Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

O Grau de Comutatividade de Subgrupos de um Grupo Finito

por

Mônica Aparecida Cruvinel Valadão

Orientador: Noraí Romeu Rocco

Brasília

2011

Aos meus pais,
irmãs e sobrinhos

Agradecimentos

Primeiramente a Deus, por essa benção concedida.

À minha família, em especial aos meus pais, Neuza Cruvinel Valadão e Manoel Matias Valadão por acreditarem em meus sonhos e mostrarem que seria possível realizá-los, a conclusão deste trabalho é um deles. Às minhas irmãs, Simone Cruvinel Valadão e Verônica Cruvinel Valadão por apoiarem meus estudos e aos meus sobrinhos, Jorge Emanuel Cruvinel Alencar e Iasmim Cruvinel Alencar.

Ao professor Noraí Romeu Rocco, pela oportunidade de trabalhar sob a sua orientação. Agradeço pela confiança, paciência e disposição com que conduziu este trabalho.

À professora Ticianne Proença Bueno e ao professor Rudolf Richard Maier, pela participação na banca examinadora.

Aos amigos, Hudson, Gardel, Jairo, Renato, Bruno, Tarcísio, Joabe e Thiago pelo apoio nas horas difíceis e por compartilharem momentos de alegria. Também aos colegas de turma, Enio, Raimundo, Thaynara, Andréia e Kaliana pela amizade e ajuda com as disciplinas.

Em especial, a amiga Grace Kelly a quem tenho grande admiração. À Maria, pela sua amizade e às meninas, Keydna, Ilana e Renata pelos momentos de alegria. Também aos amigos Eudes e Eduardo, pela disposição em assistir as minhas prévias e pelas sugestões antes da defesa.

Agradeço também os professores do departamento de matemática que contribuíram com a minha formação, enfim agradeço a todas as pessoas, que de alguma forma, me ajudaram a chegar aqui, nesta fase tão importante em minha vida.

Ao CAPES/Reuni pelo apoio financeiro durante a realização deste trabalho.

"*Não tenhamos pressa*
mas não percamos tempo."
José Saramago

Resumo

Neste trabalho estudamos questões relacionadas ao grau de comutatividade entre subgrupos de um grupo finito. Nossa abordagem é baseada em resultados de M. Tărnăuceanu, que adaptou ao contexto da teoria de reticulados alguns conceitos e técnicas dos estudos feitos por P. Lescot sobre o grau de comutatividade de um grupo finito. Para este fim, apresentamos um breve estudo sobre a teoria de reticulados, particularmente do reticulado dos subgrupos de um grupo, donde resulta uma expressão geral para determinar o grau de comutatividade de subgrupos de um grupo finito. Tal expressão mede a probabilidade com que dois subgrupos de um grupo finito comutam. Como aplicações dos resultados teóricos calculamos em detalhes os graus de comutatividade de subgrupos para algumas classes de grupos finitos.

Palavras-chave: grau de comutatividade de subgrupos, reticulados, reticulado dos subgrupos de um grupo, $p-$grupos finitos, grupos metabelianos finitos.

Abstract

In this work we study questions related to subgroup commutativity degrees in finite groups. Our approach is based on results of M. Tărnăuceanu, who adapted to the context of lattice theory some concepts and techniques of studies by P. Lescot concerning commutativity degrees of finite groups. For this purpose, we present a brief study of lattice theory, particularly of the lattice of all subgroups of a group, from which we obtain a general expression to determine the subgroup commutativity degrees of finite groups. This expression measures the probability that two subgroups of a finite group commute. As applications of the theoretical results we compute in detail the subgroup commutativity degrees of finite groups for some classes of finite groups.

Keywords: subgroup commutativity degree, lattices, lattice of subgroups of a group, finite $p-$groups, finite metabelian groups.

Sumário

Introdução

Nos últimos anos têm crescido o interesse em usar a probabilidade na teoria de grupos finitos. Como destaque temos os estudos realizados por Lescot [6], sobre o grau de comutatividade $d(G)$, de um grupo finito G, dado pela igualdade

$$d(G) = \frac{1}{|G|^2}|\{(x, y) \in G \times G \mid xy = yx\}|.$$

A expressão acima calcula a probabilidade com que dois elementos quaisquer de um grupo finito G comutam. Citamos como referência os trabalhos de Gustafson [4], Lescot [7], Erfanian - Lescot - Rezaei [2] e Rusin [13], que são artigos relacionados a comutatividade entre elementos de um grupo finito.

No presente trabalho concentramos as nossas atenções no estudo do grau de comutatividade entre subgrupos de um grupo finito, baseado principalmente no artigo *Subgroup commutativity degrees of finite groups*, de Marius Tărnăuceanu [18]. Nesse trabalho o autor adaptou ao contexto da teoria de reticulados, alguns conceitos e técnicas dos estudos feitos por P. Lescot sobre o grau de comutatividade de um grupo finito e apresentou, assim, uma expressão que determina o grau de comutatividade de subgrupos de um grupo finito.

Para facilitar a compreensão deste trabalho, dividimos o mesmo em quatro capítulos, os quais descreveremos a seguir.

O primeiro traz alguns resultados básicos em teoria de grupos que consideramos importantes para o desenvolvimento dos tópicos subsequentes, tais como grupos solúveis e nilpotentes. Uma seção de destaque deste capítulo, é a que trata dos $p-$grupos finitos que possuem um subgrupo maximal cíclico. O grau de comutatividade de subgrupos, dos grupos que pertencem a essa classe está determinado no último capítulo.

No segundo capítulo fazemos uma breve introdução à teoria de reticulados. Inici-

amos com a definição e propriedades básicas de reticulados em geral e, subsequentemente, restringimos as nossas considerações ao reticulado dos subgrupos de um grupo. Estudamos também os conceitos de isomorfismo e de produto direto entre reticulados, a modularidade e a permutabilidade de subgrupos de um grupo.

No terceiro capítulo apresentamos uma expressão geral do grau de comutatividade de subgrupos de um grupo finito G, que denotamos por $sd(G)$. Demonstramos também as propriedades básicas para $sd(G)$, fundamentadas nos conceitos da teoria de reticulados abordados no capítulo anterior.

O último capítulo está dividido em três seções. A primeira delas é voltada para dar uma expressão do grau de comutatividade de subgrupos do grupo diedral e a segunda, para expressar o grau de comutatividade de subgrupos de $p-$grupos finitos que possuem um subgrupo maximal cíclico. Na última seção apresentamos três problemas em aberto, concernentes a comutatividade de subgrupos de grupos finitos.

Capítulo 1

Preliminares

Neste capítulo apresentaremos as definições e conceitos que consideramos fundamentais para o desenvolvimento deste trabalho. Muitos desses resultados serão enunciados sem as suas respectivas demonstrações, pois as mesmas exigem outros conceitos que não apresentaremos neste capítulo.

1.1 Grupos Solúveis e Nilpotentes

Iniciaremos com as definições de série normal e subnormal, em seguida daremos o conceito de solubilidade e nilpotência.

Definição 1.1. *Uma série normal de um grupo G é uma sequência de subgrupos $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{1\}$, tal que cada G_i é um subgrupo normal de G, onde $i = 0, \cdots, n$.*

Definição 1.2. *Uma série subnormal de um grupo G é uma sequência de subgrupos $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{1\}$, tal que cada G_i é um subgrupo normal de G_{i-1}, com $i = 0, \cdots, n$.*

Seja $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{1\}$ uma série subnormal de um grupo G. Os grupos fatores desta série são os grupos $\dfrac{G_i}{G_{i+1}}$ e o comprimento de uma tal série é o número de fatores não triviais. Se na série subnormal definida acima, G_{i+1} for um subgrupo normal maximal de G_i, dizemos então que esta série é uma *série de*

composição de G. Assim, uma série de composição de G é uma série subnormal cujos fatores são todos simples.

Uma *série principal* de um grupo G é uma série normal $G = G_0 > G_1 > \cdots > G_n = 1$ tal que cada G_{i+1} é maximal entre os subgrupos normais a G contidos em G_i.

Definição 1.3. *Um grupo G é solúvel se ele possui uma série subnormal cujos fatores são todos abelianos.*

Como exemplos de grupos solúveis temos os grupos abelianos e os $p-$grupos finitos.

Enunciaremos agora um teorema que será usado para demonstrar um dos corolários do capítulo 2.

Teorema 1.1. *Um grupo finito G é solúvel se, e somente se, os grupos fatores em uma série de composição de G são cíclicos de ordem prima.*

A demonstração deste teorema encontra-se em [5], pag. 139.

Definição 1.4. *Uma série central de um grupo G é uma série normal $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{1\}$, tal que $\dfrac{G_i}{G_{i+1}} \leq \mathcal{Z}\left(\dfrac{G}{G_{i+1}}\right)$ para $i = 0, \cdots, n-1$.*

Definição 1.5. *Um grupo G é nilpotente se ele possui uma série central.*

Teorema 1.2. *Os $p-$grupos finitos são nilpotentes. Um grupo finito é nilpotente se, e somente se, ele é o produto direto dos seus subgrupos de Sylow.*

Teorema 1.3. *Seja G um grupo finito. Então G é nilpotente se, e somente se, todo subgrupo maximal de G é normal.*

Estes dois últimos teoremas encontram-se demonstrados em [11] pag. 130.

Definição 1.6. *Seja G um grupo. Definimos indutivamente os seguintes subgrupos:*

$$\begin{aligned} \gamma_1(G) &= G \\ \gamma_2(G) &= [\gamma_1(G), G] = G' \\ &\vdots \\ \gamma_i(G) &= [\gamma_{i-1}(G), G]. \end{aligned}$$

A sequência de subgrupos $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \cdots$ é chamada série central inferior *de G.*

Definição 1.7. *Dado um grupo G definimos indutivamente os subgrupos:*

$$\begin{aligned} \mathcal{Z}_0(G) &= 1 \\ \mathcal{Z}_1(G) &= \mathcal{Z}(G) \\ &\vdots \\ \frac{\mathcal{Z}_i(G)}{\mathcal{Z}_{i-1}(G)} &= \mathcal{Z}\left(\frac{G}{\mathcal{Z}_{i-1}(G)}\right). \end{aligned}$$

A sequência de subgrupos $\{1\} = \mathcal{Z}_0(G) \leq \mathcal{Z}_1(G) \leq \cdots \leq \mathcal{Z}_i(G) \leq \cdots$ *é chamada* série central superior *de G.*

Teorema 1.4. *Seja G um grupo. Então existe um índice c com $\mathcal{Z}_c = G$ se, e somente se, $\gamma_{c+1}(G) = 1$. Além disso, $\gamma_{i+1}(G) \leq \mathcal{Z}_{c-i}(G)$, para todo i. O índice c é chamado a classe de nilpotência de G.*

Para detalhes da demonstração consulte [12].

Usando o teorema anterior demonstramos a proposição a seguir.

Proposição 1.1. *Um grupo G é nilpotente de classe 2 se, e somente se, $G' \leq \mathcal{Z}(G)$.*

Proposição 1.2. *A identidade $[u^m, v] = [u, v]^{u^{m-1}+u^{m-2}+\cdots+u+1}$ é válida em qualquer grupo, (onde $x^{y+z} = x^y x^z$). Além disso, se $[u, v]$ pertence ao centro de $\langle u, v\rangle$, então $[u^m, v] = [u, v]^m = [u, v^m]$.*

Esta proposição é na verdade um exercício que se encontra em [11], pag. 128.

Proposição 1.3. *Em um grupo nilpotente de classe no máximo 2 vale a identidade $(xy)^m = x^m y^m [y, x]^{\binom{m}{2}}$.*

A demonstração desta proposição é feita usando indução sobre m e a proposição anterior. Para mais detalhes veja [11], pag. 141.

1.2 A classe de p-grupos finitos que possuem um Subgrupo Maximal Cíclico.

Consideremos $\mathcal{G}$ a classe constituída de todos os $p-$grupos finitos de ordem p^n, p primo e $n \geq 3$, que possuem um subgrupo maximal cíclico. A classe $\mathcal{G}$ contém $p-$grupos

abelianos finitos do tipo $\mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$ e $p-$grupos não abelianos finitos. Estamos interessados nos $p-$grupos não abelianos dessa classe $\mathcal{G}$. Descreveremos tais grupos no teorema seguinte, cuja demonstração é adaptada de [11].

Teorema 1.5. *Seja G um grupo não abeliano tal que G pertence a classe $\mathcal{G}$. Então G é isomorfo a um dos seguintes grupos:*

(i) $M(p^n) = \langle a, x | a^{p^{n-1}} = x^p = 1, x^{-1}ax = a^{p^{n-2}+1} \rangle$, *onde* $n > 3$ *para* $p = 2$.

(ii) Diedral $D_{2^n} = \langle a, x | a^{2^{n-1}} = x^2 = 1, x^{-1}ax = a^{-1} \rangle$.

(iii) Quatérnio Generalizado $Q_{2^n} = \langle a, x | a^{2^{n-1}} = x^2 = a^{2^{n-2}}, x^{-1}ax = a^{2^{n-1}-1} \rangle$.

(iv) Quasi-Diedral $S_{2^n} = \langle a, x | a^{2^{n-1}} = x^2 = 1, x^{-1}ax = a^{2^{n-2}-1} \rangle$ $n \geq 4$.

Demonstração. Sejam G um grupo de ordem $p^n, n \geq 3$ e $N = \langle a \rangle$ um subgrupo maximal cíclico. Temos então que $N \triangleleft G, |G : N| = p$ e $|N| = |\langle a \rangle| = p^{n-1}$. Escrevendo $G/N = \langle xN \rangle$ temos $G = \langle x, a \rangle$ e $x^p \in N$.

O elemento x induz um automorfismo em N que necessariamente tem ordem p, assim $a^x = a^m$ onde $m^p \equiv 1 (\text{mod } p^{n-1})$ e $1 < m < p^{n-1}$. Como $(m, p^{n-1}) = 1$ temos que $(m, p) = 1$ e pelo Teorema de Fermat, $m^{p-1} \equiv 1 (\text{mod } p)$ donde segue que $m \equiv 1 (\text{mod} p)$. Analisaremos a seguir os casos p ímpar e $p = 2$.

Caso 1.1. *p é ímpar.*

Neste caso, escrevemos $m = 1 + kp^i$ onde $(k, p) = 1$ e afirmamos que $0 < i < n - 1$. Assim, usando o Binômio de Newton,

$$m^p = (1 + kp^i)^p = 1 + kp^{i+1} + \frac{p-1}{2}k^2p^{2i+1} + \cdots + k^p p^{pi}.$$

Daí,

$$m^p - (1 + kp^{i+1}) = \frac{p-1}{2}k^2p^{2i+1} + \cdots + k^p p^{pi}.$$

Observamos que $2i + 1 \geq i + 1$ se, e somente se, $i \geq 1$ e como $0 < i < n - 1$ temos que $i + 2 \leq j(i + 1)$ para $j \geq 2$ e assim, $p^{i+2} | j(i + 1)$ para $j \geq 2$. Com isso,

$$m^p \equiv (1 + kp^{i+1}) (\text{mod } p^{i+2}).$$

Assim, existe $l \in \mathbb{Z}$ tal que $(m^p-1) = k.p^{i+1}+lp^{i+2}$ e como $m^p \equiv 1(\text{mod}p^{n-1})$ temos que $(k+lp)p^{i+1} \equiv 0(\text{mod } p^{n-1})$. Como $(k,p) = 1$ temos que $p^{n-1}|p^{i+1}$, daí $n-1 \leq i+1 < n$ e de $i+1 \leq n-1$ segue que $i+1 = n-1$ e $i = n-2$. Obtemos então que $m = 1+kp^{n-2}$. Agora de $(k,p) = 1$ temos que existe $k' \in \mathbb{Z}$ tal que $kk' \equiv 1(\text{mod } p)$. Novamente, usando o Binômio de Newton em $a^{x^{k'}} = a^{m^{k'}} = a^{(1+kp^{n-2})^{k'}}$ obtemos,

$$(1+kp^{n-2})^{k'} - (1+kk'p^{n-2}) = \frac{k'-1}{2}k^2p^{2(n-2)} + \cdots + k^{k'}p^{k'(n-2)}.$$

Observamos que $2(n-2) \geq n-1$ se, e somente se, $n \geq 3$. Mas $n \geq 3$, logo $n-1 \leq j(n-2)$ para $j \geq 2$ e daí $p^{n-1}|p^{j(n-2)}$ para $j \geq 2$. Assim,

$$(1+kp^{n-2})^{k'} \equiv (1+kk'p^{n-2})(\text{mod } p^{n-1}).$$

Agora de $kk' \equiv 1(\text{mod } p^{n-1})$ segue que $kk'p^{n-2} \equiv p^{n-2}(\text{mod } p^{n-2})$. Daí, $(1+kp^{n-2})^{k'} \equiv (1+p^{n-2})(\text{mod } p^{n-1})$, isto é, existe $r \in \mathbb{Z}$ tal que $(1+kp^{n-2})^{k'} = 1+p^{n-2}+rp^{n-1}$. Com isso, $a^{x^{k'}} = a^{(1+kp^{n-2})^{k'}} = a^{1+p^{n-2}+rp^{n-1}} = a^{1+p^{n-2}}$. Assim, podemos trocar x por $x^{k'}$ e assumir que $m = 1+p^{n-2}$.

Agora, voltemos à discusão sobre a posição de x^p em N. Temos que $(x^p)^x = (x^x)^p = x^p$ e como $x^p \in N$ segue que $x^p = a^i$. Daí, $a^i = (a^i)^x = a^{i+ip^{n-2}}$, ou seja, $(a^i)^{p^{n-2}} = 1$ se, e somente se, $|x^p|$ divide p^{n-2}. Assim, $x^p \in \langle a^p \rangle$, digamos $x^p = b^p$, onde $b \in N$. Notemos agora que G é nilpotente de classe 2, pois $[a,x] = a^{-1}a^x = a^{-1}a^m = a^{-1}a^{1+p^{n-2}} = a^{p^{n-2}} \in \mathcal{Z}(G)$. Pela Proposição (1.3), temos que $(xb^{-1})^p = x^pb^{-p}[b^{-1},x]^{\binom{p}{2}} = [b^{-p},x^p]^{\frac{(p-1)!}{2}} = 1$. Dessa forma, trocando x por xb^{-1} podemos assumir que $x^p = 1$ e assim, G é do tipo (i).

Caso 1.2. *p=2.*

Como $(m, 2^{n-1}) = 1$, temos que m é ímpar, digamos $m = 2k+1$. De $m^2 \equiv 1(mod\ 2^{n-1})$ segue que $k(k+1) \equiv 0(mod\ 2^{n-3})$, daí $k \equiv 0(mod\ 2^{n-3})$ ou $k \equiv -1(mod\ 2^{n-3})$. Assim, $m = 2^{n-2}l+1$ onde l é ímpar ou $m = 2^{n-2}l-1$.

Quando $m = 2^{n-2}l+1$, temos que $(l, 2^{n-2}) = 1$ e daí exixte $k' \in \mathbb{Z}$ tal que $k'l \equiv (mod\ 2^{n-1})$. De modo análogo ao que fizemos anteriormente, obtemos que $a^{m^{k'}} = a^{1+2^{n-2}}$. Assim, podemos trocar x por uma potência conveniente $x^{k'}$ e assumir que $m = 1+2^{n-2}$. Análogamente, para $m = 2^{n-2}l-1$, podemos fazer $m = 2^{n-1}-1$ se l é par ou $m = 2^{n-2}-1$ se l é ímpar. Devemos analisar cada um desses valores de m.

Suponhamos que $m = 2^{n-1} - 1$ e daí obtemos $a^x = a^{-1}$. Uma vez que $(x^2)^x = x^2$, o elemento x^2 tem ordem 1 ou 2 em N. Se $|x^2| = 1$ temos que $x^2 = 1$, daí $G \cong D_{2^n}$ e se $|x^2| = 2$ temos que $x^2 = a^{2^{n-2}}$ e assim $G \cong Q_{2^n}$.

