UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

AMANDA CAROLINA PREVIATTI

SUBGRUPOS DE SYLOW, SUBGRUPOS DE HALL E ALGUNS RESULTADOS

TRABALHO DE CONCLUSÃO DE CURSO

TOLEDO
2016

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

AMANDA CAROLINA PREVIATTI

SUBGRUPOS DE SYLOW, SUBGRUPOS DE HALL E ALGUNS RESULTADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná, Câmpus Toledo, como requisito parcial à obtenção do título de Licenciada em Matemática.

Orientador: Professor Dr. Wilian Francisco de Araujo

TOLEDO
2016

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

TERMO DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado "Subgrupos de Sylow, subgrupos de Hall e alguns resultados "foi considerado **APROVADO** de acordo com a ata nº __ de __/__/____

Fizeram parte da banca examinadora os professores:

Professor Dr. Wilian Francisco de Araujo

Professor Dr. Rodrigo M. Dias Andrade

Professora Ma. Larisssa Hagedorn Vieira

TOLEDO

2016

RESUMO

Neste trabalho é apresentado um estudo sobre subgrupos de Sylow e subgrupos de Hall, fazendo algumas comparações entre eles e, por fim, mostrando alguns resultados dos mesmos. Para isso, serão apresentados definições e teoremas importantes para o decorrer da pesquisa. São colocados conteúdos importantes para o desenvolvimento da pesquisa proposta, os quais estão relacionadas com grupos finitos e brevemente os teoremas do homomorfismos, para então estudar subgrupos de Sylow. Feito isso, serão apresentados os grupos solúveis e nilpotentes para então fazer a análise de subgrupos de Hall. Finalmente, será mostrado algumas comparações entre os dois subgrupos em questão e alguns resultados importantes e de maior interesse.

Palavras-chave: Grupo, Subgrupos de Sylow, Subgrupos de Hall.

LISTA DE SÍMBOLOS

$(G : H)$ Índice de H em G.

(a,b) Máximo divisor comum entre a e b.

G Grupo G.

$H \lhd G$ H é subgrupo normal de G.

Hx Classe lateral à direita de H.

$Id(g)$ Função identidade.

$Im(f)$ Imagem da função f.

$N_G(H)$ Normalizador de H em G.

$Nuc(f)$ Núcleo da função f.

$Z(G)$ Centro de G.

$\frac{G}{H}$ Grupo quociente de G por um subgrupo normal H.

$\emptyset$ Conjunto vazio.

$\mathbb{Z}$ Conjunto dos números inteiros.

xH Classe lateral à esquerda de H.

$|G|$ Ordem do grupo G.

SUMÁRIO

INTRODUÇÃO

Durante a graduação em Matemática, no que refere-se a Álgebra, foi estudada a teoria básica de Grupos. Com isso, surgiu o interesse em aprofundar o estudo nesta área. Em particular, alguns subgrupos foram os objetos de estudo principais para este trabalho. Com o aprofundar das pesquisas, surgiu então o interesse em estudar os subgrupos de Sylow e subgrupos de Hall.

Os subgrupos de Sylow têm a maior potência de p que divide a ordem de G, sendo p um primo. Esses subgrupos sempre existem. Já os subgrupos de Hall nem sempre existem, no entanto, podemos mencionar algumas condições sobre as quais podemos garantir que eles existem.

No primeiro capítulo deste trabalho, apresentamos alguns resultados da Teoria de Grupos, os quais são estudados ainda na graduação. Além disso, definimos os homomorfismos relevantes para o trabalho e detalhamos os Grupos de Permutações.

O segundo capítulo é reservado para fazer a apresentação dos Teoremas de Sylow, assim como os p-subgrupos de Sylow e alguns exemplos.

Finalmente, no terceiro capítulo são apresentados os subgrupos de Hall, as condições que garantem a existência desses subgrupos, alguns resultados e comparações com os subgrupos de Sylow.

1 CONHECIMENTOS PRÉVIOS

Este capítulo será uma breve revisão sobre Teoria de Grupos. Veremos alguns conceitos básicos e definições importantes para o decorrer do trabalho. Será uma revisão resumida, pois a maior parte deste conteúdo é estudada durante a graduação em Matemática. Demostrações encontram-se nos livros Garcia e Lequain (2013) e Lang (2008).

1.1 Grupos

Para iniciar, apresentaremos o que é um grupo e outras definições necessárias.

Definição 1.1 *Um conjunto não vazio G, com uma operação binária*

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$

é um grupo se as seguintes condições forem satisfeitas:

i. A operação é associativa, isto é,

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

ii. Existe um elemento neutro, isto é,

$$\exists \ e \in G \ tal \ que \ e \cdot a = a \cdot e = a, \ \forall \ a \in G.$$

iii. Todo elemento possui um elemento inverso, isto é,

$$\forall \ a \in G, \exists \ b \in G \ tal \ que \ a \cdot b = b \cdot a = e.$$

Dizemos que o grupo G é abeliano(ou comutativo) quando satisfaz a seguinte propriedade adicional:

iv. a operação é comutativa, isto é,

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

Usamos $(G, *)$ para indicar um grupo, onde G é um conjunto e $*$ uma operação binária. Porém, quando não houver ambiguidade, usaremos apenas G. Chamaremos o grupo $(G, \cdot)$ de *grupo multiplicativo* e $(G, +)$ de *grupo aditivo*, quando nos referirmos as operações de multiplicação e adição usuais, respectivamente.

