Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Partições Minimais de Grupos

por

Michell Lucena Dias

sob orientação do

Prof. Dr. Martino Garonzi

Brasília - DF
2019

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Michell Lucena Dias

Partições Minimais de Grupos

Tese apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como requisito parcial para obtenção do título de Doutor em Matemática.

Prof. Dr. Martino Garonzi

Orientador

Brasília, Dezembro de 2019.

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Dias, Michell Lucena
DD541p Partições Minimais de Grupos / Michell Lucena Dias; orientador Martino Garonzi. -- Brasília, 2019.
85 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2019.

1. Grupos Finitos. 2. Partições. 3. Coberturas. I. Garonzi, Martino, orient. II. Título.

Aos meus pais, Mairon e Socorro.

Resumo

Seja G um grupo finito. Uma cobertura de G é uma lista de subgrupos próprios $H_1, \ldots, H_n$ de G com a propriedade de que $G = H_1 \cup \cdots \cup H_n$. Uma cobertura de G é dita ser uma partição de G se $H_i \cap H_j = 1$, sempre que $i \neq j$. Neste caso, dizemos que G é particionável.

Os grupos particionáveis foram completamente classificados por Baer, Kegel e Suzuki em 1961. Vamos usar a notação $\sigma(G)$ para o tamanho de uma cobertura de menor cardinalidade de G, dita cobertura minimal (usaremos a convenção $\sigma(G) = \infty$ quando G for cíclico), e vamos usar a notação $\rho(G)$ para o tamanho de uma partição minimal de G, se G é particionável. Claramente, para um grupo particionável temos que $\sigma(G) \leqslant \rho(G)$ pois toda partição é uma cobertura. Assim, no presente texto estamos interessados em explorar propriedades da igualdade $\sigma(G) = \rho(G)$.

Se G é um grupo particionável, obtemos que $\sigma(G) = \rho(G)$ se, e somente se, G é um produto direto $C_p \times C_p$, para algum primo p, ou G é um grupo de Frobenius sendo o núcleo de Frobenius um subgrupo normal minimal abeliano com complementos de Frobenius cíclicos. Além disso, calculamos ρ para todos os grupos projetivos particionáveis.

Palavras-chave: grupos finitos, coberturas, partições.

Abstract

Let G be a finite group. A cover of G is a list of proper subgroups $H_1, \ldots, H_n$ of G with the property that $G = H_1 \cup \cdots \cup H_n$. A cover is called partition of G if $H_i \cap H_j = 1$, whenever $i \neq j$. In this case, G is called partitionable.

The partitionable groups were completely classified by Baer, Kegel and Suzuki in 1961. We use the notation $\sigma(G)$ for the size of a cover with minimal cardinality of G, called minimal cover (we use the convention $\sigma(G) = \infty$ if G is a cyclic group), and we use the notation $\rho(G)$ for the size of a minimal partition of G, if G is partitionable. Clearly, for a partitionable group we have $\sigma(G) \leqslant \rho(G)$ because every partition is a cover. Thus, in the present text we are interested in exploring properties of equality $\sigma(G) = \rho(G)$.

If G is a partitionable group, we obtain that $\sigma(G) = \rho(G)$ if and only if G is a direct produt $C_p \times C_p$, for some prime p, or G is a Frobenius group with Frobenius kernel being an abelian minimal normal subgroup and Frobenius complement cyclic. Furthemore, we calculate ρ for all partitionable projective groups.

Keywords: finite groups, covers, partitions.

Lista de Símbolos

$\sigma(G)$	tamanho de uma cobertura minimal de um grupo G
$\rho(G)$	tamanho de uma partição minimal de um grupo G
S_n	grupo simétrico de grau n
A_n	grupo alternado de grau n
D_n	grupo diedral de ordem $2n$
Q_8	grupo dos quatérnios
$\mathbb{F}_q$	corpo de tamanho q
$\mathrm{GL}_n(q)$	grupo geral linear sobre $\mathbb{F}_q$
$\mathrm{PGL}_n(q)$	grupo projetivo geral linear sobre $\mathbb{F}_q$
$\mathrm{SL}_n(q)$	grupo especial linear sobre $\mathbb{F}_q$
$\mathrm{PSL}_n(q)$	grupo projetivo especial linear sobre $\mathbb{F}_q$
$S_Z(q)$	grupo de Suzuki de ordem $q^2(q-1)(q^2+1)$, com $q = 2^{2m+1}$
$\Phi(G)$	subgrupo de Frattini de um grupo G
$Fit(G)$	subgrupo de Fitting de um grupo G
$Z(G)$	centro de um grupo G

Sumário

Introdução

Seja G um grupo finito. Uma *cobertura* de G é uma lista de subgrupos próprios $H_1, \ldots, H_n$ de G com a propriedade de que $G = H_1 \cup \cdots \cup H_n$. Uma cobertura de G é dita ser uma *partição* de G se $H_i \cap H_j = 1$, sempre que $i \neq j$. Neste caso, dizemos que G é *particionável*. Ademais, cada um dos subgrupos H_i é dito ser um *membro* da cobertura.

Todo grupo não cíclico admite uma cobertura formada, por exemplo, por alguns de seus subgrupos cíclicos. Com efeito, observe que em um grupo cíclico, o seu gerador não pertence a nenhum de seus subgrupos próprios, ou seja, a definição de cobertura não faz sentido para grupos cíclicos. Por outro lado, nem todo grupo não cíclico admite uma partição.

Observe primeiramente que se $H_1, \ldots, H_n$ é uma partição de um grupo G e g^m é uma potência não idêntica de um elemento $g \in G$ tal que $g^m \in H_i$, para algum $i \in \{1, \ldots, n\}$, então $g \in H_i$. Além disso, se H é um subgrupo particionável de G com a propriedade de que $H \nsubseteq H_i$, para todo $i \in \{1, \ldots, n\}$ então $H \cap H_i, \ldots, H \cap H_n$ é uma partição de H.

Dito isto, a família dos grupos simétricos S_n nos dá uma lista infinita de grupos que não admitem partição. De fato, para $n = 6$, observe que os elementos

$$\begin{array}{rcl} \alpha & = & (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6) \\ \beta & = & (1 \quad 2 \quad 6 \quad 4 \quad 5 \quad 3) \\ \gamma & = & (1 \quad 6 \quad 3 \quad 2 \quad 5 \quad 4). \end{array}$$

são tais que $\alpha^3 = (1 \quad 4)(2 \quad 5)(3 \quad 6) = \beta^3$ e $\alpha^2 = (1 \quad 3 \quad 5)(2 \quad 4 \quad 6) = \gamma^2$. Logo, se S_6 admite uma partição, então α, β e γ precisam necessariamente estar num mesmo membro desta partição, mas $\langle \alpha, \beta, \gamma \rangle = S_6$, o que nos dá uma contradição.

Agora assuma que $n \geqslant 7$, que S_{n-1} não admite uma partição por hipótese de indução e seja H_i o estabilizador de $i \in \{1, \ldots, n-1\}$. Então

$$H_i \cong S_{n-1}$$

e H_i é um subgrupo maximal de S_n (lembre que um subgrupo $M \neq G$ de um grupo G é dito maximal em G se não existe $L \leqslant G$ com a propriedade de que $M \subsetneq L \subsetneq G$).

Suponha por absurdo que S_n admite uma partição $\mathscr{P}$. Então a lista de subgrupos formada pela interseção dos membros de $\mathscr{P}$ com H_i não pode ser uma partição de H_i. Portanto, $H_i \in \mathscr{P}$ para todo $i \in \{1, \ldots, n\}$ (pois são subgrupos maximais de S_n), contradizendo o fato de que para $n \geqslant 4$, a interseção $H_i \cap H_j$, com $i \neq j$, contém pelo menos uma transposição.

À luz de um resgate histórico, o primeiro artigo sobre partições de grupos foi publicado em 1906 por Miller em [26]. Ele mostrou que se $\mathscr{P}$ é uma partição de um grupo G tal que $|G| = p^m$ e H é membro de $\mathscr{P}$, então $|H| = p^a$ onde a divide m. Reciprocamente, se G é um grupo abeliano elementar de ordem p^m e a divide m, então G tem uma partição $\mathscr{P} = \{H_1, \ldots, H_n\}$, com $|H_i| = p^a$, $i = 1, \ldots, n$. Miller também provou que se $\mathscr{P}$ é uma partição de um p-grupo não abeliano G, então todos os elementos de G de ordem maior do que p pertencem ao mesmo membro de $\mathscr{P}$.

No ano de 1907, Cipolla em [3] definiu um *subgrupo fundamental* de um grupo G como sendo um subgrupo de G que é o centralizador de um elemento em $G - Z(G)$, onde $Z(G)$ denota o centro de G. O centro de um subgrupo fundamental é dito *normocentro*. O conjunto de todos os subgrupos fundamentais e o conjunto de todos os normocentros são coberturas de G.

Um grupo G tem pelo menos três subgrupos fundamentais (e três normocentros). Mais do que isso, G tem exatamente três subgrupos fundamentais (normocentros) se, e somente se, $\frac{G}{Z(G)}$ é o grupo de Klein de ordem 4. Em 1926, Scorza em [29] mostrou que um grupo G é coberto exatamente por três subgrupos próprios se, e somente se, G contém um subgrupo normal N tal que $\frac{G}{N}$ é o grupo de Klein.

Em 1939, Kontorovich em [23] caracterizou todos os grupos *completamente decomponíveis*, isto é, grupos que admitem uma partição tal que todo membro desta partição é um grupo cíclico. Em 1940, o autor em [24] também apresentou condições para que produtos diretos de grupos completamente decomponíveis seja completamente decomponível. Kontorovich também estudou grupos que não são completamente decomponíveis mas que todo subgrupo próprio é completamente decomponível.

Em 1950, Suzuki em [31] mostrou que um grupo não simples e não solúvel é completamente decomponível se, e somente se, é isomorfo a $\mathrm{PGL}(q)$, com

$q = p^h$ e p ímpar.

Os grupos particionáveis foram classificados por Baer, Kegel e Suzuki em 1961. Os autores provaram que um grupo é particionável se, e somente se, é isomorfo a um dos seguintes grupos:

1) S_4,

2) um p-grupo com $H_p(G) \neq G$, onde $H_p(G) = \langle g \in G : g^p \neq 1 \rangle$,

3) um grupo do tipo Hughes-Thompson,

4) um grupo de Frobenius,

5) $\mathrm{PSL}(2, p^n)$ com $p^n \geqslant 4$,

6) $\mathrm{PGL}(2, p^n)$ com $p^n \geqslant 5$ e p é ímpar,

7) $S_Z(2^{2n+1})$, $n \geqslant 1$.

Assim, observamos que a propriedade de um grupo ter partição é uma condição muito forte, posto a seletividade da lista acima.

No ano de 1973, Isaacs publicou um artigo [17] relativo aos grupos *igualmente particionáveis*, isto é, grupos que admitem uma partição tal que todos os membros têm mesma ordem. Isaacs melhorou um resultado obtido por Miller em [26] provando que todo grupo igualmente particionável é um p-grupo de expoente p.

Em 1990, Khukhro em [22] provou que para um p-grupo G com $|G| > p$, as seguintes afirmações são equivalentes:

a) G tem uma partição

b) $H_p(G) \neq G$

c) $G = G_1\langle\alpha\rangle$ onde G_1 é um subgrupo de G de índice p e α é um elemento de G de ordem p induzindo em G_1 um automorfismo.

Consoante a Cohn em [4], vamos usar a notação $\sigma(G)$ para denotar o tamanho de uma cobertura de menor cardinalidade de um grupo G, dita *cobertura minimal* (usaremos a convenção que $\sigma(G) = \infty$ quando G for cíclico), e consoante a Sizemore em [30], vamos usar também a notação $\rho(G)$ para denotar o tamanho de uma *partição minimal* de G, se G é particionável.

Os invariantes σ e ρ têm despertado interesse também nos anos recentes. Detomi e Lucchini em [5] estudaram a estrutura dos grupos G que não contém um subgrupo normal N tal que $\sigma(G) = \sigma\left(\frac{G}{N}\right)$. Observe que a desigualdade $\sigma(G) \leqslant \sigma\left(\frac{G}{N}\right)$ sempre ocorre pois toda cobertura para um quociente de G nos dá uma cobertura para G. Garonzi e Lucchini em [11] classificaram todos os grupos cujas coberturas que não têm subcoberturas próprias são minimais. Além disso, Tomkinson em [32] calculou σ para grupos solúveis mostrando que

$$\sigma(G) = q + 1,$$

onde q é a menor ordem de um fator principal de um grupo solúvel G com mais de um complemento (lembre que um subgrupo $N \neq 1$ de um grupo G é dito normal minimal em G se não existe $L \trianglelefteq G$ com a propriedade de que $1 \subsetneq L \subsetneq N$, e também que um fator principal de G é um subgrupo normal minimal de um quociente de G).

Claramente, temos que $\sigma(G) \leqslant \rho(G)$ pois toda partição é uma cobertura. Observe que para cobrir C_p^2 precisamos necessariamente de todos os seus subgrupos, que em número são $p + 1$. Em particular, esta lista constitui a única cobertura possível, e neste caso os conceitos de cobertura e partição se confundem, ou seja, $\sigma(C_p^2) = \rho(C_p^2)$.

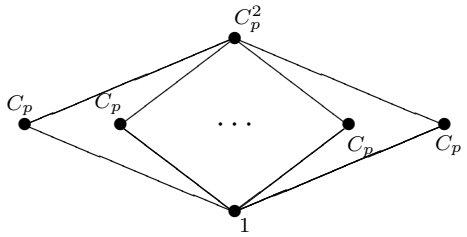

Diagrama 1: Reticulado de Subgrupos de C_p^2

Temos também que $\sigma(S_4) = 4$ e $\rho(S_4) = 10$. Como veremos no Capítulo 2, $\sigma(S_4) = 4$ está relacionado ao fato de que $\frac{S_4}{C_2^2} \cong S_3$ e daí $\sigma(S_4) \leqslant \sigma(S_3) = 4$ e do fato de que não existe $N \trianglelefteq S_4$ com a propriedade de que $\frac{S_4}{N} \cong C_2^2$. Ademais, uma partição de tamanho 10 de S_4 foi exibida primeiramente em [30] utilizando o GAP mas que pode ser obtida também de modo independente

utilizando apenas propriedades elementares de uma partição.

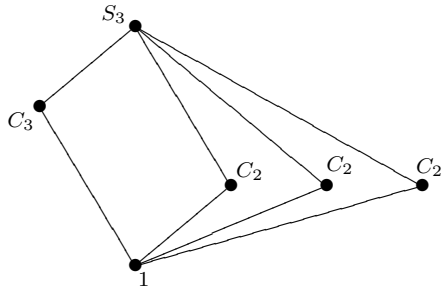

Diagrama 2: Reticulado de Subgrupos de S_3

Foguel e Sizemore em [7] e [30] levantaram um interessante problema de estudar quando ocorre a igualdade entre σ e ρ de um grupo G. Assim, no presente texto estamos interessados em explorar propriedades da igualdade

$$\sigma(G) = \rho(G),$$

isto é, estamos interessados em classificar os grupos G que admitem uma cobertura minimal que também é partição.

Podemos enunciar os nossos principais resultados como segue abaixo.

Teorema 0.0.1 *Seja G um grupo particionável. Então $\sigma(G) = \rho(G)$ se, e somente se, G é um produto direto $C_p \times C_p$, para algum primo p, ou G é um grupo de Frobenius sendo o núcleo de Frobenius um subgrupo normal minimal abeliano com os complementos de Frobenius cíclicos.*

Seja $q \geqslant 4$ uma potência de um primo e considere os grupos projetivos particionáveis $\mathrm{PGL}_2(q)$, com $q \geqslant 4$, e $\mathrm{PSL}_2(q)$, com $q \geqslant 5$ ímpar. Bryce, Fedri e Serena em [2] mostraram que

$$\sigma(\mathrm{PSL}_2(5)) = 10, \qquad \sigma(\mathrm{PSL}_2(7)) = 15, \qquad \sigma(\mathrm{PSL}_2(9)) = 16$$

e em todos os outros casos

$$\sigma(\mathrm{PSL}_2(q)) = \sigma(\mathrm{PGL}_2(q)) = \begin{cases} \frac{1}{2}q(q+1) & \text{se } q \text{ é par} \\ \frac{1}{2}q(q+1)+1 & \text{se } q \text{ é ímpar} \end{cases}.$$

O seguinte resultado combinado com as informações acima mostram que $\sigma < \rho$ para os grupos $\mathrm{PGL}_2(q)$ e $\mathrm{PSL}_2(q)$.

Teorema 0.0.2 *Seja $q = p^f$ uma potência de um primo p. Então*

$$\begin{aligned} \rho(\mathrm{PGL}_2(q)) &= q^2 + 1, \qquad \text{se } q \geqslant 3 \\ \rho(\mathrm{PSL}_2(q)) &= q^2 + 1, \qquad \text{se } q \geqslant 7. \end{aligned}$$

Observe que ele abrange todos os grupos projetivos particionáveis pois $\mathrm{PSL}_2(q) \cong \mathrm{PGL}_2(q)$ se q é par e $\mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4)$.

Mais geralmente, o *modus operandi* que adotamos na elaboração das partições de um grupo G no presente texto tem como norte:

- Escolha de um subgrupo. Em geral escolhemos os subgrupos maximais exatamente porque buscamos partições minimais. Entretanto, um tal subgrupo precisa respeitar certos princípios. Destacamos, por exemplo, o argumento que foi introduzido no estudo de uma possível partição de S_6: se $H_1, \ldots, H_n$ é uma partição de um grupo G e g^m é uma potência não idêntica de um elemento $g \in G$ tal que $g^m \in H_i$, para algum $i \in \{1, \ldots, n\}$, então necessariamente $g \in H_i$.

- Decisão de até quantas cópias do subgrupo H escolhido podemos utilizar.

- Análise de quantos elementos já foram cobertos pela partição. Assim, uma vez que escolhemos um subgrupo e decidimos até quantas cópias deste podem ser consideradas, resta-nos contabilizar quantos elementos ainda precisam ser alcançados, quais suas ordens e quais os possíveis subgrupos que ainda podem ser incluídos na partição. Esta identificação está associada, por exemplo, a comparação das ordens do subgrupos com índices dos membros da partição. De fato, sendo $H_1, \ldots, H_n$ uma partição de G temos que $|H_i||H_j| = |H_iH_j| \leqslant |G|$ e assim $|H_i| \leqslant |G : H_j|$ para quaisquer $i, j \in \{1, \ldots, n\}$.

Uma das dificuldades apresentadas neste estudo está no cálculo de ρ para os grupos de Frobenius e que, uma vez explícito, representa o análogo para o Teorema de Tomkinson para os grupos particionáveis. Como veremos no Capítulo 3, tal dificuldade está relacionada ao problema de encontrar em um espaço vetorial uma específica lista de seus subespaços com interseção trivial 2 a 2. Com efeito, $\rho(C_3^3 \rtimes C_2) = 10$ é o contraexemplo que apresentamos para a conjectura levantada em [10] de que $\rho(G) = |N| + 1$, onde G é um grupo de Frobenius com núcleo de Frobenius N.

Dispusemos o presente texto em 6 capítulos, respeitando os grupos que estão em voga na classificação dos grupos particionáveis.

No Capítulo 1 apresentamos as definições de cobertura e partição de um grupo finito e introduzimos propriedades elementares dos invariantes σ e ρ que fermentam a discussão pretendida. Além disso, calculamos ρ para p-grupos abelianos elementares e estudamos a igualdade $\sigma = \rho$ sob a hipótese de nilpotência.

No Capítulo 2 descrevemos as partições do grupo simétrico S_4.

No Capítulo 3 introduzimos um arcabouço teórico sobre a estrutura dos grupos de Frobenius, selecionamos alguns apontamentos e mostramos alguns resultados que relacionam p-nilpotência com fatores principais e o subgrupo de Frattini. Além disso, caracterizamos os grupos de Frobenius que satisfazem a igualdade $\sigma = \rho$.

No Capítulo 4 estudamos a igualdade $\sigma = \rho$ para os grupos do tipo Hughes-Thompson, que são grupos que não são p-grupos e tem a propriedade de $H_p(G) \neq G$, onde $H_p(G) = \langle g \in G : g^p \neq 1 \rangle$.

No Capítulo 5 mostramos que os grupos projetivos particionáveis não satisfazem a igualdade $\sigma = \rho$. Descrevemos também partições de $\mathrm{PGL}_2(5)$, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(9)$ e $\mathrm{PSL}_2(11)$. Além disso, calculamos ρ para todos os grupos projetivos particionáveis.

No Capítulo 6, por fim, discutimos sobre como os grupos de Suzuki não satisfazem a igualdade $\sigma = \rho$.

Enfatizamos que os resultados que compõem este texto podem ser consultados em [10].

Capítulo 1

Partições de um Grupo

Todos os grupos abordados no presente texto serão finitos.

O objetivo deste capítulo é definir os conceitos de *cobertura* e *partição* de um grupo. Apresentamos os invariantes $\sigma(G)$ e $\rho(G)$ para um grupo G, bem como abordamos aspectos elementares de suas propriedades, os quais serão utilizados ao longo de todo texto. Além disso, calculamos $\rho(G)$ para p-grupos abelianos elementares e estudamos a igualdade $\sigma(G) = \rho(G)$ sob a hipótese de nilpotência.

Será requerido por parte do leitor conhecimentos básicos acerca da Teoria dos Grupos Finitos para o qual sugerimos [28].

1.1 Coberturas e Partições

Seja G um grupo finito. Uma *cobertura* de G é uma lista de subgrupos próprios $H_1, \ldots, H_n$ de G com a propriedade de que $G = H_1 \cup \cdots \cup H_n$. Uma cobertura de G é dita ser uma *partição* de G se $H_i \cap H_j = 1$, sempre que $i \neq j$. Neste caso, dizemos que G é *particionável*. Ademais, cada um dos subgrupos H_i é dito ser um *membro* da cobertura.

Todo grupo não cíclico admite uma cobertura formada, por exemplo, por alguns de seus subgrupos cíclicos. Com efeito, observe que em um grupo cíclico, o seu elemento gerador não pertence a nenhum de seus subgrupos próprios, ou seja, a definição de cobertura não faz sentido para grupos cíclicos. Por outro lado, nem todo grupo não cíclico admite uma partição. De modo elementar, por exemplo, podemos citar o grupo dos quatérnios Q_8,

apresentado por

$$Q_8 = \langle i, j, k \quad | \quad i^2 = j^2 = k^2 = ijk, \quad (ijk)^2 = 1 \rangle.$$

De fato, observe que se existisse uma partição $\mathscr{P}$ de Q_8, então os seus subgrupos de ordem 4 seriam membros de $\mathscr{P}$ pois são subgrupos cíclicos e maximais de Q_8, o que nos leva a um absurdo posto que eles têm interseção não trivial.

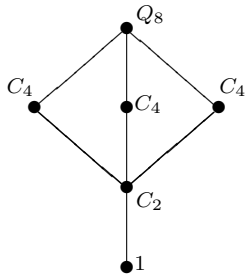

Diagrama 3: Reticulado de Subgrupos de Q_8

A classe dos grupos particionáveis não é fechada para produtos diretos finitos, como mostraremos abaixo.

No lema a seguir, usamos o fato de que se $H_1, \ldots, H_n$ é uma partição de um grupo G e H é um subgrupo particionável de G com a propriedade de que $H \nsubseteq H_i$, para todo $i \in \{1, \ldots, n\}$ então $H \cap H_1, \ldots, H \cap H_n$ é uma partição de H. Ademais, lembre também que um subgrupo $M \neq G$ de G é dito ser *maximal* em G se não existe $L \leqslant G$ tal que $M \subsetneq L \subsetneq G$.