Assumimos agora que $m = 2^{n-2} + 1$. Uma vez que x^2 não pode gerar N, temos que $x^2 = a^{2r}$, para algum r. Fazendo $b = a^{r(2^{n-3}-1)}$, calculamos que $(xb)^2 = x^2b^2[b,x] = a^{2r}a^{r(2^{n-2}-2)}a^{r(2^{n-3}-1)2^{n-2}} = a^{r2^{2n-5}}$. Se $n \geq 4$, temos que esta potência de a é igual a 1 e daí G é do tipo (i). Se $n = 3$, então $a^x = a^{-1}$ e $x^2 = 1$ ou a^2 e assim, $G \cong D_8$ ou Q_8.

Finalmente, seja $m = 2^{n-2} - 1$. Se $x^2 = a^{2r}$, então $a^{2r} = (a^{2r})^x = a^{2r(2^{n-2}-1)}$, em que $2r \equiv 0 (mod\ 2^{n-2})$ e $x^2 = 1$ ou $a^{2^{n-2}}$. Se $x^2 \neq 1$, então $(xa^{-1})^2 = a^{2n-2}a^{-2}a^{-(2^{n-2}-2)} = 1$ e G é do tipo (iv). □

Proposição 1.4. *Os grupos descritos no teorema anterior satisfazem as seguintes propriedades:*

(i) Um dos subgrupos maximais é cíclico.

(ii) No grupo $G = M(p^n)$ o centro é $\mathcal{Z}(G) = \langle a^p \rangle$ e o comutador é $G' = \langle a^{p^{n-2}} \rangle$.

(iii) Nos grupos $G = D_{2^n}, Q_{2^n}$ e S_{2^n} o centro $\mathcal{Z}(G)$ tem ordem 2 e $\dfrac{G}{\mathcal{Z}(G)} \cong D_{2^{n-1}}$.

(iv) O grupo Q_{2^n} contém exatamente um elemento de ordem 2.

A demonstração desta proposição pode ser vista em [3] ou em [16].

Capítulo 2

Uma Introdução à Teoria de Reticulados

Faremos neste capítulo, uma breve introdução à teoria de reticulados e focaremos principalmente nos resultados que envolvem o reticulado dos subgrupos $\mathscr{L}(G)$ de um grupo G. Conforme veremos no próximo capítulo, a expressão para determinar o grau de comutatividade de subgrupos de um grupo finito G depende do reticulado dos subgrupos $\mathscr{L}(G)$ de G. Para a construção deste capítulo utilizamos como referência, o artigo de Ore [9] e os livros de R. Schmidt[14] e Suzuki [17].

2.1 Conceitos Fundamentais

Iniciaremos esta seção com a definição de conjunto parcialmente ordenado pois, veremos adiante que um reticulado é um conjunto parcialmente ordenado com certas propriedades.

Definição 2.1. *Um conjunto parcialmente ordenado é um conjunto P com uma relação binária $\leq$ tal que para todo $x, y, z \in P$, as seguintes condições são satisfeitas:*

(i) $x \leq x$. *(Reflexiva)*

(ii)Se $x \leq y$ *e* $y \leq x$, *então* $x = y$. *(Antisimétrica)*

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

Um elemento x de um conjunto parcialmente ordenado P é um *limite inferior* para um subconjunto S de P se $x \leq s$ para todo $s \in S$. O elemento x é o *ínfimo* de S se x é um limite inferior de S e $y \leq x$ para qualquer limite inferior y de S. Decorre do item (ii) da definição anterior que, o ínfimo quando existe é único e denotaremos por $\wedge S$. Do mesmo modo definimos *limite superior* e *supremo*, sendo o último denotado por $\vee S$.

Podemos agora dar a definição de um reticulado.

Definição 2.2. *Um reticulado é um conjunto parcialmente ordenado L em que todo par de elementos tem um supremo e um ínfimo. Dados $x, y \in L$, definimos $\wedge\{x, y\} = x \wedge y$ e $\vee\{x, y\} = x \vee y$ como sendo, respectivamente, o ínfimo e o supremo do par $\{x, y\}$.*

Se num conjunto parcialmente ordenado, todo subconjunto possuir um supremo e um ínfimo, então esse conjunto será chamado de *reticulado completo.*

Podemos também ver reticulados como álgebras com duas operações binárias. Veja o teorema a seguir.

Teorema 2.1. *Seja $(L, \leq, \wedge, \vee)$ um reticulado. Então para todo $x, y, z \in L$:*

(i) $x \wedge y = y \wedge x$ *e* $x \vee y = y \vee x$. *(Comutatividade)*

(ii) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ *e* *(Associatividade)*
$(x \vee y) \vee z = x \vee (y \vee z)$.

(iii) $x \wedge (x \vee y) = x$ *e* *(Absorção de Identidades)*
$x \vee (x \wedge y) = x$

(iv) $x \leq y$ *se e somente se* $x = x \wedge y$ *ou* $y = y \vee x$.

Reciprocramente, se L é um conjunto com duas operações $\wedge$ e $\vee$ satisfazendo $(i) - (iii)$ e a relação $\leq$ é definida por $x \leq y$ se e somente se $x = x \wedge y$, então $(L, \leq, \wedge, \vee)$ é um reticulado com $x \wedge y = \wedge\{x, y\}$ e $x \vee y = \vee\{x, y\}$ para todo $x, y \in L$. A recíprocra é válida ainda se definirmos a relação $\leq$ em L por $x \leq y$ se e somente se $y = y \vee x$.

Se G é um grupo qualquer, indicamos por $\mathscr{L}(G)$ o conjunto de todos os subgrupos de G, o qual é parcialmente ordenado por inclusão: $H \leq K$ se, e somente se, $H \subseteq$

K, para todos $H, K \in \mathscr{L}(G)$. Define-se em $\mathscr{L}(G)$ as operações $\wedge$ e $\vee$ como sendo $H \wedge K := H \cap K$ e $H \vee K := \langle H, K \rangle$, o subgrupo de G gerado pela união $H \cup K$. Com essas operações, $(\mathscr{L}(G), \subseteq, \wedge, \vee)$ é um reticulado, chamado o *reticulado dos subgrupos* de G. Por simplicidade vamos indicá-lo por $\mathscr{L}(G)$.

Se $(L, \leq, \wedge, \vee)$ é um reticulado, então um *subreticulado* de L é, por definição, um subconjunto de L fechado pelas operações $\wedge$ e $\vee$. Como exemplo de subreticulado de um reticulado L temos, para $x, y \in L$, o intervalo $[y/x] = \{z \in L \mid x \leq z \leq y\}$ se $x \leq y$. Temos também o conjunto e $\mathscr{N}(G) = \{H \in \mathscr{L}(G) | H \trianglelefteq G\}$, que consiste de todos os sugrupos normais de um grupo G e o próprio $\mathscr{L}(G)$.

Definiremos agora um conceito de grande importancia ao nosso trabalho, que é o isomorfismo entre reticulados.

Definição 2.3. *Sejam L e $\bar{L}$ reticulados. Uma aplicação $\sigma : L \to \bar{L}$ é um homomorfismo se, para quaisquer $x, y \in L$, valem:*

(i) $(x \wedge y)^\sigma = x^\sigma \wedge y^\sigma$.

(ii) $(x \vee y)^\sigma = x^\sigma \vee y^\sigma$.

O homomorfismo σ é um isomorfismo se σ for uma aplicação bijetiva. Neste caso dizemos que L e $\bar{L}$ são isomorfos e escreveremos $L \cong \bar{L}$.

Definição 2.4. *Se G e $\bar{G}$ são grupos quaisquer, um isomorfismo de $\mathscr{L}(G)$ em $\mathscr{L}(\bar{G})$ é chamado uma* projetividade *de G em $\bar{G}$. Dizemos também que G e $\bar{G}$ são* reticulado-isomorfos *se exitir uma projetividade de G em $\bar{G}$.*

Para mostrar que uma aplicação bijetiva entre dois reticulados é um homomorfismo, é suficiente provar que ela satisfaz um dos itens da Definição (2.3) ou que preserva as relações de ordem dos reticulados, conforme o teorema a seguir.

Teorema 2.2. *Seja σ uma aplicação bijetiva de um reticulado L sobre um reticulado $\bar{L}$. Então, para todos $x, y \in L$, as seguintes condições são equivalentes:*

(i) $x \leq y$ *se, e somente se,* $x^\sigma \leq y^\sigma$.

(ii) $(x \wedge y)^\sigma = x^\sigma \wedge y^\sigma$.

(iii) $(x \vee y)^\sigma = x^\sigma \vee y^\sigma$.

Além disso, se σ *satisfaz* (i) *e* S *é um subconjunto de* L *tal que* $\wedge S$ *existe, então* $\wedge S^\sigma$ *existe e* $(\wedge S)^\sigma = \wedge S^\sigma$; *analogamente,* $(\vee S)^\sigma = \vee S^\sigma$ *se* $\vee S$ *existe.*

Demonstração. $(i) \Leftrightarrow (ii)$

Do Teorema (2.1), $x \leq y$ se, e somente se $x = (x \wedge y)$, donde segue que $x^\sigma \leq y^\sigma$ se, e somente se, $x^\sigma = (x \wedge y)^\sigma = x^\sigma \wedge y^\sigma$.

$(iii) \Rightarrow (ii)$

Se $x^\sigma = (x \wedge y)^\sigma$, então pelo Teorema (2.1), $x^\sigma \leq y^\sigma$. Mas pelo mesmo teorema, $x^\sigma \leq y^\sigma$ se, e somente se, $x^\sigma = x^\sigma \wedge y^\sigma$ ou $y^\sigma = y^\sigma \vee x^\sigma$, donde segue que $(x \wedge y)^\sigma = x^\sigma \wedge y^\sigma$.

$(ii) \Leftarrow (iii)$

Suponhamos que $y^\sigma = (x \vee y)^\sigma$, daí pelo Teorema (2.1), $x^\sigma \leq y^\sigma$ e por esse mesmo teorema, $x^\sigma \leq y^\sigma$ se, e somente se, $x^\sigma = x^\sigma \wedge y^\sigma$ ou $y^\sigma = x^\sigma \vee y^\sigma$. Logo, $(x \vee y)^\sigma = x^\sigma \vee y^\sigma$.

Se S é um subconjunto de L satisfazendo (i), então σ é um homomorfismo. Daí se $\wedge S$ existe, segue que $(\wedge S)^\sigma = \wedge S^\sigma$. Analogamente, $(\vee) S^\sigma = \vee S^\sigma$, se $\vee S$ existe. □

2.2 Construção de Projetividades

Definimos anteriormente o conceito de projetividade entre grupos. Veremos agora alguns resultados sobre projetividades induzidas por uma aplicação bijetiva entre dois grupos quaisquer.

Definição 2.5. *Dados dois grupos* G *e* $\bar{G}$ *e uma aplicação* $\sigma : G \to \bar{G}$, *para todo subconjunto* X *de* G *escreveremos* $X^\sigma = \{x^\sigma | x \in X\}$. *Se, para todo subconjunto* X *de* G, $X \leq G$ *se, e somente se,* $X^\sigma \leq \bar{G}$, *então dizemos que* σ *é uma* l-aplicação.

Proposição 2.1. *Sejam* G *e* $\bar{G}$ *grupos e* $\sigma : G \to \bar{G}$ *uma l-aplicação. Se* σ *é bijetiva, então a aplicação* $\bar{\sigma} : \mathscr{L}(G) \to \mathscr{L}(\bar{G})$ *definida por* $H^{\bar{\sigma}} = H^\sigma$ *é uma projetividade de* G *em* $\bar{G}$.

Demonstração. Dado $K \in \mathscr{L}(G)$ e sendo σ uma l-aplicação, segue que $K^\sigma \leq \bar{G}$. Agora seja $H \in \mathscr{L}(G)$, como $H^{\bar{\sigma}} = H^\sigma \leq \bar{G}$, segue que $\bar{\sigma} : G \to \bar{G}$ também é $l-$aplicação. Daí, pelo Teorema (2.2), $(H \wedge K)^{\bar{\sigma}} = H^{\bar{\sigma}} \wedge K^{\bar{\sigma}}$, para todos $H, K \in \mathscr{L}(G)$, donde

segue que $\bar{\sigma} : \mathscr{L}(G) \to \mathscr{L}(\bar{G})$ é um homomorfismo. Da bijetividade de σ segue que $\bar{\sigma}$ também é bijetiva e portanto $\bar{\sigma}$ é uma projetividade de G em $\bar{G}$. □

A projetividade $\bar{\sigma}$ dada pela Proposição (2.1) é chamada projetividade induzida por σ. De maneira geral, uma dada projetividade φ é induzida por uma l-aplicação $\sigma : G \to \bar{G}$ se $H^{\varphi} = H^{\sigma}$, para todo subgrupo H de G.

Observação 2.1. *Se σ é um isomorfismo do grupo G no grupo $\bar{G}$, então σ satisfaz $H \leq G$ se, e somente se, $H^{\sigma} \leq \bar{G}$ e daí, pela Proposição (2.1), σ induz uma projetividade de G em $\bar{G}$.*

Entretanto, uma l-aplicação não necessariamente é um isomorfismo entre grupos. Uma medida de quanto uma l-aplicação dista de ser um homomorfismo é o conceito de $amorfia$, que definiremos a seguir.

Definição 2.6. *Seja σ uma l-aplicação de G em $\bar{G}$. A aplicação $\theta : G \times G \to \bar{G}$ definida por $\theta(x, y) = (y^{\sigma})^{-1}(x^{\sigma})^{-1}(xy)^{\sigma}$, para todos $x, y \in G$, é chamada* amorfia *de σ.*

Note que $(xy)^{\sigma} = x^{\sigma}y^{\sigma}\theta(x, y)$ e assim, σ é um homomorfismo se, e somente se, $\theta(x, y) = 1$, para todos $x, y \in G$.

Proposição 2.2. *Se $\theta : G \times G \to \bar{G}$ é a amorfia da l-aplicação $\sigma : G \to \bar{G}$, então para todos $x, y, z \in G$ vale a igualdade: $\theta(x, y)^{z^{\sigma}}\theta(xy, z) = \theta(y, z)\theta(x, yz)$.*

Demonstração. Veja que para todos $x, y, z \in G$ vale a associatividade em G, isto é,$((xy)z)^{\sigma} = (xy)^{\sigma}z^{\sigma}\theta(xy, z) = x^{\sigma}y^{\sigma}\theta(x, y)\theta(xy, z) = (x(yz))^{\sigma} = x^{\sigma}(yz)^{\sigma}\theta(xy, z) = x^{\sigma}y^{\sigma}z^{\sigma}\theta(x, yz)$. Daí, $x^{\sigma}y^{\sigma}\theta(x, y)\theta(xy, z) = (x(yz))^{\sigma} = x^{\sigma}y^{\sigma}z^{\sigma}\theta(x, yz)$ e portanto $\theta(x, y)^{z^{\sigma}} = \theta(xy, z) = \theta(y, z)\theta(x, yz)$. □

Se uma aplicação $\sigma : G \to \bar{G}$ é bijetiva e induz uma projetividade, então $(xy)^{\sigma} \in \langle x, y\rangle^{\sigma} = \langle x\rangle^{\sigma} \vee \langle y\rangle^{\sigma} = \langle x^{\sigma}, y^{\sigma}\rangle$ e com isso, $\theta(x, y) \in \langle x^{\sigma}, y^{\sigma}\rangle$. Mostramos, reciprocramente, que esta propriedade juntamente com a sua correspondente para σ^{-1} é suficiente para garantir que σ induz uma projetividade. É o que assegura o teorema a seguir, cuja demonstração encontra-se em [14].

Teorema 2.3. *Seja σ uma aplicação bijetiva de G em $\bar{G}$ tal que:*

(i) $(xy)^\sigma \in \langle x^\sigma, y^\sigma \rangle$ *para todos* $x, y \in G$;

(ii) $(uv)^{\sigma^{-1}} \in \langle u^{\sigma^{-1}}, v^{\sigma^{-1}} \rangle$ *para todos* $u, v \in \bar{G}$.

Então a aplicação $\bar{\sigma} : \mathscr{L}(G) \to \mathscr{L}(\bar{G})$ *definida por* $H^{\bar{\sigma}} = H^\sigma$, *para todo* $H \in \mathscr{L}(G)$, *é uma projetividade de* G *em* $\bar{G}$.

Agora para $n \in \mathbb{N}$, seja $\mathscr{L}_n(G)$ o conjunto de todos os subgrupos de um grupo G que podem ser gerados por n elementos. Uma vez que qualquer grupo é gerado pelos seus subgrupos cíclicos, toda projetividade é determinada pela sua ação no conjunto $\mathscr{L}_1(G)$. Em geral, os subgrupos mais acessíveis de um grupo são os cíclicos. Além disso, é importante saber sob quais condições poderemos estender uma bijeção entre $\mathscr{L}_1(G)$ e $\mathscr{L}_1(\bar{G})$ a uma projetividade de G em $\bar{G}$.

Teorema 2.4. *Sejam* G *e* $\bar{G}$ *grupos e* τ *uma aplicação bijetiva de* $\mathscr{L}_1(G)$ *em* $\mathscr{L}_1(\bar{G})$ *e que satisfaz a condição:* $X \leq \langle Y, Z \rangle$ *se, e somente se,* $X^\tau \leq \langle Y^\tau, Z^\tau \rangle$, *para todos* $X, Y, Z \in L_1(G)$. *Então a aplicação* $\varphi : \mathscr{L}(G) \to \mathscr{L}(\bar{G})$, *definida por* $H^\varphi = \bigcup_{X \in \mathscr{L}_1(H)} X^\tau$ *para todo* $H \leq G$ *é uma projetividade de* G *em* $\bar{G}$.

Demonstração. Mostraremos primeiro que H^φ é um subgrupo de $\bar{G}$. Sejam $a, b \in H^\varphi$, então existem $Y, Z \in \mathscr{L}_1(H)$ tais que $a \in Y^\tau$ e $b \in Z^\tau$. Uma vez que τ é sobrejetiva, existe $X \in \mathscr{L}_1(G)$ tal que $X^\tau = \langle ab^{-1} \rangle$. Daí, $X^\tau \leq \langle a, b \rangle \leq \langle Y^\tau, Z^\tau \rangle$ e por (i) segue que $X \leq \langle Y, Z \rangle \leq H$, donde segue que $X \in \mathscr{L}_1(H)$ e $ab^{-1} \in X^\tau \subseteq H^\varphi$. Assim, $H^\varphi \leq \bar{G}$ e φ é uma aplicação de $\mathscr{L}(G)$ em $\mathscr{L}(\bar{G})$. Como τ é bijetiva, τ^{-1} satisfaz a hipótese do teorema acima com G e $\bar{G}$ intercambiados e daí existe uma aplicação $\psi : \mathscr{L}(\bar{G}) \to \mathscr{L}(G)$ definida por $H^{\varphi\psi} = \bigcup_{M \in \mathscr{L}_1(H^\varphi)} M^{\tau^{-1}}$ para todo $M \leq \bar{G}$. Dado $x \in H \leq G$, temos que $\langle x \rangle \in \mathscr{L}_1(H)$ e $\langle x^\tau \rangle \in \mathscr{L}_1(H^\varphi)$, daí $x \in H^{\varphi\psi}$ e assim, $H \leq H^{\varphi\psi}$. Seja agora $y \in H^{\varphi\psi}$, das definições de φ e ψ segue que existem $\langle u \rangle \in \mathscr{L}_1(H^\varphi)$ e $Z \in \mathscr{L}_1(H)$ tais que $y \in \langle u \rangle^{\tau^{-1}}$ e $u \in Z^\tau$. Daí, $\langle u \rangle \leq Z^\tau$ e portanto $y \in \langle u \rangle^{\tau^{-1}} \leq Z$, por (i). Assim, $y \in H$ e $H^{\varphi\psi} \leq H$, donde segue que $H^{\varphi\psi} = H$. Do mesmo modo, $K^{\psi\varphi} = K$ para todo subgrupo $K \leq \bar{G}$. Segue que φ e ψ são bijeções e preservam a inclusão. Pelo Teorema (2.2), φ é uma projetividade de G em $\bar{G}$. □

Teorema 2.5. *(Poland [1985]). Sejam* G *e* $\bar{G}$ *grupos e* $n \in \mathbb{N}$, $n \geq 2$. *Se* σ *é uma aplicação bijetiva de* $\mathscr{L}_n(G)$ *em* $\mathscr{L}_n(\bar{G})$ *tal que* $X \leq Y$ *se, e somente se,* $X^\sigma \leq Y^\sigma$, *para*

todos $X, Y \in \mathscr{L}_n(G)$, então existe uma única extensão de φ de σ a uma projetividade de G em $\bar{G}$.