Um grupo $(G, *)$ é dito finito quando o conjunto G é finito. Neste caso, o número de elementos de G é chamado **ordem** do grupo e denotado por $o(G)$ ou $|G|$.

Por exemplo, $(\mathbb{Z}, +)$ é um grupo(aditivo) abeliano infinito, uma vez que $(\mathbb{Z}, +)$ é grupo, $\mathbb{Z}$ é um conjunto infinito e a operação $+$ é comutativa.

Definição 1.2 *Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um* ***subgrupo*** *de G se H for ele próprio grupo para a operação de G.*

Proposição 1.3 *Seja H um subconjunto não-vazio do grupo G. Então H é um subgrupo de G se e somente se as duas condições seguintes são satisfeitas:*

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

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

A demonstração desta proposição está disponível em Garcia e Lequain (2013).

Observação 1.4 *Dois subgrupos triviais de um grupo G qualquer, são $\{e\}$ e o próprio G.*

O conjunto $H = \mathbb{Z} \cdot m = \{rm : r \in \mathbb{Z}\},\ m \in \mathbb{Z}$, por exemplo, é um subgrupo de $(\mathbb{Z}, +)$.

Proposição 1.5 *Seja G um grupo e H um subgrupo de G. A relação $\sim_E$ (à esquerda) sobre G definida por*

$$x \sim_E y, \Leftrightarrow \exists\ h \in H\ tal\ que\ y = xh$$

é uma relação de equivalência.

Definição 1.6 *Seja G um grupo e H um subgrupo de G. Chama-se* ***classe lateral à esquerda*** *de H em G que contém x e denota-se por xH, o seguinte conjunto*

$$xH = \{y \in G \mid y\ \sim_E\ x\} = \{xh \mid h \in H\}.$$

Da mesma forma podemos definir classe lateral à direita.

Proposição 1.7 *Seja G um grupo e H um subgrupo de G. A relação de equivalência $\sim_D$ (a direita) sobre G é definida por*

$$x \sim_D y, \Leftrightarrow \exists\ h \in H\ tal\ que\ y = hx.$$

Definição 1.8 *Seja G um grupo e H um subgrupo de G. Chama-se* ***classe lateral à direita*** *de H em G que contém x e denota-se por Hx, o seguinte conjunto*

$$\{y \in G \mid y \ \sim_D \ x\} = \{hx \mid h \in H\}.$$

Definição 1.9 *A cardinalidade do conjunto das classes laterais à esquerda é chamada de* ***índice*** *de H em G, o qual será denotado por $(G : H)$.*

Proposição 1.10 *Todas as classes laterais de H em G têm a mesma cardinalidade, igual à cardinalidade de H.*

Definição 1.11 *Seja G um grupo e H um subgrupo de G. Dizemos que H é um* ***subgrupo normal*** *se*

$$Hx = xH, \ \forall x \in G,$$

e denotamos por $H \lhd G$.

Vejamos alguns exemplos de subgrupos normais:

1) $\{e\}$ e G são subgrupos normais de G;

2) Se $(G : H) = 2$, então $H \lhd G$;

3) Se G é um grupo abeliano, então todo subgrupo H de G é normal em G. No entanto, a recíproca não é válida, como é o caso do grupo Q_3, que não é abeliano, no entanto todos seus subgrupos são normais em Q_3.

Teorema 1.12 *Sejam G um grupo e H um subgrupo normal de G. Então o conjunto das classes laterais , com a operação induzida de G, é um grupo.*

Teorema 1.13 (Teorema de Langrange) *Sejam G um grupo finito e H um subgrupo de G. Então*

$$|G| = |H|(G : H).$$

Em particular, a ordem e o índice de H dividem a ordem de G.

Corolário 1.14 *Seja G um grupo finito e $\alpha \in G$. Então a ordem de α divide a ordem de G.*

Proposição 1.15 *Seja G um grupo e $K < H < G$. Então*

$$(G : K) = (G : H)(H : K).$$

Proposição 1.16 *Seja H um subgrupo normal de G. Então, para quaisquer $a, b \in G$, vale a igualdade*

$$(aH)(bH) = (ab)H.$$

A demonstração desta proposição é feita por dupla inclusão e enconta-se no livro Domingues e Iezzi (2003).

Corolário 1.17 *Sejam G um grupo e H e K dois subgrupos de G. Se H ou K for subgrupo normal em G, então HK é um subgrupo de G.*

Corolário 1.18 *Sejam G um grupo e H e K dois subgrupos normais de G. Então HK é um subgrupo normal de G.*

Proposição 1.19 *Sejam G um grupo finito e H e K dois subgrupos de G. Então,*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

A demonstração das proposição anterior encontra-se no livro Garcia e Lequain (2013).

