x_{i_1}, x_{i_2}, x_{i_3}, \dots\}$ de B com m elementos, temos $F(X) = g_{i_1}(\{x_{i_2}, \dots, x_{i_m}\}) = j_{i_1} = h(x_{i_1}) = j$.

■

Apêndice B - O Teorema de Bertrand

Em bons livros de Introdução à Teoria dos Números, podemos encontrar o Postulado de Bertrand. Faço um esboço da prova deste teorema, e antes precisaremos de alguns lemas.

Lema 5.9 *Seja x um número real, então $[2 \cdot x] - 2 \cdot [x] = 0$ ou 1 . Onde $[y]$ denota a parte inteira do real y .*

Demonstração: Se $x = n + \alpha$, $0 \leq \alpha < 1$, $[x] = n$. Se $0 \leq \alpha < \frac{1}{2}$, então $2\alpha < 1$ e $[2x] = [2n + 2\alpha] = 2 \cdot n$, o que implica $[2x] - 2[x] = 2n - 2n = 0$. Se $\frac{1}{2} \leq \alpha < 1$, $1 < 2\alpha < 2$ e $[2x] = [2n + 2\alpha] = 2n + 1$, o que implica que $[2x] - 2[x] = 2n + 1 - 2n = 1$.



Lema 5.10 *Seja n um número natural e p um primo. Então o expoente da maior potência de p que divide $n!$ é dado por*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Demonstração: Na sequência dos n primeiros inteiros positivos: $1, 2, 3, \dots, n$, os inteiros divisíveis por p , são:

$$p \cdot 1, p \cdot 2, p \cdot 3, \dots, p \cdot t$$

onde t é o menor inteiro positivo tal que $p \cdot t \leq n$, isto é, t é o menor inteiro $\leq \frac{n}{p}$, de modo que $t = \left\lfloor \frac{n}{p} \right\rfloor$. Portanto $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p , no produto $1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot n = n!$ que são:

$$p \cdot 1, p \cdot 2, p \cdot 3, \dots, p \cdot \left\lfloor \frac{n}{p} \right\rfloor.$$

Assim, sendo, o expoente de p na fatoração canônica de $n!$ é o expoente de p no produto:

$$P = (p \cdot 1) \cdot (p \cdot 2) \cdot (p \cdot 3) \cdot \dots \cdot (p \cdot \left\lfloor \frac{n}{p} \right\rfloor)$$

$$P = p^{\left\lfloor \frac{n}{p} \right\rfloor} \cdot \left(1 \cdot 2 \cdot 3 \cdot \dots \cdot \left\lfloor \frac{n}{p} \right\rfloor \right).$$

Ora, o expoente de p em P igual a $\left\lfloor \frac{n}{p} \right\rfloor$ mais o expoente de p no produto :

$$P_1 = 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left\lfloor \frac{n}{p} \right\rfloor.$$

Fazendo sobre P_1 o mesmo raciocínio que foi feito sobre $1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot n = n!$, conclui-se que o expoente de p em P_1 é igual a:

$$\left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor = \left\lfloor \frac{n}{p^2} \right\rfloor$$

mais o expoente de p no produto:

$$P_2 = 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left\lfloor \frac{n}{p^2} \right\rfloor.$$

Por sua vez, o expoente de p em P_2 é, pelo mesmo raciocínio, igual a :

$$\left\lfloor \frac{\left\lfloor \frac{n}{p^2} \right\rfloor}{p} \right\rfloor = \left\lfloor \frac{n}{p^3} \right\rfloor$$

Aumentando o expoente de p no produto

$$P_3 = 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left\lfloor \frac{n}{p^3} \right\rfloor$$

e assim, por diante, até obter-se um $p^{r+1} > n$, o que implica que $\left\lfloor \frac{n}{p^{r+1}} \right\rfloor = 0$.

De modo que o expoente da maior potência de p que divide $n!$ é dada pela soma abaixo:

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

■

Lema 5.11 Para $n \geq 1$, temos

(i) Seja $r(p)$ satisfazendo $p^{r(p)} \leq 2n < p^{r(p)+1}$, então

$$\binom{2n}{n} \text{ divide } \prod_{p \leq 2n} p^{r(p)}.$$

(ii) Se $n > 2$ e $\frac{2n}{3} < p \leq n$, então p não divide $\binom{2n}{n}$.

(iii) $\prod_{p \leq n} p < 4^n$.

Demonstração:

(i) Pelo Lema 5.10, o expoente de p em $n!$ é

$$\sum_{j=1}^{r(p)} \left\lfloor \frac{n}{p^j} \right\rfloor,$$

e o expoente de p em $\binom{2n}{n}$ é dado por:

$$\sum_{j=1}^{r(p)} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^j} \right\rfloor \right) \leq \sum_{j=1}^{r(p)} 1 = r(p).$$

Esta última desigualdade se verifica pelo Lema 5.9. Para concluir a demonstração basta tomar o produto sobre os primos $p \leq 2n$.