Já vimos que um isomorfismo de G em $\bar{G}$ induz uma projetividade. Um dos principais problemas sobre reticulado de subgrupos é determinar sob quais condições uma dada projetividade é induzida por um isomorfismo de grupos. Finalizaremos então com resultados que garantem quando uma projetividade é induzida por um isomorfismo.

Definição 2.7. *Uma família $\mathscr{F}$ de subgrupos de um grupo G é chamado um sitema local de subgrupos de G se:*

(i) Para todos $X, Y \in \mathscr{F}$ existe $Z \in \mathscr{F}$ tal que $X \vee Y \leq Z$.

(ii) Todo elemento de G está contido em algum $X \in \mathscr{F}$.

Teorema 2.6. *(Sadovskii [1941]). Sejam φ uma projetividade de um grupo G em um grupo $\bar{G}$ e $\mathscr{F}$ um sistema local de subrupos de G. Para todo $X \in \mathscr{F}$ sejam φ_X a projetividade induzida por φ em X e A_X o conjunto de todos os isomorfismos de X em X^φ que induz φ_X. Se A_X é não vazio e finito para todo $X \in \mathscr{F}$, então φ é induzida por um isomorfismo de G em $\bar{G}$.*

Corolário 2.1. *Sejam φ uma projetividade do grupo G no grupo $\bar{G}$ e $\mathscr{F}$ um sistema local de subgrupos finitamente gerados de G. Se φ é induzida por um isomorfismo em todo $X \in \mathscr{F}$, então φ é induzida por um isomorfismo em G.*

Teorema 2.7. *(Sadoviskii [1965a]). Sejam φ uma projetividade do grupo G no grupo $\bar{G}$ e $\mathscr{F}$ uma família de subgrupos normais de G tal que:*

(i) Para quaisquer $X, Y \in \mathscr{F}$ existe $Z \in \mathscr{F}$ com $Z \leq X \wedge Y$.

(ii) Para todo $g \in G$ existe $X \in \mathscr{F}$ tal que $\langle g \rangle \wedge X = 1$.

Suponha que para todo $X \in \mathscr{F}, X^\varphi \trianglelefteq \bar{G}$ e seja A_X o conjunto de todos os isomorfismos de $\dfrac{G}{X}$ em $\dfrac{\bar{G}}{X^\varphi}$ que induz a projetividade φ_X. Se A_X é não vazio e finito para todo $X \in \mathscr{F}$, então φ é induzida por um isomorfismo de G em $\bar{G}$.

As demonstrações de tais resultados encontram-se em [14].

2.3 O Grupo das Autoprojetividades

Veremos nesta seção um resultado que relaciona o grupo dos automorfismos de um grupo G com o grupo dos automorfismos de $\mathscr{L}(G)$.

Definição 2.8. *Uma* autoprojetividade *de um grupo G é uma projetividade de G em G. O grupo de todas as autoprojetividades de G, isto é, de todos os automorfismos de $\mathscr{L}(G)$, é denotado por* P(G).

Observação 2.2. *Se σ é um automorfismo do grupo G, então σ satisfaz a condição $H \leq G$ se, e somente se, $H^\sigma \leq G^\sigma$ para todo H subgrupo de G. Daí, pela Proposição (2.1), σ induz uma projetividade de G em G.*

Teorema 2.8. *Seja G um grupo.*

(i) A aplicação $\rho : \operatorname{Aut} G \to P(G)$ definida por $H^{\alpha^\rho} = H^\alpha$ para $H \leq G, \alpha \in \operatorname{Aut} G$ é um homomorfismo. O núcleo de ρ é o grupo $\operatorname{Pot} G = \{\alpha \in \operatorname{Aut} G \mid H^\alpha = H$ para todo $H \leq G\}$ dos automorfismos de potência *de G. A imagem de ρ é o grupo $PA(G)$ de todas as autoprojetividades de G que são induzidas por automorfismos, isto é, $PA(G) = \{\varphi \in P(G) \mid H^\varphi = H^\alpha \quad$ para algum $\quad \alpha \in \operatorname{Aut} G \quad$ e todos $\quad H \leq G\}$. E ainda, $PA(G) \cong \dfrac{\operatorname{Aut} G}{\operatorname{Pot} G}$.*

(ii) A aplicação $\eta : G \to P(G)$ definida por $H^{g^\eta} = g^{-1}Hg$ para $H \leq G, g \in G$ é um homomorfismo. O núcleo de η é o grupo $K(G) = \bigcap_{H \leq G} N_G(H)$ e é chamado a norma de G. A imagem de η é denotada por $PI(G)$ e assim, $PI(G) \cong \dfrac{G}{K(G)}$.

(iii) Se $\pi : G \to \operatorname{Aut} G$ é o homomorfismo aplicando $g \in G$ no automorfismo interno induzido por g, isto é, $x^{g^\pi} = g^{-1}xg$ para $x \in G$, então $\eta = \pi\rho$ e $K(G)^\pi = G^\pi \cap \operatorname{Pot} G = \operatorname{Inn} G \cap \operatorname{Pot} G$.

Demonstração. (i) Sejam $\alpha, \beta \in \operatorname{Aut} G$ e $H \leq G$. Então as projetividades α^ρ e β^ρ são induzidas por α e β, respectivamente. Daí $H^{(\alpha\beta)^\rho} = H^{\alpha\beta} = H^\alpha H^\beta = H^{\alpha^\rho \beta^\rho}$ e, portanto, ρ é um homomorfismo. Segue do teorema do isomorfismo para grupos que $PA(G) \cong \dfrac{\operatorname{Aut} G}{\operatorname{Pot} G}$.

(ii) Sejam $a, b \in G$ e $H \leq G$. Então a^η e b^η são automorfismos internos induzidos por a e b, respectivamente. Assim, $H^{(ab)^\eta} = b^{-1}a^{-1}Hab = (H^{a^\eta})^{b^\eta}$ e, portanto, η é

um homomorfismo. Agora observe que o núcleo $K(G)$ de η é o grupo $K(G) = \{g \in G \mid H^{g^\eta} = H \quad \text{para todo} \quad H \leq G\}$. Mas $H^{g^\eta} = H \Leftrightarrow H^g = H \Leftrightarrow g \in N_G(H)$. Portanto $K(G) = \bigcap_{H \leq G} N_G(H)$. Pelo mesmo argumento dado em (i), $PI(G) \cong \dfrac{G}{K(G)}$. (iii) Seja $g \in G$ e denote por $\mathcal{I}_g$ o automorfismo interno induzido por g. Pela definição π, $g^\pi = \mathcal{I}_g$, daí $g^{\pi\rho} = \mathcal{I}_g{}^\rho = g^\eta$ e, portanto, $\eta = \pi\rho$. □

A figura abaixo elucida bem a situação.

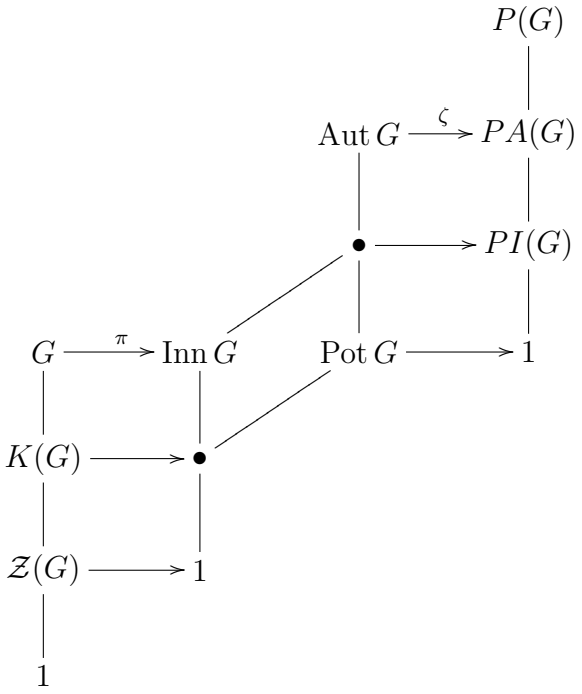

Figura 2.1: Autoprojetividade.

Exemplo 2.1. O grupo simétrico S_3 não possui automorfismo de potência diferente da identidade.

Sabemos que $S_3 = \{I, (123), (132), (12), (13), (23)\}$ e que o grupo dos automorfismos de S_3 é $\operatorname{Aut} S_3 = \langle \sigma\tau \mid \sigma^3 = \tau^2 = 1, \sigma^\tau = \sigma^{-1} \rangle$ onde: $(12)^\sigma = (13)$, $(13)^\sigma = (23)$, $(23)^\sigma = 12$, $(123)^\tau = (132)$, $(132)^\tau = (123)$, $(12)^\tau = (23)$ e $(23)^\tau = (12)$. Assim $\operatorname{Aut} S_3 = \{Id, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \cong S_3$. O reticulado dos subgrupos de S_3 é

$\mathscr{L}(S_3) = \{I, \langle(123)\rangle, \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle, S_3\}$. Vemos claramente que o único automorfismo que fixa todos os subgrupos de S_3 é o automorfismo identidade. Logo S_3 não possui automorfismo de potência não trivial.

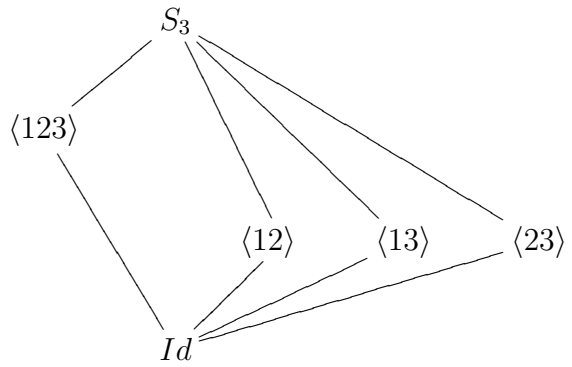

Figura 2.2: Reticulado dos subgrupos de S_3.

Exemplo 2.2. Consideremos o grupo $G = \langle x\rangle \cong (\mathbb{Z}/(n), +)$, o grupo cíclico de ordem finita $n \geq 3$. Temos que $Aut(G) \cong (\mathbb{Z}_n{}^*, \cdot)$, onde $(\mathbb{Z}_n{}^*, \cdot)$ é o grupo multiplicativo dos elementos inversíveis do anel $\mathbb{Z}_n$. Sabemos que $|Aut(G)| = \phi(n)$ em que $\phi(n)$ é a função de Euler. Como para cada divisor d de n existe um único subgrupo H de ordem $\dfrac{n}{d}$, segue que todo subgrupo H é característico em G, isto é, $H^\varphi = H$, para todo $\varphi \in \mathrm{Aut}(G)$ e todo $H \in G$. Assim, todo automorfismo de G é também um automorfismo de potência.

Definição 2.9. *Dizemos que um automorfismo de potência α de um grupo G é* universal *se existe um inteiro n tal que $x^\alpha = x^n$ para todo $x \in G$.*

Observamos que todo automorfismo de potência de um grupo abeliano finitamente gerado é universal. Mais geralmente, temos o seguinte resultado:

Lema 2.1. *Seja A um grupo abeliano finitamente gerado, com $A = \langle a_1\rangle \times \cdots \times \langle a_s\rangle$. Se um automorfismo α de A fixa $\langle a_1\rangle, \cdots, \langle a_s\rangle$ e $\langle a_1 \cdots a_s\rangle$, então existe um inteiro n tal que $a^\alpha = a^n$ para todo $a \in A$.*

Demonstração. Por hipótese, existem inteiros n, n_i tais que $a_i^\alpha = a_i^{n_i}$ e $a_1^{n_1} \cdots a_s^{n_s} = a_1^\alpha \cdots a_s^\alpha = (a_1 \cdots a_s)^\alpha = (a_1 \cdots a_s)^n = a_1^n \cdots a_s^n$. Daí segue que $a_i^\alpha = a_i^{n_i} = a_i^n$, para $i = 1, \cdots, s$ e então $a^\alpha = a^n$ para todo $a \in A$. □

Proposição 2.3. *Sejam A um p-grupo abeliano e $\alpha \in \mathrm{Pot}\, A$. Se o expoente de A é finito, então α é universal.*

Demonstração. Seja p^k o expoente de A e consideremos $x \in A$ tal que $o(x) = p^k$. Como $\alpha \in Pot\, A$, segue que α induz um automorfismo em $\langle x \rangle$ e assim existe um inteiro n tal que $0 < n < p^k$, $(n, p) = 1$ e $x^\alpha = x^n$. Para todo $a \in A$, α induz um automorfismo de potência em $\langle x, a \rangle$ e pelo Lema (2.1) existe um inteiro m tal que $a^\alpha = a^m$ e $x^\alpha = x^m$. Disto segue que $m \equiv n(mod p^k)$ e $a^\alpha = a^n$. Portanto α é universal. □

2.4 A classe $\mathcal{P}$(n,p)

Sejam p um primo e $n \geq 2$ um número natural. Dizemos que um grupo G pertence à classe $\mathcal{P}(n, p)$ se G é um grupo abeliano elementar de ordem p^n ou um produto semidireto de um subgrupo normal abeliano elementar A de ordem p^{n-1} por um grupo de ordem prima $q \neq p$, que induz um automorfismo de potência não trivial em A.

Definição 2.10. *Um grupo G é chamado $\mathcal{P}-$grupo se G pertence à classe $\mathcal{P}$(n,p).*

Observação 2.3. *Seja G um $\mathcal{P}$-grupo não abeliano, de modo que $G = A\langle t \rangle$ com A sendo um p-grupo abeliano elementar e t um elemento de ordem q que induz um automorfismo de potência não trivial em A. Pela Proposição (2.3), t é universal em A, isto é, existe um inteiro r tal que:*

(i) $t^{-1}at = a^r$ para todo $a \in A$.

Uma vez que $t \notin C_G(a)$ e $t^q = 1$,

(ii) $r \not\equiv 1(mod p)$ e $r^q \equiv 1(mod p)$.

Daí q divide $p - 1$.

Em particular, a classe $\mathcal{P}(n, 2)$ contém apenas o grupo abeliano elementar de ordem 2^n. Para $p > 2$ e para todo divisor primo q de $p - 1$, existe um inteiro satisfazendo (ii) da observação (2.3). Então o produto semidireto $G = A\langle t \rangle$ de um p-grupo abeliano elementar não tirivial A por um grupo cíclico $\langle t \rangle$ de ordem q, onde $t^{-1}at = a^r$, para todo $a \in A$ é um $\mathcal{P}$-grupo não abeliano. Quaisquer dois grupos com o mesmo A e q

são isomorfos. Assim, a classe $\mathcal{P}(n,p)$ contém o grupo abeliano elementar de ordem p^n e, para todo divisor primo q de $p-1$, exatamente um $\mathcal{P}$-grupo não abeliano contendo elementos de ordem q. Se n é finito, a ordem deste grupo é $p^{n-1}q$.

Lema 2.2. *Seja G um $\mathcal{P}-$grupo não abeliano e suponha que p,q e A são definidos como na observação (2.3). Então:*

(i) $G' = A = C_G(a)$, *para todo* $1 \neq a \in A$.

(ii) $\mathcal{Z}(G) = 1$.

(iii) Os subgrupos normais de G são G e os subgrupos de A.

(iv) Todo elemento $x \in G \setminus A$ tem ordem q. Daí, os subgrupos de ordem q geram G.

No resultado a seguir, temos uma condição que garante o isomorfismo entre reticulados de subgrupos dos grupos que pertencem à classe $P(n,p)$.

Teorema 2.9. *(Baer,1939a).Para todo primo p e todo número natural $n \geq 2$, todos os grupos em $\mathcal{P}(n,p)$ são reticulado-isomorfos.*

Demonstração. Mostraremos primeiro que todo grupo não abeliano $G \in \mathcal{P}(n,p)$ é reticulado-isomorfo a um grupo abeliano elementar em $\mathcal{P}(n,p)$. Desse modo, sejam q, r e $G = A\langle t\rangle$ como na observação (2.3). Então $\bar{G} = A \times \langle \bar{t}\rangle$, onde $\bar{t}$ tem ordem p, é o grupo abeliano elementar em $\mathcal{P}(n,p)$. Queremos construir uma aplicação bijetiva do conjunto $\mathscr{L}_1(G)$, dos subgrupos cíclicos de G, em $\mathscr{L}_1(\bar{G})$ que induz uma projetividade de G em $\bar{G}$. Se $x \in G \setminus A$, então pelo Lema (2.2), $\langle x\rangle$ tem ordem q e além disso, contém exatamente um elemento fora de cada classe de A, em particular fora de At. Daí existe exatamente um elemento $a \in A$ tal que $\langle x\rangle = \langle at\rangle$. Definiremos agora a aplicação $\tau : \mathscr{L}_1(G) \to \mathscr{L}_1(\bar{G})$ por $\langle x\rangle^\tau = \langle x\rangle$ se $x \in A$ e $\langle x\rangle^\tau = \langle a\bar{t}\rangle$ se $\langle x\rangle = \langle at\rangle \nleq A$. Uma vez que todo subgrupo cíclico do grupo abeliano elementar $\bar{G} = A \times \langle \bar{t}\rangle$ que não está contido em A também contém exatamente um elemento da forma $a\bar{t}$ com $a \in A$, vemos que τ é bijetiva. Pelo Teorema (2.4), devemos mostrar que para todo $X, Y, Z \in \mathscr{L}_1(G)$, a condição $X \leq \langle Y, Z\rangle$ se, e somente se, $X^\tau \leq \langle Y^\tau, Z^\tau\rangle$ é satisfeita. Esta condição é clara se Y e Z estão contidos em A, uma vez que τ é a identidade em $\mathscr{L}_1(A)$. Se $Y \leq A$ e $Z \nleq A$, isto é, $Y = \langle b\rangle$ e $Z = \langle ct\rangle$ com $b, c \in A$, então $\langle Y, Z\rangle \wedge A = Y$ uma vez que

todo subgrupo de A é normal em G. Do mesmo modo, $\langle Y^\tau, Z^\tau\rangle \wedge A = Y^\tau$. Assim, se $X \leq A$, então $X \leq \langle Y, Z\rangle$ se, e somente se, $X \leq Y$, e isto é o caso se, e somente se, $X^\tau \leq \langle Y^\tau, Z^\tau\rangle$. Para $X \not\leq A$, isto é, $X = \langle at\rangle$ com $a \in A$, temos que $X \leq \langle Y, Z\rangle$ se, e somente se, $at \in \langle b, ct\rangle \wedge At = (\langle b, ct\rangle \wedge)A)ct = \langle b\rangle ct$, isto é, $a \in \langle b\rangle c$, mais precisamente, este é o caso se, e somente se, $U^\tau = \langle a\bar{t}\rangle \leq \langle b\rangle \times \langle c\bar{t}\rangle = \langle Y^\tau, Z^\tau\rangle$. Finalmente, se nem $Y = \langle bt\rangle$ e nem $Z = \langle ct\rangle$ estão contidos em A, então com $W = \langle bc^{-1}\rangle \leq A$ temos $\langle Y, Z\rangle = \langle W, Z\rangle$ e $\langle Y^\tau, Z^\tau\rangle = \langle bc^{-1}, c\bar{t}\rangle = \langle W^\tau, Z^\tau\rangle$. □

2.5 Produto Direto

Para o desenvolvimento do nosso trabalho, precisamos entender como funciona o produto direto para reticulados de subgrupos. Começaremos então com a definição de produto direto de uma família de reticulados $L_\lambda, \lambda \in \Lambda$, onde $\Lambda = \{1, \cdots, n\}$ e $n \in \mathbb{N}$.

Definição 2.11. *O produto direto dos $L_\lambda, \lambda \in \Lambda$ é o produto cartesiano dos conjuntos L_λ, isto é,*

$$L = L_1 \times \cdots \times L_n = \{(x_1, \cdots, x_n) | x_i \in L_i\},$$

com a relação de ordem, $(x_1, \cdots, x_n) \leq (y_1, \cdots, y_n)$ se, e somente se, $x_i \leq y_i$ para todo $i \in \{1, \cdots, n\}$.