Lema 1.1.1 *Se G é um grupo particionável e H e K são dois distintos subgrupos de G que não admitem partição, então ocorre $\langle H, K \rangle \neq G$ ou $H \cap K = 1$. Em particular, se H e K são dois distintos subgrupos maximais de G que não admitem partição, então $H \cap K = 1$.*

Demonstração: Se $\mathscr{P}$ é uma partição de G, então a interseção de membros de $\mathscr{P}$ com H e com K não pode nos dar uma partição de H e K, respectivamente, porque estes subgrupos não são particionáveis por hipótese. Isto implica que existem membros A e B de $\mathscr{P}$ tais que $H \leqslant A$ e $K \leqslant B$. Assim, se $G = \langle H, K \rangle$ então A e B devem ser distintos, portanto, $H \cap K \leqslant A \cap B = 1$.
■

No corolário adiante, que nos dá condições suficientes para decidir quando um produto direto finito não admite partição, usamos o fato de que se G é um grupo finito não cíclico, então G tem mais do que um subgrupo maximal.

De fato, se M é o único subgrupo maximal de G, então $M = M^g$ para todo $g \in G$. Logo, M é normal em G e $\frac{G}{M} = \langle gM \rangle$ é cíclico de ordem prima, com $g \notin M$. Assim, $G = \langle g \rangle M$ e $M \neq 1$ uma vez que G é não cíclico. Portanto, $\langle g \rangle$ é um subgrupo maximal de G distinto de M, o que nos dá um absurdo.

Corolário 1.1.2 *Se A e B são grupos não triviais de ordens coprimas, então o produto direto $A \times B$ não é particionável.*

Demonstração: Vamos utilizar indução em $|G|$, onde $G = A \times B$, isto é, assuma que o resultado é válido para todos os grupos com ordem menor do que $|G|$.

Suponha por absurdo que G é particionável. Como $|A|$ e $|B|$ são coprimas, então G é cíclico se, e somente se, A e B são cíclicos, e neste caso G não admite uma partição. Assim, podemos assumir que B não é cíclico. Portanto B admite pelo menos dois subgrupos maximais distintos, digamos, M_1 e M_2, ambos diferentes de 1.

Segue que

$$L_i = A \times M_i,$$

para $i \in \{1, 2\}$, não admitem partição por hipótese de indução. Uma vez que estes subgrupos são maximais em G, temos $G = \langle L_1, L_2 \rangle$ e, pelo Lema 1.1.1, vem $L_1 \cap L_2 = 1$, contradizendo o fato de que ambos contêm $A \times 1$. ■

Exemplos menos elementares de grupos sem partição podem ser encontrados na família dos grupos simétricos. Mostraremos agora que S_n não têm partição para $n \geqslant 6$. O fato de que S_3, S_4 e S_5 têm partição será mostrado no decorrer do texto.

Lema 1.1.3 *O grupo simétrico S_n é gerado pelos ciclos $(1 \quad 2)$ e $(1 \quad 2 \ldots n)$.*

Demonstração: Vamos denotar $\alpha = (1 \quad 2 \ldots n)$. Vem

$$\begin{array}{rcl} \alpha(1 \quad 2)\alpha^{-1} & = & (2 \quad 3) \\ \alpha(2 \quad 3)\alpha^{-1} & = & (3 \quad 4) \\ & \vdots & \\ \alpha(n-2 \quad n-1)\alpha^{-1} & = & (n-1 \quad n) \end{array}$$

e assim as transposições da forma $(i \quad i+1)$ pertencem a $\langle (1 \quad 2), \alpha \rangle$, para todo $i \in \{1, \ldots, n-1\}$.

Agora observe que

$$\begin{array}{rcl} (2 \quad 3)(1 \quad 2)(2 \quad 3) & = & (1 \quad 3) \\ (3 \quad 4)(1 \quad 3)(3 \quad 4) & = & (1 \quad 4) \\ & \vdots & \\ (n-1 \quad n)(1 \quad n-1)(n-1 \quad n) & = & (1 \quad n) \end{array}$$

e assim as transposições da forma $(1 \quad i)$ também pertencem a $\langle (1 \quad 2), \alpha \rangle$, para todo $i \in \{1, \ldots, n\}$. Com isso, obtemos

$$(i \quad j) = (1 \quad i)(1 \quad j)(1 \quad i) \in \langle (1 \quad 2), \alpha \rangle,$$

ou seja, quaisquer transposições de S_n pertencem a $\langle (1 \quad 2), \alpha \rangle$. Portanto, $S_n = \langle (1 \quad 2), \alpha \rangle$ pois qualquer permutação em S_n pode ser escrito como produto de transposições. ■

Na proposição a seguir, usaremos o fato de que se $H_1, \ldots, H_n$ é uma partição de um grupo G e g^m é uma potência não idêntica de um elemento $g \in G$ tal que $g^m \in H_i$, para algum $i \in \{1, \ldots, n\}$, então $g \in H_i$.

Proposição 1.1.4 *Os grupos simétricos S_n não admitem partição, para $n \geqslant 6$.*

Demonstração: Vamos utilizar indução em n.

Considere primeiramente $n = 6$ e sejam

$$\begin{array}{rcl} \alpha & = & (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6) \\ \beta & = & (1 \quad 2 \quad 6 \quad 4 \quad 5 \quad 3) \\ \gamma & = & (1 \quad 6 \quad 3 \quad 2 \quad 5 \quad 4). \end{array}$$

Então $\alpha^3 = (1 \quad 4)(2 \quad 5)(3 \quad 6) = \beta^3$ e $\alpha^2 = (1 \quad 3 \quad 5)(2 \quad 4 \quad 6) = \gamma^2$. Suponha por contradição que S_6 tenha uma partição $\mathscr{P}$ e seja H o único membro de $\mathscr{P}$ tal que $\alpha^2 \in H$. Como $\alpha^2 = \gamma^2$ temos $\alpha \in H$ e também $\gamma \in H$. Por outro lado, H também contém $\alpha^3 = \beta^3$. Neste caso, H contém β, o que nos dá uma contradição pois $\langle \alpha, \beta, \gamma \rangle = H = S_6$ uma vez que

$$(1 \quad 2) = \alpha^3 \gamma \beta \gamma \alpha^3$$

e $S_6 = \langle \alpha, (1 \quad 2) \rangle$ (Lema 1.1.3).

Agora assuma que $n \geqslant 7$, que S_{n-1} não admite uma partição por hipótese de indução e seja H_i o estabilizador de $i \in \{1, \ldots, n-1\}$. Então $H_i \cong S_{n-1}$.

Suponha por absurdo que S_n admite uma partição $\mathscr{P}$. Então a lista de subgrupos formada pela interseção dos membros de $\mathscr{P}$ com H_i não pode ser uma partição de H_i. Portanto, $H_i \in \mathscr{P}$ para todo $i \in \{1, \ldots, n\}$ (pois são subgrupos maximais de S_n), contradizendo o fato de que para $n \geqslant 4$, a interseção $H_i \cap H_j$, com $i \neq j$, contém pelo menos uma transposição. ∎

Os grupos particionáveis foram classificados por Baer, Kegel e Suzuki em 1961. (Um bom relato sobre como esta classificação foi completada pode ser consultada em [34].)

Teorema 1.1.5 (Baer, Kegel, Suzuki, 1961) *Um grupo G é particionável se, e somente se, G é isomorfo a um dos seguintes grupos:*

1) S_4,

2) *um p-grupo com $H_p(G) \neq G$, onde $H_p(G) = \langle g \in G : g^p \neq 1 \rangle$,*

3) *um grupo do tipo Hughes-Thompson,*

4) *um grupo de Frobenius,*

5) $\mathrm{PSL}(2, p^n)$ *com* $p^n \geqslant 4$,

6) $\mathrm{PGL}(2, p^n)$ *com* $p^n \geqslant 5$ *e p é ímpar,*

7) $S_Z(2^{2n+1})$, $n \geqslant 1$.

Enfatizamos que um grupo do tipo Hughes-Thompson será definido no Capítulo 4, os grupos de Frobenius serão definidos no Capítulo 3, os grupos projetivos lineares $\mathrm{PSL}_2(p^n)$ e $\mathrm{PGL}_2(p^n)$ serão definidos no Capítulo 5 e os grupos de Suzuki serão definidos no Capítulo 6.

Consoante a [4], vamos usar a notação $\sigma(G)$ para denotar o tamanho de uma *cobertura minimal* de um grupo G, ou seja, escreveremos $\sigma(G) = n$ se G pode ser escrito como união de n de seus subgrupos próprios e não pode ser escrito como união de um número menor de seus subgrupos próprios. Se G é um grupo cíclico, usaremos a convenção que $\sigma(G) = \infty$. Consoante a [30], vamos usar também a notação $\rho(G)$ para denotar o tamanho de uma *partição minimal* de G, se G é particionável.

Claramente, temos que $\sigma(G) \leqslant \rho(G)$ pois toda partição é uma cobertura. Foguel e Sizemore em [7] e [30] levantaram um interessante problema de

estudar quando ocorre a igualdade. Assim, estamos interessados em explorar propriedades da igualdade

$$\sigma(G) = \rho(G),$$

isto é, estamos interessados em classificar os grupos G que admitem uma cobertura minimal que também é partição.

Observe que se $H_1, \ldots, H_n$ é uma partição de G, então

$$|G| = 1 + \sum_{i=1}^{n}(|H_i| - 1) = 1 - n + \sum_{i=1}^{n}|H_i|.$$

Apresentaremos agora algumas propriedades envolvendo os invariantes $\sigma(G)$ e $\rho(G)$ de um grupo G.

Lema 1.1.6 *Seja G um grupo finito.*

a) $\sigma(G) > 2$.

b) Se N é um subgrupo normal de G então $\sigma(G) \leqslant \sigma(\frac{G}{N})$.

Demonstração: (a) Suponha por absurdo que $G = H_1 \cup H_2$, onde H_1 e H_2 são subgrupos próprios de G e distintos. Assim, considere $g \in H_1 - H_2$. Logo, para todo $h \in H_2$ temos $gh \in H_1$ e, consequentemente, $h \in H_1$. Neste caso, $H_2 \subseteq H_1$ e $G = H_1$, uma contradição.

(b) Basta observar que toda cobertura do quociente $\frac{G}{N}$ nos dá uma cobertura de G. ∎

Em particular, o item (ii) do lema anterior nos dá

$$\sigma(G_1 \times \cdots \times G_n) \leqslant min\{\sigma(G_1), \ldots, \sigma(G_n)\}.$$

Lema 1.1.7 $\sigma(C_p^2) = \rho(C_p^2) = p + 1$.

Demonstração: Para cobrir C_p^2 precisamos necessariamente de todos os seus subgrupos, que em número são $p+1$. Em particular, esta lista constitui a única cobertura possível, e neste caso os conceitos de cobertura e partição se confundem.

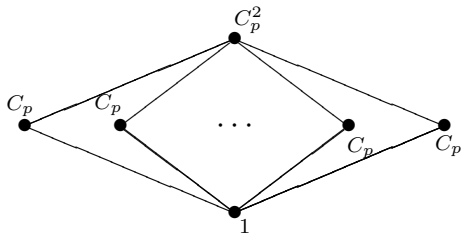

Diagrama 4: Reticulado de Subgrupos de C_p^2

■

Lema 1.1.8 *Seja G um grupo particionável. Então $\rho(G) < |G|$.*

Demonstração: Seja $H_1, \ldots, H_n$ uma partição de G, com $n = \rho(G)$. Então $|H_i| \geqslant 2$ para todo $i \in \{1, \ldots, n\}$, e assim,

$$|G| = 1 - n + \sum_{i=1}^{n} |H_i| \geqslant 1 - n + 2n = 1 + n.$$

Uma vez que qualquer partição de tamanho $\rho(G)$ consiste de subgrupos não triviais, segue que $\rho(G) \leqslant |G| - 1$. ■

Lema 1.1.9 *Seja $\mathscr{P} = \{H_1, \ldots, H_n\}$ uma partição de um grupo G com $|H_i| > 1$ para todo $i \in \{1, \ldots, n\}$. Então $|\mathscr{P}| \geqslant 1 + |H_i|$ para todo $i \in \{1, \ldots, n\}$. Se H_i é normal em G e $|G : H_i|$ é um número primo, então $|\mathscr{P}| = 1 + |H_i|$.*

Demonstração: Fixe $i \in \{1, \ldots, n\}$ e tome $j \in \{1, \ldots, n\}$, com $i \neq j$. Uma vez que $H_i \cap H_j = 1$ pois $\mathscr{P}$ é uma partição, temos

$$|G| \geqslant |H_i H_j| = |H_i||H_j| \Longrightarrow |H_j| \leqslant |G : H_i|$$

e daí

$$\begin{array}{rcl} |G| & = & 1 - n + \sum_{i=1}^{n} |H_i| \\ & \leqslant & 1 - n + |H_i| + \sum_{k \neq i}^{n} |G : H_i| \\ & = & 1 - n + |H_i| + (n-1)|G : H_i| \\ & = & (n-1)(|G : H_i| - 1) + |H_i| \end{array}$$

e portanto

$$|G| - |H_i| \leqslant (n-1)(|G:H_i| - 1) \Longrightarrow$$
$$|G| - |H_i| \leqslant (n-1)\left(\frac{|G|-|H_i|}{|H_i|}\right)$$

e isso implica que $|\mathscr{P}| = n \geqslant 1 + |H_i|$.

Agora suponha H_i normal em G. Então $H_iH_j \leqslant G$ e $|H_iH_j| = |H_i||H_j|$ divide $|G|$, donde $|H_j|$ divide $|G : H_i|$. Assim, se $|G : H_i|$ é um número primo, como $|H_j| \neq 1$ temos $|H_j| = |G : H_i|$ para todo $j \neq i$ e a desigualdade discutida acima se torna uma igualdade. ■

Considerando $H_1, \ldots, H_n$ uma partição de um grupo G, observe que utilizamos na demonstração do lema acima o argumento que $|H_j| \leqslant |G : H_i|$, para todo $i, j \in \{1, \ldots, n\}$, com $i \neq j$. Apesar de sua simplicidade, esse detalhe será um critério útil quando estivermos interessados em determinar explicitamente uma partição de G, como faremos adiante.

Sendo m um número real, vamos usar a notação $\lceil m \rceil$ para indicar o menor número inteiro n tal que $n \geqslant m$.

Corolário 1.1.10 *Se G é um grupo particionável, então $\rho(G) \geqslant 1 + \lceil \sqrt{|G|} \rceil$.*

Demonstração: É suficiente mostrar que $\rho(G) \geqslant 1 + \sqrt{|G|}$.

Seja $\mathscr{P} = \{H_1, \ldots, H_n\}$ uma partição de G. Se existe $i \in \{1, \ldots, n\}$ tal que $|H_i| \geqslant \sqrt{|G|}$, então pelo Lema 1.1.9 temos $\rho(G) \geqslant 1 + |H_i| \geqslant 1 + \sqrt{|G|}$. Suponha agora $|H_i| < \sqrt{|G|}$ para todo $i \in \{1, \ldots, n\}$. Assim

$$|G| = 1 - n + \sum_{i=1}^{n} |H_i| < 1 - n + n\sqrt{|G|} \Longrightarrow$$
$$n > \frac{|G|-1}{\sqrt{|G|}-1} = \sqrt{|G|} + 1.$$

■

Corolário 1.1.11 *Se G é um grupo particionável com um subgrupo normal cíclico N de índice primo, então $\rho(G) = 1 + |N|$.*

Demonstração: Seja $N = \langle g \rangle$ um subgrupo normal cíclico de G de índice primo. Se $\mathscr{P} = \{H_1, \ldots, H_n\}$ é uma partição de G, então $g \in H_i$ para algum $i \in \{1, \ldots, n\}$, e portanto $N = H_i$. Pelo Lema 1.1.9 segue que $|\mathscr{P}| = 1 + |N|$. Logo, $\rho(G) = 1 + |N|$. ■

Em particular, para o grupo diedral D_n de ordem $2n$ temos $\rho(D_n) = n+1$.

Corolário 1.1.12 *Se G é um grupo particionável com $|G| = pq$, onde p e q são primos distintos, então $\rho(G) = 1 + max\{p, q\} = \sigma(G)$.*

Demonstração: Considere $p < q$. Então pelos Teoremas de Sylow existe um único subgrupo normal H de G com $|H| = q$. Assim, pelo Lema 1.1.9, como $p = |G : H|$, concluímos $\rho(G) = 1 + |H| = 1 + q = 1 + max\{p, q\}$. Ademais, neste caso, observe que as definições de ρ e σ se confundem. ■

Lema 1.1.13 *Sejam G e H grupos particionáveis, com $H \leqslant G$. Então $\rho(H) \leqslant \rho(G)$.*

Demonstração: Pelo Lema 1.1.8, vem $\rho(H) < |H|$.

Seja agora $H_1, \ldots, H_n$ uma partição de G, com $\rho(G) = n$. Se existe $i \in \{1, \ldots, n\}$ tal que $H \subseteq H_i$, então pelo Lema 1.1.9 temos

$$\rho(G) \geqslant 1 + |H_i| \geqslant 1 + |H| > |H| \geqslant \rho(H).$$

Assumindo agora que $H \nsubseteq H_i$ para todo $i \in \{1, \ldots, n\}$, então

$$H_1 \cap H, \ldots, H_n \cap H$$

é uma partição de H de tamanho $n = \rho(G)$.

Logo, $\rho(H) \leqslant \rho(G)$. ■

Os lemas 1.1.14, 1.1.15 1.1.16 e 1.1.17 a seguir estão diretamente associados à demonstração do Teorema 1.1.18.

Lema 1.1.14 *Sejam G um grupo e $H, A_1 \ldots, A_n$ subgrupos de G tal que $H(A_1 \cap \cdots \cap A_n) = G$. Seja $A = A_1 \cup \cdots \cup A_n$. Então $|G||H \cap A| = |H||A|$.*

Demonstração: Considere primeiramente a função $\varphi : H \times A \longrightarrow G$ dada por

$$(h, a) \longmapsto ha.$$

Para $l \in G$ temos $(h, a) \in \varphi^{-1}(l)$ se, e somente se, $ha = l$, isto é, $la^{-1} = h \in H$, e em especial $a \in Hl$. Isto significa que (h, a) é determinado pela escolha de a em Hl, e assim $\varphi^{-1}(l)$ está em correspondência biunívoca com $Hl \cap A$.

Agora escreva $l = kx$, com $k \in H$ e $x \in A_1 \cap \cdots \cap A_n$. Assim,

$$Hl \cap A = (H \cap A)x.$$

Em particular, isso implica que $|\varphi^{-1}(l)| = |H \cap A|$ para todo $l \in G$, e o resultado segue. ∎

O lema abaixo foi dado por Tomkinson em [32].

Lema 1.1.15 *Sejam G um grupo, N um subgrupo normal de G, com $N \neq G$, e $U_1, \ldots, U_h, V_1, \ldots, V_k$, subgrupos próprios de G tais que cada $U_1, \ldots, U_h$ contém N, cada $V_1, \ldots, V_k$ suplementa N, e também $\beta_1 \leqslant \cdots \leqslant \beta_k$, onde $\beta_i = |G : V_i|$ para $i = 1, \ldots, k$. Se*

$$U_1 \cup \cdots \cup U_h \cup V_1 \cup \cdots \cup V_k = G \qquad e \qquad U_1 \cup \cdots \cup U_h \neq G,$$

então $\beta_1 \leqslant k$. Além disso, se $\beta_1 = k$, então $\beta_1 = \cdots = \beta_k = k$ e $V_i \cap V_j \leqslant U_1 \cup \cdots \cup U_h$ para quaisquer $i \neq j$ em $\{1, \ldots, k\}$.

Demonstração: Escreva $|U_1 \cup \cdots \cup U_h| = \gamma|G|$, onde $\gamma \leqslant 1$, e fixe $i \in \{1, \ldots, k\}$. Uma vez que $V_i N = G$, pelo Lema 1.1.14, vem

$$|V_i \cap (U_1 \cup \cdots \cup U_h)| = \frac{\gamma|G||V_i|}{|G|} = \gamma|V_i| = \frac{\gamma}{\beta_i}|G|.$$

Portanto,

$$|V_i - (U_1 \cup \cdots \cup U_h)| = \frac{1-\gamma}{\beta_i}|G|.$$

Uma vez que $G - (U_1 \cup \cdots \cup U_h) = (V_1 \cup \cdots \cup V_k) - (U_1 \cup \cdots \cup U_h)$, temos que

$$|(V_1 \cup \cdots \cup V_k) - (U_1 \cup \cdots \cup U_h)| = (1-\gamma)|G|.$$

Assim, escrevendo da seguinte forma

$$G - (U_1 \cup \cdots \cup U_h) \subseteq \bigcup_{i=1}^{k} (V_i - (U_1 \cup \cdots \cup U_h),$$

as igualdades acima em destaque implicam que

$$(1-\gamma)|G| \leqslant (1-\gamma)|G| \left(\frac{1}{\beta_1} + \cdots + \frac{1}{\beta_k} \right),$$

e como $1 - \gamma > 0$, vem

$$1 \leqslant \sum_{i=1}^{k} \frac{1}{\beta_i} \leqslant \frac{k}{\beta_1},$$

e então $\beta_1 \leqslant k$.

Se $\beta_1 = k$, então

$$1 = \frac{1}{\beta_1} + \cdots + \frac{1}{\beta_k} = \frac{1}{k} + \cdots + \frac{1}{\beta_k}$$

donde $\frac{k-1}{k} \leqslant \frac{k-1}{\beta_2}$ e portanto $\beta_2 \leqslant k$ (pois $k-1 \geqslant 0$). Desse modo, concluímos que $\beta_2 = k$ e, repetindo esse processo uma quantidade finita de vezes, encontramos $\beta_1 = \cdots = \beta_k = k$. Daí, os conjuntos da forma $V_i - (U_1 \cup \cdots \cup U_h)$ são disjuntos, ou seja, $V_i \cap V_j \subseteq U_1 \cup \cdots \cup U_h$ para quaisquer $i \neq j$ em $\{1, \ldots, k\}$. ■

Lema 1.1.16 *Seja G um grupo não cíclico.*

a) Escreva $G = H_1 \cup \cdots \cup H_n$ como união de $n = \sigma(G)$ subgrupos de G. Seja $\beta_i = |G : H_i|$ para todo $i \in \{1, \ldots, n\}$ e suponha que $\beta_1 \leqslant \cdots \leqslant \beta_n$. Então $\beta_1 < \sigma(G)$.

b) Seja $\mathcal{M}$ uma cobertura minimal de G consistindo de subgrupos maximais de G. Se N é um subgrupo normal próprio de G e β é o índice minimal de um suplemento próprio de N em G pertencente a $\mathcal{M}$, então $\beta < \sigma(G)$.

Demonstração: (a) Uma vez que $1 \in H_1 \cap \cdots \cap H_n$, claramente temos

$$|G| < \sum_{i=1}^{n} |H_i| = \sum_{i=1}^{n} \frac{|G|}{\beta_i} \leqslant \frac{|G|n}{\beta_1},$$

donde $\beta_1 < n = \sigma(G)$.