(ii) Se p satisfaz $\frac{2n}{3} < p \leq n$, então p ocorre uma vez na fatoração de $n!$ e duas vezes na fatoração de $(2n)!$ pois $3p > 2n$. Logo, como $p > 2$, p não divide $\binom{2n}{n}$.

(iii) Isto será provado por Indução.

Seja $P(n)$ a proposição a ser provada. É fácil ver que $P(n)$ é verdadeira para $n = 1, 2$ e 3 . Para $m > 1$, temos que $P(2m - 1)$ implica $P(2m)$ pois

$$\prod_{p \leq 2m} p = \prod_{p \leq 2m-1} p < 4^{2m-1} < 4^{2m}.$$

Desta forma, podemos supor $n = 2m + 1$ com $m \geq 2$. Como todo primo p no intervalo $[m + 2, 2m + 1]$ é um fator de $\binom{2m+1}{m}$, teremos (Assumindo que $P(m + 1)$ sse verifica):

$$\prod_{p \leq 2m+1} p \leq \binom{2m+1}{m} \prod_{p \leq m+1} p < \binom{2m+1}{m} 4^{m+1}$$

Mas

$$\binom{2m+1}{m} < \frac{1}{2}(1+1)^{2m+1} = 4^m$$

pois $\binom{2m+1}{m}$ corresponde aos dois termos centrais da expansão binomial de $(1+1)^{2m+1}$.

Logo 5.2 vemos que $P(m + 1)$ implica $P(2m + 1)$, o que completa da prova por indução. ■

Teorema 5.12 (Bertrand) *Para cada inteiro positivo n existe um primo p satisfazendo $n < p \leq 2n$.*

Demonstração: Claramente o resultado é verdadeiro para $n \leq 3$. Vamos assumir que o resultado seja falso para algum $n > 3$ e obter uma contradição. Temos do Lema 5.11, que para este n todos os fatores primos p de $\binom{2n}{n}$ satisfazem $p \leq \frac{2n}{3}$. Seja $s(p)$ a maior potência de p a qual divide $\binom{2n}{n}$. Usando o Lema, temos:

$$p^{s(p)} \leq 2n.$$

Portanto, se $s(p) > 1$, então $p \leq \sqrt{2n}$ e segue que no máximo $\lfloor \sqrt{2n} \rfloor$ primos ocorrem em $\binom{2n}{n}$ com expoente maior do que 1. Usando o Lema e nossa suposição obtemos:

$$\binom{2n}{n} \leq (2n)^{\lfloor 2n \rfloor} \prod_{p \leq \frac{2n}{3}} p.$$

Mas $\frac{4^n}{2n+1} < \binom{2n}{n}$, uma vez que $\binom{2n}{n}$ é o maior termo na expansão binomial de $(1+1)^{2n}$, a qual possui $2n+1$ termos.

Desta forma, usando (5.2) e estas duas desigualdades obtemos:

$$\frac{4^n}{2n+1} < (2n)^{\lfloor 2n \rfloor} \prod_{p \leq \frac{2n}{3}} p < 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{2n}}.$$

Sendo $2n+1 < (2n)^2$, podemos cancelar $4^{\frac{2n}{3}}$ do 1º e 3º membros da expressão acima para obtermos:

$$4^{\frac{n}{3}} < (2n)^{2+\sqrt{2n}}.$$

Disto, temos:

$$\frac{n \cdot \ln 4}{3} < (2 + \sqrt{2n}) \ln 2.$$

Claramente, isto é falso para n grande. De fato, se $n = 750$ temos ($1, 3 < \ln 4$ e $\ln 1500 < 7, 5$)

$$325 = \frac{750 \cdot 1,3}{3} < (2 + \sqrt{1500}) \ln(1500) < 41 \cdot 7,5 = 308.$$

Portanto, o resultado é verdadeiro para $n \geq 750$ e, por inspeção, ele também se verifica para $n < 750$, como pode ser visto pela sequência 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 751 de primos na qual cada um é menor do que duas vezes o seu predecessor.



Apêndice C - Uma Prova Elementar

Nas coberturas p -Sylow no Capítulo 3 usamos um Lema muito importante, que nos ajuda a determinar as coberturas p -Sylow do Grupo Simétrico S_n . Este Lema que enunciaremos e daremos uma demonstração elementar, pode ser encontrado em [11], porém demonstrado de uma maneira totalmente diferente da que daremos agora.