Consideremos agora um grupo finito $G = H \times K$. Em geral $\mathscr{L}(G) \ncong \mathscr{L}(H) \times \mathscr{L}(K)$, como é o caso de $G = C_p \times C_p$, p primo. O mesmo pode ocorrer quando G é o produto direto com mais de dois subgrupos. É importante para nós, sabermos sob quais condições esse isomorfismo ocorre. Vejamos o resultado a seguir.

Lema 2.3. *Se $G = \times G_\lambda$, onde G_λ são coprimos e $\lambda \in \Lambda = \{1, \cdots, n\}$, então $\mathscr{L}(G) \cong \times\mathscr{L}(G_\lambda)$, com $\lambda \in \Lambda$; na verdade, a aplicação definida por $\tau : \mathscr{L}(G) \to \times\mathscr{L}(G_\lambda)$, definida por $H^\tau(\lambda) = H \cap G_\lambda$ para todo $\lambda \in \Lambda$ e $H \leq G$ é um isomorfismo.*

Observação 2.4. *Dizemos que os grupos $G_\lambda, \lambda \in \Lambda$ são coprimos se cada G_λ é um grupo de torsão e $(o(x), o(y)) = 1$ para todo $x \in G_\lambda, y \in G_\mu$, com $\lambda \neq \mu$; para grupos finitos isto é equivalente à $(|G_\lambda|, |G_\mu|) = 1$ para $\lambda \neq \mu$.*

A demostração deste lema encontra-se em [14], pag. 37 e a mesma é feita para o caso geral, em que Λ é infinito.

2.6 Subgrupo Permutável e Subgrupo Modular

Nesta seção introduziremos os conceitos de subgrupo permutável e de subgrupo modular, ambos fundamentais para a determinação do grau de comutatividade de subgrupos de um grupo finito.

Definição 2.12. *Um reticulado L é chamado modular, se para todos $x, y, z \in L$, vale a lei modular:*
Se $x \leq z$, então $x \vee (y \wedge z) = (x \vee y) \wedge z$.

Temos adiante a definição de *elemento modular* em um reticulado.

Definição 2.13. *Dizemos que o elemento m do reticulado L é modular em L, e escrevemos* m mod L, *se para todos $x, y, z \in L$ temos:*

(i) $x \vee (m \wedge z) = (x \vee m) \wedge z$, *com* $x \leq z$.

(ii) $m \vee (y \wedge z) = (m \vee y) \wedge z$, *com* $m \leq z$.

Teorema 2.10. *As seguintes propriedades de um elemento $m \in L$ são equivalentes.*

(i) m é modular em L.

(ii) Para todo $a \in L$, a aplicação $\varphi_{a,m} : [a/a \wedge m] \to [a \vee m/m]$, definida por $\varphi_{a,m}(x) = x \vee m$ é um isomorfismo.

(iii) Para todo $a \in L$, a aplicação $\psi_{a,m} : [a \vee m/m] \to [a/a \wedge m]$, definida por $\psi_{a,m}(z) = z \wedge a$ é um isomorfismo.

(iv) Para todo $a \in L, \varphi_{a,m}\psi_{a,m} = Id_{[a/a\wedge m]}$ e $\psi_{a,m}\varphi_{a,m} = Id_{[a\vee m/m]}$.

Este teorema encontra-se demonstrado em [14], pag. 44.

Definição 2.14. *Seja G um grupo e consideremos um subgrupo M de G; dizemos que M é* modular *em G se M é um elemento modular em $\mathscr{L}(G)$, e escrevemos* M mod G *neste caso. Se $\mathscr{L}(G)$ é modular, isto é, se todo subgrupo de G é modular em $\mathscr{L}(G)$, então G será chamado de $\mathcal{M}-$*grupo. *Dizemos que M é* permutável *em G com a notação* M per G *se, $HM = MH$ para todo $H \in \mathscr{L}(G)$.*

Definição 2.15. *Dizemos que dois subgrupos M e H de um grupo G formam um par modular se:*

(i) $M \vee (H \wedge W) = (M \vee H) \wedge W$, *para* $M \leq W$ *e*

(ii) $H \vee (M \wedge W) = (M \vee H) \wedge W$, *para* $H \leq W$.

Vejamos no teorema a seguir como estes dois conceitos estão relacionados.

Teorema 2.11. *(Ore, 1937). Seja G um grupo.*

(i) Se $N \trianglelefteq G$, *então* $NH = HN$ *para todo* $H \leq G$.

(ii) Se $M \leq G$ *é tal que* $MH = HM$ *para todo* $H \leq G$, *então* M mod G.

Demonstração. (i) Se $N \trianglelefteq G$, então $Nx = xN$ para todo $x \in G$, donde segue que $NH = HN$ para todo $H \leq G$.
(ii) Sejam $X, Z \in \mathscr{L}(G)$ tais que $X \leq Z$. Devemos mostrar que $X \vee (M \wedge Z) = (X \vee M) \wedge Z$. Se $x \in X \vee (M \wedge Z)$, claramente temos $x \in (X \vee M) \wedge Z$ e com isso, $X \vee (M \wedge Z) \subseteq (X \vee M) \wedge Z$. Consideremos $g \in (X \vee M) \wedge Z$ e como $X \vee M = XM$, temos que existem $x \in X$ e $m \in M$ tal que $g = xm$. Uma vez que $X \leq Z$, temos que $m = x^{-1}g \in Z$ daí, $g = xm \in X \vee (M \wedge Z)$ e $X \vee (M \wedge Z) \subseteq (X \vee M) \wedge Z$, donde segue que $X \vee (M \wedge Z) = (X \vee M) \wedge Z$. Sejam agora $Y, Z \in \mathscr{L}(G)$ com $M \leq Z$. Vamos mostrar que $M \vee (Y \wedge Z) = (M \vee Y) \wedge Z$. Tomemos $g \in M \vee (Y \wedge Z)$, como $M \vee (Y \wedge Z) = M(Y \wedge Z)$ temos que existem $m \in M$ e $z \in Y \wedge Z$ tais que $g = mz$. Como $M \leq Z$ temos $g = mz \in (M \vee Y) \wedge Z$, donde segue que $M \vee (Y \wedge Z) \subseteq (M \vee Y) \wedge Z$. Consideremos agora $g \in (M \vee Y) \wedge Z$ e como $M \vee Y = MY$, segue que existem $m \in M$ e $y \in Y$ tal que $g = my$. Como $m \in M \leq Z$, segue que $y = m^{-1}g \in Z$, daí $g = my \in M \vee (Y \wedge Z)$ e com isso $(M \vee Y) \wedge Z \subseteq M \vee (Y \wedge Z)$. Logo $M \vee (Y \wedge Z) = (M \vee Y) \wedge Z$. Portanto M é modular em G. □

O teorema anterior mostra que um subgrupo normal é permutável e um subgrupo permutável é modular. Assim, um subgrupo normal é modular em G e as leis modulares descritas na Definição (2.13) são as principais propriedades de um subgrupo normal que são visíveis no reticulado dos subgrupos. Além disso, um grupo em que todos os subgrupos são permutáveis é um grupo modular; em particular é metabeliano, como mostra o teorema a seguir.

Teorema 2.12. *(Iwasawa,1943). Se dois subgrupos quaisquer de um grupo G permutam, então G é metabeliano.*

Daremos agora um resultado que garante quando dois subgrupos quaisquer, de um grupo finito G, são permutáveis.

Proposição 2.4. *Sejam G um grupo finito e M e H subgrupos de G. Então M e H são permutáveis se, e somente se,* $[M : M \wedge H] = [M \vee H : H]$. *Em particular, se o índice de M em G é relativamente primo com o de H em G, então M e H são permutáveis e* $G = M \vee H$.

Teorema 2.13. *Seja G um grupo finito. Então todo par de subgrupos modular é permutável se, e somente se, G é nilpotente.*

Demonstração. ($\Rightarrow$) Suponhamos que todo par de subgrupos modular de G é permutável. Seja S um $p-$subgrupo de Sylow de G e consideremos um subgrupo maximal M de G contendo S. Se M não é normal em G, então existe um subgrupo $L \neq M$ conjugado a M em G. Como M é maximal segue que L também é maximal. Daí M e L formam um par de subgrupos modular e pela hipótese, M e L são permutáveis, isto é, $ML = LM$. Mas, como $m \in M$, e $l \in L$, temos que $l^{-1}m^{-1}Mml = L$ implica em $M = m^{-1}Mm = lLl^{-1} = L$, um absurdo. Logo M é normal em G. Como M é arbitrário, obtemos que todo subgrupo maximal de G é normal e, portanto, G é nilpotente.

($\Leftarrow$) Suponhamos agora que G é nilpotente. Então G é um produto direto de seus $p-$subgrupos de Sylow $S_1, \cdots, S_n$. Qualquer subgrupo U de G é o produto direto dos seus $p-$subgrupos de Sylow $U_i = U \cap S_i$, $i = 1, \cdots, n$. Suponhamos que dois subgrupos $U = \times_{i=1}^{n} U_i$ e $V = \times_{i=1}^{n} V_i$ formam um par de subgrupos modular. Denotemos as ordens de $U, V, U \vee V, U \wedge V, U_i, V_i, U_i \vee V_i$ e $U_i \wedge V_i$ por $u, v, m, d, u_i, v_i, m_i$ e d_i respectivamente. Como $U \vee V = \times_{i=1}^{n}(U_i \vee V_i)$ e $U \wedge V = \times_{i=1}^{n}(U_i \wedge V_i)$, segue que $m = \prod_{i=1}^{n} m_i$ e $d = \prod_{i=1}^{n} d_i$, daí md é divisível por uv. Em outras palavaras, pelo Teorema (2.10), o intervalo $(U \vee V)/U$ de $\mathscr{L}(G)$ é aplicado isomorficamente em $V/(U \wedge V)$. Daí o comprimento de uma série principal conectando $U \wedge V$ e U não é maior que o da série principal conectando V e $U \wedge V$. Uma vez que G é nilpotente, temos que o número de

fatores primos em $(U \vee V : U) = \dfrac{m}{u}$ não é maior que o número de fatores primos em $[V : U \wedge V] = \dfrac{v}{d}$. Uma vez que md é divisível por uv, segue que $md = uv$, ou seja, $[U \vee V : U] = [V : U \wedge V]$. Daí U e V são permutáveis. □

Outro resultado que relaciona a modularidade de um grupo finito com a permutabilidade de todos os seus subgrupos é o lema seguinte.

Lema 2.4. *Um p-grupo finito, com p primo, tem o reticulado dos subgrupos modular se, e somente se, dois quaisquer de seus subgrupos permutam.*

A demonstração deste lema segue do teorema anterior.

Capítulo 3

O Grau de Comutatividade de Subgrupos de um Grupo Finito

Neste capítulo, mostraremos uma expressão para encontrar o grau de comutatividade de subgrupos de um grupo finito G, e denotaremos tal expressão por $sd(G)$. Veremos as propriedades de $sd(G)$, para estudarmos no capítulo seguinte o grau de comutatividade de subgrupos para algumas classes de grupos finitos.

3.1 Propriedades Básicas do Grau de Comutatividade de Subgrupos

Seja G um grupo finito. Sabemos que dados dois subgrupos arbitrários H e K de G, o produto $HK = \{hk \mid h \in H,\ k \in K\}$ é um subgrupo em G, ou seja, $HK \in \mathscr{L}(G)$ se, e somente se, $HK = KH$, isto é, se H e K permutam. Deste fato, podemos considerar a expressão

$$\begin{aligned} sd(G) &= \frac{1}{|\mathscr{L}(G)|^2} \, |\{(H,K) \in \mathscr{L}(G)^2 \mid HK = KH\}| \\ &= \frac{1}{|\mathscr{L}(G)|^2} \, |\{(H,K) \in \mathscr{L}(G)^2 \mid HK \in \mathscr{L}(G)\}|, \end{aligned} \tag{3.1}$$

onde $sd(G)$ é chamado o grau de comutatividade de subgrupos de G. Em outras palavras, $sd(G)$ nos dá a probabilidade com que o produto de dois subgrupos quaisquer de G é um subrupo em G.

Observe que o grau de comutatividade de subgrupos $sd(G)$ de um grupo finito G satisfaz a relação

$$0 < sd(G) \leq 1.$$

A igualdade $sd(G) = 1$ ocorre se, e somente se, todos os subgrupos de G são permutáveis. Podemos dizer então, com base nos Teoremas (2.11) e (2.12), que um grupo com grau de comutatividade de subgrupos igual a 1 é um $\mathcal{M}-$grupo e metabeliano. Estes grupos podem ser caracterizados conforme a proposição a seguir.

Proposição 3.1. *Dado um grupo finito G temos que $sd(G) = 1$ se, e somente se, G é um $\mathcal{M}-$grupo nilpotente.*

Demonstração. ($\Rightarrow$) Como $sd(G) = 1$ temos na equação (3.1) que $\{K \in \mathscr{L}(G) \mid HK = KH\} = \mathscr{L}(G)$, daí todos os subgrupos de G são permutáveis e, pelo Teorema (2.11), também são modulares. Logo G é um $\mathcal{M}-$grupo e assim, pelo Teorema (2.13) G é nilpotente.
($\Leftarrow$) Devemos mostrar que todo subgrupo de G é permutável. Notemos que G é nilpotente e todo subgrupo de G é modular, logo pelo Teorema (2.13) segue que todos os subgrupos de G permutam e portanto $sd(G) = 1$. □

Um exemplo de grupo que satisfaz a proposição anterior é o grupo quatérnio Q_8, uma vez que todos os seus subgrupos são normais e pelo Teorema (2.11) são permutáveis, segue que $sd(Q_8) = 1$.

Como vimos, o grau de comutatividade de subgrupos de um grupo finito G é dado pela igualdade

$$sd(G) = \frac{1}{|\mathscr{L}(G)|^2} \, |\{(H, K) \in \mathscr{L}(G)^2 \mid HK \in \mathscr{L}(G)\}|.$$

Queremos agora escrever a igualdade anterior de uma maneira mais simples, sendo assim, para todo subgrupo H de G, denotemos por $C(H)$ o conjunto formado por todos os subgrupos de G que comutam com H, isto é,

$$C(H) = \{K \in \mathscr{L}(G) | HK = KH\},$$

então

$$sd(G) = \frac{1}{|\mathscr{L}(G)|^2} \sum_{H \in \mathscr{L}(G)} |C(H)|. \tag{3.2}$$

Note que todos os subgrupos normais de G estão contidos em cada $C(H)$ e daí temos que $\mathscr{N}(G) \subseteq C(H)$, onde $\mathscr{N}(G)$ é o reticulado dos subgrupos normais de G. Assim,

$$\begin{aligned}
|\mathscr{N}(G)| &\leq |C(H)| \Rightarrow \\
|\mathscr{N}(G)||\mathscr{L}(G)| &\leq \sum_{H\in\mathscr{L}(G)} |C(H)| \Rightarrow \\
\frac{1}{|\mathscr{L}(G)|^2}|\mathscr{N}(G)||\mathscr{L}(G)| &\leq \frac{1}{|\mathscr{L}(G)|^2}\sum_{H\in\mathscr{L}(G)} |C(H)| \Rightarrow \\
\frac{|\mathscr{N}(G)|}{|\mathscr{L}(G)|} &\leq \frac{1}{|\mathscr{L}(G)|^2}\sum_{H\in\mathscr{L}(G)} |C(H)| \Rightarrow \\
\frac{|\mathscr{N}(G)|}{|\mathscr{L}(G)|} &\leq sd(G).
\end{aligned}$$

Observe que se $\mathscr{N}(G) = \mathscr{L}(G)$, isto é, se G é um *Grupo de Dedekind* temos então que $C(H) = \mathscr{N}(G) = \mathscr{L}(G)$, para todo H$\in \mathscr{L}(G)$, daí na equação (3.2) temos

$$\begin{aligned}
sd(G) &= \frac{1}{|\mathscr{L}(G)|^2}\sum_{H\in\mathscr{L}(G)} |\mathscr{N}(G)| \\
&= \frac{|\mathscr{N}(G)|}{|\mathscr{L}(G)|} = sd(G)
\end{aligned}.$$

Reciprocramente, se $\dfrac{|\mathscr{N}(G)|}{|\mathscr{L}(G)|} = sd(G)$, temos que

$$\begin{aligned}
\frac{|\mathscr{N}(G)|}{|\mathscr{L}(G)|} &= \frac{1}{|\mathscr{L}(G)|^2}\sum_{H\in\mathscr{L}(G)} |C(H)| \Rightarrow \\
\mathscr{N}(G) &= \mathscr{L}(G).
\end{aligned}$$

Lembramos que todos os subgrupos de G contidos no $N_G(H)$ pertencem à $C(H)$, e com isso, $\mathscr{N}(G) \cup \mathscr{L}(N_G(G)) \subseteq C(H)$, para qualquer $H \in \mathscr{L}(G)$. Vejamos agora um exemplo do que acabamos de falar.

Exemplo 3.1. Consideremos o grupo simétrico S_3. Vamos calcular o grau de comutatividade de subgrupos $sd(S_3)$ de S_3.

Solução. Temos que $S_3 = \{Id, (12), (13), (23), (123), (132)\}$ e os subgrupos de S_3 são: $I = \{(Id)\}$, $A_3 = \{Id, (123), (132)\}$, $H_1 = \{(Id), (12)\}$, $H_2 = \{(Id), (13)\}$, $H_3 = \{(Id), (23)\}$ e o próprio S_3. Assim, $\mathscr{L}(S_3) = \{I, A_3, H_1, H_2, H_3, S_3\}$, e daí, calculando $C(H)$ para todo subgrupo H de S_3 obtemos: $C(I) = \{I, A_3, H_1, H_2, H_3, S_3\}$,

$C(A_3) = \{I, A_3, H_1, H_2, H_3, S_3\}$, $C(H_1) = \{I, H_1, A_3, S_3\}$, $C(H_2) = \{I, H_2, A_3, S_3\}$, $C(H_3) = \{I, H_3, A_3, S_3\}$ e $C(S_3) = \{I, A_3, H_1, H_2, H_3, S_3\}$. Finalmente, usando (3.1) encontramos $sd(S_3) = \dfrac{30}{36} = \dfrac{5}{6}$.

Ainda do exemplo acima, é fácil ver que $\dfrac{|\mathscr{N}(S_3)|}{|\mathscr{L}(S_3)|} \leq sd(S_3)$, e também $\mathscr{N}(S_3) \cup \mathscr{L}(N_{S_3}(H)) \subseteq C(H)$, para todo H em S_3.

Exemplo 3.2. O grau de comutatividade de subgrupos do grupo alternado A_4 é $\dfrac{16}{25}$.

Solução. Sabemos que $A_4 = \{Id, (12)(34), (13)(24), (14)(23), (234), (243), (134), (143), (124), (142), (123), (132)\}$ e os subgrupos de A_4 são: $I = \{Id\}$, $B_1 = \{Id, (12)(34)\}$, $B_2 = \{Id, (14)(23)\}$, $B_3 = \{Id, (13)(24)\}$, $V = \{Id, (12)(34), (13)(24), (14)(23)\}$, $B_4 = \{Id, (123), (132)\}$, $B_5 = \{Id, (124), (142)\}$, $B_6 = \{Id, (134), (143)\}$, $B_7 = \{Id, (234), (243)\}$ e o próprio A_4. Calculando agora $C(H)$ para todo subgrupo H de A_4 obtemos: $C(I) = \mathscr{L}(A_4)$, $C(V) = \mathscr{L}(A_4)$, $C(A_4) = \mathscr{L}(A_4)$, $C(B_1) = \{Id, B_1, B_2, B_3, V, A_4\}$, $C(B_2) = \{Id, B_1, B_2, B_3, V, A_4\}$, $C(B_3) = \{Id, B_1, B_2, B_3, V, A_4\}$, $C(B_4) = \{Id, B_4, V, A_4\}$, $C(B_5) = \{Id, B_5, V, A_4\}$, $C(B_5) = \{Id, B_5, V, A_4\}$, $C(B_6) = \{Id, B_6, V, A_4\}$ e $C(B_7) = \{Id, B_7, V, A_4\}$. Assim, usando (3.1) encontramos $sd(A_4) = \dfrac{16}{25}$.