(b) Se todos os membros em $\mathcal{M}$ são suplementos de N, o resultado segue de (i). Caso contrário, segue do Lema 1.1.15. ■

Lema 1.1.17 *Sejam G um grupo e p o menor divisor primo de $|G|$. Então todo subgrupo de índice p é normal em G.*

Demonstração: Seja H um subgrupo de G de índice p e suponha, por contradição, que $H^g \neq H$ para algum $g \in H$. Sabemos que

$$|HH^g| = \frac{|H||H^g|}{|H \cap H^g|}.$$

Uma vez que $H \cap H^g$ é um subgrupo próprio de H (pois $H \neq H^g$), temos que $|H \cap H^g|$ é um divisor próprio de $|H|$ e, como todo divisor primo de $|H|$ é maior do que ou igual a p, vem

$$\frac{|H|}{|H \cap H^g|} \geqslant p.$$

Assim $|HH^g| \geqslant p|H^g| = |G|$. Portanto, $G = HH^g$.

Assim, $g = hk^g$, com $h, k \in H$. Neste caso, $g = hk \in H$ e $H^g = H$, uma contradição. ∎

Vimos no Lema 1.1.6 que nenhum grupo G pode ser escrito como união de dois subgrupos próprios. O Teorema a seguir nos dá informações para saber, por exemplo, quando podemos ter $\sigma(G) = 3$. Em especial, este caso foi considerado pela primeira vez por Scorza em [29]. Ademais, o teorema a seguir, pontuado pelo Professor Boaz Tsaban, está demonstrado conforme Garonzi em [9].

Teorema 1.1.18 *Sejam G um grupo finito e p o menor primo divisor de $|G|$. Então $\sigma(G) = p + 1$ se, e somente se, existe um subgrupo normal N de G tal que $\frac{G}{N} \cong C_p \times C_p$.*

Demonstração: Suponha que $G = H_1 \cup \cdots \cup H_{p+1}$ pode ser escrito como união de $p + 1$ de seus subgrupos próprios, e seja $\beta_i = |G : H_i|$ para todo $i \in \{1, \ldots, p+1\}$, com $\beta_1 \leqslant \cdots \leqslant \beta_{p+1}$. Como p é o menor primo divisor de $|G|$, pelo Lema 1.1.16 temos que $\beta_1 = p$ e, portanto, H_1 é normal em G (Lema 1.1.17). Daí, pelo Lema 1.1.15 aplicado a $U_1 = H_1$, $h = 1$, $V_1 = H_2, V_2 = H_3, \ldots, V_k = H_{p+1}$ e $k = p$, vem $\beta_2 = \cdots = \beta_{p+1} = p$ e $\frac{G}{H_1 \cap H_2} \cong C_p \times C_p$.

Reciprocamente, temos $\sigma(G) \leqslant \sigma(\frac{G}{N}) = p + 1$ (Lema 1.1.7). Pelo Lema 1.1.16 vem $p < \sigma(G) \leqslant p + 1$ donde concluímos o resultado. ∎

1.2 p-Grupos Abelianos Elementares

Sejam p um primo e n um inteiro positivo maior do que 1. Denotaremos por C_p^n o p-grupo abeliano elementar de dimensão n. Observe que este grupo é particionável tendo em vista o Teorema 1.1.5 pois

$$H_p(C_p^n) = \langle g \in C_p^n : g^p \neq 1 \rangle = 1.$$

Proposição 1.2.1 $\rho(C_p^n) = 1 + p^{\lceil n/2 \rceil}$.

Demonstração: Suponha primeiro n par. Então podemos ver C_p^n como um espaço vetorial de dimensão 2 sobre um corpo F de tamanho $p^{n/2}$. Observando que dois F-subespaços unidimensionais de G se intersectam trivialmente e que C_p^n é a união desses subespaços, segue que

$$\rho(G) \leqslant \frac{|G|-1}{|F|-1} = \frac{p^n-1}{p^{n/2}-1} = 1 + p^{n/2} = 1 + \sqrt{|G|}.$$

Tendo em vista o Corolário 1.1.10, vem $\rho(G) = 1 + p^{n/2}$.

Assuma agora n ímpar. Vamos mostrar que $\rho(C_p^n) = 1+p^{(n+1)/2}$. Observe primeiramente que C_p^n mergulha em C_p^{n+1} como subgrupo normal de índice p. Pelo Lema 1.1.13, temos $\rho(C_p^n) \leqslant \rho(C_p^{n+1}) = 1 + p^{(n+1)/2}$.

Consideremos agora uma partição $\mathscr{P} = \{H_1, \ldots, H_m\}$ de C_p^n de tamanho $m = \rho(C_p^n)$. Então

$$1 + p^{(n+1)/2} \geqslant \rho(C_p^n) \geqslant 1 + |H_i| \Longrightarrow |H_i| \leqslant p^{(n+1)/2},$$

para todo $i \in \{1, \ldots, m\}$.

Se $|H_i| = p^{(n+1)/2}$ para algum $i \in \{1, \ldots, m\}$, então pelo Lema 1.1.9 vem $\rho(C_p^n) = 1 + p^{(n+1)/2}$. Agora assuma que $|H_i| \leqslant p^{(n+1)/2-1} = p^{(n-1)/2}$ para todo $i \in \{1, \ldots, m\}$, então

$$|C_p^n| = p^n = 1-m+\sum_{i=1}^{m} |H_i| \leqslant 1-m+mp^{(n-1)/2} \leqslant 1+(p^{(n+1)/2}+1)(p^{(n-1)/2}-1),$$

o que nos dá uma contradição. ∎

Pretendemos agora generalizar o Lema 1.1.7 no sentido de calcular σ para um p-grupo não cíclico qualquer.

Lema 1.2.2 *Se G é um p-grupo não-cíclico, então $\sigma(G) = p + 1$.*

Demonstração: Uma vez que todo subgrupo próprio não trivial tem índice no mínimo p, então pelo Lema 1.1.16, temos $\sigma(G) \geqslant p+1$. Por outro lado, se G é não cíclico e abeliano, então G possui um quociente isomorfo a $C_p \times C_p$, donde $\sigma(G) \leqslant \sigma(C_p \times C_p) = p + 1$.

Vamos mostrar agora o caso geral por indução em k, onde estamos considerando $|G| = p^k$, $k \geqslant 2$.

O caso $k = 2$ foi feito no Lema 1.1.7. Suponha agora por hipótese de indução que o resultado é válido para todos os grupos de ordem menor do que $|G|$. Se G é abeliano, então G possui um quociente isomorfo a $C_p \times C_p$ e seguimos como feito acima. Caso contrário, $\frac{G}{Z(G)}$ é um p-grupo não cíclico e não trivial com $\left|\frac{G}{Z(G)}\right| \leqslant |G|$, pois $Z(G)$ é não trivial. Por hipótese de indução, segue que $\sigma(G) \leqslant \sigma\left(\frac{G}{Z(G)}\right) = p + 1$. Portanto, $\sigma(G) = p + 1$. ■

Corolário 1.2.3 *Se G é um grupo particionável, então $\rho(G) \leqslant |G| - 1$ e a igualdade ocorre se, e somente se, $G \cong C_2 \times C_2$.*

Demonstração: A desigualdade $\rho(G) \leqslant |G| - 1$ segue do Lema 1.1.8. Se a igualdade ocorre, então na demonstração do Lema 1.1.8 teremos $|H_i| = 2$ para todo $i \in \{1, \ldots, n\}$ e G é um 2-grupo abeliano elementar. Logo, o resultado segue diretamente do Lema 1.2.2. ■

À luz do lema a seguir, poderemos calcular σ para um produto direto finito no caso em que os termos desse produto direto têm ordens relativamente primas. Este resultado nos auxiliará, por exemplo, no cálculo do σ de um grupo nilpotente finito. O lema a seguir e o seu corolário foram dados por Cohn em [4].

Lema 1.2.4 *Seja $G = H \times K$ um produto direto, com $|H|$ e $|K|$ relativamente primas. Então $\sigma(G) = min\{\sigma(H), \sigma(K)\}$.*

Demonstração: Observe primeiramente que $G = H \times K$ é cíclico se, e somente se, H e K são cíclicos. Neste caso não há nada a mostrar.

Suponha então G não cíclico e considere

$$H \times Y_1, \ldots, H \times Y_p, X_1 \times K, \ldots, X_q \times K$$

uma cobertura minimal de G e $\sigma(G) = n = p+q$. Uma vez que $mdc(|H|, |K|) = 1$, então observe que todo subgrupo de G é de fato da forma

$$X \times Y, \quad \text{onde} \quad X \leqslant H \quad \text{e} \quad Y \leqslant K,$$

e todo subgrupo maximal de G é da forma $H \times Y$, com Y maximal em K, ou vice-versa. Assim,

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

onde $p + q = n$, $p, q \geqslant 0$ e

$$G_1 = \bigcup_{r=1}^{p}(H \times Y_r) \qquad \text{e} \qquad G_2 = \bigcup_{s=1}^{q}(X_s \times K).$$

Vamos mostrar agora que p ou q é nulo. (Neste caso, dizer que $p = 0$, por exemplo, significa dizer que não existe na cobertura um subgrupo da forma $H \times Y$, com $Y \leqslant K$.)

Note que se $q \neq 0$, então $G \neq G_1$ e então existe $(h_1, k_1) \in G - G_1$. Logo, $k_1 \notin Y_j$, para todo $j \in \{1, \ldots, p\}$, e portanto, $(h, k_1) \notin G_1$, para todo $h \in H$. Assim, $(h, k_1) \in G_2$ para todo $h \in H$. Neste caso, $H = \cup_{s=1}^{n} X_s$ e $p = 0$ donde concluímos $G = H \times K \subseteq G_2$.

Logo,

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

donde $\sigma(H) \leqslant \sigma(G) = n$. ∎

Corolário 1.2.5 *Se G é um grupo nilpotente não cíclico, então $\sigma(G) = p+1$, onde p é o menor primo para o qual o p-subgrupo de Sylow é não cíclico.*

Demonstração: Sendo G o produto direto dos seus subgrupos de Sylow, segue do lema anterior que

$$\sigma(G) = min\{\sigma(S) : S \text{ } p\text{-subgrupo de Sylow de } G\}$$

donde concluímos (Lema 1.2.2) $\sigma(G) = p + 1$. ∎

A proposição a seguir se insere na classificação dos grupos particionáveis que satisfazem $\sigma = \rho$.

Proposição 1.2.6 *Seja G um grupo nilpotente particionável. Então $\sigma(G) = \rho(G)$ se, e somente se, $G \cong C_p \times C_p$ para algum primo p.*

Demonstração: Como G é nilpotente e particionável, então $\sigma(G) \leqslant p+1$, para algum divisor primo p de $|G|$. Logo, pelo Corolário 1.1.10 vem

$$\rho(G) = \sigma(G) \leqslant p+1 \Longrightarrow p+1 \geqslant \sqrt{|G|}+1 \Longrightarrow |G| \leqslant p^2.$$

Assim, como um tal p-subgrupo de Sylow de G tem ordem de no mínimo p^2 (pois não é cíclico), então $|G| = p^2$, donde $G \cong C_p \times C_p$. A recíproca foi mostrada no Lema 1.1.7. ■

Capítulo 2

O Grupo Simétrico S_4

O objetivo deste capítulo é investigar a construção de uma partição de S_4. Consoante a [4], temos $\sigma(S_4) = 4$ e, de fato, podemos constatar este resultado utilizando o que foi mostrado no capítulo anterior. Observe primeiramente que

$$\frac{S_4}{C_2^2} \cong S_3$$

e assim $\sigma(S_4) \leqslant \sigma(S_3) = 4$ (Lema 1.1.6).

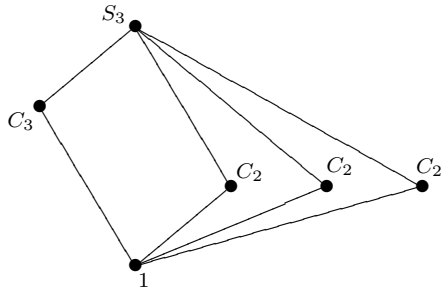

Diagrama 5: Reticulado de Subgrupos de S_3

Agora, pelo Teorema 1.1.18, temos que $\sigma(S_4) = 3$ se, e somente se, existe $N \trianglelefteq S_4$ com a propriedade de que $\frac{S_4}{N} \cong C_2^2$, o que não é possível pois um tal subgrupo N não existe.

A proposição a seguir implica que $\sigma(S_4) \neq \rho(S_4)$. Este resultado também pode ser consultado em [30] onde foi obtido de modo independente usando GAP.

Proposição 2.0.7 $\rho(S_4) = 10$.

Demonstração: Seja $\mathscr{P}$ uma partição de S_4. Queremos mostrar que se $\mathscr{P}$ é de tamanho minimal, então possui 10 elementos. Para tanto, nossa estratégia será analisar o comportamento dos subgrupos maximais de S_4 com respeito à $\mathscr{P}$.

Vamos destacar primeiramente as seguintes informações:

- $|S_4| = 24 = 2^3 \cdot 3$
- Os subgrupos maximais de S_4 são de um dos seguintes tipos: A_4 (grupo alternado de grau 4), S_3 (estabilizador de um ponto) e D_4 (o 2-subgrupo de Sylow)
- S_4 tem 9 elementos de ordem 2, 8 elementos de ordem 3 e 6 elementos de ordem 4

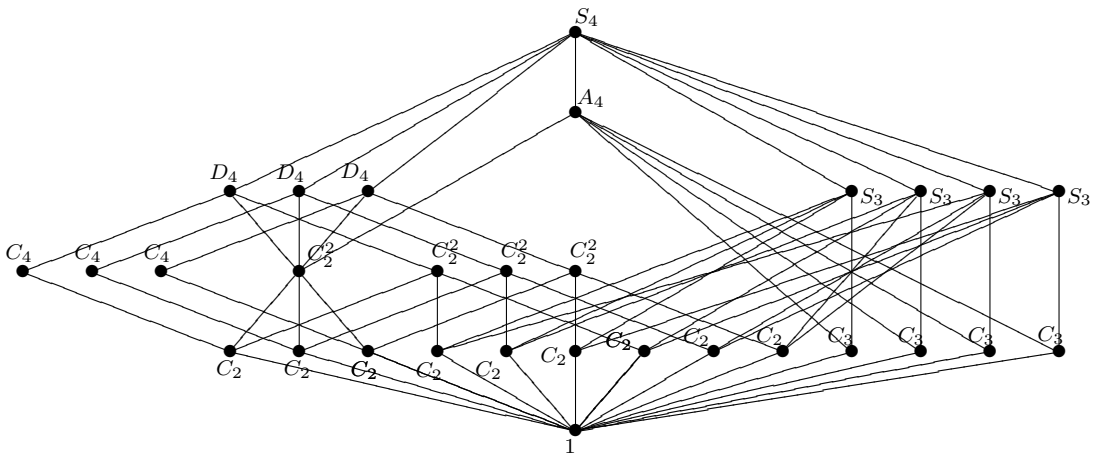

Diagrama 6: Reticulado de Subgrupos de S_4

Observe primeiramente que $A_4 \notin \mathscr{P}$ pois, em caso contrário, qualquer outro membro de $\mathscr{P}$ tem ordem no máximo igual a

$$\frac{|S_4|}{|A_4|} = 2$$

(vide demonstração do Lema 1.1.9) e, portanto, os elementos de ordem 4 não são cobertos por $\mathscr{P}$ (uma vez que nenhum deles pertence a A_4), o que nos dá um absurdo.

Agora, $D_4 \notin \mathscr{P}$ pois, em caso contrário, qualquer outro membro de $\mathscr{P}$ tem ordem no máximo igual a

$$\frac{|S_4|}{|D_4|} = 3.$$

Portanto, existe uma única cópia de D_4 nesta partição. Observando agora que em S_4 temos 6 elementos de ordem 4 e cada D_4 possui apenas dois deles, a desigualdade anterior nos mostra que existem elementos de ordem 4 não cobertos por $\mathscr{P}$, o que nos dá um absurdo novamente.

Suponha, por fim, $H = S_3$ um subgrupo em $\mathscr{P}$. Como

$$\frac{|S_4|}{|S_3|} = 4,$$

então não existe outro membro em $\mathscr{P}$ isomorfo a H. Assim, para particionar os elementos de ordem 4 precisamos necessariamente de 3 cópias de C_4, para particionar os elementos de ordem 3 (não contidos em H) precisamos necessariamente de 3 cópias C_3 e, finalmente, para particionar os demais elementos de ordem 2 precisamos necessariamente de 3 cópias de C_2. Observe que para os elementos de ordem 2 não podemos utilizar cópias do grupo de Klein. De fato, temos que cada subgrupo de Klein $K = C_2^2$ de S_4 está contido em algum D_4 (que é o 2-subgrupo de Sylow de S_4). Assim, se $x, y \in K$ são elementos de ordem dois distintos, então $xy \in K \cap C_4$, para algum C_4.

Portanto, $|\mathscr{P}| = 1 + 3 + 3 + 3 = 10$.

Se $S_3 \notin \mathscr{P}$, então $\mathscr{P}$ consiste apenas de subgrupos cíclicos. Com efeito, precisamos necessariamente de 3 cópias de C_4 e 4 cópias de C_3 e de 6 cópias de C_2, totalizando uma partição de tamanho $|\mathscr{P}| = 3 + 4 + 6 = 13$.

Logo, $\rho(S_4) = 10$, como queríamos. ∎

Observe que a partição minimal de S_4 é única (S_4 admite apenas duas partições), mas, em geral, partições de tamanho $\rho(G)$ de um grupo particionável G não precisam ser únicas.

Por exemplo, considere o grupo $G = C_3^2 \rtimes C_2$ com ação de inversão. Temos que G admite apenas 3 partições descritas da seguinte forma.

$1\ C_3^2 + 9\ C_2$	partição de tamanho 10
$1\ C_3 \rtimes C_2 + 3\ C_3 + 6\ C_2$	partição de tamanho 10
$4\ C_3 + 9\ C_2$	partição de tamanho 13

De Fato, se C_3^3 é membro de uma partição de G, então os demais membros desta partição são precisamente todas as cópias de C_2 de G. Se existe $H = C_3 \rtimes C_2$ em uma partição de G, então os demais membros desta partição têm ordem no máximo

$$\frac{|G|}{|C_3 \rtimes C_2|} = 3,$$

e assim, os demais membros desta partição são os grupos cíclicos de G não contidos em H. Por fim, uma outra partição é dada apenas pelos subgrupos cíclicos de G.

Logo, $\rho(G) = 10$ e as partições de tamanho 10 de G são distintas. Em especial G é um grupo de Frobenius, o qual será estudado no próximo capítulo.

Capítulo 3

Grupos de Frobenius

O objetivo deste capítulo é classificar os *grupos de Frobenius* G que satisfazem a igualdade $\sigma = \rho$.

Apresentamos algumas característica estruturais destes grupos, sem viés didático mas suficientes como arcabouço teórico para fundamentar a discussão subsequente. Relacionamos o conceito de *p-nilpotência* com o conceito de *fatores principais* em uma *série principal* e com o *subgrupo de Frattini*. Além disso, abordamos também questões gerais tangentes ao cálculo de ρ.

Para um estudo aprofundado sobre a estrutura dos grupos de Frobenius indicamos consultar [19].

3.1 Estrutura dos Grupos de Frobenius

Vamos introduzir primeiramente uma breve discussão sobre *ação de Frobenius*.

Sejam A e N grupos finitos, e suponha que A age em N via automorfismo. A ação de A em N é dita ser de *Frobenius* (ou livre de ponto fixo) se $n^a \neq n$, para quaisquer $n \in N$ e $a \in A$ não triviais. Equivalentemente, a ação é dita ser de Frobenius se

$$C_N(a) = 1 \quad \text{e} \quad C_A(n) = 1$$

para quaisquer $n \in N$ e $a \in A$ não triviais.

Se $n \in N$ e $n \neq 1$, então o tamanho da A-órbita de n é $|A : C_A(n)|$, e assim, se a ação é de Frobenius, então $|A : C_A(n)| = |A|$. Neste caso, o conjunto N é decomposto em A-órbitas. Uma destas é 1 e todas as outras têm tamanho $|A|$, o que nos leva ao seguinte resultado.

Lema 3.1.1 *Sejam A e N grupos finitos e suponha que exista uma ação de Frobenius de A em N. Então $|N| \equiv 1 \pmod{|A|}$, e assim $|N|$ e $|A|$ são coprimos.*

Por exemplo, se A tem ordem 2, com elemento não idêntico a, e N abeliano de ordem ímpar, podemos definir uma ação de Frobenius de A em N por $n^a = n^{-1}$, para todo $n \in N$.

O próximo resultado sugere que nem todo grupo A age com uma ação de Frobenius em um grupo N, e nem todo grupo N admite uma ação de Frobenius de um grupo não trivial A, cuja demonstração pode ser consultada em [18] (Teorema 6.3).

Teorema 3.1.2 *Sejam A e N grupos finitos, e suponha que existe uma ação de Frobenius de A em N. Assuma que $|A|$ é par e N é não trivial. Então A contém uma única involução e N é abeliano.*

Um grupo finito A é dito ser um *complemento de Frobenius* se age por uma ação de Frobenius em algum grupo não trivial N. Neste caso, N é dito ser um *núcleo de Frobenius*. Sendo $G = N \rtimes A$, e a ação de A em N é de Frobenius, então dizemos que G é um *grupo de Frobenius*.

Assim, observe que os grupos diedrais $D_n = C_n \rtimes C_2$, com n ímpar, constituem uma família de grupos de Frobenius.

Observe também que se $G = N \rtimes A$ é um grupo de Frobenius, então $A \cap A^g = 1$, para todo $g \in G - A$. De fato, suponha $A \cap A^g \neq 1$ para algum $g \in G$. Vamos mostrar que $g \in A$. Uma vez que $G = AN$, podemos escrever $g = an$, com $a \in A$ e $n \in N$, e assim, $A^g = A^{an} = A^n$. Então $A^n \cap A \neq 1$ implica que existe $b \in A - 1$ tal que $b^n \in A$. Daí, vem

$$[b, n] = b^{-1}b^n \in A \cap N = 1$$

(pois N é normal), e assim, b centraliza n. Sendo a ação de Frobenius, por hipótese, e $b \neq 1$, então $n = 1$ donde $g = an = a$.

Em particular, o raciocínio acima esclarece também que $N_G(A) = A$.

Lema 3.1.3 *Seja G um grupo de Frobenius. Então o seu núcleo de Frobenius em conjunto com todos os seus complementos de Frobenius formam uma partição de G.*

Demonstração: Sejam N o núcleo de Frobenius e H um complemento de Frobenius de G. Como

$$N \cap H^x = 1 \quad \text{e} \quad H \cap H^y = 1$$

para todo $x \in G$ e $y \in G - H$, então o conjunto $N \cup (\cup_{g \in G} H^g)$ tem ordem

$$|N| + |G : H|(|H| - 1) = |G|.$$

Logo, $G = N \cup \left(\bigcup_{g \in G} H^g\right)$. ∎

O lema acima é utilizado para estabelecer algumas caracterizações para grupos de Frobenius finitos, como no teorema que segue, cuja demonstração pode ser consultada em [18] (Teorema 6.4).

Teorema 3.1.4 *Seja $G = N \rtimes A$ um grupo finito. São equivalentes:*

a) A ação de conjugação de A em N é de Frobenius.

b) $A \cap A^g = 1$, para todo $g \in G - A$.

c) $C_G(a) \subseteq A$, para todo $a \in A - 1$.

d) $C_G(n) \subseteq N$, para todo $n \in N - 1$.