Definição 1.20 *Sejam G um grupo e H um subgrupo de G. Dois elementos x, y de G são ditos **conjugados** em G se*

$$\exists g \in G \text{ tal que } y = gxg^{-1}.$$

Definição 1.21 *Seja G um grupo e H um subconjunto de G. Se, $C = ghg^{-1}$, com $h \in H$, também forma um subconjunto de G, então dizemos que C é um **subgrupo conjugado** de G.*

A partir disso, podemos verificar que a relação de conjugação é uma relação de equivalência em G.

Definição 1.22 *Sejam G um grupo e H um subgrupo de G. O conjunto $\{gHg^{-1} \mid g \in G\}$ é chamado **normalizador** de H em G e é denotado por $N_G(H)$.*

Definição 1.23 *Seja G um grupo e H um subgrupo normal de G. O grupo de suas classes laterais, com a operação induzida de G, é chamado de **grupo quociente** de G por H, denotado por G/H ou por $\frac{G}{H}$.*

1.2 Homomorfismo

Os homomorfismos serão importantes para o estudo sobre os subgrupos de Sylow. Para isso apresentaremos apenas definição de homomorfismo e o Teorema Fundamental do Homomorfismo.

Definição 1.24 *Sejam $(G, *)$ e $(G', \cdot)$ dois grupos. Uma função $f : G \longrightarrow G'$ é um homomorfismo se ela é compatível com as estruturas dos grupos, isto é, se*

$$f(a * b) = f(a) \cdot f(b), \ \forall \ a, b \in G.$$

A função $Id : (G, \cdot) \longrightarrow (G, \cdot)$, $Id(g) = g$, é um homomorfimo chamado *identidade*. Outro exemplo de homomorfismo é a função definida por

$$f : (G, +) \longrightarrow (G, +)$$

$$x \longmapsto -x.$$

uma vez que

$$f(x + y) = -(x + y) = -x - y = (-x) + (-y) = f(x) + f(y), \ \forall \ x, y \in G.$$

Teorema 1.25 (Fundamental do Homomorfismo) *Sejam G e G' grupos com identidade e e e', respectivamente, e $f : G \longrightarrow G'$ um homomorfismo. Então*

i. $Im(f) = f(G) = \{f(g) : g \in G'\}$.

ii. $Nuc(f) = \{g \in G : f(g) = e'\}$ *é um subgrupo normal de G, chamado* ***núcleo*** *do homomorfismo, e mais*

$$f \text{ injetiva se e somente se } Nuc(f) = \{e\}.$$

iii. $G/Nuc(f) \cong Imf$.

1.3 Grupos de Permutações

Os Grupos de Permutações serão utilizados para exemplificar os subgrupos em estudo. Para isso, apresentamos brevemente algumas das definições básicas para apresentar estes grupos.

S_n é o grupo das permutações de n elementos $\{1, \cdots, n\} = J_n$, chamado **grupo simétrico**. Vejamos, como exemplo, S_3:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Uma **transposição** τ é uma permutação que troca as posições de dois números e que deixa os outros dois fixos, isto é,

$$\exists \ i, j \in J_n, \ i \neq j, \ tais \ que \ \tau(i) = j, \ \tau(j) = i \ e \ \tau(k) = k \ se \ k \neq i \ e \ k \neq j.$$

Como τ é uma transposição, então $\tau^{-1} = \tau$ e $\tau^2 = Id$. Vejamos então que as transposições geram S_n.

Teorema 1.26 *Toda permutação de J_n pode ser expressa como um produto de transposições.*

DEMONSTRAÇÃO: Vamos provar, por indução matemática sobre n.

Para $n = 1$ não há o que mostrar, uma vez que $J_1 = \{1\}$.

Suponhamos então que $n > 1$ e que é válido para $n - 1$. Provemos então, que é válido para n.

Sejam σ uma permutação de J_n tal que $\sigma(n) = k$ e τ uma transposição de J_n tal que $\tau(k) = n$ e $\tau(n) = k$. Então, $\tau\sigma$ é uma permutação que deixa n fixo, isto é,

$$\tau\sigma(n) = \tau(k) = n.$$

Com isso, podemos dizer que $\tau\sigma$ é uma permutação de J_{n-1}. Por indução, existem as transposições $\tau_1, \cdots, \tau_s \in J_{n-1}$, que deixam n fixo, de modo que

$$\tau\sigma = \tau_1 \cdots \tau_s.$$

Então, podemos escrever

$$\sigma = \tau^{-1}\tau_1 \cdots \tau_s.$$

□

Por exemplo, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ é uma permutação de J_3 tal que $\sigma(1) = 2$, $\sigma(2) = 1$ e $\sigma(3) = 3$, ou seja, $\sigma = (1\ 2)$.