Vimos no capítulo anterior que se G e $\bar{G}$ são grupos isomorfos, então são também reticulado-isomorfos e com isso, podemos concluir para G e $\bar{G}$ finitos que, $sd(G) = sd(\bar{G})$. O mesmo não pode ser dito quando G e $\bar{G}$ são apenas reticulado-isomorfos, como é o caso do exemplo a seguir.

Exemplo 3.3. Sejam G o grupo abeliano elementar de ordem 3^n onde $n \geq 2$ e $\bar{G} \in \mathcal{P}(n, 3)$ o $\mathcal{P}-$grupo não abeliano com elementos de ordem 2. Pelo Teorema (2.9), G e $\bar{G}$ são reticulado-isomorfos. Como G é abeliano, segue que $sd(G) = 1$. Sabemos que $\bar{G}$ é um produto semidireto de um subgrupo normal abeliano elementar A de ordem 3^{n-1} por um grupo $B \cong \mathbb{Z}_2$. Tomando agora um elemento $a \in A$ e considerando b um gerador de B, vemos facilmente que $\langle b\rangle\langle ba\rangle \neq \langle ba\rangle\langle a\rangle$, isto é, que os subgrupos de $\bar{G}$ não são todos permutáveis, assim $sd(G) < 1$ e daí, $sd(G) \neq sd(\bar{G})$.

Exemplo 3.4. Seja o grupo $S_3 \times \mathbb{Z}_2$, temos que $sd(S_3 \times \mathbb{Z}_2) = \dfrac{101}{128} \neq \dfrac{5}{6} = sd(S_3)sd(\mathbb{Z}_2)$. Em geral, não temos $sd(G_1 \times \cdots \times G_k) = sd(G_1) \cdots sd(G_k)$, onde $(G_i)_{i=\overline{1,k}}$ é uma família de grupos finitos. No teorema seguinte, temos uma condição suficiente para a igualdade anterior ser verdadeira.

Proposição 3.2. *Seja* $(G_i)_{i=\overline{1,k}}$ *uma família de grupos finitos de ordens coprimas. Então* $sd(\times_{i=1}^{k} G_i) = sd(\times_{i=1}^{k} G_i) = \prod_{1}^{k} sd(G_i)$.

Demonstração. Mostraremos a proposição para $i = 2$. Sejam H e K dois grupos finitos quaisquer tendo ordens coprimas, tais que $G = H \times K$. Então

$$sd(G) = sd(H \times K) = \frac{1}{|\mathscr{L}(H \times K)|^2} \sum_{X \in \mathscr{L}(H \times K)} |C(X)|,$$

como $(|H|, |K|) = 1$, segue pelo Lema 2.3, que

$$\begin{aligned} sd(H \times K) &= \frac{1}{|\mathscr{L}(H) \times \mathscr{L}(K)|^2} \sum_{X \in \mathscr{L}(H) \times \mathscr{L}(K)} |C(X)| \\ &= \frac{1}{|\mathscr{L}(H)|^2 |\mathscr{L}(K)|^2} \sum_{X \in \mathscr{L}(H) \times \mathscr{L}(K)} |C(X)|. \end{aligned}$$

Temos que

$$C(X) = \{W \in \mathscr{L}(H \times K) | XW = WX\} = \{W \in \mathscr{L}(H) \times \mathscr{L}(K) | XW = WX\}$$

e oberve que para todo $A \in \mathscr{L}(H)$, para todo $B \in \mathscr{L}(K)$, temos que $AB = BA$, pois $G = H \times K$.

Considermos então, s.p.g, que $X = AB$ e $W = YZ$, com $A, Y \in \mathscr{L}(H)$ e $B, Z \in \mathscr{L}(K)$. Daí

$$C(X) = C(AB) = \{YZ \in \mathscr{L}(H) \times \mathscr{L}(K) | ABYZ = YZAB\}.$$

Por outro lado, $C(A) = \{Y \in \mathscr{L}(H) | AY = YA\}$ e $C(B) = \{Z \in \mathscr{L}(K) | BZ = ZB\}$ e assim,

$$\begin{aligned} C(A) \times C(B) &= \{YZ \in \mathscr{L}(H) \times \mathscr{L}(K) | AYBZ = YAZB\} \\ &= \{YZ \in \mathscr{L}(H) \times \mathscr{L}(K) | ABYZ = YZAB\} \\ &= C(AB) \\ &= C(X). \end{aligned}$$

Daí temos,

$$\begin{aligned} \sum_{X \in \mathscr{L}(H) \times \mathscr{L}(K)} |C(X)| &= \sum_{AB \in \mathscr{L}(H) \times \mathscr{L}(K)} |C(A)||C(B)| \\ &= \sum_{A \in \mathscr{L}(H)} |C(A)| \sum_{B \in \mathscr{L}(K)} |C(B)| \end{aligned}$$

donde,

$$\begin{aligned} sd(H\times K) &= \frac{1}{|\mathscr{L}(H)|^2|\mathscr{L}(K)|^2}\sum_{A\in\mathscr{L}(H)}|C(A)|\sum_{B\in\mathscr{L}(K)}|C(B)| \\ &= \frac{1}{|\mathscr{L}(H)|^2}\sum_{A\in\mathscr{L}(H)}|C(A)|\frac{1}{|\mathscr{L}(K)|^2}\sum_{B\in\mathscr{L}(K)}|C(B)| \\ &= sd(H)sd(K). \end{aligned}$$

Desse modo, sendo $G=(\times_{i=1}^{k}G_i)$, onde $(G_i)_{i=\overline{1,k}}$ é uma família de grupos finitos tendo ordens coprimas, segue que,

$$\begin{aligned} sd(\times_{i=1}^{k}G_i) &= sd(G_1\times\cdots\times G_k) \\ &= \frac{1}{|\mathscr{L}(G_1\times\cdots\times G_k)|^2}\sum_{M\in\mathscr{L}(G_1\times\cdots\times G_k)}|C(M)| \\ &= \frac{1}{|\mathscr{L}(G_1)\times\cdots\times\mathscr{L}(G_k)|^2}\sum_{M\in\mathscr{L}(G_1)\times\cdots\times\mathscr{L}(G_k)}|C(M)| \\ &= \frac{1}{|\mathscr{L}(G_1)|^2\times\cdots\times|\mathscr{L}(G_k)|^2}\sum_{M\in\mathscr{L}(G_1)\times\cdots\times\mathscr{L}(G_k)}|C(M)|. \end{aligned}$$

Agora de $M\in\mathscr{L}(G_1)\times\cdots\times\mathscr{L}(G_k)$, temos que $M=M_1\cdots M_k$, onde $M_i\in\mathscr{L}(G_i), i=1,\cdots,k$, daí

$$\begin{aligned} sd(\times_{i=1}^{k}) &= \frac{1}{|\mathscr{L}(G_1)|^2\cdots|\mathscr{L}(G_k)|^2}\sum_{M_1\in\mathscr{L}(G_1)}|C(M_1)|\quad\cdots\sum_{M_k\in\mathscr{L}(G_k)}|C(M_k)| \\ &= \frac{1}{|\mathscr{L}(G_1)|^2}\sum_{M_1\in\mathscr{L}(G_1)}|C(M_1)|\quad\cdots\quad\frac{1}{|\mathscr{L}(G_k)|^2}\sum_{M_k\in\mathscr{L}(G_k)}|C(M_k)| \\ &= sd(G_1)\cdots sd(G_k) \\ &= \prod_{i=1}^{k}sdG_i. \end{aligned}$$

□

Corolário 3.1. *Se G é um grupo nilpotente finito e $(G_i)_{i=\overline{1,k}}$ são os subgrupos de Sylow de G, então $sd(G)=\prod_{i=1}^{k}sd(G_i)$.*

Demonstração. Pelo Teorema 1.2, temos que $G=G_1\times\cdots\times G_k$. Como os G_i com $i=1,\cdots,k$ têm ordens coprimas, segue da Proposição (3.2) que $sd(G)=sd(\times_{i=1}^{k}G_i)=\prod_{i=1}^{k}sd(G_i)$. □

Proposição 3.3. *Seja G um grupo finito e N um subgrupo normal de G. Então a seguinte desigualdade é válida:*

$$\begin{aligned} sd(G) \;\geq\; & \frac{1}{|\mathscr{L}(G)|^2}\left[\left(|\mathscr{L}(N)|+\left|\mathscr{L}\left(\frac{G}{N}\right)\right|-1\right)^2+(sd(N)-1)|\mathscr{L}(N)|^2+\right. \\ & \left.+\left(sd\left(\frac{G}{N}\right)-1\right)\left|\mathscr{L}\left(\frac{G}{N}\right)\right|^2\right]. \end{aligned} \tag{3.3}$$

Demonstração. Para demonstrar a proposição acima, vamos definir a seguinte função $f:\mathscr{L}(G)^2\to\{0,1\}$, tal que

$$f(H,K)=\begin{cases} 1, & KH=HK \\ 0, & HK\neq KH \end{cases} \tag{3.4}$$

Como $C(H)=\{K\in\mathscr{L}(G)|HK=KH\}$ segue que $|C(H)|=\sum\limits_{K\in\mathscr{L}(G)} f(H,K)$ para qualquer $H\in\mathscr{L}(G)$ e assim na equação (3.2) temos

$$sd(G)=\frac{1}{|\mathscr{L}(G)|^2}\sum_{H\in\mathscr{L}(G)}\sum_{K\in\mathscr{L}(G)} f(H,K).$$

Agora fixemos um subgrupo normal N de G e consideremos os conjuntos $\mathcal{A}_1=\{H\in\mathscr{L}(G)|N\subseteq H\}$ e $\mathcal{A}_2=\{H\in\mathscr{L}(G)|H\subset N\}$. Observe que $\mathcal{A}_1$ corresponde ao reticulado de $\dfrac{G}{N}$, isto é, $\mathcal{A}_1=\mathscr{L}\left(\dfrac{G}{N}\right)$ e $\mathcal{A}_2$ corresponde ao conjunto $\mathscr{L}(N)\setminus N$, ou seja, $\mathscr{L}(N)=\mathcal{A}_2\cup\{N\}$. Temos então que os conjuntos $\mathcal{A}_1$ e $\mathcal{A}_2$ são subconjuntos de $\mathscr{L}(G)$ e assim, $\mathcal{A}_1\cup\mathcal{A}_2\subseteq\mathscr{L}(G)$. Daí, $\sum\limits_{H,K\in\mathscr{L}(G)} f(H,K)\geq\sum\limits_{H,K\in\mathcal{A}_1\cup\mathcal{A}_2} f(H,K)$ e ainda

$$\begin{aligned} sd(G) &= \frac{1}{|\mathscr{L}(G)|^2}\sum_{H,K\in\mathscr{L}(G)} f(H,K)\geq\frac{1}{|\mathscr{L}(G)|^2}\sum_{H,K\in\mathcal{A}_1\cup\mathcal{A}_2} f(H,K) \\ &= \frac{1}{|\mathscr{L}(G)|^2}\left(\sum_{H,K\in\mathcal{A}_1} f(H,K)+\sum_{H,K\in\mathcal{A}_2} f(H,K)\right. \\ &\quad \left.+\sum_{H\in\mathcal{A}_1}\sum_{K\in\mathcal{A}_2} f(H,K)+\sum_{K\in\mathcal{A}_1}\sum_{H\in\mathcal{A}_2} f(H,K)\right) \\ &= \frac{1}{|\mathscr{L}(G)|^2}\left(\sum_{H,K\in\mathcal{A}_1} f(H,K)+\sum_{H,K\in\mathcal{A}_2} f(H,K)\right. \\ &+ \left. 2\sum_{H\in\mathcal{A}_1}\sum_{K\in\mathcal{A}_2} f(H,K)\right). \end{aligned} \tag{3.5}$$

Agora vamos calcular o lado direito da equação (3.5).

$$\sum_{H,K\in\mathcal{A}_1} f(H,K) = \sum_{H,K\in\mathscr{L}\left(\frac{G}{N}\right)} f(H,K) = sd\left(\frac{G}{N}\right)\left|\mathscr{L}\left(\frac{G}{N}\right)\right|^2$$

$$\begin{aligned}\sum_{H,K\in\mathcal{A}_2} f(H,K) &= \sum_{H,K\in\mathcal{A}_2\cup\{N\}} f(H,K) - \sum_{H\in\mathcal{A}_2\cup\{N\}} f(H,N)\\ &\quad - \sum_{K\in\mathcal{A}_2\cup\{N\}} f(K,N) + f(N,N)\\ &= \sum_{H,K\in\mathcal{A}_2\cup\{N\}} f(H,K) - 2\sum_{H\in\mathcal{A}_2\cup\{N\}} f(H,N) + 1\\ &= \sum_{H,K\in\mathscr{L}(N)} f(H,K) - 2\sum_{H\in\mathscr{L}(N)} f(H,K) + 1\\ &= sd(N)|\mathscr{L}(N)|^2 - 2|\mathscr{L}(N)| + 1.\end{aligned}$$

Finalmente, sejam respectivamente n, m as ordens de $\mathcal{A}_1$ e $\mathcal{A}_2$, daí

$$\begin{aligned}2\sum_{H\in\mathcal{A}_1}\sum_{K\in\mathcal{A}_2} f(H,K) &= 2\sum_{H\in\mathcal{A}_1}\big(f(H,K_1)+\cdots+f(H,K_m)\big)\\ &= 2\big(f(H_1,K_1)+\cdots+f(H_n,K_1)+\cdots+\\ &\quad +f(H_1,K_m)+\cdots+f(H_n,K_m)\big).\end{aligned}$$

Mas observe que $H\in\mathcal{A}_1$ e $K\in\mathcal{A}_2$, daí temos $K\subset N\subseteq H$ e com isso $HK=H=KH$. Portanto $f(H_i,K_j)=1$, para todo $i=1,\cdots,n$ e para todo $j=1,\cdots,m$. Voltando na igualdade acima temos,

$$2\sum_{H\in\mathcal{A}_1}\sum_{K\in\mathcal{A}_2} f(H,K) = 2n.m = |\mathcal{A}_1||\mathcal{A}_2| = 2\left|\mathscr{L}\left(\frac{G}{N}\right)\right|\left(|\mathscr{L}(N)|-1\right).$$

Obtemos então que

$$\begin{aligned}\sum_{H,K\in\mathcal{A}_1} f(H,K) &= sd\left(\frac{G}{N}\right)\left|\mathscr{L}\left(\frac{G}{N}\right)\right|^2\\ \sum_{H,K\in\mathcal{A}_2} f(H,K) &= sd(N)|\mathscr{L}(N)|^2 - 2|\mathscr{L}(N)| + 1\\ 2\sum_{H\in\mathcal{A}_1}\sum_{K\in\mathcal{A}_2} &= 2\left|\mathscr{L}\left(\frac{G}{N}\right)\right|(|\mathscr{L}(N)|-1),\end{aligned}$$

substituindo esses três termos na equação (3.5) segue que

$$\begin{aligned} sd(G) \;\geq\; & \frac{1}{|\mathscr{L}(G)|^2}\Bigg[sd\left(\frac{G}{N}\right)\left|\mathscr{L}\left(\frac{G}{N}\right)\right|^2 + sd(N)|\mathscr{L}(N)|^2 - 2|\mathscr{L}(N)| + 1 + \\ & + 2\left|\mathscr{L}\left(\frac{G}{N}\right)\right|(|\mathscr{L}(N)| - 1)\Bigg], \end{aligned}$$

reorganizando, obtemos a desigualdade

$$\begin{aligned} sd(G) \;\geq\; & \frac{1}{|\mathscr{L}(G)|^2}\Bigg[\left(|\mathscr{L}(N)| + \left|\mathscr{L}\left(\frac{G}{N}\right)\right| - 1\right)^2 + (sd(N) - 1)|\mathscr{L}(N)|^2 + \\ & + \left(sd\left(\frac{G}{N}\right) - 1\right)\left|\mathscr{L}\left(\frac{G}{N}\right)\right|^2\Bigg]. \end{aligned}$$

□

Corolário 3.2. *Sejam G um grupo finito e N um subgrupo normal de G com N e $\frac{G}{N}$ abelianos. Então*

$$sd(G) \geq \left(\frac{|\mathscr{L}(N)| + \left|\mathscr{L}\left(\frac{G}{N}\right)\right| - 1}{|\mathscr{L}(G)|}\right)^2 \tag{3.6}$$

Demonstração. Como N e $\frac{G}{N}$ são abelianos temos que $sd(N) = 1$ e $sd(\frac{G}{N}) = 1$, daí na desigualdade (3.3) segue que

$$\begin{aligned} sd(G) \;\geq\; & \frac{1}{|\mathscr{L}(G)|^2}\Bigg[\left(|\mathscr{L}(N)| + \left|\mathscr{L}\left(\frac{G}{N}\right)\right| - 1\right)^2 + (1-1)|\mathscr{L}(N)|^2 + \\ & + (1-1)\left|\mathscr{L}\left(\frac{G}{N}\right)\right|^2\Bigg] = \left(\frac{|\mathscr{L}(N)| + \left|\mathscr{L}\left(\frac{G}{N}\right)\right| - 1}{|\mathscr{L}(G)|}\right)^2. \end{aligned}$$

Portanto,

$$sd(G) \geq \left(\frac{|\mathscr{L}(N)| + \left|\mathscr{L}\left(\frac{G}{N}\right)\right| - 1}{|\mathscr{L}(G)|}\right)^2.$$

□

Corolário 3.3. *Se G é um grupo finito que possui um subgrupo normal N de índice primo, então*

$$sd(G) \geq \frac{1}{|\mathscr{L}(G)|^2}(sd(N)|\mathscr{L}(N)|^2 + 2|\mathscr{L}(N)| + 1).$$

Demonstração. Seja N um subgrupo normal de G tal que N tem índice primo p. De $\left|\frac{G}{N}\right| = p$ segue que $\frac{G}{N}$ é abeliano. Logo $sd\left(\frac{G}{N}\right) = 1$ e substituindo na desigualdade (3.3) obtemos,

$$sd(G) \geq \frac{1}{|\mathscr{L}(G)|^2}\left[\left(|\mathscr{L}(N)| + \left|\mathscr{L}\left(\frac{G}{N}\right)\right| - 1\right)^2 + sd(N)|\mathscr{L}(N)|^2 - |\mathscr{L}(N)|^2\right].$$

Agora como $\left|\frac{G}{N}\right| = p$, p primo segue que $\frac{G}{N}$ não possui subgrupos diferentes dos triviais, donde $\left|\mathscr{L}\left(\frac{G}{N}\right)\right| = 2$. Daí na desigualdade anterior temos,

$$\begin{aligned} sd(G) &\geq \frac{1}{|\mathscr{L}(G)|^2}[(|\mathscr{L}(N)| + 2 - 1)^2 + sd(N)|\mathscr{L}(N)|^2 - |\mathscr{L}(N)|^2] \\ &= \frac{1}{|\mathscr{L}(G)|^2}(|\mathscr{L}(N)|^2 + 2|\mathscr{L}(N)| + 1 + sd(N)|\mathscr{L}(N)|^2 - |\mathscr{L}(N)|^2) \\ &= \frac{1}{|\mathscr{L}(G)|^2}(sd(N)|\mathscr{L}(N)|^2 + 2|\mathscr{L}(N)| + 1), \end{aligned}$$

assim,

$$sd(G) \geq \frac{1}{|\mathscr{L}(N)|^2}(sd(G)|\mathscr{L}(N)|^2 + 2|\mathscr{L}(N)| + 1).$$

□

Corolário 3.4. *Se G é um grupo solúvel finito, então*

$$sd(G) \geq \frac{1}{|\mathscr{L}(G)|^2}\left(2\sum_{i=1}^{k}|\mathscr{L}(G_{i-1})| + k + 1\right). \tag{3.7}$$

Demonstração. Seja G um grupo solúvel finito e considere a seguinte série de composição $\{1\} = G_0 < G_1 < \cdots < G_k = G$. Como todos os grupos fatores $\frac{G_i}{G_{i-1}}$ são cíclicos de ordem prima e cada $G_{i-1} \lhd G_i$ com $i = 1, 2 \cdots k$, segue do Corolário (3.3) que

$$sd(G_i)|\mathscr{L}(G_i)|^2 \geq sd(G_{i-1})|\mathscr{L}(G_{i-1)}|^2 + 2|\mathscr{L}(G_{i-1})| + 1,$$

$\forall\, i = 1, 2, \cdots, k$.