Corolário 3.1.5 *Todo grupo de Frobenius G tem centro trivial.*

Assim, se G é um grupo de Frobenius, então existe H subgrupo de G tal que $H \cap H^g = 1$ para todo $G - H$ (na definição que apresentamos, H é exatamente um complemento de Frobenius). Reciprocamente, também este fato ocorre, enunciado conforme o teorema abaixo devido a Frobenius e cuja demonstração pode ser consultada em [16].

Teorema 3.1.6 *Sejam G um grupo e $H \leqslant G$ tal que $H \cap H^g = 1$ para todo $g \in G - H$. Então existe $N \trianglelefteq G$ com $HN = G$ e $H \cap N = 1$, ou seja G é um produto semidireto $N \rtimes H$.*

Uma outra caracterização bastante útil, que neste documento será por exemplo empregada de modo mais efetivo no Capítulo 4 com os grupos do tipo Hughes-Thompson, será estabelecida conforme o teorema abaixo, cuja demonstração pode ser consultada em [19] (Capítulo 37, Teorema 1.5).

Teorema 3.1.7 *As seguintes afirmações são equivalentes.*

a) G *é um grupo de Frobenius com núcleo de Frobenius* N *de ordem* m*.*

b) $|G| = mn$*, com* $m \neq 1 \neq n$*,* $mdc(m,n) = 1$*,* $N = \{g : g^m = 1\}$ *é um subgrupo normal de* G *e para cada* $g \in G$*,* $g^m = 1$ *ou* $g^n = 1$*.*

Uma das aplicações dos Teoremas 3.1.4 e 3.1.7 diz respeito a entender o comportamento dos subgrupos e dos quocientes de um grupo de Frobenius conforme o teorema abaixo, cuja demonstração pode ser consultada em [19] (Capítulo 37, Teorema 1.6).

Teorema 3.1.8 *Seja* G *um grupo de Frobenius e com núcleo de Frobenius* N *e seja* K *um subgrupo de* G*. Então uma das seguintes afirmações ocorre.*

a) $K \subseteq N$*.*

b) $N \cap K = 1$*.*

c) K *é um grupo de Frobenius com núcleo de Frobenius* $N \cap K$*.*

Além disso, se $K \trianglelefteq G$*, então uma das seguintes afirmações ocorre.*

d) $N \subseteq K$*.*

e) $K \subset N$ *e* $\frac{G}{K}$ *é um grupo de Frobenius com núcleo de Frobenius* $\frac{N}{K}$*. Ademais, os complementos de Frobenius de* $\frac{G}{K}$ *são os respectivos quocientes de complementos de Frobenius de* G*.*

O *subgrupo de Fitting* de um grupo finito G, denotado por $Fit(G)$, é definido como sendo o produto de todos os seus subgrupos normais nilpotentes. Assim, como o produto finito de normais nilpotentes é normal nilpotente (como é bem conhecido da Teoria de Grupos Finios), concluímos que $Fit(G)$ é o maior subgrupo normal nilpotente de G. Em especial, ele contém o *subgrupo de Frattini* de G.

Dadas estas informações, relacionaremos agora o subgrupo de Fitting com os grupos de Frobenius. Lembraremos ainda o Teorema de Thompson e o Teorema de Schur-Zassenhaus, amplamente conhecidos da Teoria dos Grupos Finitos, os quais utilizaremos na demonstração do Teorema 3.1.11. (As demonstrações de ambos os teoremas podem ser consultadas em [28].)

Teorema 3.1.9 (Thompson) *Se um grupo finito G admite um automorfismo livre de ponto fixo de ordem prima, então G é nilpotente.*

No sentido do Teorema de Thompson, um automorfismo φ de G é dito ter um ponto fixo g em G se $\varphi(g) = g$. Se o elemento identidade 1 é o único ponto fixo de φ, o automorfismo φ é dito ser livre de ponto fixo.

Teorema 3.1.10 (Schur-Zassenhaus) *Se um grupo finito G admite um subgrupo normal N com $mdc(|N|, |G : N|) = 1$, e N ou $\frac{G}{N}$ é solúvel, então N é complementado e dois complementos quaisquer de N em G são conjugados.*

No sentido do Teorema de Schur-Zassenhaus, dizer que N é complementado em G significa dizer que existe um subgrupo M de G tal que

$$NM = G \quad \text{e} \quad N \cap M = 1.$$

Além disso, a hipótese de N ou $\frac{G}{N}$ solúvel vem do Teorema de Feit-Thompson que acerta que todo grupo de ordem ímpar é solúvel.

Teorema 3.1.11 *Seja G um grupo de Frobenius com núcleo de Frobenius N e complemento de Frobenius H. Então as seguintes afirmações ocorrem.*

a) N é o subgrupo de Fitting de G.

b) O núcleo de Frobenius de G é único, enquanto que os complementos de Frobenius de G são únicos a menos de conjugação.

Demonstração: *a*) Sendo $G = N \rtimes H$ um grupo de Frobenius, temos que N admite um automorfismo livre de ponto fixo de ordem prima $N \longrightarrow N$ dado por $n \longmapsto n^h$, onde $h \in H$ tem ordem prima. Assim, pelo Teorema de Thompson, N é nilpotente. Logo, $N \subseteq Fit(G)$. Neste caso, $N \cap Z(Fit(G)) \neq 1$. Sendo $g \in N \cap Z(Fit(G))$ e $g \neq 1$, pelo Teorema 3.1.4, vem

$$Fit(G) \subseteq C_G(g) \subseteq N,$$

e assim $N = Fit(G)$.

b) A unicidade do núcleo de Frobenius é uma consequência do item (a). Uma vez que $mdc(|N|, |G : N|) = 1$ (Lema 3.1.1), a afirmação sobre os complementos de Frobenius decorre do Teorema de Schur-Zassenhaus. ■

Diante do resultado acima, observe que um grupo de Frobenius G não pode ser nilpotente. De fato, em caso contrário, $G = Fit(G)$, e portanto, todos os complementos de Frobenius seriam triviais. Daí, teríamos $C_G(1) = 1$ (pelo Teorema 3.1.4), uma contradição.

Observe que $A_4 = K \rtimes C_3$ é um grupo de Frobenius, onde K denota o grupo de Klein C_2^2. Entretanto, S_4 não é de Frobenius pois, em caso contrário, o seu núcleo de Frobenius (que coincide com seu subgrupo de Fitting) seria K (único subgrupo normal nilpotente não trivial) e, portanto, os complementos de Frobenius de S_4 seriam C_3 (Lema 3.1.1). Daí, $S_4 = K \rtimes C_3$, uma contradição.

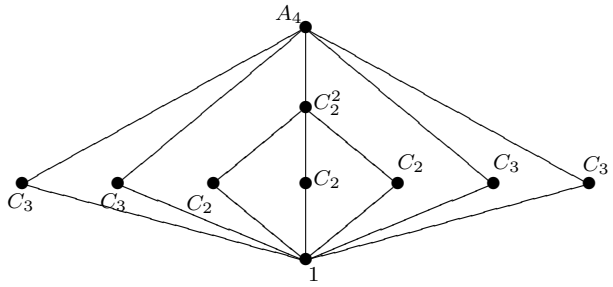

Diagrama 7: Reticulado de Subgrupos de A_4

3.2 Séries Principais e Fatores Principais

Vamos introduzir a seguir um conceito que generaliza a definição de grupo. Um Ω-grupo G (ou *grupo operador*) é uma tripla (G, Ω, α) consistindo de um grupo G, um conjunto Ω chamado *domínio operador* e uma função $\alpha : G \times \Omega \longrightarrow G$ tal que $g \longmapsto \alpha(g, w)$ é um endomorfismo de G para cada $w \in \Omega$. Por simplicidade, vamos escrever g^w para $\alpha(g, w)$, deixando a função α subentendida.

Da definição acima, qualquer grupo G pode ser visto como Ω-grupo, com Ω vazio. Observe também que é possível generalizar em termos de grupos operadores vários outros conceitos. Se G é um Ω-grupo, um Ω-subgrupo de G é um subgrupo H tal que $h^w \in H$ para quaisquer $h \in H$ e $w \in \Omega$. Logo, todo Ω-subgrupo é por si um Ω-grupo. Se N é um Ω-subgrupo normal, então $\frac{G}{N}$ é um Ω-*grupo quociente* se definirmos $(gN)^w = g^w N$. Um Ω-*homomorfismo* $\varphi : G \longrightarrow H$ é um homomorfismo entre Ω-grupos G e H tal que

$$\varphi(g^w) = \varphi(g)^w$$

para quaisquer $g \in G$ e $w \in \Omega$.

A partir disso, podemos falar naturalmente em Ω-*endomorfismos*, Ω-*automorfismos* e Ω-*isomorfismos*. Em particular, vamos escrever $G \cong_\Omega H$ se G e H são Ω-grupos Ω-isomorfos.

Seja G um grupo e considere $\Omega = End(G)$. Então G é um Ω-grupo se considerarmos que os endomorfismos agem naturalmente em G. Observe que os Ω-subgrupos de G são os seus subgrupos H invariantes por endomorfismos de G, isto é, $\varphi(H) = H$ para todo $\varphi \in End(G)$. Do mesmo modo, G é um Ω-grupo se $\Omega = Aut(G)$. Neste caso, os Ω-subgrupos de G são os seus subgrupos característicos. Ademais, G também é um grupo operador com respeito a $\Omega = Inn(G)$, no qual os Ω-subgrupos são os subgrupos normais de G.

Seja G um Ω-grupo. Uma Ω-*série* (de comprimento finito) é uma sequência finita de Ω-subgrupos de G da seguinte forma

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

Cada G_i é dito um *termo* da série e cada quociente $\frac{G_{i+1}}{G_i}$ é dito um *fator* da série. Uma Ω-série como acima é dita de comprimento n se os seus termos são distintos.

Considere agora o conjunto de todas as Ω-séries de um Ω-grupo G, que é não-vazio pois podemos sempre considerar

$$1 \trianglelefteq G.$$

Se $\mathbf{S}$ e $\mathbf{T}$ são Ω-séries de G, dizemos que $\mathbf{S}$ é um refinamento de $\mathbf{T}$ se todo termo de $\mathbf{T}$ também é um termo de $\mathbf{S}$. Se existe algum termo de $\mathbf{S}$ que não é termo de $\mathbf{T}$, então dizemos que o refinamento é próprio. Neste sentido, uma Ω-série que não pode ser refinada propriamente é dita *série de composição* (e portanto seus fatores são Ω-simples). Quando $\Omega = Inn(G)$, a série é chamada *série principal*.

Duas $\Omega-$séries $\mathbf{S}$ e $\mathbf{T}$ de um Ω-grupo G são ditas Ω-isomorfas se existe uma bijeção entre o conjunto dos fatores de $\mathbf{S}$ e o conjunto dos fatores de $\mathbf{T}$ tal que fatores correspondentes são Ω-isomorfos.

Na direção do que foi introduzido no parágrafo anterior, vamos agora enunciar o mais importante resultado sobre séries de composição (cuja demonstração pode ser consultada em [28]).

Teorema 3.2.1 (Jordan-Holder) *Se* $\mathbf{S}$ *é uma* Ω*-série de composição e* $\mathbf{T}$ *é alguma* Ω*-série de um* Ω*-grupo* G*, então* $\mathbf{T}$ *tem algum refinamento que é*

uma série de composição e é Ω-isomorfa a $\mathbf{S}$. *Em particular, se* $\mathbf{T}$ *é uma série de composição, então ela é Ω-isomorfa com* $\mathbf{S}$.

Considere agora $\Omega = Inn(G)$. Consoante a [1], esclarecemos que o número de complementos de fatores principais de uma dada série principal de um grupo solúvel G não depende, a menos de permutação, da escolha da série. Em particular, se nenhum fator principal de uma dada série principal de G tem n complementos, então nenhum fator principal de G tem precisamente n complementos.

Usaremos, quando lhe couber, a proposição a seguir sem menção explícita. Esta proposição destaca as ideias sinalizadas no parágrafo anterior.

Proposição 3.2.2 *Se G é um grupo solúvel e $1 = K_0 < K_1 < \cdots < K_t = G$ é uma série principal de G, com n_i o número de complementos de $\frac{K_i}{K_{i-1}}$ em $\frac{G}{K_{i-1}}$ para todo $i \in \{1, \ldots, t\}$ (por exemplo, $n_i = 0$ se, e somente se, $\frac{K_i}{K_{i-1}}$ é Frattini), então a sequência de números $(n_1, \ldots, n_t)$, a menos de reordenamento, não depende da escolha da série principal.*

3.3 p-Nilpotência

Vamos definir um *p-complemento H* de um grupo G como sendo um subgrupo normal que é complementado e cujo complemento é um p-subgrupo de Sylow. Assim, um grupo que tem um p-complemento normal é dito ser *p-nilpotente*.

Se G é um grupo de ordem pq, com p e q primos distintos e $p < q$, então G é p-nilpotente pois os p-subgrupos de Sylow de G são os complementos para o (único) q-subgrupo de Sylow de G.

De modo mais especial, temos o seguinte resultado.

Proposição 3.3.1 *Seja G um grupo finito. Então G é nilpotente se, e somente se, G é p-nilpotente para todo primo p divisor de $|G|$.*

Demonstração: Considere $p_1, \ldots, p_n$ todos os primos na decomposição de $|G|$ e seja P_i um p_i-subgrupo de Sylow de G para todo $i \in \{1, \ldots, n\}$

Suponha G nilpotente. Então $P_i \trianglelefteq G$ e assim $P_1 \cdots P_n$ é um subgrupo de G com $|P_1 \cdots P_n| = |P_1| \cdots |P_n| = |G|$. Logo, $G = P_1 \cdots P_n$. Observando agora que

$$P_i \cap P_1 \cdots P_{i-1} P_{i+1} \cdots P_n = 1$$

para todo $i \in \{1, \ldots, n\}$ pois $mdc(|P_i|, |P_i \cap P_1 \cdots P_{i-1} P_{i+1} \cdots P_n|) = 1$ para todo $i \in \{1, \ldots, n\}$, temos que $P_1 \cdots P_{i-1} P_{i+1} \cdots P_n$ é um p_i-complemento normal de G para todo $i \in \{1, \ldots, n\}$.

Reciprocamente, suponha que G é p_i-nilpotente para todo $i \in \{1, \ldots, n\}$ e seja N_i um p_i-complemento normal de G para todo $i \in \{1, \ldots, n\}$. Afirmamos que

$$P_i = \bigcap_{j \neq i}^{n} N_j.$$

De fato, uma vez que $|N_j| = \frac{|G|}{|P_j|}$, então P_i é um p_i-subgrupo de Sylow de N_j, para $j \neq i$, e assim $P_i \subseteq \bigcap_{j \neq i}^{n} N_j$. Por outro lado, p_i é o único primo na decomposição de $|G|$ que divide $|\bigcap_{j \neq i}^{n} N_j|$ donde concluímos que $|\bigcap_{j \neq i}^{n} N_j|$ é uma potência de p_i e assim $P_i = \bigcap_{j \neq i}^{n} N_j$, como afirmamos. Ademais, $P_i \trianglelefteq G$ para todo $i \in \{1, \ldots, n\}$ (pois é interseção de subgrupos normais) implicando que G é nilpotente. ∎

Para finalizar esta breve abordagem, vamos mostrar que se um grupo G é p-nilpotente, então qualquer quociente de G também é p-nilpotente. De fato, sejam H um p-complemento normal de G e $N \trianglelefteq G$. Vamos mostrar que $\frac{HN}{N}$ é um p-complemento normal de $\frac{G}{N}$. Com efeito, já temos naturalmente $\frac{HN}{N}$ normal em $\frac{G}{N}$ e $p \nmid |\frac{HN}{N}|$ (pois $p \nmid |H|$), e daí se $\frac{P}{N}$ é um p-subgrupo de Sylow de $\frac{G}{N}$ então $mdc(|\frac{HN}{N}|, |\frac{P}{N}|) = 1$. Logo, $\frac{HN}{N} \cap \frac{P}{N} = 1$ e

$$\left|\frac{HN}{N}\right| \left|\frac{P}{N}\right| = \left|\frac{HP}{N}\right| = \left|\frac{G}{N}\right|,$$

como queríamos. Veremos no Lema 3.3.5 que a recíproca deste resultado está relacionada com o *subgrupo de Frattini* de G.

3.3.1 Subgrupo de Frattini e p-Nilpotência

Se G é um grupo finito, definimos o *subgrupo de Frattini* de G, e denotamos por $\Phi(G)$, como sendo a interseção de todos os subgrupos maximais de G. Claramente, este subgrupo é característico em G. Além disso, tem a importante propriedade de coincidir com o conjunto de todos os elementos não-geradores de G, cuja demonstração pode ser consultada em [28] (Teorema 5.2.12). Aqui, um elemento $g \in G$ é dito *não-gerador* de G se $G = \langle g, X \rangle$ implica $G = \langle X \rangle$, para todo subconjunto X de G.

Proposição 3.3.2 *Em qualquer grupo G, o subgrupo de Frattini é igual ao conjunto dos elementos não-geradores de G.*

O teorema abaixo é um resultado bem conhecido na Teoria dos Grupos Finitos.

Teorema 3.3.3 *Seja $G = G_1 \times \cdots \times G_n$ uma decomposição em produto direto de grupos finitos. Então*

$$\Phi(G) = \Phi(G_1) \times \cdots \times \Phi(G_n).$$

A demonstração do lema a seguir pode ser consultada em [28] (Teorema 5.2.13).

Lema 3.3.4 *Seja G um grupo finito.*

a) Sejam $N \trianglelefteq G$ e $H \leqslant G$ satisfazendo $N \leqslant \Phi(H)$. Então $N \leqslant \Phi(G)$.

b) Se K é um subgrupo normal de G, então $\Phi(K) \leqslant \Phi(G)$.

c) Se N é um subgrupo normal de G, então $\frac{\Phi(G)N}{N} \leqslant \Phi\left(\frac{G}{N}\right)$, e a igualdade ocorre se $N \leqslant \Phi(G)$.

Relacionaremos agora o subgrupo de Frattini com o conceito de p-nilpotência.

Lema 3.3.5 *Sejam G um grupo finito e K um subgrupo normal de G, com $\Phi(G) \subseteq K$. Se $\frac{K}{\Phi(G)}$ é p-nilpotente então K é p-nilpotente.*

Demonstração: Sejam $\frac{L}{\Phi(G)}$ um p-complemento normal de $\frac{K}{\Phi(G)}$ e P um p-Sylow de $\Phi(G)$. Como $p \nmid |\frac{L}{\Phi(G)}|$ então P é um p-subgrupo de Sylow de L, donde $P \trianglelefteq L$. De fato, $P \trianglelefteq \Phi(G)$ (pois este último é nilpotente) e assim P é característico em $\Phi(G)$ que por sua vez é normal em L. Neste caso, pelo Teorema de Schur-Zassenhaus, existe H complemento de P em L, e assim, $L = PH$; além disso, todos os complementos de P em L são conjugados.

Observe agora que, dado $g \in G$, temos

$$H^g \cap P = (H \cap P)^g = 1 \quad \text{e} \quad |H^g P| = |H^g||P| = |H||P| = |L|,$$

ou seja, H^g também é complemento de P em L. Assim, existe $x \in L$ tal que $H^g = H^x$. Daí,

$$gx^{-1} \in N_G(H) \Longrightarrow g \in N_G(H)L \Longrightarrow$$
$$G = N_G(H)L = N_G(H)HP \subseteq N_G(H)\phi(G)$$

donde $N_G(H) = G$ e, portanto, $H \trianglelefteq G$.

Isto mostra que H é um p-complemento normal de K. De fato, se P^* é um p-subgrupo de Sylow de K então $H \cap P = 1$ pois $p \nmid |H|$. Ademais, $\frac{P^*\Phi(G)}{\Phi(G)}$ é um p-subgrupo de Sylow de $\frac{K}{\Phi(G)}$ e então

$$\frac{K}{\Phi(G)} = \frac{L}{\Phi(G)}\frac{P^*\Phi(G)}{\Phi(G)} \Longrightarrow$$

$$K = LP^*\Phi(G) = HPP^*\Phi(G) = HP^*\Phi(G) = HP^*\Phi(K) = HP^*,$$

pois $P \subseteq \Phi(G)$ e $\Phi(G) = \Phi(K)$ (Lema 3.3.4). ∎

3.3.2 Fatores Principais e p-Nilpotência

Um subgrupo normal $N \neq 1$ de um grupo G é dito ser normal minimal de G se não existe $L \trianglelefteq G$ tal que $1 \subsetneq L \subsetneq N$.

Introduzimos na Seção 2.2 o conceito de fator principal de um grupo G, o qual define-se como um subgrupo normal minimal de um quociente de G. Pretendemos agora relacioná-lo com o conceito de p-nilpotência.

Assim, por *menor* ordem de um fator principal de G entende-se um fator principal em alguma série principal. Além disso, um complemento de um fator principal $\frac{L}{N}$ de G (com $N \trianglelefteq G$) é um subgrupo $\frac{K}{N}$ de $\frac{G}{N}$ tal que $KL = G$ e $K \cap L = N$.

Lema 3.3.6 *Sejam G um grupo solúvel finito e N um subgrupo normal minimal de G. Então N é um p-grupo abeliano elementar para algum primo p e, se N é complementado, então os complementos de N em G são exatamente os subgrupos maximais de G que não contêm N.*

Primeiramente, vamos mostrar um teorema obtido por Tomkinson em [32] que relaciona fatores principais e coberturas e que terá fundamental importância na classificação dos grupos de Frobenius G que satisfazem $\sigma(G) = \rho(G)$.

Pensando nesta demonstração, vamos destacar as seguintes definições.

Sejam G e um grupo e H subgrupo de G. Definimos o *core normal* de H em G denotado por H_G, como sendo

$$H_G := \bigcap_{g \in G} g^{-1} H g.$$

Ele é um subgrupo normal de G com a seguinte propriedade universal: se $N \trianglelefteq G$ então $N \subseteq H$ se, e somente se, $N \leqslant H_G$. G é dito ser *primitivo* (de grau n) se G admite um subgrupo maximal (de índice n) com core normal e trivial.

Na demonstração do Teorema de Tomkinson também será requerido um teorema devido a Gaschütz (que pode ser consultado em [12]) que diz que em um grupo solúvel primitivo G, o único subgrupo normal minimal tem ordem maior do que qualquer outro fator principal de G.

Observação 3.3.7 *Se $\frac{H_i}{H_{i-1}}$ é um fator principal de um grupo solúvel G com complemento normal $\frac{L}{H_{i-1}}$, então $\frac{G}{H_{i-1}} \cong \frac{H_i}{H_{i-1}} \times \frac{L}{H_{i-1}}$. Logo, a conjugação de qualquer elemento de $\frac{H_i}{H_{i-1}}$ por um elemento de $\frac{G}{H_{i-1}}$ é trivial, já que $\frac{H_i}{H_{i-1}}$ é abeliano. Portanto, $\frac{H_i}{H_{i-1}}$ é central em $\frac{G}{H_{i-1}}$.*

Teorema 3.3.8 (Tomkinson) *Seja G um grupo finito solúvel. Então $\sigma(G) = q + 1$, onde q é a menor ordem de um fator principal de G com mais de um complemento.*

Demonstração: Seja $\frac{H}{K}$ o menor fator principal de G com mais de um complemento. Vamos provar o resultado por indução em $|G|$. Seja também $|\frac{H}{K}| = p^a$.

(a) $\sigma(G) \leqslant p^a + 1$.