O grupo A_n é o grupo **Alterno** de J_n, composto dos elementos de S_n que são permutações pares, ou seja, são produtos de número par de transposições.

2 SUBGRUPOS DE SYLOW

Para iniciar o estudo sobre os subgrupos de Sylow, precisamos do Teorema de Cauchy que será necessário para os próximos teoremas.

Teorema 2.1 (Cauchy) *Seja G um grupo abeliano finito e p um número primo que divide $|G|$. Então existe $x \in G$ de ordem p.*

DEMONSTRAÇÃO: Faremos a demonstração por indução sobre a ordem de G.

Se $|G| = 1$, a demonstração é imediata.

Suponhamos agora, por hipótese de indução, que o teorema é válido para todos os grupos abelianos de ordem menor que $|G|$. Mostremos então, que é válido também para $|G|$.

Se $p = |G|$, não é necessário ursar a hipótese de indução, pois G é cíclico e qualquer gerdor de G tem ordem p. Se $p \neq |G|$, suponhamos que existe um subgrupo H tal que $1 < |H| < |G|$. Seja $y \in G$, tal que $y \neq e$. Se $\langle y \rangle \neq G$, então $H = \langle y \rangle$ e a afirmação é válida. Se $\langle y \rangle = G$, então $y^p \neq e$ e $H = \langle y^p \rangle$, novamente a afirmação é válida, pois

$$|H| = o(y^p) = |G|/p < |G|.$$

Agora, se p divide $|H|$ então, por hipótese de indução, $\exists\ x \in H \subseteq G$, tal que $o(x) = p$ e este caso está provado.

Se $p \nmid |H|$ então, como $|G| = |H| \left|\frac{G}{H}\right|$, vemos que p divide $\left|\frac{G}{H}\right|$ e que $\left|\frac{G}{H}\right| < |G|$. Logo, por hipótse de indução, $\exists\ \bar{z} \in \frac{G}{H}$, tal que $o(\bar{z})$. Consideremos o homomorfismo canônico $\varphi : G \to \frac{G}{H}$, onde $\varphi(z) = \bar{z},\ z \in G$. Seja r a ordem deste elemento z. Temos que $z^r = e$, logo $\varphi(z^r) = \varphi(e)$, ou seja, $\bar{z}^r = \bar{e}$ e, portanto, r é múltiplo da ordem de $\bar{z}$, isto é, r é um múltiplo de p, digamos $r = kp$ com $k \geq 1$. Então, z^k é um elemento de G de ordem p.

□

O Teorema de Cauchy é um caso particular do 1º Teorema de Sylow que apresentaremos a seguir.

Teorema 2.2 (1º Teorema de Sylow) *Sejam p um número primo e G um grupo de ordem $p^m b$ com $(p, b) = 1$. Então, para cada n, $0 \leq n \leq m$, existe um subgrupo H de G tal que $|H| = p^n$.*

DEMONSTRAÇÃO: Faremos esta demonstração por indução sobre a ordem de G.

Se $|G| = 1$, a demosntração é imediata.

Se $|G| > 1$, suponhamos por hipótese de indução que o teorema vale para todos os grupos de ordem menor que $|G|$. Mostremos então, que o teorema também é válido para o grupo G.

Seja n um inteiro positivo tal que p^n divide a ordem de G.

1º Caso: Se existe um subgrupo próprio H de G tal que p^n divide a ordem de H. Neste caso, por hipótese de indução, temos que H possui um subgrupo de ordem p^n e, por consequância, G também.

2º Caso: Se não existe um subgrupo p´roprio H de G tal que p^n divide sua ordem. Neste caso, considere a equação das classes de conjugação:

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} (G : Z(x_\alpha)).$$

Para $x_\alpha \notin Z(G)$, temos $Z(x_\alpha) \subsetneq G$, logo, por hipótese, p^n não divide $|Z(x_\alpha)|$, e portanto, p divide $(G : Z(x_\alpha))$. Como p divide $|G|$, obtemos então que p divide $|Z(G)|$. Como $Z(G)$ é um grupo abeliano, pelo Teorema de Cauchy sabemos que existe um elemento $y \in Z(G)$ de ordem p. Como $y \in Z(G)$, então $\langle y \rangle \rhd G$, de modo que podemos considerar o grupo quociente $\dfrac{G}{\langle y \rangle}$. Sabemos ainda que $\left|\dfrac{G}{\langle y \rangle}\right| < |G|$ e p^{n-1} divide $\left|\dfrac{G}{\langle y \rangle}\right|$. Logo, por hipótese de indução, o grupo $\dfrac{G}{\langle y \rangle}$ possui um subgrupo K' de ordem p^{n-1}. Considere o homomorfismo canônico $\varphi : G \to \dfrac{G}{\langle y \rangle}$ e tome $K = \varphi^{-1}(K')$. Então K é um subgrupo de G e

$$|K| = |Nuc(\varphi)||K'| = |\langle y \rangle||K'| = p^n.$$

□

Apresentaremos agora a definição de p-subgrupo de Sylow.

