UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA E ESTATÍSTICA

EWERTON BRUNO SILVA ARAÚJO

OS TEOREMAS DE SYLOW E ALGUMAS APLICAÇÕES

Campina Grande/PB
2011

EWERTON BRUNO SILVA ARAÚJO

OS TEOREMAS DE SYLOW E ALGUMAS APLICAÇÕES

Trabalho de Conclusão do Curso Licenciatura Plena em Matemática da Universidade Estadual da Paraíba. Em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

Orientador: Vandenberg Lopes Vieira

Campina Grande/PB
2011

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

Ar12t Araújo, Ewerton Bruno Silva.

Os teoremas de Sylow e algumas aplicações [manuscrito] / Ewerton Bruno Silva Araújo. – 2011.

39 f.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) – Centro de Ciências Tecnológicas, 2011.

"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática e Estatística".

1. Matemática – Teoria dos Números. 2. Teorema de Sylow – Aplicação. 3. Teoria dos Grupos Finitos. I. Título.

21. ed. CDD 512.7

EWERTON BRUNO SILVA ARAÚJO

OS TEOREMAS DE SYLOW E ALGUMAS APLICAÇÕES

Monografia apresentada no Curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

BANCA EXAMINADORA

Prof. Dr. Vandenberg Lopes Vieira
Departamento de Matemática e Computação – CCT/UEPB
Orientador

Profª. Drª. Luciana Roze de Freitas
Departamento de Matemática e Computação – CCT/UEPB
Examinador

Prof. Msc. Fernando Luiz T. Silva
Departamento de Matemática e Computação – CCT/UEPB
Examinador

Campina Grande, 29 de Junho de 2011

A minha mãe, Elizabeth, e a minha namorada, Melânia. Aos meus familiares e amigos, enfim a todos que sempre me incentivaram e, acima de tudo, me compreenderam.

Agradecimentos

Ao meu Senhor, por sempre estar ao meu lado e ter me dado todas as condições para que eu pudesse chegar ao singelo lugar onde estou, mas que foi qual desejei.

Declaro ainda minha gratidão aos professores do Departamento de Matemática que tão diretamente influenciaram nessa conquista, aliás, não só influenciaram mas que foram os principais responsáveis para que eu tivesse força para chegar até aqui. Em especial aos maiores incentivadores e exemplos de competência: Aldo Trajano, Célia Maria, Cícero Pereira, Daniel Cordeiro, Fernando Luiz, Luciana Freitas, Maria de Jesus e Orlando Almeida. Em particular, agradeço ao meu orientador, o Dr. Vandenberg Lopes Vieira, por ter sido tão decisivo no direcionamento da minha vida acadêmica e a quem devo boa parte dos frutos que casualmente eu venha a colher, como também volto a agradecer aos componentes da banca examinadora, Luciana Freitas e Fernando Luiz, por terem sido tão prestativos ao aceitarem o convite, apesar do tempo avançado.

Ainda no âmbito acadêmico, eu não poderia passar sem dizer o meu "Muito obrigado"aos colegas de sala por tamanho companheirismo e ajuda em todos esses dias de caminhada.

A minha mãe, Elizabeth, por ter me dado a vida, tanto no sentido de ter me trazido ao mundo quanto no sentido de doação, de ter se dedicado a minha educação e formação da minha personalidade. Agradeço também aos meus familiares que sempre me incentivaram e me apoiaram, colocaram-se a disposição para ajuda de qualquer natureza, em especial as minhas avós, Maria (que Deus a tenha ao seu lado) e Josefa, por em qualquer oportunidade declararem o orgulho em me ter como neto, o que só mostra o quão gentis foram/são. Minhas tias Josélia e Andrea Brito também merecem citação

especial por terem me criado como se fosse um filho. Bem como a minha irmã, Eweny Bruna, e aos meus primos-irmãos: Anderson, Deyvison, Érida, Érika, Esterfânia, Izabela e Joannderson.