Agora observe que

$$\begin{aligned} sd(G_k)|\mathscr{L}(G_k)|^2 &\geq sd(G_{k-1})|\mathscr{L}(G_{k-1})|^2 + 2|\mathscr{L}(G_{k-1})| + 1 \\ sd(G_{k-1})|\mathscr{L}(G_{k-1})|^2 &\geq sd(G_{k-2})|\mathscr{L}(G_{k-2})|^2 + 2|\mathscr{L}(G_{k-2})| + 1 \\ &\vdots \\ sd(G_2)|\mathscr{L}(G_2)|^2 &\geq sd(G_1)|\mathscr{L}(G_1)|^2 + 2|\mathscr{L}(G_1)| + 1 \\ sd(G_1)|\mathscr{L}(G_1)|^2 &\geq sd(G_0)|\mathscr{L}(G_0)|^2 + 2|\mathscr{L}(G_0)| + 1 \end{aligned}$$

substituindo sucessivamente as desigualdades anteriores, obtemos que

$$\begin{aligned} sd(G_k)|\mathscr{L}(G_k)|^2 &\geq sd(G_{k-2})|\mathscr{L}(G_{k-2})|^2 + 2|\mathscr{L}(G_{k-1})| + 2|\mathscr{L}(G_{k-2})| + 1 + 1 \\ &\geq sd(G_0)|\mathscr{L}(G_0)|^2 + 2|\mathscr{L}(G_{k-1})| + 2|\mathscr{L}(G_{k-2})| + \\ &\quad + \cdots + 2|\mathscr{L}(G_0)| + 1 + \cdots + 1 \\ &= sd(G_0)|\mathscr{L}(G_o)|^2 + 2\sum_{i=1}^{k} |\mathscr{L}(G_{i-1})| + k. \end{aligned}$$

Mas $sd(G_0) = 1$ e $|\mathscr{L}(G_0)| = 1$ pois $G_0 = \{1\}$, daí

$$sd(G_k)|\mathscr{L}(G_k)|^2 \geq 2\sum_{i=1}^{k} |\mathscr{L}(G_{i-1})| + k + 1,$$

ou melhor,

$$sd(G) \geq \frac{1}{|\mathscr{L}(G)|^2}\left(2\sum_{i=1}^{k} |\mathscr{L}(G_{i-1})| + k + 1\right).$$

□

Corolário 3.5. *Se G é um p-grupo finito de ordem p^k, com p primo, que tem um subgrupo maximal cíclico, então*

$$sd(G) \geq \left(\frac{k+1}{|\mathscr{L}(G)|}\right)^2. \tag{3.8}$$

Demonstração. Seja G um grupo de ordem p^k, onde p é primo. Como todo p-grupo finito é solúvel, podemos considerar a série de composição $\{1\} = G_0 < G_1 < \cdots < G_k = G$, que é uma série solúvel de G. Observe que cada G_{i-1} é maximal em G_i e por hipótese, G possui um subgrupo maximal cíclico, daí podemos assumir que G_{k-1} é cíclico, donde segue que todos os G_{i-1} são cíclicos para todo $i = 1, \cdots, k-1$.

Resta mostrar que $|\mathscr{L}(G_{i-1})| = i$, para qualquer $i = 1, \cdots, k$. Note então que G_{k-1} tem ordem p^{k-1} para todo $i = 1, \cdots, k$. Como para cada divisor a de p^{i-1}, existe um único subgrupo de ordem a, pois G_{i-1} é cíclico, segue que $|\mathscr{L}(G_{i-1})| = i$ para todo $i = 1, \cdots, k$.

Finalmente, usando o Corolário (3.4) temos

$$\begin{aligned} sd(G) &\geq \frac{1}{|\mathscr{L}(G)|^2}[2(1 + 2 + \cdots + k) + k + 1] = \frac{1}{|\mathscr{L}(G)|^2}\left[\frac{2k(k+1)}{2} + k + 1\right] \\ &= \frac{1}{|\mathscr{L}(G)|^2}(k^2 + 2k + 1) = \left(\frac{k+1}{|\mathscr{L}(G)|}\right)^2. \end{aligned}$$

Portanto $sd(G) \geq \left(\frac{k+1}{|\mathscr{L}(G)|}\right)^2$. □

Capítulo 4

O Grau de Comutatividade em Algumas Classes de Grupos Finitos

Veremos neste capítulo o grau de comutatividade de subgrupos de um grupo finito para algumas classes de grupos. Apartir do que estudamos no capítulo anterior, construíremos expressões para determinar o grau de comutatividade de subgrupos do grupo diedral finito D_{2n} e de p-grupos finitos que possuem um subgrupo maximal cíclico.

4.1 O Grau de Comutatividade de Subgrupos do Grupo Diedral Finito D_{2n}

Sabemos que o grupo diedral é gerado por uma rotação x de ordem n e uma reflexão y de ordem 2. Podemos escrever então $D_{2n} = \langle x, y | x^n = y^2 = 1, yxy = x^{-1} \rangle$. Para cada divisor r de n, D_{2n} possui um subgrupo isomorfo à $\mathbb{Z}_r$, a saber, $H_0^r = \langle x^{\frac{n}{r}} \rangle$ e $\frac{n}{r}$ subgrupos isomorfos a D_{2r}, são eles, $H_i^r = \langle x^{\frac{n}{r}}, x^{i-1}y \rangle$, onde $i \in \{1, \cdots, \frac{n}{r}\}$. Assim obtemos que $|\mathscr{L}(D_{2n})| = \tau(n) + \sigma(n)$, onde $\tau(n)$ e $\sigma(n)$ são funções aritméticas multiplicativas e denotam respectivamente, o número e a soma dos divisores de n.

Agora observamos que o subgrupo $\langle x \rangle$ é normal em D_{2n}, onde $\langle x \rangle$ é o "grupo das rotações". Como $\langle x \rangle$ tem ordem n segue que para cada divisor r de n, $\langle x \rangle$ possui um único subgrupo $H_0^r = \langle x^{\frac{n}{r}} \rangle$ de ordem r. Da unicidade de H_0^r temos que ele é característico em $\langle x \rangle$ e do fato de $\langle x \rangle$ ser normal em D_{2n} segue que H_0^r é normal em

D_{2n}, para cada divisor r de n. Assim temos,

$$\begin{aligned}\sum_{H\in\mathscr{L}(D_{2n})}|C(H)| &= \sum_{r|n}|C(H_0^r)|+\sum_{r|n}\sum_{i=1}^{\frac{n}{r}}|C(H_i^r)|\\ &= \tau(n)|\mathscr{L}(D_{2n})|+\sum_{r|n}\sum_{i=1}^{\frac{n}{r}}|C(H_i^r)|.\end{aligned}$$

Para determinar $\sum_{H\in\mathscr{L}(D_{2n})}|C(H)|$ precisamos controlar a soma $\sum_{r|n}\sum_{i=1}^{\frac{n}{r}}|C(H_i^r)|$. Para fazer isto, fixemos o divisor r de n e o índice $i\in\{1,\cdots,\frac{n}{r}\}$, com isso

$$C(H_i^r)=\Big\{\Big(\bigcup_{r|n}\{H_0^r\}\Big)\cup\{K\in\mathscr{L}(D_{2n})\mid K=diedral, H_i^rK=KH_i^r\Big\}.$$

Consideremos um subgrupo arbitrário $K=H_j^s$ onde s divide n e $j\in\{1,\cdots,\frac{n}{s}\}$, observamos que $H_j^s\in C(H_i^r)$ se, e somente se, $H_i^rH_j^s=H_j^sH_i^r$. Mas $H_i^rH_j^s=H_j^sH_i^r$ se, e somente se, $hk=\bar{k}\bar{h}$, onde $h,\bar{h}\in H_i^r$ e $k,\bar{k}\in H_j^s$ são arbitrários. Agora como

$$H_i^r = \Big\{\big(x^{\frac{n}{r}}\big)^l(x^{i-1}y)^\delta; l=0,\cdots,r-1 \quad \text{e} \quad \delta=0 \quad \text{ou} \quad 1\Big\}$$

e

$$H_j^s = \Big\{\big(x^{\frac{n}{s}}\big)^m(x^{j-1}y)^\varepsilon; m=0,\cdots,s-1 \quad \text{e} \quad \varepsilon=0 \quad \text{ou} \quad 1\Big\},$$

temos para $h,\bar{h}$ e $k,\bar{k}$ arbitrários que $H_i^rH_j^s=H_j^sH_i^r$ se, e somente se, $hk=\bar{h}\bar{k}$ se, e somente se,

$$\big(x^{\frac{n}{r}}\big)^l\big(x^{i-1}y\big)^\delta\big(x^{\frac{n}{s}}\big)^m\big(x^{j-1}y\big)^\varepsilon=\big(x^{\frac{n}{s}}\big)^{\bar{m}}\big(x^{j-1}y\big)^{\bar{\varepsilon}}\big(x^{\frac{n}{r}}\big)^{\bar{l}}\big(x^{i-1}y\big)^{\bar{\delta}} \tag{4.1}$$

Observamos que para resolver a equação (4.1) basta alternar os valores de ε,δ e $\bar{\varepsilon},\bar{\delta}$ e manter $l,m,\bar{l}$ e $\bar{m}$. Vejamos como fica a igualdade (4.1) para o caso em que $\varepsilon=1,\delta=1$ e $\bar{\varepsilon}=1,\bar{\delta}=1$.

$$\begin{aligned}x^{\frac{n}{r}l}x^{i-1}yx^{\frac{n}{s}m}x^{j-1}y &= x^{\frac{n}{s}\bar{m}}x^{j-1}yx^{\frac{n}{r}\bar{l}}x^{i-1}y \Leftrightarrow\\ x^{\frac{n}{r}l}x^{i-1}x^{-j+1}x^{\frac{-n}{s}m} &= x^{\frac{n}{s}\bar{m}}x^{j-1}x^{-i+1}x^{\frac{-n}{r}\bar{l}} \Leftrightarrow\\ x^{2(i-j)} &= x^{\frac{n}{r}(-\bar{l}-l)+\frac{n}{s}(\bar{m}+m)} \Leftrightarrow\\ x^{2(i-j)} &= x^{\frac{n}{[r,s]}[u(-\bar{l}-l)+v(\bar{m}+m)]}.\end{aligned}$$

Dessa forma, para o caso geral obtemos que $H_j^s\in C(H_i^r)$ se, e somente se, $x^{2(i-j)}\in\left\langle x^{\frac{n}{[r,s]}}\right\rangle$, isto é, se, e somente se,

$$\frac{n}{[r,s]}\Big|2(i-j) \tag{4.2}$$

Finalmente, denotando por x_i^r o número de soluções de (4.2), obtemos que

$$|C(H_i^r)| = \tau(n) + x_i^r,$$

donde segue que

$$\begin{aligned}
\sum_{H\in\mathscr{L}(D_{2n})} |C(H)| &= \tau(n)(\tau(n)+\sigma(n)) + \sum_{r|n}\sum_{i=1}^{\frac{n}{r}}(\tau(n)+x_i^r) \\
&= \tau(n)(\tau(n)+\sigma(n)) + \sum_{r|n}\sum_{i=1}^{\frac{n}{r}}\tau(n) + \sum_{r|n}\sum_{i=1}^{\frac{n}{r}}x_i^r \\
&= \tau(n)^2 + \tau(n)\sigma(n) + \sum_{r|n}(\tau(n)+\cdots+\tau(n)) + \sum_{r|n}\sum_{i=1}^{\frac{n}{r}}x_i^r \\
&= \tau(n)^2 + \tau(n)\sigma(n) + \sum_{r|n}\frac{n}{r}\tau(n) + \sum_{r|n}\sum_{i=1}^{\frac{n}{r}}x_i^r \\
&= \tau(n)^2 + \tau(n)\sigma(n) + \tau(n)\sigma(n) + \sum_{r|n}\sum_{i=1}^{\frac{n}{r}}x_i^r \\
&= \tau(n)^2 + 2\tau(n)\sigma(n) + \sum_{r|n}\sum_{i=1}^{\frac{n}{r}}x_i^r.
\end{aligned}$$

Agora como $sd(D_{2n}) = \dfrac{1}{|\mathscr{L}(D_{2n})|^2}\displaystyle\sum_{H\in\mathscr{L}(D_{2n})}|C(H)|$, obtemos uma formula explícita para $sd(D_{2n})$.

Teorema 4.1. *O grau de comutatividade de subgrupos do grupo diedral D_{2n} é dado pela seguinte igualdade:*

$$sd(D_{2n}) = \frac{\tau(n)^2 + 2\tau(n)\sigma(n) + \displaystyle\sum_{r|n}\sum_{s|n}^{\frac{n}{r}}x_i^r}{(\tau(n)+\sigma(n))^2} \tag{4.3}$$

Vejamos que para calcular o grau de comutatividade de subgrupos $sd(D_{2n})$ do grupo diedral, precisamos determinar a quantidade de soluções de (4.2). Para fazer isto, devemos analizar dois casos particulares de n, a seguir.

Caso 4.1. *Quando n é ímpar.*

Neste caso, (4.2) é equivalente à $i \equiv j \left(mod\ \dfrac{n}{[r,s]}\right)$. Dessa congruência fazemos a seguinte afirmação.

Afirmação 4.1. *A congruência* $i \equiv j \left(mod\ \frac{n}{[r,s]}\right)$ *tem* $\frac{[r,s]}{s}$ *soluções* $j \in \{1, \cdots, \frac{n}{s}\}$.

Demonstração. Observe que para um s fixo, $\frac{n}{[r,s]} \Big| (i-j)$ se, e somente se, $(i-j)$ for um múltiplo de $\frac{n}{[r,s]}$. Como $i \in \{1, \cdots, \frac{n}{r}\}$ e $j \in \{1, \cdots, \frac{n}{s}\}$ segue que

$$\begin{aligned}
&\text{para} \quad i = 1 \quad , \quad \text{temos} \quad j = 0\frac{n}{[r,s]} + 1, 1\frac{n}{[r,s]} + 1, \cdots, \alpha\frac{n}{[r,s]} + 1 \\
&\text{para} \quad i = 2 \quad , \quad \text{temos} \quad j = 0\frac{n}{[r,s]} + 2, 1\frac{n}{[r,s]} + 2, \cdots, \alpha\frac{n}{[r,s]} + 2 \\
&\qquad\qquad \vdots \\
&\text{para} \quad i = \frac{n}{r}, \quad \text{temos} \quad j = 0\frac{n}{[r,s]} + \frac{n}{r}, 1\frac{n}{[r,s]} + \frac{n}{r}, \cdots, \alpha\frac{n}{[r,s]} + \frac{n}{r},
\end{aligned}$$

ou melhor, temos $j = \frac{n}{r}, \cdots, \frac{n}{s}$, onde $0 \leq \alpha \leq \frac{[r,s]}{s} - 1$. Obtemos então que para um s fixo a congruência $i \equiv j \left(mod\ \frac{n}{[r,s]}\right)$ tem $\frac{[r,s]}{s}$ soluções $j \in \{1, \cdots, \frac{n}{s}\}$.

Como x_i^r representa o número de soluções de (4.2), segue neste caso que

$$x_i^r = \sum_{s|n} \frac{[r,s]}{s} = \sum_{s|n} \frac{r}{(r,s)} = r \sum_{s|n} \frac{1}{(r,s)}$$

e assim,

$$\sum_{r|n} \sum_{i=1}^{\frac{n}{r}} x_i^r = \sum_{r|n} \sum_{i=1}^{\frac{n}{r}} r \sum_{s|n} \frac{1}{(r,s)} = \sum_{r|n} \frac{n}{r} r \sum_{s|n} \frac{1}{(r,s)} = n \sum_{r|n} \sum_{s|n} \frac{1}{(r,s)}.$$

Podemos escrever então que $\sum_{r|n} \sum_{i=1}^{\frac{n}{r}} x_i^r = g(n)$, onde g é a função definida por $g(k) = k \sum_{r|k} \sum_{s|k} \frac{1}{(r,s)}$, para todo $k \in \mathbb{N}$. Sobre essa função g fazemos a afirmação à seguir.

Afirmação 4.2. *A função* $g(k) = k \sum_{r|k} \sum_{s|k} \frac{1}{(r,s)}$ *para todo* $k \in \mathbb{N}$ *é uma função aritmética multiplicativa.*

Demonstração. Note que $g : \mathbb{N} \to \mathbb{N}$ e ainda, dados dois inteiros a, b tais que $(a,b) = 1$ e considerando x, y divisores de a e z, w divisores de b, temos que $g(ab) = ab \sum_{xz|ab} \sum_{yw|ab} \frac{1}{(xz, yw)}$. Como $(x,z) = 1 = (y,w)$, segue que

$$g(ab) = ab \sum_{x|a} \sum_{z|b} \sum_{y|a} \sum_{w|b} \frac{1}{(x,y)(z,w)} = a \sum_{x|a} \sum_{y|b} \frac{1}{(x,y)} b \sum_{z|b} \sum_{w|b} \frac{1}{(z,w)} = g(a)g(b)$$

e portanto g é uma função aritmética multiplicativa.

Queremos agora escrever a função g de maneira mais simples. Vejamos então a afirmação à seguir.

Afirmação 4.3. *Seja p um número primo qualquer e $\alpha \in \mathbb{N}$, então:*

$$g(p^\alpha) = \frac{(2\alpha+1)p^{\alpha+2} - (2\alpha+3)p^{\alpha+1} + p + 1}{(p-1)^2}.$$

Demonstração. Para verificar esta igualdade, basta fazer indução sobre α.

Se $\alpha = 1$, temos que os divisores de p são 1 e p, e daí

$$\begin{aligned} g(p) &= p\sum_{r|p}\sum_{s|p}\frac{1}{(r,s)} = p\sum_{r|p}\left(\frac{1}{(r,1)} + \frac{1}{(r,p)}\right) \\ &= \frac{p}{(1,1)} + \frac{p}{(p,1)} + \frac{p}{(1,p)} + \frac{p}{(p,p)} = 3p+1. \end{aligned}$$

Multiplicando $g(p)$ por $(p-1)^2$, temos

$$g(p) = \frac{3p^3 - 5p^2 + p + 1}{(p-1)^2} = \frac{(2\alpha+1)p^{\alpha+2} - (2\alpha+3)p^{\alpha+1} + p + 1}{(p-1)^2}.$$

Se $\alpha = 2$, segue que os divisores de p^2 são $1, p$ e p^2, donde

$$\begin{aligned} g(p^2) &= p^2\sum_{r|p}\sum_{s|p}\frac{1}{(r,s)} = p\sum_{r|p}\left(\frac{1}{(r,1)} + \frac{1}{(r,p)} + \frac{1}{(r,p)}\right) \\ &= \frac{p}{(1,1)} + \frac{p}{(p,1)} + \frac{p}{(p^2,p)} + \frac{p}{(1,p)} + \frac{p}{(p,p)} + \frac{p}{(p^2,p)} + \\ &\quad + \frac{p}{(1,p^2)} + \frac{p}{(p,p^2)} + \frac{p}{(p^2,p^2)} = 5p^2 + 3p + 1. \end{aligned}$$

Novamente, multiplicando $g(p^2)$ por $(p-1)^2$ obtemos

$$g(p^2) = \frac{5p^4 - 7p^3 + p + 1}{(p-1)^2} = \frac{(2\alpha+1)p^{\alpha+2} - (2\alpha+3)p^{\alpha+1} + p + 1}{(p-1)^2}.$$

Assim,

$$g(p^\alpha) = \frac{(2\alpha+1)p^{\alpha+2} - (2\alpha+3)p^{\alpha+1} + p + 1}{(p-1)^2}.$$

Por fim, se $n = p_1^{\alpha_1}\cdots p_m^{\alpha_m}$ é a decomposição de n em fatores primos, onde $p_1, \cdots, p_m$ são primos distintos e $\alpha_1, \cdots, \alpha_m \in \mathbb{N}$, segue então pelas afirmações 4.2 e 4.3 que

$$\begin{aligned} g(n) &= g(p_1^{\alpha_1}\cdots p_m^{\alpha_m}) = g(p_1^{\alpha_1})\cdots g(p_m^{\alpha_m}) \\ &= \frac{\prod_{i=1}^{m}(2\alpha_i+1)p_i^{\alpha_i+2} - 2(\alpha_i+3)p_i^{\alpha_i+1} + p_i + 1}{(p_i-1)^2} \end{aligned} \tag{4.4}$$

Corolário 4.1. *Se n é ímpar e g denota a função aritmética definida pela equação (4.4), então o grau de comutatividade de subgrupos do grupo diedral D_{2n} é:*

$$sd(D_{2n}) = \frac{\tau(n)^2 + 2\tau(n)\sigma(n) + g(n)}{(\tau(n) + \sigma(n))^2}$$

Demonstração. De fato, como no caso (4.1) mostramos que $\sum_{r|n} \sum_{i=1}^{\frac{n}{r}} x_i^r = g(n)$, onde $g(n)$ é a função aritmética dada pela equação (4.4) e da equação (4.3) segue que

$$sd(D_{2n}) = \frac{\tau(n)^2 + 2\tau(n)\sigma(n) + g(n)}{(\tau(m) + \sigma(n))^2}.$$

□

Agora vejamos o outro caso a ser analisado.