Definição 2.3 *Sejam G um grupo finito, p um número primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que têm ordem p^m são chamados de* **p-*subgrupos de Sylow de* G**.

Definição 2.4 *Seja p um primo. Um grupo G, não necessariamente finito, no qual todo elemento tem sua ordem igual a uma potência de p é chamado um* **p-*grupo.***

Observemos que se p é um número primo que não divide a ordem de G, então o elemento neutro e é o único p-subgrupo de Sylow de G. Além disso, os p-grupos finitos dão exatamente os grupos cuja ordem é uma potência do primo p.

Nestas condições, o teorema anterior garante que G tem pelo menos um p-subgrupo de Sylow.

O grupo D_4 é um exemplo de 2-grupo de ordem $8 = 2^3$. Já o grupo $\left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}, \oplus_{p^n}\right)$ é um p-grupo de ordem p^n.

Mostraremos a seguir que todos os p-subgrupos de Sylow de G são os p-subgrupos maximais de G e como são obtidos.

Para a demosntração do $2^{\underline{o}}$ Teorema de Sylow, precisamos do seguinte lema:

Lema 2.5 *Sejam H um p-subgrupo de G e S um p-subgrupo de Sylow de G. Então existe $x \in G$ tal que $H \leq xPx^{-1}$.*

DEMONSTRAÇÃO: Seja P o conjunto das classes laterais de S em G. H opera em P por translação esquerda.

Temos que $|P_0| \equiv |P| = (G : S) \pmod{p}$.

Como S é um p-subgrupo de Sylow, $(G : S) = k$, pelo que $p \nmid (G : P)$. Logo, $|P_0| \equiv 0 \pmod{p}$ e $P_0 \neq \emptyset$. Consideremos então $xS \in P_0$, então temos

$$xS \in P_0$$

$$hxS = xS, \ \forall h \in H$$

$$x^{-1}hxS = S, \ \forall h \in H$$

$$x^{-1}Hx \leq S$$

$$H \leq xSx^{-1}$$

□

Teorema 2.6 ($2^{\underline{o}}$ Teorema de Sylow) *Sejam G um grupo finito, tal que $|G| = p^n k$, com $p \nmid k$. Todos os p-subgrupos de Sylow de G são conjugados entre si.*

DEMONSTRAÇÃO: Do lema anterior temos que, se H é um p-subgrupo de Sylow de G, então $|H| = |S| = p^n$.

□

Essas demonstrações enconstram-se no livro Monteiro e Matos (2001).
Um outro resultado que temos é que se S é um p-subgrupo de Sylow de G, então os p-subgrupos de Sylow de G são os conjugados de P e só esses. Vejamos agora o $3^{\underline{o}}$ Teorema de Sylow.

Teorema 2.7 ($3^{\underline{o}}$ Teorema de Sylow) *Sejam p um número primo e G um grupo finito de ordem $p^m b$, com $(p, b) = 1$. Seja n_p o número de p-subgrupos de Sylow de G. Então:*

i. n_p *divide* b.

ii. $n_p \equiv 1 \pmod{p}$.

DEMONSTRAÇÃO: Seja S um p-subgrupo de Sylow de G. Temos que $(G : N_G(S))$ divide $(G : S) = b$.

Agora, consideremos P um p-subgrupo qualquer de G, $S_i = g_i S g_i^{-1}$ e

$$(G : N_G(S)) = \sum_{i=1}^{k} (P : P \cap S).$$

Tomando $P = S$ na expressão acima, temos que

$$(G : N_G(S)) = \sum_{i=1}^{k} (S : S \cap S_i),$$

onde $S_1, \cdots, S_k$ são representantes das distintas órbitas $\mathfrak{D}_1, \cdots, \mathfrak{D}_k$ da representação

$$\mathcal{I} : S \longrightarrow \mathcal{P}(C),$$

onde C é o conjunto dos p-subgrupos de Sylow de G. Então, podemos tomar $S_1 = S$. Com isso, obtemos

$$(G : N_G(S)) = (S : S \cap S) + \sum_{i=2}^{k} (S : S \cap S_i) \equiv 1 \pmod{p}$$

Pelo 2º Teorema sw Sylow, sabemos que $n_p = (G : N_G(S))$. Portanto, temos o resultado esperado sobre n_p.

□

Por exemplo, consideremos um grupo G tal que $|G| = 24 = 2^3 \cdot 3$. Sabemos que existe um subgrupo de de G com ordem 8, que é a maior potência de 2 que divide a ordem de G o qual é um 2-subgrupo de Sylow de G. Da mesma forma, existe um 3-subgrupo de Sylow de ordem 3.

Podemos concluir que, dados um grupo finito G e p um primo divisor da ordem de G, um p-subgrupo de Sylow de G é um subgrupo de G com ordem sendo a maior potência de p que divide a ordem de G.