Lema 5.13 *Seja α uma permutação em S_n . Suponhamos que α tem decomposição com exatamente a_i i -ciclos, $a_i \geq 0$. Então $|C_{S_n}(\alpha)| = \prod (a_i!) i^{a_i}$, onde $n = a_1 + 2a_2 + 3a_3 + \dots + na_n$*

Demonstração: (Luís Farias/2010)

Sabemos, pelo Capítulo 1, que:

$$|S_n : C_{S_n}(\alpha)| = |\alpha^{S_n}|,$$

como $|S_n| = n!$ teremos que:

$$|C_{S_n}(\alpha)| = \frac{|S_n|}{|\alpha^{S_n}|} = \frac{n!}{|\alpha^{S_n}|}.$$

Agora vamos determinar o valor de $|\alpha^{S_n}|$. Temos que $\alpha^{S_n} = \{\beta\alpha\beta^{-1}; \beta \in S_n\}$. Vimos que α e $\beta\alpha\beta^{-1}$ possuem a mesma estrutura cíclica. Assim, para contarmos o número de elementos do conjunto α^{S_n} , basta contarmos o número de permutações com a mesma estrutura cíclica de α . Em nossa prova usaremos

fatos básicos de contagem como por exemplo: Permutações simples e circulares, Combinações simples.

Para esta contagem, precisaremos de início saber responder, a seguinte pergunta: Dados a_1, a_2, \dots, a_k k elementos distintos, quantos são os k -ciclos distintos que podemos formar? É claro que a resposta não é $k!$, pois estaríamos contando vários ciclos iguais como distintos, como por exemplo, se considerarmos os elementos 1, 2 e 3 e formarmos todas as $3! = 6$ permutações: (123), (132), (231), (213), (312) e (321) veja que existem somente 2 3-ciclos distintos, os outros são meras repetições.

Nós podemos pensar da seguinte maneira: Um k -ciclo pode ser pensado como uma representação dos k elementos distintos a_1, a_2, \dots, a_k em uma circunferência (uma representação circular).

Na circunferência, o que importa é a posição relativa dos elementos. Se girarmos a roda, fica sendo a mesma configuração e representamos o mesmo k -ciclo. Assim, para contarmos o número de k -ciclos distintos com os elementos a_1, a_2, \dots, a_k é o mesmo que contarmos o número de permutações circulares que podemos formar com os elementos a_1, a_2, \dots, a_k , que é fácil ver que é $(k - 1)!$.

Agora, contemos o número de permutações que possuem a mesma estrutura cíclica de α . Digamos que α possui a seguinte estrutura cíclica:

$$\alpha = \underbrace{(\cdot)(\cdot) \dots (\cdot)}_{a_1} \underbrace{(\cdot\cdot) \dots (\cdot\cdot)}_{a_2} \underbrace{(\cdot\cdot\cdot) \dots (\cdot\cdot\cdot)}_{a_3} \dots$$

onde $n = a_1 + 2a_2 + 3a_3 + \dots + na_n$.

Primeiramente, temos $\binom{n}{a_1}$ modos de escolher a_1 elementos que formarão os a_1 1-ciclos. Escolhidos os a_1 elementos temos somente 1 modo de colocá-los nos 1-ciclos. Feito isso, temos $\binom{n-a_1}{2a_2}$ modos de escolher estes $2a_2$ elementos temos $\frac{(2a_2)!}{a_2!2!}$ modos de dividir estes $2a_2$ elementos em a_2 grupos de 2 elementos. Feito esta divisão, temos $((2 - 1)!)^{a_2}$ modos de formar os a_2 2-ciclos. Do mesmo

modo, temos $\binom{n-a_1-2a_2}{3a_3}$ modos de escolher os $3a_3$ elementos que formarão os a_3 3-ciclos, feito isto, temos $\frac{(3a_3)!}{a_3!3^{a_3}}$ modos de dividir os $3a_3$ elementos em a_3 grupos de 3 elementos cada, depois temos $((3-1)!)^{a_3}$ modos de formar os a_3 3-ciclos. Prosseguindo, com o mesmo raciocínio, temos que o número de elementos do conjunto α^{S_n} é:

$$\binom{n}{a_1} \cdot \binom{n-a_1}{2a_2} \cdot \frac{(2a_2)!}{a_2!2^{a_2}} \cdot 1^{a_2} \cdot \binom{n-a_1-2a_2}{3a_3} \cdot \frac{(3a_3)!}{a_3!3^{a_3}} \cdot 2^{a_3} \cdot \binom{n-a_1-2a_2-3a_3}{4a_4} \cdot \frac{(4a_4)!}{4!^{a_4}a_4!} \cdot 3^{a_4} \cdot \dots$$