Caso 4.2. *Quando $n = 2^{m-1}$, $m > 1$ natural.*

Para $r = n$ a equação (4.2) é satisfeita por todos os s que dividem n e todos os $j \in \{1, \cdots, \frac{n}{s}\}$. Assim, $x_i^r = x_i^n = \sum_{s|n} \sum_{j=1}^{\frac{n}{s}} 1 = \sum_{s|n} \frac{n}{s} = \sigma(n) = \frac{2^{m-1+1} - 1}{2 - 1} = 2^m - 1.$

Para $r < n$, faça $r = 2^u$, onde $0 \leq u \leq m-2$. Se $s = n$, então a equação (4.2) tem exatamente uma solução j, que é $j = 1$. Se $s < n$, então fazendo $s = 2^v$ com $0 \leq v \leq m-2$, decorre que a equação (4.2) é equivalente à $i \equiv j \left(mod\ 2^{m-2-max\{u,v\}}\right)$. Observe que $2^{m-2-max\{u,v\}} | (i-j)$ se, e somente se, $(i-j)$ for um múltiplo de $2^{m-2-max\{u,v\}}$ e como $i \in \{1, \cdots, 2^{m-1-u}\}$ e $j \in \{1, \cdots, 2^{m-2-v}\}$ temos que

$$\begin{aligned}
\text{para} \quad i &= 1, \quad \text{temos} \quad j = 0.2^{m-2-max\{u,v\}} + 1, 1.2^{m-2-max\{u,v\}} + 1, \\
&\quad \cdots, \bar{\alpha}.2^{m-2-max\{u,v\}} + 1 \\
\text{para} \quad i &= 2, \quad \text{temos} \quad j = 0.2^{m-2-max\{u,v\}} + 2, 1.2^{m-2-max\{u,v\}} + 2, \\
&\quad \cdots, \bar{\alpha}.2^{m-2-max\{u,v\}} \\
&\vdots \\
\text{para} \quad i &= 2^{m-1-u}, \quad \text{temos} \quad j = 0.2^{m-2-max\{u,v\}} + 2^{m-1-u}, 1.2^{m-2-max\{u,v\}} + 2^{m-1-u}, \\
&\quad \cdots, \bar{\alpha}.2^{m-2-max\{u,v\}} + 2^{m-1-u},
\end{aligned}$$

ou melhor, $j = 2^{m-1-u}, \cdots, 2^{m-1-v}$, onde $0 \leq \bar{\alpha} \leq 2^{max\{u,v\}+1-v} - 1$. Dessa forma, obtemos que a congruência $i \equiv \left(mod\, 2^{m-2-max\{u,v\}}\right)$ tem $\frac{2[2^u, 2^v]}{2^v} = 2^{max\{u,v\}-v+1}$ soluções $j \in \{1, \cdots, 2^{m-1-v}\}$ e assim,

$$\begin{aligned} x_i^r &= 1 + \sum_{v=0}^{m-2} 2^{max\{u,v\}-v+1} = 1 + \sum_{v=0}^{u} 2^{max\{u,v\}-v+1} + \sum_{v=u}^{m-2} 2^{max\{u,v\}-v+1} \\ &= 1 + 2^{u+1} + 2^u + 2^{u-1} + 2^{u-2} + \cdots + 2^2 + 2 + 2(m-2-u) \\ &= 1 + 2^{u+2} - 2 + 2m - 4 - 2u = 2^{u+2} - 2u + 2m - 5. \end{aligned}$$

Finalmente, juntando os casos em que $r = n$ e $r < n$, obtemos que

$$\begin{aligned} \sum_{r|n} \sum_{i=1}^{\frac{n}{r}} x_i^r &= 2^m - 1 + \sum_{u=0}^{m-2} \sum_{i=1}^{\frac{n}{r}} (2^{u+2} - 2u + 2m - 5) \\ &= 2^m - 1 + \sum_{u=0}^{m-2} \frac{n}{r} (2^{u+2} - 2u + 2m - 5) \\ &= 2^m - 1 + \sum_{u=0}^{m-2} 2^{m-1-u} (2^{u+2} - 2u + 2m - 5) \\ &= 2^m - 1 + 2^{m+1} \sum_{u=0}^{m-2} 1 - 2^m \sum_{u=0}^{m-2} \frac{u}{2^u} + 2^m m \sum_{u=0}^{m-2} \frac{1}{2^u} - 2^{m-1} 5 \sum_{u=0}^{m-2} \frac{1}{2^u} \\ &= 2^m - 1 + 2^{m+1}(m-1) - 2^m \left(-2 \left(\frac{1}{2}\right)^{m-1} (m-1) - 2 \left(\frac{1}{2}\right)^{m-1} + 2 \right) + \\ &\quad + \left(2^m m - 2^{m-1} 5\right) \sum_{u=0}^{m-2} \frac{1}{2^u} \\ &= 2^m - 1 + 2^{m+1} m - 2^{m+1} - 2^m (-2^{-m+2} m + 2) + \\ &\quad + (2^m m - 2^{m-1} 5) \frac{(2^{m-1} - 1)}{2^{m-2}} \\ &= 2^m - 1 + 2^{m+1} m - 2^{m+1} + 2^2 m - 2^{m+1} + 2^{m+1} m - 2^2 m - 2^m 5 + 10 \\ &= 2^{m+2} m - 2^{m+2} - 4.2^m + 9 \\ &= 2^{m+2} m - 2.2^{m+2} + 9 \\ &= (m-2) 2^{m+2} + 9. \end{aligned}$$

□

Corolário 4.2. *Se $n = 2^{m-1}$, m um inteiro positivo maior que 1, então o grau de comutatividade de subgrupos $sd(D_{2^m})$ do grupo diedral D_{2^m} é dado pela seguinte igualdade:*

$$sd(D_{2^m}) = \frac{(m-2)2^{m+2} + m2^{m+1} + (m-1)^2 + 8}{(m - 1 + 2^m)^2}.$$

Demonstração. Se $n = 2^{m-1}$, temos pelo Teorema (4.1) e pelo caso 4.2 que

$$\begin{aligned} sd(D_{2^m}) &= \frac{\tau(2^{m-1})^2 + 2\tau(2^{m-1})\sigma(2^{m-1}) + (m-2)2^{m+2} + 9}{(\tau(2^{m-1}) + \sigma(2^{m-1}))^2} \\ &= \frac{(m-1+1)^2 + 2(m-1+1)(2^m-1) + (m-2)2^{m+2} + 9}{(m-1+1+2^m-1)^2} \\ &= \frac{(m-2)2^{m+2} + m^2 + m2^{m+1} - 2m + 1 + 8}{(m-1+2^m)^2} \\ &= \frac{(m-2)2^{m+2} + m2^{m+1} + (m-1)^2 + 8}{(m-1+2^m)^2}. \end{aligned}$$

□

Uma consequência do corolário anterior é o seguinte corolário.

Corolário 4.3. $\lim_{m\to\infty} sd(D_{2^m}) = 0$

Como vimos anteriormente, os Corolários (4.1) e (4.2) nos dão uma expressão para o grau de comutatividade de $sd(D_{2n})$ para dois casos particulares de n. Veremos no teorema a seguir uma expressão para $sd(D_{2n})$ quando n é arbritrário.

Teorema 4.2. *Seja $n = 2^\alpha n'$ um inteiro positivo, onde n' é ímpar, $\alpha \in \mathbb{N}$ e g é a função aritmética definida pela equação (4.4). Então o grau de comutatividade de subgrupos do grupo diedral D_{2n} é dado por:*

$$sd(D_{2n}) = \frac{\tau(n)^2 + 2\tau(n)\sigma(n) + [(\alpha-1)2^{\alpha+3} + 9]g(n')}{(\tau(n) + \sigma(n))^2} \tag{4.5}$$

Demonstração. Suponhamos que $n = 2^\alpha n'$ com $\alpha \in \mathbb{N}$ e n' ímpar. Devemos mostrar que neste caso, a soma $\sum_{r|n} \sum_{i=1}^{\frac{n}{r}} x_i^r$ é igual ao produto dos valores calculados para $n = 2^\alpha$ e $n = n'$ nos casos 4.1 e 4.2 respectivamente.

Usando a notação acima, o divisor r de n é da forma $2^\beta r'$, onde $\beta \leq \alpha$ e $r'|n'$.

Se $\beta = \alpha$, para cada divisor $s = 2^\gamma s'$ (s' ímpar) temos que a equação (4.2) é da forma $\frac{n'}{[r', s']} \Big| 2(i-j)$ e como $i \in \{1, \cdots, \frac{n'}{r'}\}$ e $j \in \{1, \cdots, \frac{2^{\alpha-\gamma}n'}{s'}\}$, obtemos que a equação (4.2) tem $\frac{2^{\alpha-\gamma}[r', s']}{s'}$ soluções $j \in \{1, \cdots, \frac{2^{\alpha-\gamma}n'}{s'}\}$. Mas $[r', s'](r', s') = r's'$ e portanto a equação (4.2) tem $\frac{2^{\alpha-\gamma}r'}{(r', s')}$ soluções $j \in \{1, \cdots, \frac{2^{\alpha-\gamma}n'}{s'}\}$. Com isso, obtemos que

$$x_i^r = \sum_{\gamma=0}^{\alpha} \sum_{s'|n'} \frac{2^{\alpha-\gamma}r'}{(r', s')} = \sum_{\gamma=0}^{\alpha} 2^{\alpha-\gamma}r' \sum_{s'|n'} \frac{1}{(r', s')} = (2^{\alpha+1} - 1)r' \sum_{s'|n'} \frac{1}{(r', s')}. \tag{4.6}$$

Agora suponha que $\beta < \alpha$ e faça s como acima. Se $\gamma = \alpha$, escrevemos a equação (4.2) como $\frac{n'}{[r', s']} \Big| 2(i-j)$, onde $i \in \{1, \cdots, \frac{2^{\alpha-\beta}n'}{r'}\}$ e $j \in \{1, \cdots, \frac{n'}{s'}\}$ e daí a equação (4.2) possui $\frac{r'}{(r', s')}$ soluções $j \in \{1, \cdots, \frac{n'}{s'}\}$. Agora se $\gamma < \alpha$, então a equação (4.2) é da forma $\frac{2^\alpha n'}{[2^\beta r', 2^\gamma s']} \Big| 2(i-j)$ e ainda, $i \in \{1, \cdots, \frac{2^{\alpha-\beta}n'}{r'}\}$ e $j \in \{1, \cdots, \frac{2^{\alpha-\gamma}n'}{s'}\}$, daí a equação (4.2) tem $\frac{2[2^\beta r', 2^\gamma s']}{2^\gamma s'} = 2^{\beta+1-min\{\beta,\gamma\}} \frac{r'}{(r', s')}$ soluções $j \in \{1, \cdots, 2^{\alpha-\gamma}\frac{n'}{s'}\}$. Assim segue que

$$\begin{aligned}
x_i^r &= \sum_{\gamma=0}^{\alpha=1} \sum_{s'|n'} \left(\frac{r'}{(r', s')} + 2^{\beta+1-min\{\beta,\gamma\}} \frac{r'}{(r', s')} \right) \\
&= \left(1 + \sum_{\gamma=0}^{\alpha-1} 2^{\beta+1-min\{\beta,\gamma\}} \right) r' \sum_{s'|n'} \frac{1}{(r', s')} \\
&= \left(1 + \sum_{\gamma=0}^{\beta} 2^{\beta+1-min\{\beta,\gamma\}} + \sum_{\gamma=\beta}^{\alpha-1} 2^{\beta+1-min\{\beta,\gamma\}} \right) r' \sum_{s'|n'} \frac{1}{(r', s')} \\
&= \left(1 + \sum_{\gamma=0}^{\beta} 2^{\beta+1-\gamma} + 2\sum_{\gamma=\beta}^{\alpha-1} \right) r' \sum_{s'|n'} \frac{1}{(r', s')} \\
&= \left(2^{\beta+2} - 2\beta + 2\alpha - 3\right) r' \sum_{s'|n'} \frac{1}{(r', s')}. \qquad (4.7)
\end{aligned}$$

Agora, usando as igualdades (4.6) e (4.7), obtemos que

$$\begin{aligned}
\sum_{r|n} \sum_{i=1}^{\frac{n}{r}} x_i^r &= \sum_{r'|n'} \sum_{i=1}^{\frac{n'}{r'}} \left(2^{\alpha+1} - 1\right) r' \sum_{s'|n'} \frac{1}{(r', s')} + \\
&\quad + \sum_{\beta=0}^{\alpha-1} \sum_{r'|n'} \sum_{i=1}^{\frac{n}{r}} \left(2^{\beta+2} - 2\beta + 2\alpha - 3\right) r' \sum_{s'|n'} \frac{r'}{(r', s')} \\
&= \sum_{r'|n'} \left(2^{\alpha+1} - 1\right) n' \sum_{s'|n'} \frac{1}{(r', s')} + \\
&\quad + \sum_{\beta=0}^{\alpha-1} \sum_{r'|n'} \frac{n}{r} \left(2^{\beta+2} - 2\beta + 2\alpha - 3\right) r' \sum_{s'|n'} \frac{r'}{(r', s')} \\
&= \sum_{r'|n'} \left(2^{\alpha+1} - 1\right) n' \sum_{s'|n'} \frac{1}{(r', s')} + \\
&\quad + \sum_{\beta=0}^{\alpha-1} 2^{\alpha-\beta} \left(2^{\beta+2} - 2\beta + 2\alpha - 3\right) n' \sum_{r'|n} \sum_{s'|n'} \frac{1}{(r', s')}
\end{aligned}$$

$$\begin{aligned}
\sum_{r|n}\sum_{i=1}^{\frac{n}{r}} x_i^r &= \left[2^{\alpha+1}-1+2^{\alpha+2}\sum_{\beta=0}^{\alpha-1}1-2^{\alpha+1}\sum_{\beta=0}^{\alpha-1}\frac{\beta}{2^\beta}+\right.\\
&\quad \left.+\left(2^{\alpha+1}\alpha-2^\alpha 3\right)\sum_{\beta=0}^{\alpha-1}\frac{1}{2^\beta}\right]n'\sum_{r'|n'}\sum_{s'|n'}\frac{1}{(r',s')}\\
&= \left[2^{\alpha+1}-1+2^{\alpha+2}\alpha-2^{\alpha+1}\left(-2\left(\frac{1}{2}\right)^\alpha\alpha-2\left(\frac{1}{2}\right)^\alpha+2\right)+\right.\\
&\quad \left.+\left(2^{\alpha+1}\alpha-2^\alpha 3\right)\frac{(2^\alpha-1)}{2^{\alpha-1}}\right]n'\sum_{r'|n'}\sum_{s'|n'}\frac{1}{(r',s')}\\
&= \Big(2^{\alpha+1}-1+2^{\alpha+2}\alpha+2^2\alpha+2^2-2^{\alpha+2}+\\
&\quad +2^{\alpha+2}\alpha-2^2\alpha-3.2^{\alpha+1}+6\Big)n'\sum_{r'|n'}\sum_{s'|n'}\frac{1}{(r',s')}\\
&= \left(-2.2^{\alpha+1}+2.2^{\alpha+2}\alpha-2^{\alpha+2}+9\right)n'\sum_{r'|n'}\sum_{s'|n'}\frac{1}{(r',s')}\\
&= \left(-2^{\alpha+2}-2^{\alpha+2}+2.2^{\alpha+2}\alpha+9\right)n'\sum_{r'|n'}\sum_{s'|n'}\frac{1}{(r',s')}\\
&= \left[(\alpha-1)2^{\alpha+3}+9\right]n'\sum_{r'|n'}\sum_{s'|n'}\frac{1}{(r',s')}\\
&= \left[(\alpha-1)2^{\alpha-3}\right]g(n')
\end{aligned}$$

onde g é função aritmética multiplicativa definida pela equação (4.4).

Finalmente, substituindo na equação (4.3) o valor que acabamos de encontrar para $\sum_{r|n}\sum_{i=1}^{\frac{n}{r}} x_i^r$, obtemos

$$sd(D_{2n}) = \frac{\tau(n)^2+2\tau(n)\sigma(n)+\left[(\alpha-1)2^{\alpha+3}+9\right]g(n')}{(\tau(n)+\sigma(n))^2}$$

□

Exemplo 4.1. Se considerarmos $n=6$ no teorema anterior temos $sd(D_{12}) = \frac{101}{128}$, que é o mesmo valor calculado para $sd(S_3\times\mathbb{Z}_2)$, mas isso é não é uma surpresa, uma vez que $D_{12}\cong S_3\times\mathbb{Z}_2$.

4.2 O Grau de Comutatividade de Subgrupos de $p-$grupos finitos que possuem um subgrupo maximal cíclico

Teorema 4.3. *O grau de comutatividade de subgrupos do grupo $M(p^m)$ é igual a um.*

Demonstração.

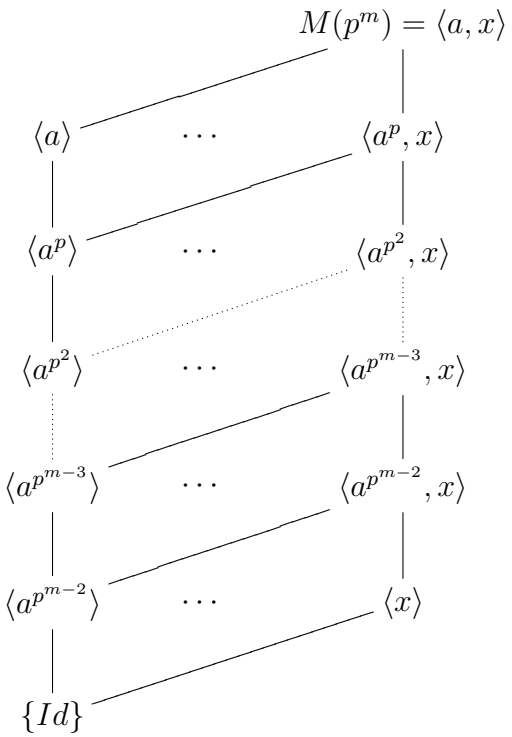

Figura 4.1: $\mathscr{L}(M(p^m))$.

Vamos mostrar que os subgrupos do grupo $M(p^m) = \langle a, x \mid a^{p^{m-1}} = x^p = 1, a^x = a^{p^{m-2}+1}\rangle$, onde $m > 3$ quando $p = 2$, são permutáveis. Temos que $M(p^m)' = \langle a^{p^{m-2}}\rangle$ pois $[a, x] = a^{p^{m-2}}$ e ainda, $\mathcal{Z}(M(p^m)) = \langle a^p\rangle$, visto que $x \notin \mathcal{Z}(M(p^m))$.

Consideramos agora um subgrupo H de $M(p^m)$ e observamos que se $|H| \geq p^2$, então H é normal em $M(p^m)$, logo pelo Teorema (2.11) é permutável.