3 SUBGRUPOS DE HALL

Iniciamos o estudo sobre o subgrupos de Hall vendo as definições de grupos solúvel e nilpotentes para então estudarmos os subgrupos de Hall e o Teorema de P. Hall. As demonstrações aqui apresentadas foram baseadas em Araujo (2009).

Definição 3.1 *Um grupo G é dito* ***solúvel*** *se G possuir um série subnormal*

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1,$$

onde cada grupo fator $\frac{G_i}{G_{i+1}}$ é abeliano.

Uma cadeia de subgrupos de G com esta característica é chamada de **série subnormal** abeliana de G e os seus quocientes respectivos são chamados de **fatores da série**.

Definição 3.2 *Um grupo G é* ***nilpotente*** *se possui uma série normal*

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1,$$

onde cada grupo fator $\frac{G_i}{G_{(i+1)}}$ está contido em $\mathbb{Z}\left(\frac{G_i}{G_{i+1}}\right)$, para $i = 1, 2, \cdots, n-1$.

Definição 3.3 *Seja π um conjunto não vazio de números primos. Um π-número é um inteiro n tal que todos seus fatores primos pertencem a π.*

O complemento de π é π', portanto, π'-número é um inteiro m tal que nenhum de seus fatores primos pertencem a π.

Definição 3.4 *Seja π um conjunto de primos. Um grupo G é um π-**grupo** se a ordem de cada um de seus elementos é um π-número.*

Definição 3.5 *Se G é um grupo finito, então um π-subgrupo H de G tal que $[G : H]$ é um π'-número é chamado de π-**subgrupo de Hall** de G.*

Os π-subgrupos de Hall nem sempre existem. Por exemplo, consideremos o grupo $G = A_5$ e $\pi = \{3, 5\}$ o conjunto dos números primos. Como $|G| = |A_5| = 60 = = 2^2 \cdot 3 \cdot 5$, se existisse um π-subgrupo de Hall nessas condições, ele teria índice 4 e ordem 15, mas esse subgrupo não existe. Queremos então, estudar as condições necessárias para esses subgrupos existirem. Além disso, quando existem, queremos saber se são conjugados entre si.

O teorema a seguir garante que, em grupos solúveis finitos, os π-subgrupos de Hall existem sempre e são conjugados.

Teorema 3.6 (P. Hall) *Se G é um grupo finito solúvel de ordem ab, onde $(a,b)=1$, então G contém um subgrupo de ordem a. Além disso, quaisquer dois subgrupos de ordem a são conjugados ente si.*

DEMONSTRAÇÃO: Faremos a demonstração por indução sobre a ordem de G.

- Se $|G| = 2 = 2\cdot 1$ o resultado é imediato, pois e os únicos subgrupos de G são $\{1\}$ e o próprio G, que têm ordens 1 e 2, respectivamente Se considerarmos dois subgrupos de mesma ordem, eles serão conjugados entre si, pois um subgrupo é conjugado dele mesmo.

- Vejamos agora se $|G| > 2$.

  1° caso: Seja $H \lhd G$ com $|H| = a'b'$, onde $a'|a$, $b'|b$ e $b' < b$.

  Existência: Se G é solúvel, $\left|\dfrac{G}{H}\right| = \dfrac{a}{a'}\dfrac{b}{b'} < ab$.

  Por hipótese de indução, $\dfrac{A}{H} \lhd \dfrac{G}{H}$ e $\dfrac{A}{H} = \dfrac{a}{a'}$. Então,

  $$\left|\frac{A}{H}\right| = \frac{a}{a'} \;\Rightarrow\; \frac{|A|}{|H|} = \frac{a}{a'} \Rightarrow\; |A| = \frac{a}{a'}|H| \;\Rightarrow\; |A| = \frac{a}{a'}a'b' \;\Rightarrow\; |A| = a.b' < ab.$$

  Como A é solúvel, A possui um subgrupo de ordem a que também é, um subgrupo de G.

  Conjugação: Sejam $A \leq G$, $B \leq G$ tais que $|A| = |B| = a$ e $AH \lhd G$.

  Pelo Teorema de Lagrange, $|AH|$ divide $|G|$, logo $|AH| = \alpha\beta$, onde $\alpha|a$ e $\beta|b$. Como $(a,b) = 1$ e $A \leq AH$, segue que

  $$|A| \,|\, |AH| \;\Rightarrow\; a|\alpha\beta \;\Rightarrow\; a|\alpha.$$

  Mas como $\alpha|a$ e $a|\alpha$, então $a = \alpha$.
  Como $H \leq AH$, temos que

  $$|H| \,|\, |AH| \;\Rightarrow\; a'b'|\alpha\beta \;\Rightarrow\; a'b'|a\beta \;\Rightarrow\; a\beta = ka'b',\ \textit{para algum}\ k \in \mathbb{Z},$$

  e como $a'|a$, ou seja, $a = a'q,\ q \in \mathbb{Z}$, segue que

  $$a'q\beta = ka'b' \;\Rightarrow\; q\beta = kb',\ q,k \in \mathbb{Z}.$$

  Então b' divide $q\beta$, mas como b' não divide q, pois $(a'q,b) = 1$, então $b'|\beta$.
  Agora, a fórmula do produto nos diz que $|AH|$ divide $|A|\cdot|H|$, ou seja,