Escolha um fator principal $\frac{V}{W}$ de G de ordem p^a tal que $\frac{V}{W}$ tem mais de um complemento e $|\frac{V}{W}|$ é minimal com estas propriedades. Assim, se $\frac{S}{T}$ é um fator principal complementado de G com $V < S$ e $|\frac{S}{T}| \leqslant p^a$, então $\frac{S}{T}$ tem um único complemento (que é normal pois coincide com seus conjugados) e portanto $\frac{S}{T}$ é central (Observação 3.3.7) donde concluímos que $\frac{S}{T}$ tem ordem prima.

Sejam $\frac{M}{W}$ um complemento para $\frac{V}{W}$ e $Y = M_G \geqslant W$. Então $\frac{G}{Y}$ é um grupo solúvel primitivo com único subgrupo normal minimal $\frac{X}{Y} \cong \frac{V}{W}$. Se $X \neq V$, então $\frac{X}{Y}$ é central e assim $\frac{V}{W}$ também é central de ordem p. Assim, os complementos de $\frac{V}{W}$ são normais e G tem um quociente isomorfo a C_p^2.

Logo, $\sigma(G) \leqslant p+1$. Portanto, podemos assumir que $X = V$, $Y = W$ e então $\frac{G}{W}$ é um grupo solúvel primitivo com único subgrupo normal minimal $\frac{V}{W}$.

Pelo resultado de Gaschütz em [12], todo fator principal de $\frac{G}{V}$ tem ordem menor do que p^a e, portanto, tal fator principal é Frattini ou é central (se tem 0 ou 1 complemento, respectivamente). Consequentemente, $\frac{G}{V}$ é nilpotente e cada primo q divisor de $|\frac{G}{V}|$ é menor do que p^a. Se $\frac{G}{V}$ não fosse cíclico, então ele teria um quociente isomorfo a C_q^2 e assim teria um fator principal de ordem q com mais de um complemento. Logo, $\frac{G}{V}$ é cíclico e $\sigma(G) \leqslant \sigma(\frac{G}{W}) = p^a + 1$.

(b) $p^a + 1 \leqslant \sigma(G)$.

Escolha $N \trianglelefteq G$ maximal com a propriedade de que $\sigma(\frac{G}{N}) = \sigma(G)$. Seja $\frac{K}{N}$ um subgrupo normal minimal de $\frac{G}{N}$. Então $\frac{G}{K}$ é cíclico ou $\sigma(\frac{G}{K}) > \sigma(G)$ (pela maximalidade de N).

Seja $G = X_1 \cup \cdots \cup X_{\sigma(G)}$, onde cada X_i é um subgrupo maximal de G contendo N. Observe que nem todos os X_i contêm K pois, em caso contrário, $\frac{G}{K} = \frac{X_1}{K} \cup \cdots \cup \frac{X_{\sigma(G)}}{K}$ e daí $\sigma(\frac{G}{K}) \leqslant \sigma(G)$. Portanto, $\frac{K}{N}$ não é Frattini e assim tem algum complemento $\frac{M}{N}$.

Se $\frac{K}{N}$ tem um único complemento, digamos $\frac{X_1}{N}$ (Lema 3.3.6), então $X_2, \ldots, X_{\sigma(G)}$ devem todos conter K. Mas isso contraria o Lema 5 de [4]. Portanto, $\frac{K}{N}$ tem mais de um complemento.

Se $\frac{K}{N}$ tem complementos normais, então $\frac{G}{N}$ e descrito como um produto direto, logo $|\frac{K}{N}| = p$ e G tem um quociente isomorfo a C_p^2. Portanto, $\sigma(G) = p + 1 = |\frac{K}{N}| + 1$.

Se $\frac{K}{N}$ não tem complementos normais, então ele tem $|\frac{K}{N}|$ complementos, digamos $\frac{M_1}{N}, \ldots, \frac{M_k}{N}$. Uma vez que

$$M_i = \bigcup_{j=1}^{\sigma(G)} (M_i \cap X_j)$$

e $\frac{M_i}{N} \cong \frac{G}{K}$ é cíclico ou satisfaz $\sigma(\frac{M_i}{N}) > \sigma(G)$, devemos ter $M_i = X_j$ para algum j. Portanto, $|\frac{K}{N}| < \sigma(G)$.

Em ambos os casos, $\frac{K}{N}$ é um fator principal de G com mais de um complemento e $\sigma(G) \geqslant |\frac{K}{N}| + 1$. ∎

Para finalizar esta seção, apresentaremos abaixo uma proposição que relaciona os conceitos de p-nilpotência com séries principais.

Lema 3.3.9 *Seja G um grupo solúvel e seja p um divisor primo de $|G|$. Assuma que todos os fatores principais complementados de G que são p-grupos são centrais. Então G é p-nilpotente.*

Demonstração: Indução em $|G|$, isto é, assuma por hipótese de indução o resultado válido para todos os grupos de ordem menor do que $|G|$.

Seja N um subgrupo normal minimal de G. Observe primeiramente que um fator principal de $\frac{G}{N}$ é um fator principal de G. Logo, todos os fatores principais complementados de $\frac{G}{N}$ que são p-grupos são centrais, e assim $\frac{G}{N}$ é p-nilpotente (por hipótese de indução).

Se $N \subseteq \Phi(G)$, então G é p-nilpotente. De fato, como $\frac{G}{N}$ é p-nilpotente, então qualquer quociente deste grupo também é p-nilpotente, e assim

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

é p-nilpotente, donde temos o resultado pelo Lema 3.3.5.

Agora assuma que $N \not\subseteq \Phi(G)$. Então pelo Lema 3.3.6 N é complementado em G por um subgrupo maximal M de G que não contém N.

Se N é um p-grupo, então por hipótese N é central (já que é normal minimal e, portanto, é um fator principal de G). Daí, $G = M \times N$, com $M \cong \frac{G}{N}$ p-nilpotente. Assim, existe $L \trianglelefteq M$ tal que $p \nmid |L|$ e $|M : L|$ é a ordem de um p-subgrupo de Sylow de M. Daí, $L \times 1$ é um subgrupo normal de G, com $p \nmid |L \times 1|$ e $|G : L \times 1|$ é a ordem de um p-subgrupo de Sylow de G. Portanto, $L \times 1$ é um p-complemento normal de G e G é p-nilpotente.

Assuma por fim que N não é um p-grupo (para o primo p). Tendo em vista o Lema 3.3.6, temos que $p \nmid |N|$. Seja então $\frac{K}{N}$ um p-complemento normal de $\frac{G}{N}$. Assim, $K \trianglelefteq G$ e $p \nmid |K|$. Ademais, se P é um p-subgrupo de Sylow de G, então $\frac{PN}{N}$ é um p-subgrupo de Sylow de $\frac{G}{N}$, donde

$$\left|\frac{K}{N}\right|\left|\frac{PN}{N}\right| = \left|\frac{KP}{N}\right| = \left|\frac{G}{N}\right|.$$

Portanto, $|KP| = |K||P| = |G|$. Logo, K é um p-complemento normal de G e G é p-nilpotente. ∎

3.4 Grupos de Frobenius e $\sigma = \rho$

Vamos introduzir esta sessão mencionando o seguinte teorema, devido a Zassenhaus, o qual classificou os complementos de Frobenius não solúveis (cuja demonstração pode ser consultada em [27]).

Teorema 3.4.1 *Seja $G = N \rtimes H$ um grupo de Frobenius, cujo complemento de Frobenius H é não solúvel. Então H tem um subgrupo normal H_0 com $|H : H_0| = 1$ ou 2 tal que $H_0 = SL(2,5) \times U$, com U um grupo de ordem coprima a 30.*

Proposição 3.4.2 *Seja G um grupo de Frobenius com $\sigma(G) = \rho(G)$. Então G é solúvel.*

Demonstração: Seja $G = N \rtimes H$ um grupo de Frobenius satisfazendo $\sigma(G) = \rho(G)$. Vamos mostrar que G é solúvel. Para provar isto, suponha por contradição que G não é solúvel.

Uma vez que N é o subgrupo de Fitting de G (Teorema 3.1.11), temos que H não é solúvel. Pelo Teorema 3.4.1, H tem um subgrupo normal H_0 de índice 1 ou 2 tal que $H_0 = SL(2,5) \times U$, onde U é um grupo de ordem coprima a 30.

Como $mdc(|SL(2,5)|, |U|) = 1$ (pois $|U|$ é coprima com 30 e portanto com $120 = |SL(2,5)|$), U é característico em H_0 e assim normal em H. Logo, $\sigma(G) \leqslant \sigma(H) \leqslant \sigma(H/U)$ e H/U é $SL(2,5)$ ou uma extensão $SL(2,5).2$.

Passando ao quociente pelo centro de $SL(2,5)$ (que é característico) nós encontramos $\sigma(G) \leqslant \sigma(A_5)$ ou $\sigma(G) \leqslant \sigma(A_5.2)$. Em qualquer caso, $\sigma(G) \leqslant min\{\sigma(A_5), \sigma(S_5)\} = \sigma(S_5) = 16$. Assim, vem

$$1 + \sqrt{|G|} \leqslant \rho(G) = \sigma(G) \leqslant 16$$

donde $|G| \leqslant 225$. Mas $120 \mid |G|$, então $|G| = 120$.

Concluímos, então, $G = SL(2,5)$, que não é um grupo de Frobenius pois não tem centro trivial, por exemplo. Uma contradição pelo Corolário 3.1.5. Portanto, G é solúvel, como queríamos. ∎

Antes de passarmos ao próximo resultado, vamos discutir de modo menos geral um dos argumentos que compõe a demonstração deste resultado.

Seja $G = C_{p^a} \times C_{q^b}$, com p e q primos distintos, um grupo cíclico. Um fator principal $\frac{H}{N}$ de G é um subgrupo normal minimal de $\frac{G}{N}$. Queremos estudar a quantidade de complementos de $\frac{H}{N}$ em $\frac{G}{N}$. Neste sentido, podemos então reduzir ao caso de $N = 1$ e H normal minimal de G. Assim, H é isomorfo a C_p ou C_q. Assuma sem perda de generalidade $H \cong C_p$. Então

$$H \leqslant \Phi(C_{p^a}) = C_{p^{a-1}} \Longleftrightarrow a > 1,$$

e neste caso H tem 0 complementos em G. Se $a = 1$, então um complemento de H em G tem ordem q^b, que por sua vez é a ordem do único q-subgrupo de Sylow de G. Logo, H tem um único complemento em G.

Teorema 3.4.3 *Seja G um grupo solúvel finito. Então G é cíclico se, e somente se, seus fatores principais têm no máximo um complemento.*

Demonstração: Suponha primeiramente G cíclico, então

$$G \cong C_{p_1^{l_1}} \times \cdots \times C_{p_n^{l_n}},$$

onde p_i é um primo para todo $i \in \{1, \ldots, n\}$ e $p_i \neq p_j$ para $i \neq j$. Os fatores principais de G são fatores principais de seus fatores diretos, que são todos grupos cíclicos de ordem potência de um primo p_i. Mas p-grupos cíclicos têm uma única série principal, e todos os fatores tem 0 complementos, exceto o fator principal "mais alto", que tem 1 complemento.

Para a recíproca, vamos usar indução em $|G|$, isto é, suponha por hipótese de indução que o resultado é válido para todos os grupos de ordem menor do que $|G|$.

Consideremos primeiramente o quociente $\frac{G}{\Phi(G)}$. Os fatores principais deste quociente são fatores principais de G. Logo, os fatores principais de $\frac{G}{\Phi(G)}$ têm no máximo um complemento, e assim, se $\Phi(G) \neq 1$, teremos $\left|\frac{G}{\Phi(G)}\right| < |G|$ e, por hipótese de indução, $\frac{G}{\Phi(G)}$ cíclico, digamos $\frac{G}{\Phi(G)} = \langle g\Phi(G)\rangle$. Neste caso, $G = \langle g, \Phi(G)\rangle$ donde concluímos $G = \langle g\rangle$.

Suponha agora $\Phi(G) = 1$ e considere N um subgrupo normal minimal de G. Uma vez que G é solúvel, temos que N é abeliano (Lema 3.3.6). Se N não tivesse complemento, então $N \subseteq \Phi(G)$, uma contradição pois $N \neq 1$ por definição. Logo, N possui um único complemento em G e, portanto, $N \subseteq Z(G)$ (Observação 3.3.7). Agora, como $\left|\frac{G}{N}\right| < |G|$, por hipótese de indução temos $\frac{G}{N}$ cíclico, e daí $\frac{G}{Z(G)}$ é cíclico (pois $\frac{G}{Z(G)} \cong \frac{G/N}{Z(G)/N}$). Neste caso, concluímos que G é abeliano e podemos descrever

$$G \cong \prod_{i=1}^{n} C_{p_i^{k_i}}.$$

Mas $\Phi(G) = 1$ implica $\Phi(C_{p_i^{k_i}}) = 1$ para todo $i \in \{1, \ldots, n\}$ (Teorema 3.3.3), donde obtemos $k_i = 1$ para todo i. Assim, se todos os primos na

decomposição de $|G|$ são distintos, então $G \cong \prod_{i=1}^{n} C_{p_i} \cong C_{p_1 p_2 \cdots p_n}$, e o teorema estará provado.

Suponha então que pelo menos dois dos primos na decomposição de $|G|$ coincidem, isto é, $G \cong C_p^2 \times C$ para algum primo p, onde C é um produto direto de grupos cíclicos de ordens primas e distintas. Vamos mostrar que isso é um absurdo. Se $C \neq 1$, então $\left|\frac{G}{C}\right| < |G|$ e por hipótese de indução teríamos $\frac{G}{C} \cong C_p^2$ cíclico, um absurdo. Portanto, $C = 1$ e $G \cong C_p^2$. Assim, C_p é um fator principal de G. Todavia, C_p possui p complementos em G, uma contradição com a hipótese dos fatores principais de G terem no máximo um complemento. Portanto, todos os primos na decomposição de G são distintos e G é cíclico. ■

Vamos agora ao nosso resultado principal.

Teorema 3.4.4 *Seja G um grupo de Frobenius finito solúvel. Então as seguintes afirmações são equivalentes.*

a) $\rho(G) = \sigma(G)$.

b) O núcleo de Frobenius é um subgrupo normal minimal de G e os complementos de Frobenius são cíclicos.

Demonstração: Sejam G um grupo de Frobenius finito satisfazendo a identidade $\sigma(G) = \rho(G)$. Pela Proposição 3.4.2 temos que G é solúvel. Ademais, pelo Teorema de Tomkinson (Teorema 3.3.8), $\sigma(G) = q + 1$, onde $q = p^l$ é a ordem do menor fator principal de G com mais de um complemento. Portanto, $\rho(G) = q + 1$ e, se

$$U_1, \ldots, U_{\rho(G)}$$

é uma partição de G de tamanho $\rho(G)$, então pelo Lema 1.1.9 vem

$$1 + q = \rho(G) \geqslant 1 + |U_i|$$

e assim $|U_i| \leqslant q$ para todo $i \in \{1, \ldots, \rho(G)\}$. Além disso, pelo Corolário 1.1.10 vem

$$1 + q = \rho(G) \geqslant 1 + \sqrt{|G|},$$

donde $|G| \leqslant q^2$.

Considere agora uma fixada série principal de G. Como $|G| \leqslant q^2$, então G tem no máximo dois fatores principais de ordem q. Se G tem exatamente dois

fatores principais de ordem q, então $|G| = q^2$ e, portanto, G é um p-grupo, o que não é possível pois G é um grupo de Frobenius. Logo, G tem um único fator principal de ordem q, isto é, precisamente um único fator principal na fixada série principal de G tem mais de um complemento.

Vamos tomar q^* como sendo a ordem de um outro fator principal $\frac{H_i}{H_{i-1}}$ da série principal fixada, com $q \neq q^*$. Observe que $qq^* \leqslant |G| \leqslant q^2$ e, portanto, $q^* < q$. Neste caso, tal fator principal não pode ter mais de um complemento (por definição de q).

Tendo em vista o que foi discutido no parágrafo anterior, vamos mostrar que $\frac{H_i}{H_{i-1}}$ é central ou não tem complementos. De fato, se $\frac{H_i}{H_{i-1}}$ tem complemento, então este complemento é único por hipótese. Logo, este complemento é normal (pois coincide com todos os seus conjugados), e portanto $\frac{H_i}{H_{i-1}}$ é central (Observação 3.3.7). Deste fato, pelo Lema 3.3.9, concluímos que G é r-nilpotente para todo primo $r \neq p$ divisor de $|G|$.

Com base nisto, denotemos por K_r o r-complemento normal de G. Observe primeiramente que $p||K_r|$, para todo primo $r \neq p$. Logo, p é o único primo na decomposição de $|G|$ que divide $|\bigcap_{r\neq p} K_r|$. Assim, a ordem desta interseção é uma potência de p. Agora, todo p-subgrupo de Sylow está contido em todo K_r para $r \neq p$ e portanto está contido em $\bigcap_{r\neq p} K_r$. Consequentemente, esta interseção é um p-subgrupo de Sylow de G e é normal (pois é interseção de subgrupos normais de G). Logo, este p-Sylow é único.

Denotando por P o único p-Sylow, pelo Teorema de Schur-Zassenhaus (Teorema 3.1.10) G é um produto semidireto $P \rtimes H$, onde H é isomorfo a $\frac{G}{P}$. Observando ainda que $p \nmid |H|$, pelo Teorema 3.4.3 temos H cíclico.

Feito isto, vamos estudar um pouco mais a estrutura de P.

Sendo G um grupo de Frobenius, e P um p-grupo (que é nilpotente e normal em G), temos que P está contido no subgrupo de Fitting de G, que por sua vez coincide com o núcleo de Frobenius N de G (Teorema 3.1.11). Se $P \neq N$, então $\frac{G}{P}$ é um grupo de Frobenius (Teorema 3.1.8) contradizendo o fato de que $\frac{G}{P}$ e cíclico (Teorema 3.4.3). Portanto, $P = N$, isto é, o p-subgrupo de Sylow P é exatamente o núcleo de Frobenius de G e todos os complementos de Frobenius de G são cíclicos.

Queremos mostrar agora que P é exatamente o fator principal de G com mais de um complemento.

Para tanto, suponha que existam P_1 e P_2 subgrupos normais de G tais que

$$P_2 \leqslant P_1 \leqslant P$$

e $\frac{P_1}{P_2}$ é o fator principal com mais de um complemento em uma série principal de G, isto é $\left|\frac{P_1}{P_2}\right| = q$ (podemos reduzir a esta situação tomando uma série principal que passa por P). Assim, vamos mostrar que $P_1 = P$ e $P_2 = 1$, e assim a implicação $(a) \Longrightarrow (b)$ está mostrada.

Se $P_1 \neq P$, então $\frac{G}{P_1}$ é um grupo de Frobenius (Teorema 3.1.8) contradizendo o fato de que $\frac{G}{P_1}$ é cíclico (Teorema 3.4.3). Portanto, $P_1 = P$.

Também $P_2 \subseteq \Phi(G)$. De fato, seja

$$P_2 = H_1 > H_2 > \cdots > H_t = 1$$

parte de uma série principal de G passando por P_2. Uma vez que $\frac{G}{H_i}$ é um grupo de Frobenius para todo $i \in \{1, \ldots, t\}$ (Teorema 3.1.8), temos $Z\left(\frac{G}{H_i}\right) = 1$ para todo i (Corolário 3.1.5) e os fatores principais $\frac{H_i}{H_{i+1}}$ são todos Frattini (têm 0 complementos). Observe que se algum destes fatores fosse complementado, seu complemento seria único (por construção) e, portanto, tal fator seria central (Observação 3.3.7), um absurdo. Portanto,

$$H_{t-1} = \frac{H_{t-1}}{H_t} \subseteq \Phi\left(\frac{G}{H_t}\right) = \Phi(G),$$

pois $H_t = 1$. Daí,

$$\frac{H_{t-2}}{H_{t-1}} \subseteq \Phi\left(\frac{G}{H_{t-1}}\right) = \frac{\Phi(G)}{H_{t-1}}.$$

Assim, $H_{t-2} \subseteq \Phi(G)$. Suponha por hipótese de indução $H_k \subseteq \Phi(G)$ para algum $1 \leqslant k \leqslant t-1$. Então,

$$\frac{H_{k+1}}{H_k} \subseteq \Phi\left(\frac{G}{H_k}\right) = \frac{\Phi(G)}{H_k},$$

e assim obtemos $H_{k+1} \subseteq \Phi(G)$. Desse modo, por indução concluímos que $H_1 = P_2 \subseteq \Phi(G)$.

Lembre agora que $1 + q = \rho(G) = \sigma(G)$. Seja

$$H_1, \ldots, H_{q+1}$$

uma partição de G. Como $P_2 \subseteq \Phi(G)$, temos $P_2 H_i \neq G$ para todo $i \in \{1, \ldots, q+1\}$, e assim a lista

$$\frac{H_1 P_2}{P_2}, \ldots, \frac{H_{q+1} P_2}{P_2}$$

é uma cobertura de $\frac{G}{P_2}$ e os q complementos de Frobenius de $\frac{G}{P_2}$ são subgrupos cíclicos e maximais (Lema 3.3.6) da forma $\frac{\langle x\rangle P_2}{P_2}$, onde x gera um complemento de Frobenius de G (Teorema 3.1.8). Portanto, cada $\frac{H_iP_2}{P_2}$ contém um único complemento de Frobenius $\frac{\langle x\rangle P_2}{P_2}$, e daí, a menos de reordenamento, $H_iP_2 = \langle x_i\rangle P_2$ para todo $i \in \{1,\ldots,q\}$ onde x_i gera um complemento de Frobenius de G para todo $i \in \{1,\ldots,q\}$. Em particular, P_2 é o único p-subgrupo de Sylow de H_iP_2 (pois $p \nmid |\langle x_i\rangle|$), e isso implica que

$$P = G \cap P = \bigcup_{i=1}^{q+1}(H_i \cap P) \subseteq P_2 \cup H,$$

onde $H = H_{q+1}$. Uma vez que nenhum grupo é a união de dois subgrupos próprios, deduzimos $P \subseteq H$, e assim, pelo Lema 1.1.9,

$$1 + q = \rho(G) \geqslant 1 + |H| \geqslant 1 + |P|$$

implicando $|P| \leqslant q = \left|\frac{P}{P_2}\right|$ e então $P_2 = 1$, como queríamos.

Nosso objetivo agora é obter a implicação $(b) \Longrightarrow (a)$.

Assuma agora que o núcleo de Frobenius N de G é um subgrupo normal minimal de G e que os complementos de Frobenius são cíclicos. Se H é um complemento de Frobenius de G, então pelo Lema 3.3.6 temos que H é um subgrupo maximal de G.

Sejam $\mathscr{P}$ uma partição de G e $\langle x_1\rangle, \langle x_2\rangle, \ldots, \langle x_t\rangle$ os complementos de Frobenius de G. Então cada x_i está contido em um único membro de $\mathscr{P}$ (pois $\langle x_i\rangle$ é maximal em G) e, portanto, $\langle x_i\rangle \in \mathscr{P}$. Por outro lado,

$$N \cap (\langle x_1\rangle \cup \cdots \cup \langle x_t\rangle) = 1$$

e assim $|\mathscr{P}| \geqslant t+1 = |N|+1$. Como este argumento vale para toda partição $\mathscr{P}$, temos $\rho(G) \geqslant |N| + 1$. Por outro lado, uma partição de um grupo de Frobenius é dada pelo seu núcleo de Frobenius e pelos seus complementos de Frobenius, temos $\rho(G) = |N| + 1$. Como N é o único fator principal com mais de um complemento, pelo Teorema de Tomkinson (Teorema 3.3.8) concluímos $\rho(G) = \sigma(G)$. ∎

3.5 Grupos de Frobenius e o Cálculo de ρ

Seja G um grupo de Frobenius.