Ainda, a minha namorada, Melânia Almeida, por ter sido fiel companheira desde o primeiro dia de aula e que posteriormente veio a assumir o atual *posto*. Jamais poderei retribuir o auxílio por ele não ter sido apenas em conhecimento, mas de contribuição ímpar para a lapidação da minha personalidade, por ter sido afetivo mesmo durante os aproximadamente quatro anos em que fomos "apenas" amigos.

Por fim, mas não menos importante, eu deixo os agradecimentos aos meus grandes, velhos e maravilhosos amigos. Foram eles quem mais me seguraram e, principalmente, suportaram as minhas lamentações, e ouviram minhas dificuldades, sem jamais deixar de incentivar e mostrar extrema confiança no meu potencial (até mais do que deviam, diga-se de passagem):

Bruna Sousa, alguém com quem me sinto perfeitamente à vontade, uma irmã, a sua companhia é sempre muito divertido, particularmente pelo seu jeito atrapalhado que eu tanto adoro.

Camila Brito, personalidade ímpar por, embora habitemos em uma sociedade maliciosa, manter a pureza em suas ações.

A integante do "Quarteto Fantástico", Gérsica Freitas, que chegou na cidade como uma menina dorminhoca e rapidamente atingiu uma maturidade admirável.

A baixinha corinthiana que tão rápido conquistou minha amizade poe seus sentimentos instáveis que tanto me intrigam. Não posso viver sem seus *scraps* e torpedos diários que tanto me fazem rir, Magnólia Ramos.

À morena mais charmosa e elegante que eu conheço, Maricelle Ramos, minha irmã em Cristo que eu tanto me orgulho e que sempre nos coloca na linha.

Por fim, obrigado a Jéssica Sousa, Juliana Vidal, Larissa Araújo, Luana Alves, Luis Lemos, Priscila Almeida, Poliana Leão, Thayse Barbosa e Viviane Almeida.

Eu, de boa vontade, morreria queimado como Faetonte, se fosse o preço a pagar para alcançar o Sol e saber qual sua forma, tamanho e substância.

Eudoxo de Cnidos

Resumo

Devido ao caráter de um trabalho de conclusão de curso, prezamos por utilizar recursos de nível de graduação, objetivando a compreensão de todos. Supomos inicialmente o conhecimento básico do leitor sobre conceitos como funções, operações, equivalência, congruência e divisibilidade. Assim, após uma breve visão histórica, apresentamos uma introdução à Teoria dos Grupos, onde foram fundamentadas noções de grupos, subgrupos, classes laterais, subgrupos normais, grupos quocientes, homomorfismos, grupo das simetrias e representações de grupos, além de resultados de destaque na Teoria dos Grupos Finitos, tais como o Teorema de Lagrange, o Teorema do Homomorfismo, o Teorema de Cayley e o Teorema Órbita-estabilizador dando assim todo o suporte teórico necessário à abordagem ao nosso foco, os Teoremas de Sylow. Neste item, foi necessário conceituar p-Grupos para finalmente podermos chegar ao nosso objetivo de enunciar os Teoremas de Sylow, demonstrá-los e, em seguida, exibirmos algumas aplicações.

Palavras chave: Teoria dos Grupos Finitos, Teorema de Lagrange, Representações de Grupos, Teoremas de Sylow.

Abstract

Due to the character of a completion of course work, cherish to use resources at the undergraduate level, aiming at the understanding of all. We assume initially the reader's basic knowledge about concepts such as functions, operations, equivalence, congruence and divisibility. So, after a brief historical overview, we present an introduction to Group Theory, which were based notions of groups, subgroups, cosets, normal subgroups, quotient groups, homomorphisms, the group of symmetries and representations of groups, as well as outstanding results in theory of Finite Groups, such as Lagrange's Theorem, the Homomorphism Theorem, Cayley's Theorem and Theorem Orbit-stabilizer thus giving all the support necessary theoretical approach to our focus, the Sylow theorems. In this section, it was necessary to conceptualize p-Groups to finally be able to reach our goal of listing the Sylow theorems, and show them, then display some applications.