  $$\alpha\beta|aa'b' \;\Rightarrow\; a\beta|aa'b' \;\Rightarrow\; \beta|a'b'$$

e como β não divide a', segue que $\beta|b'$. Logo, se $\beta|b'$ e $b'|\beta$, então $b' = \beta$.
Concluímos então que $|AH| = \alpha\beta = ab'$.
Utilizando novamente o Teorema de Lagrange, temos que $|BH|$ divide $|G|$.
Então, $|BH| = xy$, onde $x|a$ e $y|b$. Como $(a, b) = 1$ e $B \leq BH$, temos que

$$|B| \mid |BH| \;\Rightarrow\; a|xy \;\Rightarrow\; a|x.$$

Mas como $x|a$ e $a|x$, então $a = x$.
Como $H \leq BH$, temos que

$$|H| \mid |BH| \;\Rightarrow\; a'b'|xy \;\Rightarrow a'b'|ay \;\Rightarrow\; ay = sa'b',\ \textit{para algum}\ s \in \mathbb{Z}.$$

Como $a = a'z,\ z \in \mathbb{Z}$,

$$a'zy = sa'b' \;\Rightarrow\; zy = sb',\ z, s \in \mathbb{Z}.$$

Então b' divide zy, mas como b' não divide z, pois $(a'z, b) = 1$, então $b'|y$.
Agora, a fórmula do produto nos diz que $|BH|$ divide $|B| \cdot |H|$, ou seja,

$$xy|aa'b' \;\Rightarrow\; ay|aa'b' \;\Rightarrow\; y|a'b',$$

e como y não divide a', segue que $y|b'$. Logo, se $y|b'$ e $b'|y$, então $b' = y$.
Concluímos então que $|BH| = xy = ab'$.
Portanto, $\left|\dfrac{AH}{H}\right| = \dfrac{|AH|}{|H|} = \dfrac{ab'}{a'b'} = \dfrac{a}{a'}$ e $\left|\dfrac{BH}{H}\right| = \dfrac{|BH|}{|H|} = \dfrac{ab'}{a'b'} = \dfrac{a}{a'}$.
Como, por hipótese de indução, $\dfrac{G}{H} \leq G$, então $\dfrac{AH}{H}$ e $\dfrac{BH}{H}$, são conjugados, isto é, $\left(\dfrac{AH}{H}\right)^{xH} = \dfrac{BH}{H}$, *para algum* $xH \in \dfrac{G}{H}$. Vejamos então, que $x^{-1}Ax$ e B são subgrupos de BH, ambos de orde a. De fato, B é um subgrupo de BH. Falta provar que $x^{-1}Ax \leq BH$.
Seja $aH \in \dfrac{AH}{H}$ e $b_1H \in \dfrac{BH}{H}$. Temos que,

$$x^{-1}HaHxH = b_1H,$$

$$x^{-1}axH = b_1H.$$

Segue que, ${b_1}^{-1}(x^{-1}ax) \in H$, ou seja,

$${b_1}^{-1}(x^{-1}ax) = h,\ h \in H,$$

$$x^{-1}ax = b_1h,\ h \in H.$$

Se $aH = a_1h_1,\ h_1 \in H,\ a_1 \in A$, temos que

$$x^{-1}a_1h_1x = b_1h,\ h, h_1 \in H\ e\ a_1 \in A,$$

$$x^{-1}a_1xh_1 = b_1h,\ h, h_1 \in H\ e\ a_1 \in A,$$

$$x^{-1}a_1x = b_1h_2,\ h_2 \in H\ e\ a_1 \in A.$$

Então, $x^{-1}a_1x \in BH$. Logo, $x^{-1}Ax$ e B são subgrupos de BH de ordem a. Novamente por indução, temos que eles são conjugados.

Vejamos que, se existe algum subgrupo próprio normal de G cuja ordem não é divisível por b, então cairemos no primeiro caso. Podemos então, assumir que b é um divisor de $|H|$, para todo tubgrupo normal não trivial H de G.

Se H é um subgrupo normal minimal, como G é solúvel finito, H é um p-grupo abeliano elementar para algum p primo. Assumiremos então que $b = p^m$. Assim, H é um p-subgrupo de Sylow de G e a normalidade de H nos diz que H é único, passando assim para o segundo caso.

2° caso: Seja $|G| = ap^m$ onde $p \mid a$. G contém um subgrupo de Sylow normal abeliano H, o qual é o único subgrupo normal minimal de G.

Existência: Seja $\dfrac{G}{H}$ sulúvel, $\left|\dfrac{G}{H}\right| = a$. Segue que $|H| = p^m$.

Se $\dfrac{K}{H}$ é um subgrupo normal minimal de $\dfrac{G}{H}$, então $\left|\dfrac{K}{H}\right| = q^n,\ q \neq p$, e $|K| = q^n|H| = q^np^m$.