Na seção anterior apresentamos uma condição necessária e suficiente para que $\sigma(G) = \rho(G)$. Uma interessante questão a respeito dos grupos de Frobenius levantada pelos autores em [10] é a seguinte. Será verdade que $\rho(G) = |N| + 1$, onde N é o núcleo de Frobenius de G?

A resposta a esta questão é negativa, conforme o teorema abaixo, e, de modo geral, algum trabalho ainda precisa ser desenvolvido a fim de explicitarmos $\rho(G)$.

Teorema 3.5.1 *Seja $G = C_3^3 \rtimes C_2$ um grupo de Frobenius com a ação de inversão, onde $C_2 = \langle f_1 \rangle$ e $C_3^3 = \langle f_2, f_3, f_4 \rangle$, e considere*

$$\begin{array}{ll} H_1 = \langle f_2, f_3 \rangle & H_6 = \langle f_2 f_3 f_4 \rangle \rtimes \langle f_3^2 f_4 f_1 \rangle \\ H_2 = \langle f_4 \rangle \rtimes \langle f_1 \rangle & H_7 = \langle f_2 f_4^2 \rangle \rtimes \langle f_3^2 f_1 \rangle \\ H_3 = \langle f_2 f_4 \rangle \rtimes \langle f_3 f_1 \rangle & H_8 = \langle f_3 f_4^2 \rangle \rtimes \langle f_2 f_1 \rangle \\ H_4 = \langle f_2 f_3^2 f_4^2 \rangle \rtimes \langle f_3 f_4^2 f_1 \rangle & H_9 = \langle f_2 f_3^2 f_4 \rangle \rtimes \langle f_3^2 f_4^2 f_1 \rangle \\ H_5 = \langle f_3 f_4 \rangle \rtimes \langle f_2^2 f_1 \rangle & H_{10} = \langle f_2 f_3 f_4^2 \rangle \rtimes \langle f_3 f_4 f_1 \rangle. \end{array}$$

Então $H_1, \ldots, H_{10}$ é uma partição de G e $\rho(G) = 10$.

Demonstração: Temos em G:

- 13 cópias de C_3;
- 27 cópias de C_2.

Seja $\mathscr{P}$ uma partição de G.

Se C_3^3 pertence a $\mathscr{P}$, então todas as cópias de C_2 também pertencem (pois $\frac{|G|}{|C_3^3|} = 2$), totalizando uma partição de tamanho $|\mathscr{P}| = 1 + 3^3 = 28$.

Suponha então que $H = C_3^2$ pertence a $\mathscr{P}$. Como $\frac{|G|}{|C_3^2|} = 6$, nenhum outro membro de $\mathscr{P}$ pode ser isomorfo a H e, neste caso, para particionar os demais elementos de G não contidos em H podemos usar apenas cópias de $C_3 \rtimes C_2$ e dos cíclicos C_2 e C_3. Mostraremos agora que existe uma partição de G com 9 cópias de $C_3 \rtimes C_2$, totalizando $|\mathscr{P}| = 1 + 9 = 10$.

Para tanto, vamos destacar os seguintes pontos.

Interseção de dois subgrupos de Frobenius de G

Considere $G = C_3^3 \rtimes C_2$ gerado por f_1, f_2, f_3 e f_4, onde

$$C_2 = \langle f_1 \rangle \qquad \text{e} \qquad C_3^3 = \langle f_2, f_3, f_4 \rangle.$$

Assim, todo elemento de ordem 2 em G é da forma gf_1, com $g \in C_3^3$. Além disso, observe que dois subgrupos de Frobenius

$$N_1 \rtimes \langle g_1 f_1 \rangle \qquad \text{e} \qquad N_2 \rtimes \langle g_2 f_1 \rangle$$

de G (com $g_1, g_2 \in C_3^3$ e $N_1, N_2 \leqslant C_3^3$) têm interseção trivial se, e somente se,

$$N_1 \cap N_2 = 1 \qquad \text{e} \qquad g_1 g_2^2 \notin N_1 N_2$$

pois: $n_1 g_1 f_1 = n_2 g_2 f_1 \iff n_1 g_1 = n_2 g_2 \iff g_1 g_2^2 = n_1^2 n_2 \in N_1 N_2$.

Determinantes

Vamos interpretar $V = C_3^3$ como um espaço vetorial 3-dimensional sobre $\mathbb{F}_3$ e considerar $v_1 = (x_1, y_1, z_1)$ e $v_2 = (x_2, y_2, z_2)$ vetores em V. Então o vetor $v = (a, b, c) \in V$ pertence ao subespaço $\langle v_1, v_2 \rangle$ gerado por v_1 e v_2 se, e somente se, o determinante da matriz dos coeficientes destes vetores é igual a zero, ou seja:

$$det \begin{pmatrix} a & x_1 & x_2 \\ b & y_1 & y_2 \\ c & z_1 & z_2 \end{pmatrix} = 0.$$

Lembre que estamos trabalhando sobre $\mathbb{F}_3$ e, portanto, dizer que um tal determinante é igual a zero significa dizer que este determinante é múltiplo de 3. Ademais, no que segue, usaremos a notação multiplicativa para $V = C_3^3$ (na qual os coeficientes aparecem como expoente de f_2, f_3 e f_4).

$H_1, \ldots, H_{10}$ é uma partição de G

É claro que $H_1 \cap H_i = 1$, para $i \in \{2, \ldots, 10\}$. Se $i > 1$, então H_i é da forma $\langle \alpha_i \rangle \rtimes \langle t_i \rangle$ e

$$\langle \alpha_i \rangle \cap \langle \alpha_j \rangle = 1$$

para quaisquer distintos $i, j \in \{2, \ldots, 10\}$. Assim, para mostrar que vale $H_i \cap H_j = 1$ para quaisquer distintos $i, j \in \{2, \ldots, 10\}$, precisamos mostrar que uma vez escrito $t_i = g_i f_1$ (com $g_i \in C_3^3$) temos $g_i g_j^2 \notin \langle \alpha_i, \alpha_j \rangle$, ou seja,

$$det(g_i g_j^2, \alpha_i, \alpha_j) \neq 0,$$

o qual vamos denotar por $det(i, j)$. Neste caso, vamos mostrar que, fixado $i \in 3, \ldots, 10$, temos $det(i, j) \neq 0$ para todo $j \in \{2, \ldots, i-1\}$.

- $i = 3$.

$$det(3,2) = det \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} = -1$$

- $i = 4$.

$$det(4,2) = det \begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & 0 \\ 2 & 2 & 1 \end{pmatrix} = -1 \qquad det(4,3) = det \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 0 \\ 2 & 2 & 1 \end{pmatrix} = 1$$

- $i = 5$.

$$det(5,2) = det \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = 2 \qquad det(5,3) = det \begin{pmatrix} 2 & 0 & 1 \\ 2 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix} = 2$$

$$det(5,4) = det \begin{pmatrix} 2 & 0 & 0 \\ 2 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix} = 4$$

- $i = 6$.

$$det(6,2) = det \begin{pmatrix} 0 & 1 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = -2 \qquad det(6,3) = det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = -1$$

$$det(6,4) = det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 2 \end{pmatrix} = 1 \qquad det(6,5) = det \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = -1$$

- $i = 7$.

$$det(7,2) = det \begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 0 \\ 0 & 2 & 1 \end{pmatrix} = -2, \qquad det(7,3) = det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 2 & 1 \end{pmatrix} = 1,$$

$$det(7,4) = det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 2 \\ 1 & 2 & 2 \end{pmatrix} = 2 \qquad det(7,5) = det \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} = -4$$

$$det(7,6) = det \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 2 & 2 & 1 \end{pmatrix} = 2$$

- $i = 8$.

$$det(8,2) = det\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} = 1 \qquad det(8,3) = det\begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} = 5$$

$$det(8,4) = det\begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix} = 1 \qquad det(8,5) = det\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix} = -2$$

$$det(8,6) = det\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 2 & 2 & 1 \end{pmatrix} = -1 \qquad det(8,7) = det\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 2 & 2 \end{pmatrix} = 4$$

- $i = 9$.

$$det(9,2) = det\begin{pmatrix} 0 & 1 & 0 \\ 2 & 2 & 0 \\ 2 & 1 & 1 \end{pmatrix} = -2 \qquad det(9,3) = det\begin{pmatrix} 0 & 1 & 1 \\ 1 & 2 & 0 \\ 2 & 1 & 1 \end{pmatrix} = -4$$

$$det(9,4) = det\begin{pmatrix} 0 & 1 & 1 \\ 1 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix} = -1 \qquad det(9,5) = det\begin{pmatrix} 1 & 1 & 0 \\ 2 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix} = 1$$

$$det(9,6) = det\begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix} = -2 \qquad det(9,7) = det\begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 0 \\ 2 & 1 & 2 \end{pmatrix} = -4$$

$$det(9,8) = det\begin{pmatrix} 2 & 1 & 0 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix} = 4$$

- $i = 10$.

$$det(10,2) = det\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} = -1 \qquad det(10,3) = det\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} = -1$$

$$det(10,4) = det\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 2 \\ 2 & 2 & 2 \end{pmatrix} = 2 \qquad det(10,5) = det\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} = -1$$

$$det(10,6) = det\begin{pmatrix} 0 & 1 & 1 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix} = 2 \qquad det(10,7) = det\begin{pmatrix} 0 & 1 & 1 \\ 2 & 1 & 0 \\ 1 & 2 & 2 \end{pmatrix} = -1$$

$$det(10,8) = det\begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 2 \end{pmatrix} = -1 \qquad det(10,9) = det\begin{pmatrix} 0 & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix} = 4$$

Com isso, criamos uma partição de G de tamanho 10.

Suponha agora que queremos utilizar m cópias de $C_3 \rtimes C_2$ em $\mathscr{P}$, com $0 \leqslant m \leqslant 9$ e $H = C_3^2 \in \mathscr{P}$. Então teremos uma partição de tamanho

$$1 + m + \underbrace{(27 - 3m)}_{\text{número de } C_2} + \underbrace{(9 - m)}_{\text{número de } C_3} = 37 - 3m.$$

Se $H = C_3^2 \notin \mathscr{P}$, então para m cópias de $C_3 \rtimes C_2$ em $\mathscr{P}$, com $0 \leqslant m \leqslant 9$, teremos uma partição de tamanho

$$m + \underbrace{(27 - 3m)}_{\text{número de } C_2} + \underbrace{(13 - m)}_{\text{número de } C_3} = 40 - 3m.$$

Caso utilizemos apenas subgrupos cíclicos de G, teremos uma partição de tamanho $|\mathscr{P}| = 13 + 27 = 40$.

Portanto, $\rho(G) = 10$, como queríamos. ■

Os subgrupos que compõem a partição descrita no teorema anterior foram originalmente obtidos utilizando o GAP, muito embora a demonstração apresentada acima contenha apenas argumentos algébricos e livre de recursos computacionais.

Capítulo 4

Grupos do Tipo Hughes-Thompson

O objetivo desse capítulo é classificar os grupos G do tipo Hughes-Thompson que satisfazem a igualdade $\sigma(G) = \rho(G)$.

Sejam G um grupo e p um primo. Dizemos que G é *do tipo Hughes-Thompson* relativo ao primo p se G não é p-grupo e $H_p(G) \neq G$, onde

$$H_p(G) = \langle g \in G : g^p \neq 1 \rangle.$$

Hughes em [13] perguntou se o índice de $H_p(G)$ em G é necessariamente 1, p ou $|G|$, tendo resultado positivo para grupos finitos que não são p-grupos, mas negativo para grupos em geral. Khukhro em [21] mostrou que para grupos finitos a resposta é sim "quase sempre". Hughes e Thompson e Kegel formularam o seguinte resultado (cuja demonstração pode ser consultada em [14] e [20]).

Teorema 4.0.2 (Hughes e Thompson, Kegel) *Sejam G um grupo finito e p um primo. Suponha $H_p(G) \neq G$. Então $H_p(G)$ é nilpotente. Se G não é p-grupo, então $H_p(G)$ é normal e de índice p em G.*

Observe que a classe dos grupos do tipo Hughes-Thompson não está contida na classe dos grupos de Frobenius. De fato, considere como um exemplo o grupo diedral D_6 de ordem 12 do qual destacamos $H_2(D_6) = C_6$. Lembre que D_6 tem centro não trivial e por isso não pode ser um grupo de Frobenius (Corolário 3.1.5). Veremos, no entanto, que o estudo da igualdade $\sigma = \rho$ para grupos do tipo Hughes-Thompson recai no caso de Frobenius.

Observe também que se G é um grupo do tipo Hughes-Thompson, então, diante do Teorema 4.0.2, temos que um elemento fixado $g \in G - H_p(G)$ tem ordem p e daí podemos definir $\varphi_g \in Aut(H_p(G))$ dado por $\varphi(x) = x^g$. Logo, G pode ser visto como o produto semidireto

$$G = H_p(G) \rtimes C_p.$$

Teorema 4.0.3 *Sejam G um grupo do tipo Hughes-Thompson relativo ao primo p.*

a) Se G não é um grupo de Frobenius, então $H_p(G)$ é um membro de toda partição de G e $\rho(G) = |H_p(G)| + 1$.

b) $\sigma(G) = \rho(G)$ se, e somente se, G é um grupo de Frobenius, onde núcleo de Frobenius é um subgrupo normal minimal e os complementos de Frobenius têm ordem p.

Demonstração: (a) Pela contrapositiva, seja $\mathscr{P}$ uma partição de G e suponha que $H_p(G)$ não pertence a $\mathscr{P}$. Então intersectando os membros de $\mathscr{P}$ com $H_p(G)$ obtemos uma partição de $H_p(G)$. Logo, $H_p(G)$ é um grupo nilpotente (pelo Teorema 4.0.2) e também é particionável. Assim, pela classificação dos grupos particionáveis (Teorema 1.1.5), existe um primo r tal que $H_p(G)$ é um r-grupo, e $r \neq p$ porque G não é um p-grupo.

Vamos denotar então $|G| = mp$, onde $m = |H_p(G)|$ é uma potência de r e $mdc(m, p) = 1$. Observe que

$$H_p(G) = \{g \in G : g^m = 1\}.$$

De fato, a inclusão $H_p(G) \subseteq \{g \in G : g^m = 1\}$ é óbvia (pois $m = |H_p(G)|$). Agora, se $g \in G$ é tal que $g^m = 1$, então a ordem de g divide m, e uma vez que $mdc(m, p) = 1$, então $g^p \neq 1$ e $g \in H_p(G)$.

Sabendo disso, note também que, se $g \in G$ tem ordem rp, então

$$x = g^r \qquad \text{e} \qquad y = g^p$$

têm ordens p e r, respectivamente. Portanto, x e y comutam e assim $(xy)^p = y^p \neq 1$, e assim $xy \in H_p(G)$. Mas $y \in H_p(G)$ implicando $x \in H_p(G)$, um absurdo pois $p \nmid m$. Este raciocínio mostra que para todo $g \in G$ temos $g^p = 1$ ou $g^m = 1$. Sendo $H_p(G) = \{g \in G : g^m = 1\}$, como mostrado acima,

pelo Teorema 3.1.7, concluímos que G é um grupo de Frobenius com núcleo $H_p(G)$ e complemento C_p.

A afirmação sobre $\rho(G)$ decorre do Lema 1.1.9.

(b) Seja G um grupo do tipo Hughes-Thompson relativo ao primo p, com a propriedade de que $\sigma(G) = \rho(G)$.

Se G é um grupo de Frobenius, o resultado segue diretamente do Teorema 3.4.4 pois $H_p(G) = Fit(G)$ e $|G : H_p(G)| = p$ (Teorema 4.0.2).

Mostraremos agora que não existe outra possibilidade para G. Desse modo, suponha por absurdo que G não é um grupo de Frobenius e seja $\mathscr{P}$ uma partição de G de cardinalidade $\rho(G)$. Pelo item (a), $H_p(G) \in \mathscr{P}$ e então pelo Lema 1.1.9 e pelo Teorema de Tomkinson (Teorema 3.3.8) vem

$$1 + |H_p(G)| = \rho(G) = \sigma(G) = 1 + q,$$

onde q é a menor ordem de um fator principal de G com mais de um complemento. Assim, $H_p(G)$ é um subgrupo normal minimal de $G = H_p(G) \rtimes \langle t \rangle$, onde t tem ordem p. Uma vez que $H_p(G)$ é abeliano, se $C_{\langle t \rangle}(g) = \langle t \rangle$, para um elemento $g \in H_p(G)$ não idêntico, então $gt = tg$, e assim $\langle g \rangle \trianglelefteq G$, donde concluímos $H_p(G) = \langle g \rangle$ e G abeliano. Logo, G é nilpotente particionável satisfazendo $\sigma(G) = \rho(G)$ e, pela Proposição 1.2.6, temos $G \cong C_p \times C_p$, um absurdo pois $H_p(G) \neq G$ por hipótese. Portanto, $C_{\langle t \rangle}(g) = 1$, para todo $g \in H_p(G)$ não idêntico, donde concluímos G um grupo de Frobenius, uma nova contradição.

A recíproca decorre do Teorema 3.4.4. ∎

Capítulo 5

Grupos Projetivos Particionáveis

O objetivo deste capítulo é estudar a igualdade $\sigma = \rho$ para os *grupos projetivos particionáveis* $\mathrm{PGL}_2(q)$ e $\mathrm{PSL}_2(q)$.

Mostramos que nenhuma cobertura minimal para os grupos projetivos particionáveis pode ser uma partição e calculamos o invariante ρ para todos estes grupos utilizando ciclos de Singer.

5.1 Grupos Projetivos Particionáveis e $\sigma = \rho$

Seja F um corpo com q elementos. Denotamos por $\mathrm{GL}_2(q)$ o *grupo linear*, formado pelas matrizes quadradas de ordem 2 sobre F com determinante diferente de zero, e por $\mathrm{SL}_2(q)$ o *grupo especial linear*, formado pelas matrizes quadradas de ordem 2 sobre F com determinante igual a 1.

Definimos, então, os grupos *linear geral projetivo* $\mathrm{PGL}_2(q)$ e *especial linear projetivo* $\mathrm{PSL}_2(q)$ respectivamente por

$$\mathrm{PGL}_2(q) = \frac{\mathrm{GL}_2(q)}{Z(\mathrm{GL}_2(q))} \quad \text{e} \quad \mathrm{PSL}_2(q) = \frac{\mathrm{SL}_2(q)}{Z(\mathrm{SL}_2(q))}.$$

Bryce, Fedri e Serena em [2] mostraram que toda cobertura minimal para $\mathrm{PGL}_2(q)$, com $q \geqslant 7$, e para $\mathrm{PSL}_2(q)$, com $q \geqslant 4$ mas $q \neq 5, 7, 9, 11$, contém uma estrutura rígida, formada pelo conjunto de todos os estabilizadores de espaços unidimensionais de $V = \mathbb{F}_q^2$, a menos de dois deles (Lema 4.1 do artigo [2]), e trataram os demais casos de modo especial. Neste contexto, vamos mostrar que uma cobertura minimal como esta não pode ser uma partição. Isto significa que $\sigma \neq \rho$ para os grupos projetivos particionáveis.

Para tanto, vamos desenvolver nossa análise a partir dos casos excepcionais tratados pelos autores supracitados exibindo uma partição minimal para os respectivos grupos. Consoante ao Teorema 1.1.5, os casos excepcionais são:

$$\mathrm{PGL}_2(5), \quad \mathrm{PSL}_2(5), \quad \mathrm{PSL}_2(7), \quad \mathrm{PSL}_2(9) \quad \text{e} \quad \mathrm{PSL}_2(11).$$

$\mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4)$ será tratado de maneira geral no Teorema **??**. Ademais, reafirmaremos duas observações sobre partições de um grupo G que já foram utilizadas no presente texto e das quais continuaremos a usá-las sem menção explícita. Se $H_1, \ldots, H_n$ é uma partição de G e $g \in G$ é tal que alguma potência $g^m \neq 1$ pertence a H_i para algum $i \in \{1, \ldots, n\}$, então g também pertence a H_i. Além disso, vamos usar repetidamente que $|H_i| \leqslant |G : H_j| = \frac{|G|}{|H_j|}$ para todo $i, j \in \{1, \ldots, n\}$ (vide a demonstração do Lema 1.1.9). Em especial, um subgrupo H de G não pertence a nenhuma partição de G se G contém elementos de ordem maior do que $|G : H|$ não contidos em H.

5.1.1 $\mathrm{PGL}_2(5)$

Proposição 5.1.1 $\rho(\mathrm{PGL}_2(5)) = 26$.

Demonstração: Vamos destacar primeiramente as seguintes informações.

- $|\mathrm{PGL}_2(5)| = 120 = 2^3 \cdot 3 \cdot 5$.
- Cada subgrupo maximal de $\mathrm{PGL}_2(5)$ é isomorfo a um dentre A_5, S_4, $S_3 \times S_2$ e $C_5 \rtimes C_4$.
- $\mathrm{PGL}_2(5)$ tem 25 elementos de ordem 2, 20 elementos de ordem 3, 30 elementos de ordem 4, 24 elementos de ordem 5 e 20 elementos de ordem 6.
- $\mathrm{PGL}_2(5) \cong S_5$.

Seja $\mathscr{P}$ uma partição de $\mathrm{PGL}_2(5)$.

Observe primeiramente que $A_5 \notin \mathscr{P}$ por conta dos elementos de ordem 4 e $S_4 \notin \mathscr{P}$ por conta dos elementos de ordem 6.

Suponha $C_5 \rtimes C_4 \in \mathscr{P}$. Assim, um outro membro de $\mathscr{P}$ deve ter ordem no máximo

$$\frac{|\operatorname{PGL}_2(5)|}{|C_5 \rtimes C_4|} = 6.$$

Neste caso, existe uma única cópia de $C_7 \rtimes C_3$ em $\mathscr{P}$ e para particionar os demais elementos de $\operatorname{PGL}_2(5)$ precisamos necessariamente utilizar subgrupos cíclicos, ou seja, 10 cópias de C_6, 5 cópias de C_5 e 10 cópias de C_4 (que particionam também os demais elementos de ordem 2), totalizando uma partição de tamanho $|\mathscr{P}| = 1 + 10 + 5 + 10 = 26$.

Suponha agora $C_5 \rtimes C_4 \notin \mathscr{P}$. Daí, o número de membros de $\mathscr{P}$ que contém elementos de ordem 4 é $\frac{30}{2} = 15$ (que *a priori* podem ser D_4 ou C_4). Nenhum dos subgrupos listados até então contêm elementos de ordem 6 e, em especial, qualquer subgrupo próprio de $\operatorname{PGL}_2(5)$ contém apenas dois elementos de ordem 6. Portanto, precisamos de pelo menos $\frac{20}{2} = 10$ destes subgrupos contendo elementos de ordem 6. Agora, nenhum dos subgrupos listados até então contém elementos de ordem 5 e qualquer subgrupo próprio de $\operatorname{PGL}_2(5)$ diferente de A_5 contém 4 elementos de ordem 5. Assim, para particioná-los precisamos de pelo menos $\frac{24}{4} = 6$ deles. Com isto, observamos que $|\mathscr{P}| \geqslant 15 + 10 + 6 = 31$.

Portanto, $\rho(\operatorname{PGL}_2(5)) = 26$. ∎

5.1.2 $\operatorname{PSL}_2(7)$

Proposição 5.1.2 $\rho(\operatorname{PSL}_2(7)) = 50$.

Demonstração: Vamos destacar primeiramente as seguintes informações.