Reescrevendo o produto de outra forma, temos:

$$\binom{n}{a_1} \cdot \binom{n-a_1}{2a_2} \cdot \binom{n-a_1-2a_2}{3a_3} \cdot \dots \cdot \binom{n-a_1-\dots-(n-1)a_{n-1}}{na_n} \cdot \frac{(2a_2)!}{a_2!2^{a_2}} \cdot \frac{(3a_3)!}{a_3!3^{a_3}} \cdot \dots \cdot \frac{(na_n)!}{a_n!n^{a_n}} \cdot 1^{a_2} \cdot 2^{a_3} \cdot 3^{a_4} \cdot \dots \cdot (n-1)^{a_n}.$$

O produto,

$$\binom{n}{a_1} \cdot \binom{n-a_1}{2a_2} \cdot \dots \cdot \binom{n-a_1-\dots-(n-1)a_{n-1}}{na_n}$$

pode ser facilmente calculado, que é $\frac{n!}{a_1!(2a_2)!(3a_3)! \cdot \dots \cdot (na_n)!}$ (Pode ser encontrado em livros básicos de contagem).

Reescrevendo novamente o produto, temos que:

$$\begin{aligned} & \frac{n!}{a_1!(2a_2)!(3a_3)! \cdot \dots \cdot (na_n)!} \cdot \frac{(2a_2)!(3a_3)! \cdot \dots \cdot (na_n)! \cdot 1^{a_2} \cdot 2^{a_3} \cdot 3^{a_4} \cdot \dots \cdot (n-1)^{a_n}}{a_2!a_3!a_4! \cdot \dots \cdot a_n!2^{a_2} \cdot 3^{a_3} \cdot \dots \cdot n^{a_n}} \\ &= \frac{n!}{a_1!a_2!a_3! \cdot \dots \cdot a_n!} \cdot \left(\frac{1!}{2!}\right)^{a_2} \cdot \left(\frac{2!}{3!}\right)^{a_3} \cdot \left(\frac{3!}{4!}\right)^{a_4} \cdot \dots \cdot \left(\frac{(n-1)!}{n!}\right)^{a_n} \\ &= \frac{n!}{a_1!a_2!a_3! \cdot \dots \cdot a_n! \cdot 2a_2 \cdot 3a_3 \cdot 4a_4 \cdot \dots \cdot na_n} \end{aligned}$$

Como $|C_{S_n}(\alpha)| = \frac{n!}{|\alpha^n|}$, temos:

$$|C_{S_n}(\alpha)| = a_1!a_2!a_3! \cdot \dots \cdot a_n! \cdot 2a_2 \cdot 3a_3 \cdot 4a_4 \cdot \dots \cdot na_n,$$

isto é,

$$|C_{S_n}(\alpha)| = \prod (a_i!)i^{a_i}.$$

■

Referências Bibliográficas

- [1] BASTOS, G. G., *Notas de Álgebra*, Fortaleza: Editora Premius : Edições Livro Técnico, 2002. 160p.
- [2] BRUCKHEIMER, M.; BRIAN A. C.; MUIR, A., *Groups which are the union of three subgroups*. **American Mathematical Monthly**, v. 77, p. 52-57, 1970.
- [3] COHN, J. H. E., *On n -sum groups*. **Math. Scandinavia**, n. 75, p. 44- 58, 1994.
- [4] GRECO, D. *Sui gruppi che sono somma di quattro o cinque sottogruppi*. **Rend. Acc. Sc. Fis. Mat. Napoli**, v. 23, p. 49-59, 1956.
- [5] BRODIE, R. F. CHAMBERLAIN, L. C. KAPPE. *Finite coverings by normal subgroups*. **Proc. American Mathematical Society**. v. 104, p. 669 - 674, 1988.
- [6] M. A. BRODIE; L. -C. KAPPE. *Finite coverings by subgroups with a given property*. **Glasgow Mathematical**, v. 35, p. 179 - 188, 1993.
- [7] MEHRABADI K.; IRANMANESH A. *Finite Groups with p -Sylow covering*. **Bulletin of the Iranian Mathematical Society**, v. 33, p. 1 - 10, 2007.

- [8] NEUMANN, B. H. *A problem of Paul Erdős in groups*. **Journal of the Australian Mathematical Society**, v. 21, p. 467 - 472, 1976.
- [9] ROBINSON, D. A. *A Course in the theory of groups*, Springer - Verlag, Second Edition, 1996.
- [10] SANTOS, A. PLINIO dos. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 1998.
- [11] SUZUKI, M. *Group Theory*, New York: Springer - Verlag, v.1, 1982.
- [12] TOMKINSON, M. I., *Groups as the union of proper subgroups*. **Math. Scandinavia**, n. 81, p. 191 - 198, 1997.