Se Q é um q-subgrupo de Sylow de K, então $K = HQ$. Sejam $N^* = N_G(Q)$ o normalizador de Q em G e $N = N^* \cap K = N_K(Q)$ o normalizado de Q em K. Mostremos que $|N^*| = a$.

O Argumento de Frattini nos garante que, se $K \lhd G$ e Q é um q-subgrupo de Sylow de K, então $G = KN_G(Q)$. Temos então, que $G = KN^*$. Logo,

$$\frac{G}{K} = \frac{KN^*}{K} \cong \frac{N^*}{N^* \cap K} = \frac{N^*}{N}.$$

Assim,

$$|N^*| = \frac{|G||N|}{|K|}.$$

Como $K = HQ$ e $Q \leq N \leq K$, então $K = HQ \leq HN$. Mas $HN \leq K$, logo

$$|K| = |HN| = \frac{|H||N|}{|H \cap N|},$$

e

$$|N^*| = \frac{|G||N|}{|K|} = \frac{|G||N|}{\frac{|H||N|}{|H\cap N|}} = \frac{|G||N||H \cap N|}{|H||N|} = \frac{|G|}{|H|}|H \cap N| =$$

$$= \left|\frac{G}{H}\right| |H \cap N| = a|H \cap N|.$$

Precisamos que

$$|N^*| = a \ \Rightarrow \ a|H \cap N| = a \ \Rightarrow \ |H \cap N| = 1.$$

Mostremos que $H \cap N \leq Z(K)$ e $Z(K) = 1$.
Seja $x \in H \cap N$. Se $k \in K$, como $K = HQ$, então $k = hs$, onde $h \in H$ e $s \in Q$. Sendo H abeliano, x comuta com h, portanto basta provarmos que x comuta com s. Mas $(xsx^{-1})s^{-1} \in Q$, pois x normaliza Q e $x(sx^{-1}s^{-1}) \in H$ já que H é normal em G. Portanto, $xsx^{-1}s{-}1 \in Q \cap H = 1$, ou seja, $x \in Z(K)$. Logo, $H \cap N \leq Z(K)$.
Mostremos agora que $Z(K) = 1$.
Como $Z(K)$ é subgrupo característico de K e $K \lhd G$, então $Z(K) \lhd G$.
Suponhamos que $Z(K) \neq 1$, então ele contém um subgrupo normal minimal de G. Assim, $H \leq Z(K)$, pois H é o único subgrupo normal minimal de G. Mas, como $K = HQ$ e Q é o único q-subgrupo de Sylow de HQ, então Q é subgrupo característico de K. Logo $Q \lhd G$ e $H \leq Q$, o que é uma contradição.
Portanto, $Z(K) = 1$, $H \cap N = 1$ e $|N^*| = a$.

Conjugação: Temos já que $|N^*| = a$. Seja $A \leq G$ e $|A| = a$. Queremos mostrar que A é conjugado de N^*. Como $|AH|$ é divisível por a e por $|K| = p^m q^n$, então $|AK| = ab = |G|$. Logo $AK = G$, então

$$\frac{G}{K} = \frac{AK}{K} \cong \frac{A}{A \cap H},$$

e

$$|A \cap H| = \frac{|A||K|}{|G|} = q^n.$$

Pelo Teorema de Sylow, $A \cap H$ é conjugado de Q. Como subgrupos conjugados possuem normalizadores conjugados, temos que N^* é conjugado de $N_G(A \cap H)$ e $|N_G(A \cap H)| = a$.
Como $A \cap H \lhd A$, segue que $A \leq N_G(A \cap H)$ e $A = N + G(A \cap H)$.
Portanto, A é um conjugado de N^*.

□

Em Scott (1964) também é apresentada uma demonstração para este teorema por indução sobre a ordem de G, no entanto, usa o complemento de H para provar a conjugação.

Podemos concluir que, os p-subgrupos de Sylow sempre existem, pois são os

subgrupos de G com ordem sendo a maior potência de p que divide a ordem de G. Além disso, são conjugados entre si. Como já vimos, os π-subgrupos de Hall nem sempre existem, mas se considerarmos um grupos solúvel finito podemos garantir que eles existem e também são conjugados entre si, assim como provamos no teorema anterior.

Referências Bibliográficas

ARAUJO, W. F. *A Infuência dos Subgrupos Minimais na Estrutura de Grupos Finitos*. Dissertação (Mestrado) — Universidade Estadual de Maringá, 2009.

DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 4. ed. São Paulo: Atual, 2003.

GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. 6. ed. Rio de Janeiro: IMPA, 2013.

LANG, S. *Álgebra para Graduação*. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

MONTEIRO, A. A.; MATOS, I. T. *Álgebra-Um primeiro curso*. 2. ed. São Paulo: Escolar, 2001.

SCOTT, W. R. *Group Theory*. New Jersey: Prentice-Hall, 1964.