- $|\operatorname{PSL}_2(7)| = 168 = 2^3 \cdot 3 \cdot 7$.
- Cada subgrupo maximal de $\operatorname{PSL}_2(7)$ é isomorfo a um dentre S_4 e $C_7 \rtimes C_3$.
- Em $\operatorname{PSL}_2(7)$ temos 21 elementos de ordem 2, 56 elementos de ordem 3, 42 elementos de ordem 4 e 48 elementos de ordem 7.

Seja $\mathscr{P}$ uma partição de $\operatorname{PSL}_2(7)$.

Suponha que $S_4 \in \mathscr{P}$. Observe que um outro membro de $\mathscr{P}$ deve ter ordem no máximo

$$\frac{|\operatorname{PSL}_2(7)|}{|S_4|} = 7.$$

Assim, existe uma única cópia de S_4 em $\mathscr{P}$ e, neste caso, faltam ser cobertos 12 elementos de ordem 2 e 36 elementos de ordem 4, em particular. Portanto, para particionar os elementos de ordem 4 precisamos exatamente de $\frac{36}{2} = 18$ cópias de C_4, o que nos dá um absurdo (pois cada C_4 possui um elemento de ordem 2 e $18 > 12$). Logo, $S_4 \notin \mathscr{P}$.

Suponha agora que $C_7 \rtimes C_3 \in \mathscr{P}$. Observe que um outro membro de $\mathscr{P}$ deve ter ordem no máximo

$$\frac{|\operatorname{PSL}_2(7)|}{|C_7 \rtimes C_3|} = 8.$$

Assim, existe uma única cópia de $C_7 \rtimes C_3$ em $\mathscr{P}$ e, neste caso, faltam ser cobertos $56 - 14 = 42$ elementos de ordem 3 e $48 - 6 = 42$ elementos de ordem 7, em particular.

Para particionar os elementos de ordem 4 podemos escolher utilizar *a priori* cópias de D_4 ou C_4. Mas em $\operatorname{PSL}_2(7)$ todo elemento de ordem 4 é raiz quadrada de um elemento de ordem 2, e portanto, $D_4 \notin \mathscr{P}$ (pois D_4 contém elementos de ordem 2 que não são raízes quadradas de nenhum elemento de ordem 4). Logo, em $\mathscr{P}$ temos necessariamente 21 cópias de C_4 (que particionam também os elementos de ordem 2).

Para particionar os elementos de ordem 3 *a priori* podemos considerar S_3 ou C_3. Mas, diante do que foi discutido acima, não é possível utilizar S_3 porque todos os elementos de ordem 2 já foram cobertos. Assim, só nos resta utilizar 21 cópias de C_3 e, por fim, 7 cópias de C_7 para cobrir os elementos de ordem 7, implicando $|\mathscr{P}| = 1 + 21 + 21 + 7 = 50$.

Observe que se $C_7 \rtimes C_3 \notin \mathscr{P}$, precisamos necessariamente de 8 cópias de C_7 para particionar os elementos de ordem 7. Agora, para os elementos de ordem 4, tendo em vista o que mostramos acima, precisamos necessariamente de 21 cópias de C_4 (que particionam também os elementos de ordem 2). Logo, para os elementos de ordem 3 só nos resta tomar 28 cópias de C_3 (pois desconsideramos S_3 que contém elementos de ordem 2). Com isso, temos uma partição de tamanho $|\mathscr{P}| = 8 + 21 + 28 = 57$.

Portanto, $\rho(\operatorname{PSL}_2(7)) = 50$. ∎

5.1.3 $\operatorname{PSL}_2(9)$

Proposição 5.1.3 $\rho(\operatorname{PSL}_2(9)) = 82$.

Demonstração: Vamos destacar primeiramente as seguintes informações.

- $|\operatorname{PSL}_2(9)| = 360 = 2^3 \cdot 3^2 \cdot 5$.
- Cada subgrupo maximal de $\operatorname{PSL}_2(9)$ é isomorfo a um dentre S_4, A_5 e $C_3^2 \rtimes C_4$.
- $\operatorname{PSL}_2(9)$ possui 45 elementos de ordem 2, 80 elementos de ordem 3, 90 elementos de ordem 4 e 144 elementos de ordem 5.
- S_4 possui 9 elementos de ordem 2, 8 elementos de ordem 3 e 6 elementos de ordem 4.
- A_5 possui 15 elementos de ordem 2, 20 elementos de ordem 3 e 24 elementos de ordem 5.
- $C_3^2 \rtimes C_4$ possui 9 elementos de ordem 2, 8 elementos de ordem 3 e 18 elementos de ordem 4.
- $\operatorname{PSL}_2(9) \cong A_6$.

Seja $\mathscr{P}$ uma partição de $\operatorname{PSL}_2(9)$.

Suponha que $A_5 \in \mathscr{P}$. Observe que um outro membro de $\mathscr{P}$ deve ter ordem no máximo

$$\frac{|\operatorname{PSL}_2(9)|}{|A_5|} = 6.$$

Assim, existe uma única cópia de A_5 em $\mathscr{P}$ e, neste caso, faltam ser cobertos $45-15 = 30$ elementos de ordem 2 e 90 elementos de ordem 4, em particular. Portanto, para particionar os elementos de ordem 4 precisamos exatamente de $\frac{90}{2} = 45$ cópias de C_4, um absurdo (pois cada C_4 possui um elemento de ordem 2 e $45 > 30$). Portanto, $A_5 \notin \mathscr{P}$.

Suponha $S_4 \in \mathscr{P}$. Observe que um outro membro de $\mathscr{P}$ deve ter ordem no máximo

$$\frac{|\operatorname{PSL}_2(9)|}{|S_4|} = 15.$$

Assim, existe uma única cópia de S_4 em $\mathscr{P}$ e, neste caso, faltam ser cobertos $45 - 9 = 36$ elementos de ordem 2 e $90 - 6 = 84$ elementos de ordem 4, em particular. Observe também que para particionar os elementos de ordem 4 podemos decidir utilizar entre cópias de D_4 ou C_4. Mas em $\operatorname{PSL}_2(9)$ todo elemento de ordem 2 é o quadrado de um elemento de ordem 4, e portanto, $D_4 \notin \mathscr{P}$ (pois D_4 contém elementos de ordem 2 que não são quadrados de nenhum elemento de ordem 4). Logo, em $\mathscr{P}$ temos necessariamente $\frac{84}{2} = 42$

cópias de C_4, o que nos dá um absurdo (pois cada C_4 possui um elemento de ordem 2 e $42 > 36$). Portanto, $S_4 \notin \mathscr{P}$.

Suponha agora $C_3^2 \rtimes C_4 \in \mathscr{P}$. Observe que um outro membro de $\mathscr{P}$ deve ter ordem no máximo

$$\frac{|\operatorname{PSL}_2(9)|}{|C_3^2 \rtimes C_4|} = 10.$$

Assim, existe uma única cópia de $C_3^2 \rtimes C_4$ em $\mathscr{P}$ e, neste caso, faltam ser cobertos 36 elementos de ordem 2 e 72 de ordem 4, em particular. Portanto, tendo em vista o que já argumentamos no parágrafo anterior, em $\mathscr{P}$ temos necessariamente 36 cópias de C_4 (que particionam também os elementos de ordem 2). Consequentemente, precisamos necessariamente de 36 cópias de C_5 para os elementos de ordem 5 e das 9 cópias de C_3^2 não contidas em $C_3^2 \rtimes C_4$ para os elementos de ordem 3, totalizando uma partição de tamanho $|\mathscr{P}| = 1 + 36 + 36 + 9 = 82$.

Se $C_{11} \rtimes C_5 \notin \mathscr{P}$ então precisamos necessariamente de 45 cópias de C_4 para particionar os elementos de ordem 4 (pois S_4 e D_4 não podem estar numa partição, como vimos acima) e que particionam também os elementos de ordem 2. Consequentemente, só nos resta tomar 36 cópias de C_5 para os elementos de ordem 5 e 40 cópias de C_3 para os elementos de ordem 3, totalizando uma partição de tamanho $|\mathscr{P}| = 45 + 36 + 40 = 121$.

Portanto, $\rho(\operatorname{PSL}_2(9)) = 109$. ∎

5.1.4 $\operatorname{PSL}_2(11)$

Proposição 5.1.4 $\rho(\operatorname{PSL}_2(11)) = 82$.

Demonstração: Vamos destacar primeiramente as seguintes informações.

- $|\operatorname{PSL}_2(11)| = 660 = 2^2 \cdot 3 \cdot 5 \cdot 11$.
- Cada subgrupo maximal de $\operatorname{PSL}(2, 11)$ é isomorfo a um dentre D_6, $C_{11} \rtimes C_5$ e A_5.
- $\operatorname{PSL}_2(11)$ possui 55 elementos de ordem 2, 110 elementos de ordem 3, 264 elementos de ordem 5, 110 elementos de ordem 6 e 120 elementos de ordem 11.

Seja $\mathscr{P}$ uma partição de $\operatorname{PSL}_2(11)$.

Observe que para particionar os elementos de ordem 6 podemos *a priori* decidir utilizar entre cópias de D_6 ou C_6. No entanto, em $\mathrm{PSL}_2(11)$ todo elemento de ordem 2 é a terceira potencia de um elemento de ordem 6 e, portanto, $D_6 \notin \mathscr{P}$ (pois D_6 contém elementos de ordem 2 que não são potência de nenhum elemento de ordem 6). Logo, em $\mathscr{P}$ temos necessariamente 55 cópias de C_6 (que além dos elementos de ordem 6, particionam também os elementos de ordem 2 e 3).

Precisamos agora cobrir os elementos de ordem 5 e 11 utilizando subgrupos de ordem coprima com 6 (uma vez que os elementos de ordem 2 e 3 já foram particionados).

Se $C_{11} \rtimes C_5 \in \mathscr{P}$ então qualquer outro subgrupo em $\mathscr{P}$ deve ter ordem no máximo

$$\frac{|G|}{|C_{11} \rtimes C_5|} = 12.$$

Assim, $\mathscr{P}$ deve conter todo subgrupo de ordem 5 e 11 fora de $C_{11} \rtimes C_5 \in \mathscr{P}$, totalizando uma partição de tamanho $|\mathscr{P}| = 55 + 1 + 55 + 11 = 122$.

Se $C_{11} \rtimes C_5 \notin \mathscr{P}$, então $\mathscr{P}$ contém todos os subgrupos de ordem 5 e 11, totalizando uma partição de tamanho $|\mathscr{P}| = 55 + 66 + 12 = 133$.

Portanto, $\rho(\mathrm{PSL}_2(11)) = 122$. ∎

5.2 Grupos Projetivos Particionáveis e o Cálculo de ρ

Seja $q \geqslant 4$ uma potência de um primo e considere os grupos projetivos particionáveis $\mathrm{PGL}_2(q)$, com $q \geqslant 4$, e $\mathrm{PSL}_2(q)$, com $q \geqslant 5$ ímpar. Bryce, Fedri e Serena mostraram em [2] que

$$\sigma(\mathrm{PSL}_2(5)) = 10, \qquad \sigma(\mathrm{PSL}_2(7)) = 15, \qquad \sigma(\mathrm{PSL}_2(9)) = 16$$

e em todos os outros casos

$$\sigma(\mathrm{PSL}_2(q)) = \sigma(\mathrm{PGL}_2(q)) = \begin{cases} \frac{1}{2}q(q+1) & \text{se } q \text{ é par} \\ \frac{1}{2}q(q+1)+1 & \text{se } q \text{ é ímpar} \end{cases}.$$

Conforme a Seção 5.1, encontramos também os seguintes valores para

$\rho(G)$ de um grupo projetivo particionável G em destaque:

G	$\sigma(G)$	$\rho(G)$
$\mathrm{PGL}_2(5)$	16	$26 = 5^2 + 1$
$\mathrm{PSL}_2(7)$	15	$50 = 7^2 + 1$
$\mathrm{PSL}_2(9)$	16	$82 = 9^2 + 1$
$\mathrm{PSL}_2(11)$	67	$122 = 11^2 + 1$

donde temos $\sigma \neq \rho$ para estes grupos. No resultado a seguir, vamos generalizar o cálculo de ρ para todos os grupos projetivos particionáveis motivados pela estratégia apresentada até então. Observe que ele abrange todos os grupos projetivos particionáveis pois $\mathrm{PSL}_2(q) \cong \mathrm{PGL}_2(q)$ se q é par e $\mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4)$. Para tanto, utilizamos a classificação de Dickson dos subgrupos maximais de $\mathrm{PGL}_2(q)$ e $\mathrm{PSL}_2(q)$ que pode ser consultada em [6].

Um dos conceitos em destaque na demonstração que vamos apresentar são os *ciclos de Singer*.

Seja F um corpo de tamanho q^n. Então o seu grupo multiplicativo $F^* = F - \{0\}$ é cíclico e tem ordem $q^n - 1$. Escrito $F^* = \langle s \rangle$, podemos definir um isomorfismo $\mathbb{F}_q$-linear

$$f : F \longrightarrow F \qquad \text{dado por} \qquad f(x) = sx.$$

Assim, interpretando F como um $\mathbb{F}_q$-espaço vetorial de dimensão n, temos que $f \in \mathrm{GL}(F)$ e tem ordem $q^n - 1$.

Assim, sendo $V = \mathbb{F}_q^n$ um $\mathbb{F}_q$-espaço vetorial de dimensão n, então um elemento de $\mathrm{GL}(V)$ de ordem $|V| - 1$ é dito um *ciclo de Singer* e induz elementos em $\mathrm{SL}(V), \mathrm{PGL}(V)$ e $\mathrm{PSL}(V)$ também ditos ciclos de Singer. Além disso, por simplicidade, o subgrupo cíclico gerado por um tal elemento também é dito ciclo de Singer.

Sejam $V = \mathbb{F}_q^n$ e $g \in \mathrm{GL}(V)$. Se W é um subespaço de V, então

$$gW = \{gw : w \in W\}.$$

Assim, g age no conjunto dos subespaços de W. No contexto do estudo que apresentamos, temos $V = \mathbb{F}_q^2$, e assim, temos que $\mathrm{GL}_2(q)$ age no conjunto $\{\langle v \rangle : v \in V\}$ dos subespaços unidimensionais de V, o qual é dito *linha projetiva*.

Se $g \in \mathrm{GL}_2(q)$ tem polinômio característico $f(X) \in \mathbb{F}_q[X]$ que é redutível, então g está contido em um estabilizador de um ponto na linha projetiva, que é um grupo de Frobenius com núcleo de Frobenius abeliano elementar de ordem q. De fato, escrito $V = \mathbb{F}_q^2$ e $g \in \mathrm{GL}(V)$, temos que se $f(X) = (X-a)(X-b)$, com $a, b \in \mathbb{F}_q$, então existe $v \in V$ com $gv = av$, e assim $g\langle v\rangle = \langle v\rangle$. Logo, g estabiliza v e considerando $\{v, v_0\}$ uma base qualquer de V contendo v, temos que g pode ser escrito como

$$g = \begin{pmatrix} \lambda & \beta \\ 0 & \alpha \end{pmatrix},$$

onde $\lambda, \alpha \in \mathbb{F}_q^*$ e $\beta \in \mathbb{F}_q$, e $\alpha = \lambda^{-1}$ se $g \in \mathrm{SL}_2(q)$. Logo, $g \in C_q \rtimes C_{q-1}$.

Se $f(X)$ é irredutível em $\mathbb{F}_q[X]$, então

$$\mathbb{F}_q[g] \cong \frac{\mathbb{F}_q[X]}{(f(X))} \cong \mathbb{F}_{q^2}$$

e assim $\mathbb{F}_q[g]$ é um corpo de ordem q^2 donde concluímos que g pertence a um ciclo de Singer, que é um subgrupo de ordem q^2-1 correspondente a um elemento de $F = \mathbb{F}_q^2$ agindo em F por multiplicação.

Isto implica que o estabilizador de um ponto junto com os ciclos de Singer formam uma cobertura de $\mathrm{GL}_2(q)$ e induz coberturas de $\mathrm{PGL}_2(q)$ e $\mathrm{PSL}_2(q)$.

Observe que os ciclos de Singer tem ordem $q+1$ em $\mathrm{PSL}_2(q)$ quando q é par, $q+1$ em $\mathrm{PGL}_2(q)$ quando q é ímpar e $\frac{q+1}{2}$ em $\mathrm{PSL}_2(q)$ quando q é ímpar.

De fato, se g é um ciclo de Singer de $\mathrm{GL}_2(q)$, então g tem ordem q^2-1 e

$$det(g^{q-1}) = det(g)^{q-1} = 1,$$

pois $|\mathbb{F}_q^*| = q-1$. Assim, $g^{q-1} \in \mathrm{SL}_2(q)$ e tem ordem $q+1$. Se q é par, então $Z(\mathrm{SL}_2(q)) = 1$ e portanto g^{q-1} visto em $\mathrm{PSL}_2(q)$ tem ordem $q+1$. Se q é ímpar, então

$$|Z(\mathrm{GL}_2(q))| = q-1 \qquad \text{e} \qquad |Z(\mathrm{SL}_2(q))| = 2.$$

Logo, g visto em $\mathrm{PGL}_2(q)$ tem ordem $q+1$ e g^{q-1} visto em $\mathrm{PSL}_2(q)$ tem ordem $\frac{q+1}{2}$.

Por fim, observe que a afirmação acima nos diz que g^{q+1} é escalar. De fato, temos que $\mathbb{F}_{q^2}$ tem um único subcorpo de tamanho q, e se trata de

$$\{x \in \mathbb{F}_{q^2} : x^q = x\}.$$

Assim, se $g \in \mathrm{GL}_2(q)$ é um ciclo de Singer, então

$$(g^{q+1})^q = g^{q^2+q} = g^{q^2-1}g^{q+1} = g^{q+1}$$

e portanto, g^{q+1} pertence ao subcorpo $\mathbb{F}_q$ de $\mathbb{F}_{q^2}$.

Teorema 5.2.1 *Seja $q = p^f$ uma potência de um primo p. Então*

$$\begin{array}{ll} \rho(\mathrm{PGL}_2(q)) = q^2+1, & \text{se } q \geqslant 3 \\ \rho(\mathrm{PSL}_2(q)) = q^2+1, & \text{se } q \geqslant 7. \end{array}$$

Demonstração: Suponha $q = 2^f$. Seja

$$G = \mathrm{PSL}_2(q) \cong \mathrm{PGL}_2(q) \cong \mathrm{SL}_2(q).$$

Então o grupo G tem ordem $|G| = q(q^2-1)$, expoente $2(q^2-1)$, contém q^2-1 involuções e os subgrupos maximais de G são:

- $C_2^f \rtimes C_{q-1}$ (vamos chamá-lo de *estabilizador de um ponto*);
- D_{q-1} (normalizador de um subgrupo cíclico gerado por um elemento semissimples de ordem $q-1$);
- D_{q+1} (normalizador de um ciclo de Singer);
- $\mathrm{PGL}_2(q_0)$, onde $q = q_0^r$ para algum primo r e $q_0 > 2$.

Antes de computarmos $\rho(G)$, precisamos de três observações.

Existe um conjugado de $D = D_{q-1}$, distinto de D, que intersecta-o de modo não trivial.

De fato, vamos pensar G como $\mathrm{SL}_2(q)$. Seja α um gerador do grupo multiplicativo $\mathbb{F}_q^*$ e, sem perda de generalidade, considere

$$D = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle = \bigcup_{m=0}^{q-2} \left\{ \begin{pmatrix} \alpha^m & 0 \\ 0 & \alpha^{-m} \end{pmatrix}, \begin{pmatrix} 0 & \alpha^m \\ \alpha^{-m} & 0 \end{pmatrix} \right\}.$$

Seja t um elemento de $\mathbb{F}_q$ diferente de 0 e 1, e seja $g = \begin{pmatrix} t & t+1 \\ 1 & 1 \end{pmatrix} \in G$. Uma vez que $|\mathbb{F}_q^*| = q-1$ é ímpar, existe $s \in \mathbb{F}_q$ tal que $s^2 = t(t+1)$. Assim, o conjugado

$$g^{-1} \begin{pmatrix} 0 & s \\ s^{-1} & 0 \end{pmatrix} g = \begin{pmatrix} 0 & st^{-1} \\ s^{-1}t & 0 \end{pmatrix}$$

é uma involução pertencente a $D \cap D^g$ e $D \neq D^g$ pois $g \notin D = N_G(D)$.

A interseção de quaisquer dois subgrupos maximais do tipo D_{q+1} tem ordem 2.

De fato, seja D um subgrupo maximal de G do tipo D_{q+1}. Primeiro observe que, uma vez que quaisquer dois ciclos de Singer tem interseção trivial, então a interseção entre quaisquer dois conjugados de D tem ordem no máximo 2.

Seja d o número de pares (H, x), onde H é um conjugado de D e x é uma involução pertencente a H. Como D tem $\frac{q(q-1)}{2}$ conjugados e cada um deles contém $q+1$ involuções, então

$$d = \frac{q(q-1)(q+1)}{2} = \frac{|G|}{2}.$$

Por outro lado, todas as involuções de G são conjugadas em pares, então cada uma delas pertence a um número constante c de conjugados de D. Daí,

$$\frac{|G|}{2} = d = c(q^2-1)$$

e assim, $c = \frac{q}{2}$.

Isto significa que toda involução pertence a $\frac{q}{2}$ conjugados de D. Cada uma das $q+1$ involuções em D pertence a $\frac{q}{2}-1$ conjugados de D distintos de D, e duas involuções de D não pertencem ao mesmo conjugado de D diferente de D porque a interseção de D com seus distintos conjugados tem ordem no máximo 2. Isto significa que D tem interseção não trivial com

$$(q+1)(\frac{q}{2}-1)+1 = \frac{q^2-q}{2}$$

de seus conjugados, e, portanto, com todos os seus conjugados.

Quaisquer dois 2-subgrupos de Sylow de G intersectam-se trivialmente.

Como $|G| = q(q^2-1)$ então um 2-subgrupo de Sylow tem ordem q. Considerando

$$P = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} : t \in \mathbb{F}_q \right\} \leqslant G,$$

temos que P é um 2-subgrupo de Sylow (pois $\mathbb{F}_q$ tem q elementos). Seja então $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(q)$ (isto é, com $ad - bc = 1$) cujo elemento inverso é $g^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Vem

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 + cdt & d^2 t \\ -c^2 t & 1 - cdt \end{pmatrix}$$

Como quaisquer dois 2-subgrupos de Sylow de G são conjugados em G, temos que se $c \neq 0$, então $g \notin N_G(P)$ e

$$g^{-1}Pg \neq P \qquad \text{e} \qquad g^{-1}Pg \cap P = 1.$$

Agora vamos provar que $\rho(G) = q^2 + 1$.

Considere $\mathscr{P}$ a lista de subgrupos de G formada por um estabilizador de um ponto H, os $\frac{q(q-1)}{2} - q$ subgrupos cíclicos de ordem $q-1$ não contidos em H, os $\frac{q(q+1)}{2}$ subgrupos cíclicos de ordem $q+1$ e os q 2-subgrupos de Sylow não contidos em H.