Keywords: Finite Group Theory, Lagrange's Theorem, Representations of Groups, Sylow theorems.

Sumário

Introdução

Uma breve visão histórica

A Teoria dos Grupos foi, sem dúvida, uma peça chave no desenvolvimento da Matemática Moderna. A estrutura de grupo, por sua vez, é básica à Álgebra Abstrata, basta observar que outras estruturas algébricas podem ser consideradas grupos com certas características mais específicas. O termo grupo foi usado pela primeira vez pelo matemático francês Evarist Galois (1811 - 1832) em "Memoiron the Conditions for Solvability of Equations by Radicals", em 1830.

Galois, enquanto estudava a solubilidade de equações polinomiais por meio de radicais, deu origem a esse novo ramo da matemática. O que só veio a confirmar o que D'Alembert (1717 - 1783), com brilhantismo, afirmou "A álgebra é generosa: frequentemente ela dá mais do que se lhe pediu".

Esse jovem matemático e revolucionário (até mais revolucionário do que matemático), que faleceu antes mesmo de completar 22 anos, estava tão à frente de sua época que seu novo conceito foi inicialmente rejeitado por não ser compreendido nem mesmo pelos grandes matemáticos da época, dentre eles, Fourier (1768 - 1830). Apenas quando Liouville (1809 - 1882) teve acesso a uma cópia do seu trabalho e o interpretou, em 1846, é que sua obra foi finalmente reconhecida e hoje é considerada uma das maiores da matemática do século.

Não podemos deixar de citar que são inúmeras e grandiosas as contribuições do inglês Arthur Cayley (1821 - 1895)[1], como a criação do próprio termo grupo abstrato, por exemplo.

[1] Brilhante matemático e advogado que tem contribuições em praticamente todas as áreas da Matemática, superado em publicações apenas por Leonhard Euler e Augustin Louis Cauchy.

No século XIX o estudo de grupos limitou-se a grupos de permutações, especialmente de raízes de polinômios.

No entanto, o estudo de grupos veio ganhar aceitação mais posteriormente com o estudo de grupos infinitos, representações de grupos e classificação dos grupos simples finitos. Aliás, em 1872, o matemático norueguês Peter Ludwig Mejdell Sylow (1832 - 1918), divulgou um trabalho intitulado "Théorèmes sur lês groupes de substitutions", onde apresentou os teoremas que constituem o foco do nosso trabalho e, a partir daí, quase todos os avanços no tocante aos grupos finitos tiveram como base esses resultados.

Galois, quando pensou nessa estrutura, certamente não tinha ideia de quão importante ela viria a ser. Atualmente, muitas pesquisas da Matemática Moderna seguem essa linha, cujas aplicações estão nos mais diversos ramos da ciência, tais como: criptografia - na codificação de dados computacionais; química - na Teoria Quântica são bastante utilizados os chamados grupo de Poincaré[2] e grupo de Lorentz (1853 - 1928)[3]; física - onde constitui uma ferramenta essencial para compreender as propriedades dos sistemas atômicos e moleculares; entre outras. Isso só mostra quão certo estava Lobachevsky (1792 - 1856), quando sabiamente declarou: "Não há ramo da Matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real."

Outra aplicação curiosa desse tão belo ramo da matemática é o uso da simetria de grupos na resolução do famoso quebra-cabeça chamado "Cubo de Rubik"ou "Cubo Mágico"que consiste, originalmente, num cubo cujas faces são coloridas, onde as cores são diferentes duas a duas, e compostas por outros nove quadrados menores. Conceitos como permutações e r-ciclos escritos como produto de ciclos disjuntos são utilizados na busca pela solução com menor número de movimentos. Infelizmente, os grupos das simetrias espaciais[4] não serão abordados nesse trabalho por não haver ligação direta com nossos objetivos.

[2] Uma homenagem ao matemático, físico e filósofo francês Jules Henri Poincaré.

[3] Em honra ao físico holandês ganhador do Prêmio Nobel, 1902, por seu trabalho sobre radiações eletromagnéticas.