Resta mostrar a permutabilidade quando $|H| = p$. Seja $(a^r x^s) \in M(p^m)$ um elemento de ordem p, onde $1 \leq r \leq p^{m-1}$ e $1 \leq s \leq p$. Podemos considerar $H = \langle a^r x^s\rangle$. Observamos que $(a^r x^s) = a^{kp^{m-2}} x^s$, onde $p^{m-2} \leq k \leq p^{m-1}$ e $1 \leq s \leq p$ quando p é ímpar e $(a^r x^s) = Id, a^{2^{m-2}}, a^{2^{m-2}}x$ ou x quando $p = 2$ e $m > 3$.

Assim, $(a^r x^s) \in \langle a^{p^{m-2}}, x\rangle$ e com isso, todos os subgrupos H de ordem p permutam entre si.

Como $M(p^m)$ é um grupo finito nilpotente e todos os seus subgrupos são permutáveis, podemos aplicar a Proposição (3.1) e concluir que $sd(M(p^m) = 1$. □

Teorema 4.4. *O grau de comutatividades de subgrupos $sd(Q_{2^m})$ do grupo quatérnio generalizado Q_{2^m} é dado pela seguinte igualdade:*

$$sd(Q_{2^m}) = \frac{(m-3)2^{m+1} + m2^m + (m-1)^2 + 8}{(m-1+2^{m-1})^2} \tag{4.8}$$

Demonstração. Lembramos que $sd(Q_{2^m}) = \dfrac{1}{|\mathscr{L}(Q_{2^m})|^2} \displaystyle\sum_{H \in \mathscr{L}(Q_{2^m})} |C(H)|$.

Sabemos que Q_{2^m} tem um único subgrupo minimal, que é $\mathcal{Z}(Q_{2^m}) = \left\langle x^{2^{m-2}} \right\rangle$, e ainda que $\dfrac{Q_{2^m}}{\mathcal{Z}(Q_{2^m})} \cong D_{2^{m-1}}$. Dessa forma, obtemos que

$$\begin{aligned} |\mathscr{L}(Q_{2^m})| &= 1 + |\mathscr{L}(D_{2^{m-1}})| = 1 + |\mathscr{L}(D_{2.2^{m-2}})| \\ &= 1 + \tau(2^{m-2}) + \sigma(2^{m-2}) = m - 1 + 2^{m-1}. \end{aligned} \tag{4.9}$$

Vamos calcular agora $|C(H)|$, onde H é um subgrupo arbitrário de Q_{2^m}. Observe então que para dois subgrupos não triviais H e K de Q_{2^m} temos que $HK = KH$ se, e somente se, $\dfrac{H}{\mathcal{Z}(Q_{2^m})}\dfrac{K}{\mathcal{Z}(Q_{2^m})} = \dfrac{K}{\mathcal{Z}(Q_{2^m})}\dfrac{H}{\mathcal{Z}(Q_{2^m})}$ se, e somente se, $H'K' = K'H'$, onde H', K' são subgrupos arbitrários de $D_{2^{m-1}}$, donde resulta

$$\begin{aligned} \sum_{H \in \mathscr{L}(Q_{2^m})} |C(H)| &= |C(\{Id\})| + \sum_{\substack{H \in \mathscr{L}(Q_{2^m}) \\ H \neq \{Id\}}} |C(H)| \\ &= |\mathscr{L}(Q_{2^m})| + \sum_{\frac{H}{\mathcal{Z}(Q_{2^m})} \in \mathscr{L}\left(\frac{Q_{2^m}}{\mathcal{Z}(Q_{2^m})}\right)} \left(1 + \left|C\left(\frac{H}{\mathcal{Z}(Q_{2^m})}\right)\right|\right) \\ &= |\mathscr{L}(Q_{2^m})| + \sum_{H' \in \mathscr{L}(D_{2^{m-1}})} 1 + \sum_{H' \in \mathscr{L}(D_{2^{m-1}})} |C(H')| \\ &= |\mathscr{L}(Q_{2^m})| + |\mathscr{L}(D_{2^{m-1}})| + sd(D_{2^{m-1}})|L(D_{2^{m-1}})|^2 \end{aligned}$$

mas,

$$\begin{aligned} sd(D_{2^{m-1}}) &= \frac{(m-1-2)2^{m-1+2} + (m-1)2^{m-1+1} + (m-1-1)^2 + 8}{(m-2+2^{m-1})^2} \\ &= \frac{(m-3)2^{m+1} + (m-1)2^m + (m-2)^2 + 8}{(m-2+2^{m-1})^2} \end{aligned}$$

daí, usando $sd(D_{2^{m-1}})$ e a igualdade (4.9) chegamos em

$$\begin{aligned}\sum_{H\in L(Q_{2^m})}|C(H)| &= m-1+2^{m-1}+m-2+2^{m-1}+\frac{(m-2+2^{m-1})^2}{(m-2+2^{m-1})^2}\cdot\\ &\quad .\left((m-3)2^{m+1}+(m-1)2^m+(m-2)^2+8\right)\\ &= 2m+2^m-3+(m-3)2^{m+1}+m2^m-2^m+m^2-4m+4+8\\ &= m^2-2m+1+m2^m(m-3)2^{m+1}+8\\ &= (m-3)2^{m+1}+m2^m+(m-1)^2+8.\end{aligned}$$

Finalmente, a igualdade anterior juntamente com a equação (4.9) nos dá

$$sd(Q_{2^m})=\frac{(m-3)2^{m+1}+m2^m+(m-1)^2+8}{(m-1+2^{m-1})^2}.$$

□

Temos como consequência deste teorema o corolário a seguir.

Corolário 4.4. $\lim_{m\to\infty} sd(Q_{2^m})=0.$

Teorema 4.5. *O grau de comutatividade de subgrupos $sd(S_{2^m})$ do grupo quasi-diedral S_{2^m} é dado pela seguinte igualdade*

$$sd(S_{2^m})=\frac{(m-3)2^{m+1}+m2^m+(3m-2)2^{m-1}+(m-1)^2+8}{(m-1+3.2^{m-2})^2}. \tag{4.10}$$

Demonstração. Sabemos que o subgrupos minimais de S_{2^m} são $\mathcal{Z}(S_{2^m})=\left\langle x^{2^{m-2}}\right\rangle$ e $\langle x^{2i}y\rangle, i=0,\cdots,2^{m-2}-1$. Como no caso de Q_{2^m}, temos o isomorfismo $\frac{S_{2^m}}{\mathcal{Z}(S_{2^m})}\cong D_{2^{m-1}}$.

Além disso, para qualquer subgrupo H de S_{2^m}, temos $\mathcal{Z}(S_{2^m})\subseteq H$ ou $H\in\left\{1,\langle y\rangle,\langle x^2y\rangle,\cdots,\left\langle x^{2^{m-1}-2}y\right\rangle\right\}$. Isto implica que

$$\begin{aligned}|\mathscr{L}(S_{2^m})| &= 2^{m-2}+1+|\mathscr{L}(D_{2^{m-1}})|=2^{m-2}+1+|\mathscr{L}(D_{2.2^{m-2}})|\\ &= 2^{m-2}+1+\tau(2^{m-2})+\sigma(2^{m-2})\\ &= 2^{m-2}+m-1+2^{m-1}=3.2^{m-2}+(m-1).\end{aligned} \tag{4.11}$$

Precisamos determinar agora $\sum_{H\in\mathscr{L}(S_{2^m})}|C(H)|$. Veja que

$$\sum_{H\in\mathscr{L}(S_{2^m})}|C(H)|=\sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}}|C(H)|+|C(\{Id\})|+\sum_{i=0}^{2^{m-2}-1}|C(\langle x^{2i}y\rangle)|. \tag{4.12}$$

Vamos determinar cada termo do lado direito da equação acima. Já temos que

$$|C(\{Id\})| = |\mathscr{L}(S_{2^m})|.$$

Para determinar os outros dois termos usaremos a função f definida no capítulo 2, dada pela equação (3.4).

$$\begin{aligned}
\sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} |C(H)| &= \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \left(f(H,\{Id\}) + \sum_{\substack{K\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq K}} f(H,K) + \sum_{i=0}^{2^{m-2}-1} f(H,\langle x^{2i}y\rangle)\right) \\
&= \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} 1 + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{\substack{K\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq K}} f(H,K) + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{i=0}^{2^{m-2}-1} f(H,\langle x^{2i}y\rangle) \\
&= \sum_{H'\in\mathscr{L}(D_{2^{m-1}})} + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{\substack{K\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq K}} f(H,K) + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{i=0}^{2^{m-2}-1} f(H,\langle x^{2i}y\rangle) \\
&= |\mathscr{L}(D_{2^{m-1}})| + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{\substack{K\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq K}} f(H,K) + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{i=0}^{2^{m-2}-1} f(H,\langle x^{2i}y\rangle)
\end{aligned}$$

e por fim,

$$\begin{aligned}
\sum_{i=0}^{2^{m-2}-1} |C(\langle x^{2i}y\rangle)| &= \sum_{i=0}^{2^{m-2}-1} \Big(f(\langle x^{2i}y\rangle,\{Id\}) + \sum_{j=0}^{2^{m-2}-1} f(\langle x^{2i}y\rangle,\langle x^{2j}y\rangle) + \\
&+ \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} f(H,\langle x^{2i}y\rangle)\Big) \\
&= 2^{m-2} + \sum_{i=0}^{2^{m-2}-1}\sum_{j=0}^{2^{m-2}-1} f(\langle x^{2i}y\rangle,\langle x^{2j}y\rangle) + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{i=0}^{2^{m-2}-1} f(H,\langle x^{2i}y\rangle).
\end{aligned}$$

Obtemos então que

$$\begin{aligned}
\sum_{H\in\mathscr{L}(S_{2^m})} |C(H)| &= |\mathscr{L}(D_{2^{m-1}})| + \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{\substack{K\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq K}} f(H,K) \\
&\quad +2 \sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}} \sum_{i=0}^{2^{m-2}-1} f(H,\langle x^{2i}y\rangle) + |\mathscr{L}(S_{2^m})| \\
&\quad +2^{m-2} + \sum_{i=0}^{2^{m-2}-1}\sum_{j=0}^{2^{m-2}-1} f(\langle x^{2i}y\rangle,\langle x^{2j}y\rangle). \qquad (4.13)
\end{aligned}$$

Resta calcular o lado direito da equação (4.13). Já calculamos anteriormente que $|\mathscr{L}(D_{2^{m-1}})| = m-2+2^{m-1}$ e $|\mathscr{L}(S_{2^m})| = m-1+3.2^{m-2}$. Como $\dfrac{S_{2^m}}{\mathcal{Z}(S_{2^m})} \cong D_{2^{m-1}}$,

segue que

$$\begin{aligned}\sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}}\sum_{\substack{K\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq K}} f(H,K) &= \sum_{H'\in\mathscr{L}(D_{2^{m-1}})}\sum_{K'\in\mathscr{L}(D_{2^{m-1}})} f(H',K')\\ &= \sum_{H'\in\mathscr{L}(D_{2^{m-1}})} |C(H')| = sd(D_{2^{m-1}})|\mathscr{L}(D_{2^{m-1}})|^2.\end{aligned}$$

Veja que na demonstração do teorema anterior, calculamos $sd(D_{2^{m-1}})$, portanto

$$\sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}}\sum_{\substack{K\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq K}} f(H,K) = (m-3)2^{m+1} + (m-1)2^m + (m-2)^2 + 8. \tag{4.14}$$

Para calcular $\sum_{i=0}^{2^{m-2}-1}\sum_{j=0}^{2^{m-2}-1} f(\langle x^{2i}y\rangle, \langle x^{2j}y\rangle)$, observe que $f(\langle x^{2i}y\rangle, \langle x^{2j}y\rangle) = 1$ se e somente se $\langle x^{2i}y\rangle\langle x^{2j}y\rangle = \langle x^{2j}y\rangle\langle x^{2i}y\rangle$ se e somente se $2^{m-3}\big|(i-j)$, ou melhor, se e somente se $j \equiv i \pmod{2^{m-3}}$. Dessa congruência temos que $j = i + k.2^{m-3}$, onde $k = 0 \quad \text{ou} \quad 1$ e daí,

$$\begin{aligned}\sum_{i=0}^{2^{m-2}-1}\sum_{j=0}^{2^{m-2}-1} f(\langle x^{2i}y\rangle, \langle x^{2j}y\rangle) &= \sum_{i=0}^{2^{m-2}-1}\sum_{k=0}^{1} f\left(\langle x^{2i}y\rangle, \langle x^{2(i+k.2^{m-3})}y\rangle\right)\\ &= \sum_{i=0}^{2^{m-2}-1}\left(f(\langle x^{2i}y\rangle, \langle x^{2i}y\rangle) + f\left(\langle x^{2i}y\rangle, \langle x^{2(i+2^{m-3})}y\rangle\right)\right)\\ &= \sum_{i=0}^{2^{m-2}-1}\left(f(\langle x^{2^i}y\rangle, \langle x^{2i}y\rangle) + f\left(\langle x^{2i}y\rangle, \langle (x^{2i}y)x^{2^{m-2}}\rangle\right)\right)\\ &= \sum_{i=0}^{2^{m-2}-1}(1+1) = 2^{m-1}.\end{aligned} \tag{4.15}$$

Seja $H \in \mathscr{L}(S_{2^m})$ tal que $\mathcal{Z}(S_{2^m}) \subseteq H$ e $i \in \{0, \cdots, 2^{m-2}-1\}$. Então $f(H, \langle x^{2i}y\rangle) = 1$ se, e somente se, $x^{2i}y \in N_{S_{2^m}}(H)$ se, e somente se, $x^{2i}y\mathcal{Z}(S_{2^m}) \in N_{\frac{S_{2^m}}{\mathcal{Z}(S_{2^m})}}(\frac{H}{\mathcal{Z}(S_{2^m})})$, o que mostra que

$$\begin{aligned}2 &\sum_{\substack{H\in\mathscr{L}(S_{2^m})\\ \mathcal{Z}(S_{2^m})\subseteq H}}\sum_{i=0}^{2^{m-2}-1} f(H, \langle x^{2i}y\rangle) = 2\sum_{H'\in\mathscr{L}(D_{2^{m-1}})}\sum_{i=0}^{2^{m-2}-1} f(H', \langle x^{2i}y\rangle)\\ &= 2\big|\{M \in \mathscr{L}(D_{2^{m-1}}) | M = \text{minimal e não está contido no subgrupo cíclico}\\ &\text{de ordem } 2^{m-2}, M \subseteq N_{D_{2^{m-1}}}(H') \text{ para algum } H' \in \mathscr{L}(D_{2^{m-1}})\}\big|.\end{aligned}$$

Lembramos que, para todo $\alpha = 0, \cdots, m-2$, $D_{2.2^{m-2}}$ possui um subgrupo cíclico do tipo $\mathbb{Z}_{2^\alpha}$, a saber, $H_0^\alpha = \langle x^{\frac{2^{m-2}}{2^\alpha}}\rangle = \langle x^{2^{m-2-\alpha}}\rangle$ e $\dfrac{2^{m-2}}{2^\alpha} = 2^{m-2-\alpha}$ subgrupos do tipo $D_{2.2^\alpha} =$

$D_{2^{\alpha+1}}$, dados por $H_\beta^\alpha = \langle x^{\frac{2^{m-2}}{2^\alpha}}, x^{\beta-1}y\rangle = \langle x^{2^{m-2-\alpha}}, x^{\beta-1}y\rangle$, com $\beta \in \{1, \cdots, \frac{2^{m-2}}{2^\alpha}\} = \{1, \cdots, 2^{m-2-\alpha}\}$. Seus normalizadores são: $N_{D_{2^{m-1}}}(H_0^\alpha) = D_{2^{m-1}}, N_{2^{m-1}}(H_\beta^\alpha) = H_\beta^{\alpha+1}$ para $\alpha < m-2$ e $N_{D_{2^{m-1}}}(H_1^{m-2}) = D_{2^{m-1}}$. Assim,

$$2 \sum_{\substack{H \in \mathscr{L}(S_{2^m}) \\ \mathcal{Z}(S_{2^m}) \subseteq H}} \sum_{i=0}^{2^{m-2}-1} f(H, \langle x^{2i}y\rangle) = (3m-4)2^{m-1}. \tag{4.16}$$

Obtemos então que

$$\sum_{H \in \mathscr{L}(S_{2^m})} |C(H)| = (m-3)2^{m+1} + m2^m + (3m-2)2^{m-1} + (m-1)^2 + 8.$$

Finalmente, usando o valor que acabamos de calcular e a equação (4.11) encotramos a equação desejada. □

Corolário 4.5. $\lim_{m\to\infty} sd(S_{2^m}) = 0$

Finalizamos esta seção mencionando que o grau de comutatividade de subgrupos de um grupo finito nilpotente qualquer, cujos subgrupos de Sylow pertencem a classe $\mathcal{G}$, pode ser explicitamente calculado, tendo em vista o corolário (3.1).

4.3 Alguns Problemas

Apresentaremos nesta seção três problemas em aberto, sobre o grau de comutatividade de subgrupos de um grupo finito, deixados por Tărnăuceanu [18].

Problema 4.1. Quais são as conexões entre o grau de comutatividade de subgrupos de um grupo finito e o grau de comutatividade de subgrupos de seus subgrupos (quocientes?)

Problema 4.2. Para um $\alpha \in (0,1)$ fixo, descreva a estrutura de grupos finitos G satisfazendo $sd(G) = (\leq, \geq)\alpha$. O que pode ser dito sobre dois grupos finitos quaisquer tendo o mesmo grau de comutatividade de subgrupos?

Problema 4.3. Como mostram os Corolários (4.3), (4.4) e (4.5), temos $\lim_{m\to\infty} sd(D_{2^m}) = 0 = \lim_{m\to\infty} sd(Q_{2^m}) = 0 = \lim_{m\to\infty} sd(S_{2^m}) = 0$. Isto é verdade para outra classe "natural"de grupos finitos?

Após a elaboração dessa dissertação tomamos conhecimento do conteúdo do artigo *Subgroup s-commutativity degree of finite groups* em que os autores, Otera e Russo [10] apresentaram uma resposta aos problemas (4.1) e (4.3) .

Referências Bibliográficas

[1] A. Castelaz, Commutativity degree of finite groups. Winston-Salem, North Carolina, 2010.

[2] A. Erfanian, P. Lescot, R. Rezaei, On the relative commutativity degree of a subgroup of a finite group. *Communications in Algebra* 35, 2007, 4183-4197.

[3] D. Gorenstein, Finite Groups, 2 ed., Chelsea Publishing Company, New York, 1980.

[4] W.H. Gustafson, What is the probability that two group elements commute?. *Amer. Math. Monthly* 80, 1973, 1031-1034.

[5] M. Hall Jr., *The theory of groups*, Macmillan, New York, 1959.

[6] P. Lescot, Isoclinism classes and commutativity degrees of finite groups. *J. Algebra* 177, 1995, 847-869.

[7] P. Lescot, Central extensions and commutativity degree. *Communications in Algebra* 29, 2001, 4451-4460.

[8] C.P. Milies, Grupos Nilpotentes: Uma introdução. *Matemática Universitária*, v.34, 55-100, 2003.

[9] O. Ore, Contribuitions to Theory of Groups of Finite Order. *Duke Math.* Jornal 5, 1939, 431-460.

[10] D.E. Otera and F.G Russo, *Subgroup s-commutativity degree of finite groups*. e-print, 2010, arXiv: 1009. 2171v3.

[11] D.J.S. Robinson, *A course in the theory of groups*, 2 ed., Graduate Texts in Mathematics, Springer-Velag, New York, 1996.

[12] J.J. Rotman, An Introduction to the Theory of Groups, 4 ed., Graduate Texts in Mathematics, Springer-Velag, New York, 1995.

[13] D.J. Rusin, What is the probability that two elements of a finite group commute? *Pacific J. Math.* 82, 1979, 237-247.

[14] R. Schmidt, *Subgroup Lattices of Groups*. Exp. Math, v. 14, de Gruyter, Berlin, 1994.

[15] M. Suzuki, *Group Theory I*. Springer-Verlag, Berlin, 1982.

[16] M. Suzuki, *Group Theory II*. Springer-Verlag, Berlin, 1986 .

[17] M. Suzuki, *Structure of a Group and the Structure of its Lattice of Subgroups*. Springer-Verlag, Berlin Heidelberg New York, 1956.

[18] M. Tărnăuceanu, Subgroup commutativity degrees of finite groups. *Journal of Algebra* 321, 2009, 2508-2520.