$\mathscr{P}$ determina uma partição de G

De fato, por uma simples análise da ordem destes grupos, temos que eles têm interseção trivial 2 a 2. Ademais, esta lista cobre uma quantidade de elementos igual a

$$q(q-1) + \left(\tfrac{q(q+1)}{2} - q\right)(q-1) + \tfrac{q(q-1)}{2}(q+1) + qq - \underbrace{\left[\frac{q(q+1)}{2} - q + \frac{q(q-1)}{2} + q\right]}_{\text{número de vezes que a identidade foi recontada}} =$$

$$(q-1)\left(q + \tfrac{q^2-q}{2} + \tfrac{q^2+q}{2}\right) + q^2 - q^2 = (q-1)(q+q^2) = q(q^2-1) = |G|$$

Portanto, uma vez que estes subgrupos determinam uma partição de G de tamanho $q^2 + 1$, temos $\rho(G) \leqslant q^2 + 1$.

Seja agora $\mathscr{P}$ uma partição qualquer de G. Vamos mostrar que $|\mathscr{P}| \geqslant q^2 + 1$.

Se $\mathscr{P}$ contém algum estabilizador de ponto $H \cong C_2^f \rtimes C_{q-1}$, então qualquer outro membro da partição tem ordem no máximo

$$\frac{|G|}{|H|} = q + 1.$$

Como $2(q-1) > q+1$ e, se $q = q_0^r$, com $q_0 > 2$ e r primo, então $\mathrm{PGL}_2(q_0)$ não contém elementos de ordem $q-1$ e nem de ordem $q+1$, com uma simples examinação dos subgrupos maximais mostra. Segue que $\mathscr{P}$ deve conter todos os subgrupos cíclicos de ordem $q-1$ não contidos em H e todos os subgrupos cíclicos de ordem $q+1$ (ciclos de Singer), que são todos conjugados nos dando um total de

$$\frac{|G|}{2(q-1)} - q + \frac{|G|}{2(q+1)} = q^2 - q$$

subgrupos.

Note que G contém $q^2 - 1$ involuções e todo subgrupo próprio de G contém no máximo $q+1$ involuções. Contudo, qualquer subgrupo próprio de G que não é do tipo D_{q+1} contém no máximo $q-1$ involuções. Seja n o número de membros de $\mathscr{P}$ contendo involuções. Como quaisquer dois D_{q+1} intersectam-se não trivialmente, $\mathscr{P}$ contém no máximo um deles, e então temos

$$\begin{gathered} q + 1 + (n-1)(q-1) \geqslant q^2 - 1 \Longrightarrow \\ q + 1 + nq - n - q + 1 \geqslant q^2 - 1 \Longrightarrow \\ n(q-1) \geqslant q^2 - 3 \Longrightarrow \\ n \geqslant \tfrac{q^2-1}{q-1} - \tfrac{2}{q-1} = q + 1 - \tfrac{2}{q-1} \geqslant q + 1, \end{gathered}$$

ou seja, $n \geqslant q+1$ (lembrando que $\frac{2}{q-1} < 1$ pois $q \geqslant 4$ neste caso). Como H contém involuções, isto implica que precisamos de pelo menos q subgrupos adicionais para cobrir os 2-subgrupos de Sylow e junto com H nos dá

$$|\mathscr{P}| \geqslant 1 + q^2 - q + q = q^2 + 1.$$

Se $\mathscr{P}$ não contém nenhum estabilizador de ponto, então para cobrir os elementos de ordem $q-1$ e $q+1$, $\mathscr{P}$ deve conter todos os subgrupos cíclicos de ordem $q-1$ (ou seus normalizadores) e todos os ciclos de Singer (ou seus normalizadores), o que nos dá

$$\frac{|G|}{2(q+1)} + \frac{|G|}{2(q-1)} = q^2$$

subgrupos.

Sejam a o número de subgrupos diedrais D_{q-1} em $\mathscr{P}$ e b o número de subgrupos diedrais D_{q+1} em $\mathscr{P}$. Se $\mathscr{P}$ é igual a família dos q^2 subgrupos listados acima, então olhando para os elementos de ordem 2 temos

$$a(q-1) + b(q+1) = q^2 - 1.$$

Entretanto, como existem dois D_{q-1} intersectando-se não trivialmente temos que $a \leqslant q$, e como quaisquer dois D_{q+1} intersectam-se não trivialmente temos $b \leqslant 1$. Se $b = 0$, então $q^2 - 1 = a(q-1) \leqslant q(q-1)$, uma contradição. Se $b = 1$, então $a(q-1) + q + 1 = q^2 - 1$ implicando $a = \frac{q^2-q-2}{q-1}$ contradizendo o fato de que a é um inteiro, sendo $q \geqslant 4$, o que nos dá um absurdo.

Seja agora $G = \mathrm{PGL}_2(q)$ com $q = p^f \geqslant 5$ e p um primo ímpar. (Observe que a hipótese inicial é $q \geqslant 3$, mas o caso $q = 3$ corresponde a $\mathrm{PGL}_2(3) \cong S_4$ que já foi tratado no Capítulo 2.) O grupo G tem ordem $|G| = q(q^2-1)$, expoente $\frac{p(q^2-1)}{2}$ e contém $q^2 - 1$ elementos de ordem p, todos contidos em $\mathrm{PSL}_2(q)$. Os subgrupos maximais de G não contendo $\mathrm{PSL}_2(q)$ são:

- $C_p^f \rtimes C_{q-1}$ (vamos chamá-lo de *estabilizador de um ponto*);
- D_{q-1}, onde $q \neq 5$ (normalizador de um subgrupo cíclico gerado por um elemento semissimples de ordem $q-1$);
- D_{q+1} (normalizador de um ciclo de Singer);
- S_4 para $3 < q = p \equiv \pm 3 \bmod 8$;
- $\mathrm{PGL}_2(q_0)$, onde $q = q_0^r$ e r primo.

Considere a lista $\mathscr{P}$ consistida de um estabilizador de um ponto H, os $\frac{q(q+1)}{2} - q$ subgrupos cíclicos de ordem $q-1$ não contidos em H, os $\frac{q(q-1)}{2}$ subgrupos cíclicos de ordem $q+1$ e os q p-subgrupos de Sylow de G não contidos em H.

C_{q-1} e C_{q+1} se intersectam trivialmente

Se $\langle C_{q-1}, C_{q+1} \rangle \neq G$, então existiria algum subgrupo maximais de G contendo $\langle C_{q-1}, C_{q+1} \rangle$. Mas, dada a lista acima, um tal subgrupo maximal não existe. Portanto, $\langle C_{q-1}, C_{q+1} \rangle = G$. Daí, pelo Lema 1.1.1, $C_{q-1} \cap C_{q+1} = 1$.

$\mathscr{P}$ determina uma partição de G

De fato, é claro que H intersecta os demais subgrupos desta lista de modo trivial. Como $p \nmid (q-1)$ e $p \nmid (q+1)$, posto que $q = p^f$), então as interseções de um p-subgrupo de Sylow com C_{q-1} e com C_{q+1} são triviais.

Portanto, todos os subgrupos em $\mathscr{P}$ se intersectam trivialmente 2 a 2. Ademais, esta lista cobre uma quantidade de elementos igual a

$$q(q-1) + \left(\tfrac{q(q+1)}{2} - q\right)(q-1) + \tfrac{q(q-1)}{2}(q+1) + qq - \underbrace{\left[\frac{q(q+1)}{2} - q + \frac{q(q-1)}{2} + q\right]}_{\text{número de vezes que a identidade foi recontada}} =$$

$$(q-1)\left(q + \tfrac{q^2-q}{2} + \tfrac{q^2+q}{2}\right) + q^2 - q^2 = (q-1)(q+q^2) = q(q^2-1) = |G|$$

Portanto, uma vez que estes subgrupos determinam uma partição de G de tamanho q^2+1, temos $\rho(G) \leqslant q^2+1$.

Como $\mathrm{PSL}_2(q)$ é um subgrupo de $\mathrm{PGL}_2(q)$, e ambos são particionáveis, deduzimos que

$$\rho(\mathrm{PSL}_2(q)) \leqslant \rho(\mathrm{PGL}_2(q)) \leqslant q^2+1.$$

Assim, se mostramos que $q^2+1 \leqslant \rho(\mathrm{PSL}_2(q))$, então vamos obter imediatamente $\rho(\mathrm{PSL}_2(q)) = \rho(\mathrm{PGL}_2(q)) = q^2+1$, para $q \neq 5$. Adiante, vamos mostrar $q^2+1 \leqslant \rho(\mathrm{PSL}_2(q))$ para $q \geqslant 13$. Observe que os casos $q = 5$, $q = 7$, $q = 9$ e $q = 11$ já foram mostrados.

Seja $G = \mathrm{PSL}_2(q)$, com $q = p^f \geqslant 5$ e p um primo ímpar. O grupo G tem ordem $|G| = \frac{q(q^2-1)}{2}$, expoente $\frac{p(q^2-1)}{4}$ e os subgrupos maximais de G são:

- $C_p^f \rtimes C_{q-1/2}$ (vamos chamá-lo de *estabilizador de um ponto*);
- D_{q-1}, onde $q \geqslant 13$ (normalizador de um subgrupo cíclico gerado por um elemento semissimples de ordem $q-1$);
- D_{q+1}, onde $q \neq 7, 9$ (normalizador de um ciclo de Singer);
- $\mathrm{PGL}_2(q_0)$, onde $q = q_0^2$;
- $\mathrm{PSL}_2(q_0)$, onde $q = q_0^r$ e r é um primo ímpar;

- A_4, S_4 ou A_5 para alguns valores de q.

Suponha $q \geqslant 13$. Os casos $q = 7, 9, 11$ foram feitos nas Seções 5.1.2, 5.1.3 e 5.1.4, respectivamente, e o caso $q = 5$ corresponde a $\mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4) \cong A_5$.

Vamos provar que $q^2 + 1$ é uma cota inferior para $\rho(G)$ trabalhando com elementos de ordem $\frac{q-1}{2}$, $\frac{q+1}{2}$ e p.

Observe que $\frac{q-1}{2} \geqslant 6$ pois $q \geqslant 13$. Portanto, os subgrupos A_4, S_4 e A_5 não contém elementos de ordem $\frac{q-1}{2}$ e $\frac{q+1}{2}$, e o mesmo é verdade para os subgrupos $\mathrm{PGL}_2(q_0)$ e $\mathrm{PSL}_2(q_0)$ pela simples examinação de seus subgrupos maximais.

Seja $\mathscr{P}$ uma partição de G.

Se $\mathscr{P}$ contém o estabilizador de um ponto $H = C_p^f \rtimes C_{q-1/2}$, então qualquer outro subgrupo em $\mathscr{P}$ tem ordem no máximo

$$\frac{|G|}{|C_p^f \rtimes C_{q-1/2}|} = q + 1.$$

Neste caso, para cobrir os elementos de ordem $\frac{q-1}{2}$ e $\frac{q+1}{2}$ precisamos dos subgrupos cíclicos de ordem $\frac{q-1}{2}$ ou os seus normalizadores $D_{q-1/2}$ e dos subgrupos cíclicos de ordem $\frac{q+1}{2}$ ou os seus normalizadores $D_{\frac{q+1}{2}}$. Como G contém $q^2 - 1$ elementos de ordem p e os subgrupos listados acima apenas H contém elementos de ordem p, precisamente $q - 1$ deles, precisamos necessariamente adicionar q subgrupos para cobrir estes elementos.

De fato, uma vez que $q \geqslant 13$ então todo subgrupo próprio de G contém no máximo $q - 1$ elementos de ordem p, incluindo A_4, S_4 e A_5. Como H contém q subgrupos cíclicos de ordem $\frac{q-1}{2}$ temos

$$|\mathscr{P}| \geqslant 1 + q\frac{q+1}{2} - q + q\frac{q-1}{2} + q = q^2 + 1.$$

Se $\mathscr{P}$ não contém nenhum estabilizador de ponto então para cobrir os elementos de ordem $\frac{q-1}{2}$ e $\frac{q+1}{2}$ a partição $\mathscr{P}$ deve conter todos os subgrupos cíclicos de ordem $\frac{q-1}{2}$ e $\frac{q+1}{2}$, ou os seus normalizadores, totalizando $q\frac{q+1}{2} + q\frac{q-1}{2} = q^2$ subgrupos. Uma vez que estes subgrupos não formam uma partição pois nenhum deles contém elementos de ordem p, concluímos $|\mathscr{P}| \geqslant q^2 + 1$.

■

Capítulo 6

Os Grupos de Suzuki

O objetivo deste capítulo é estudar a igualdade $\sigma = \rho$ para os *grupos de Suzuki*, o qual denotamos por $Sz(q)$, onde $q = 2^{2m+1}$. Para um estudo aprofundado sobre estes grupos indicamos consultar [15] e [33].

Seja $q = 2^{2m+1}$, com $m > 0$. O grupo de Suzuki $Sz(q)$ é definido como sendo o seguinte subgrupo de $\mathrm{GL}_4(q)$:

$$Sz(q) = \langle S(a,b), M(\lambda), T \quad | \quad a \in \mathbb{F}_q, b \in \mathbb{F}_q, \lambda \in \mathbb{F}_q^* \rangle,$$

onde

$$S(a,b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & \pi(a) & 1 & 0 \\ a^2\pi(a) + ab + \pi(b) & a\pi(a) + b & a & 1 \end{pmatrix},$$

$$M(\lambda) = \begin{pmatrix} \lambda^{1+2^m} & 0 & 0 & 0 \\ 0 & \lambda^{2^m} & 0 & 0 \\ 0 & 0 & \lambda^{-2^m} & 0 \\ 0 & 0 & 0 & \lambda^{-1-2^m} \end{pmatrix},$$

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

e π é o único automorfismo de $\mathbb{F}_q$ tal que $\pi^2(x) = x^2$.

A ordem de $G = Sz(q)$ é $|G| = q^2(q-1)(q^2+1)$. Consoante a [25], temos

$$\sigma(G) = \frac{1}{2}q^2(q^2+1).$$

Teorema 6.0.2 *Seja $G = Sz(q)$ um grupo de Suzuki. Então $\sigma(G) < \rho(G)$.*

Demonstração: Vamos destacar primeiramente algumas informações sobre G.

Seja U o subgrupo de G consistindo das matrizes unitriangulares. Temos que U é um 2-subgrupo de Sylow de G com expoente 4 e $|U| = q^2$. Seja H o subgrupo de G consistindo das matrizes diagonais. Então H é isomorfo a $\mathbb{F}_q^*$ e portanto $|H| = q - 1$.

Seja $r = 2^{m+1}$. Então $(q + r + 1)(q - r + 1) = q^2 + 1$. Sejam T_1 um torus maximal cíclico de ordem $q + r + 1$ e T_2 um torus maximal cíclico de ordem $q - r + 1$. Pelo Teorema 3.10 do capítulo XI de [15], o conjunto consistido de todos os conjugados de

$$H,\ U,\ T_1 \text{ e } T_2$$

é uma partição de G. O único subgrupo maximal de G contendo T_i é $N_i = N_G(T_i) = T_i\langle t_i\rangle$ para $i = 1, 2$, onde t_i é um elemento de ordem 4 e $|N_i : T_i| = 4$ para $i = 1, 2$.

O subgrupo $B = UH$ é um produto semidireto entre U e H, e tem a estrutura de grupo de Frobenius com núcleo de Frobenius U e complemento de Frobenius H. B é um subgrupo maximal de G de ordem $q^2(q - 1)$ e H é autonormalizado em B. Em particular, B contem q^2 conjugados de H. A interseção entre quaisquer dois conjugados de B é um conjugado de H.

Neste contexto, Lucido em [25] mostrou que

$$\{N_1^g, N_2^g, B^x : g \in G, x \in G - B\}$$

é uma cobertura minimal de G consistindo de subgrupos maximais.

Seja $\mathscr{P}$ uma partição de G.

Observe que os únicos subgrupos maximais de G contendo conjugados T_i^x de T_i (para $i = 1, 2$) são os normalizadores $N_G(T_i^x)$, que contém T_i^x como um subgrupo de índice 4, e quaisquer dois subgrupos distintos da forma T_i^x geram G. Uma vez que T_i é cíclico, isto prova que para cobrir estes conjugados precisamos de pelo menos

$$|G : N_G(T_1)| + |G : N_G(T_2)| = \frac{|G|}{4(q + r + 1)} + \frac{|G|}{4(q - r + 1)} = \frac{1}{2}q^2(q^2 - 1)$$

subgrupos na partição $\mathscr{P}$.

Uma vez que $|H| = q - 1$ é ímpar e os conjugados de T_i têm interseção trivial com os conjugados de H, então os seus normalizadores também tem interseção trivial com os conjugados de H. Os únicos subgrupos maximais contendo conjungados H^x são os correspondentes subgrupos de Borel B^x, onde $B = UH$, e os normalizadores $N_G(H^x)$, nos quais H^x tem índice 2.

Na partição $\mathscr{P}$ existe no máximo um conjugado de B porque quaisquer dois conjugados de B se intersectam em um conjugado de H. Seja $K \in \mathscr{P}$ tal que não é um conjugado de B e que contém um conjugado H^x de H. Se K contém mais de um conjugado de H então ele está contido em algum conjugado B_0 de B, que é um grupo de Frobenius, e assim $|B_0 : K| > 2$. De fato, se $|B_0 : K| = 2$ então K é normal em B_0 e isto contradiz o fato de qualquer subgrupo normal de um grupo de Frobenius está contido ou contém o núcleo de Frobenius. Agora, como H^x é autonormalizado em B_0, ele é autonormalizado em K também. Portanto, K contém no máximo $\frac{q^2}{4}$ conjugados de H pois

$$|K : N_K(H)| = |K : H| = \frac{|K|}{|H|} \geqslant \frac{|B_0/4|}{|H|} = \frac{q^2}{4}$$

uma vez que $|B_0| = q^2(q-1)$ e $|H| = q - 1$

Seja l o número de membros de $\mathscr{P}$ contendo conjugados de H. Uma vez que H tem $\frac{1}{2}q^2(q^2+1)$ conjugados em G, devemos ter

$$q^2 + (l-1)\frac{q^2}{4} \geqslant \frac{1}{2}q^2(q^2+1)$$

e assim $l \geqslant 2q^2 - 1$. Com isto, deduzimos que

$$|\mathscr{P}| \geqslant \frac{1}{2}q^2(q^2-1) + 2q^2 - 1 = \sigma(G) + q^2 - 1.$$

Portanto, $\rho(G) > \sigma(G)$.

■

Referências Bibliográficas

[1] BARNES, D. W., *On Complemented Chief Factors of Finite Soluble Groups*, Bull. Aust. Math. Soc. 7 (1972) 101-104.

[2] BRYCE, R. A., FEDRI, V., SERENA, L., *Subgroup Coverings of Some Linear Groups*, Bull. Aust. Math. Soc. 60 (2) (1999) 227-238.

[3] CIPOLLA, M., *Sulla Struttura dei Gruppi di Ordine Finito*. Rend. Acc. Sci. Fis. Mat. Napoli (3) 15 (1909), 44?54, 113?124; 17 (1911), 220?232; 18 (1917), 29?35.

[4] COHN, J. H. E., *On n-Sum Groups*, Math. Scand. 75 (1) (1994) 44-58.

[5] DETOMI, E., LUCCHINI, A., *On the Structure of Primitive n-Sum Groups*, CUBO Math. J. 10 (03) (2008) 195-210.

[6] DICKSON, L. E., *Linear Groups, With an Exposition of the Galois Field Theory*, Dover Publications, 2003.

[7] FOGUEL, T., SIZEMORE, N., *Partition Numbers of Finite Solvable Groups* (preprint), Adv. Group Theory Appl. (2019), https://doi.org /10.4399/9788825, in press.

[8] GAP - Groups, Algorithms, and Programming, Version 1.9.6. URL http://www.gap-system.org

[9] GARONZI, M., *Covering of Groups by Subgroups*. Tese de Doutorado, 2013.

[10] GARONZI. M., DIAS, M. L., *Group Partitions of Minimal Size*, Journal of Algebra 531 (2019) 1-18.

[11] GARONZI, M., LUCCHINI, A., *Irredundant and Minimal Covers of Finite Groups*, Comm. Algebra 44 (4) (2016) 1722-1727.

[12] GASCHÜTZ, W., *Existenz und Konjugiertsein von Untergruppen, die in endlichen auflösbaren Gruppen durch gewisse Indexschranken definiertsind,* J Algebra 53 (1978), $1 - 20$.

[13] HUGHES, D. R., *Research Problem No. 3*, Bull. Amer. Math. Soc. 63 (1957), p. 209.

[14] HUGHES, D. R., THOMPSON, J.G., *The H_p-problem and the structure of H_p-groups*, Pacific J. Math. 9 (1959), $1097 - 1101$.

[15] HUPPERT, B., BLACKBURN, N., *Finite Group III*, Springer-Verlag, Berlin - Heidelberg - New York, 1982.

[16] ISAACS, I. M., *Character Theory of Finite Groups*. Dover Publications, Inc., New York, 1994 ou AMS Chelsea Publishing, Providence RI, 2006.

[17] isaacs, I. M., *Equally Partioned Groups*. Pacific J. Math. 49 (1973), 109-116. MR 49417.

[18] ISAACS, I. M., *Finite Group Theory*, Graduate Studies in Mathematics, v. 92. American Mathematical Society, Providence, Rhode Island, 2008.

[19] KARPILOVSKY, G., *Groups Representations Volume 1 Part B: Introduction to Group Representations and Characters*, Elsevier Science Publishers B.V., 1992.

[20] KEGEL, O., *Die Nilpotenz der H_p-Gruppen*, Math. Z. 75 (1961), $373 - 376$.

[21] KHUKHRO, E.J., *On Hughes problem for finite p-groups*, Algebra and Logic 26 (1987), $398 - 401$.

[22] KHUKHRO, E. I., *The Structure of Finite Splittable p-Groups*. Sibirsk. Mat. Zh. 30 (1989), 208-218 (Russian); translation in Siberian Math. J. 30 (1990), 1010?1019. MR91d:20023.

[23] KONTOROVICH, P., *On the Representation of a Finite Group as a Direct Sum of its Subgroups I*. Mat. Sb. 5 (1939), 283-286.

[24] KONTOROVICH, P., *On the Representation of a Finite Group as a Direct Sum of its Subgroups II*. Mat. Sb. 7 (1940), 27-33.

[25] LUCIDO, M., *On the Covers of Finite Groups*, Groups St. Andrews 2001 in Oxford. Vol. II, London Math. Soc. Lecture. Note Ser., vol. 305, Cambridge Univ. Press, Cambridge, 2003, pp. 395-399.

[26] MILLER, G. A., *Groups in Which All the Operators are Contained in a Series of Subgroups such that Any Two Have Only Identity in Commun*. Bull. Amer. Math. Soc. 17 (1906/1907), 446-449.

[27] PASSMAN, D. S., *Permutation Group*. Benjamin, New York, 1968.

[28] ROBINSON, D. J. S., *A Course in the Theory of Groups*. Springer-Verlag New York Inc, New York, 1982.

[29] SCORZA, G., *I Gruppi che Possono Pensarsi Come Somme di Tre Loro Sottogruppi*. Boll. Un Mat. Ital. (1926) 216-218.

[30] SIZEMORE, N., *Group Covers and Partitions: Covering and Partition Numbers*. Tese de Mestrado, 2013.

[31] SUZUKI, M., *On the Finite Groups with a Complete Partition*. J. Math. Soc. Japan 2 (1950), 165-185. MR 13,907b.

[32] TOMKINSON, M. J., *Groups As the Union of Proper Subgroups*. Math. Scand. 81 (1997), 191 − 198.

[33] WILSON, R. A. *The Finite Simple Groups*. Springer-Verlag London Limited 2009.

[34] ZAPPA, G., *Partitions and Other Coverings of Finite Groups*. Illinois Journal of Mathematics, vol. 47, Number 1/2, Spring/Summer 2003, pp. 571-580.