[4] Caso o leitor tenha interesse em conhecê-los, ver Modern Algebra, DURBIN, 1992.

1 Grupos

Admitiremos que o leitor tenha os conhecimentos preliminares necessários à compreensão da teoria apresentada, tais como: noções de conjuntos, números inteiros, relações de equivalência, classes de equivalência e conjuntos quociente, congruências, dentre outros inerentes.

O estudo de grupos nos permite generalizar as operações binárias aritméticas, a idéia é a de operar dois elementos de um conjunto de modo que o elemento encontrado pertença também ao conjunto, no entanto, não trabalhamos apenas com conjuntos numéricos.

Inicialmente veremos o conceito de grupo e as propriedades básicas dessa estrutura, obviamente estivemos bastante atentos em fundamentar toda a teoria necessária à compreensão dos resultados subsequentes. Cayley, em sua famosa frase "Um grupo é definido por meio de leis que combinam seus elementos."definiu de forma clara e sucinta esse objeto que opera elementos de um conjunto e obtém como resultado um elemento do próprio conjunto, onde, não necessariamente, os elementos são números e nem as operações são as usuais; no caso dos grupos simétricos, inclusive, podem ser rotações, translações.

Interior ao conceito de grupo, estudaremos subgrupos dos mais diversos tipos, dentre os quais os subgrupos normais e p-subgrupos de Sylow serão os mais trabalhados. Assim como, obviamente, todos os conceitos citados no primeiro parágrafo.

Apresentaremos ainda um resultado que nos ajudará a identificar quais subconjuntos poderão vir a ser subgrupos, denominado o Teorema de Lagrange (1736 - 1813)[1], cuja importância em nossos estudos é enorme. Outro teorema de destaque será o Teorema do Homomorfismo, pois não há estrutura algébrica que não tenha dependência dessa aplicação particular, e a proposição irá nos permitir trabalhar com grupos iguais em sua essência.

[1] Em homenagem ao italiano Joseph Louis Lagrange.

Como já foi dito, por muito tempo o estudo de grupo se resumiu aos grupos de permutações e estes estão intrinsecamente ligados aos nossos objetivos, por este motivo, fomos mais cuidadosos e os apresentamos de forma mais detalhada.

O Teorema de Cayley ou Teorema da Representação, por sua vez, usa os dois últimos conceitos citados para facilitar atividades ao nos permitir trabalhar com conjuntos mais concretos. Devemos citar também a explanação do Teorema Órbita-Estabilizador e da Equação das Classes como parte indispensável deste item.

De posse dos conceitos e proposições supracitados, estaremos assim em condições de abordarmos o nosso foco, os famosos teoremas de Sylow, um dos quais consiste na proposição mais próxima de uma recíproca do também famoso Teorema de Lagrange. Ao enunciá-los e demonstrá-los, faremos algumas classificações de grupos finitos utilizando as ferramentas nos foram dadas pelo norueguês.

Para as demostrações dos resultados neste trabalho que não forem apresentadas sugerimos as referências FRALEIGH (1994), HERSTEIN (1980) ou GARCIA (2010).

1.1 Conceito de Grupos

Definição 1.1.1 *Sejam G um conjunto não -vazio e $*$ uma operação sobre G. Diz-se que G munido com esta operação é um* ***grupo*** *quando as seguintes propriedades são satisfeitas:*

(a) A operação $*$ é associativa, ou seja,

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

(b) Existe elemento neutro para a operação, ou seja,

$$\exists \ \ e \in G, \quad talque \quad e * a = a * e = a, \quad \forall \ a \in G.$$

(c) Todo elemento em G possui inverso,

$$\forall \ \ a \in G, \quad \exists \ \ a' \in G \quad talque \quad a * a' = a' * a = e.$$

Indicaremos o grupo assim definido por $(G, *)$ ou simplesmente por G, caso não haja dúvidas quanto à operação em G.

Se o grupo $(G, *)$ satisfaz a condição

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

então diz-se que G é **comutatitivo** ou **abeliano**.

Alguns exemplos clássicos de grupos abelianos aditivos são: $(\mathbb{Z},+)$, $(\mathbb{Z}_n,+)$, $(\mathbb{Q},+)$ e $(\mathbb{R},+)$. Por sua vez, $(\mathbb{Z}_p-\{0\},.)$, $(\mathbb{Q}-\{0\},.)$ e $(\mathbb{R}-\{0\},.)$ são exemplos de grupos abelianos multiplicativos.

Agora, seja G o conjunto das matrizes de ordem $n\times n$ com a multiplicação usual. É fácil ver que o conjunto não constitui estrutura de grupo, pois é possível exibir uma matriz quadrada A tal que a equação matricial $A.X=I_n$ não possui solução, logo nem todo elemento possui inverso em G.

No entanto, se $G=\{A\in M_n(\mathbb{R});|A|\neq 0\}$, então G é um grupo denominado *grupo linear real* e denotado por $GL_n(\mathbb{R})$.

Observação 1.1.1 Os elementos e e a' das propriedades 1 e 2 são únicos e são chamados ***identidade*** *de* G e ***inverso*** de a, respectivamente. Quando um grupo G for multiplicativo, então indicaremos o inverso de a por a^{-1}. Já para um grupo aditivo, o indicaremos por $-a$. Ademais, se $a,b\in G$, *então*

$$(a^{-1})^{-1}=a \quad e \quad (ab)^{-1}=b^{-1}a^{-1}.$$

Exemplos 1.1.1 *Seja C um conjunto finito de n elementos. Considere $S_n=\{f:C\to C; f$ é uma bijeção$\}$. O conjunto S_n com a composição de funções é um grupo. Em especial, este virá a ser bastante utilizado em nossos estudos, o chamado* grupo simétrico ou grupos das permutações de n letras.

Para $n=3$, temos o conjunto $C=\{1,2,3\}$ e o grupo S_3, cujas permutações são:

$$\alpha_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \alpha_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\quad \alpha_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$

$$\alpha_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \alpha_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \alpha_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Considerando os elementos

$$\alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad e\quad \beta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

temos

$$\alpha^2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id,$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Observe que a partir de α e β é possível construir o grupo S_3. Isso se traduz dizendo que α e β *geram* o grupo S_3. Foi possível observar também que $\alpha\beta \neq \beta\alpha$, assim, S_3 não é comutativo.

Observação 1.1.2 Por questão de praticidade, quando não houver confusão, usaremos G para denotar o grupo $(G, \cdot)$, como também poderemos omitir o sinal da operação. Com efeito de ilustração: ao invés de anotar $a \cdot b$ anotamos ab.

1.2 Subgrupos

Definição 1.2.1 *Se G é um grupo e H é um subconjunto não-vazio de G, então dizemos que H é um subgrupo de G quando a operação de G restringida a H faz deste um grupo, isto é, quando as condições seguintes são satisfeitas:*

1. $h_1h_2 \in H$, $\forall\ h_1,h_2 \in H$
2. $h_1(h_2h_3) = (h_1h_2)\, h_3$, $\forall\ h_1,h_2,h_3 \in H$
3. $\exists\ e_H \in H$ tal que $e_Hh = he_H = h$, $\forall\ h \in H$
4. Para cada $h \in H$, existe $k \in H$ tal que $hk = kh = e_H$.

Para indicar que H é um subgrupo de G, usaremos a notação $H < G$.

Exemplos 1.2.1 Para um grupo qualquer G, $\{e\}$ e G são claramente subgrupos de G, chamados ***subgrupos triviais*** de G.

Exemplos 1.2.2 Com a adição usual, temos que $\mathbb{Z} < \mathbb{Q}$. Aliás, temos os subgrupos

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}.$$

Exemplos 1.2.3 Sob a multiplicação usual, obtemos

$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*.$$

Exemplos 1.2.4 O conjunto $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ é um subgrupo de $\mathbb{Z}$. Mais geralmente, se $n \in \mathbb{Z}$, então $n\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$. Reciprocamente, se H é um subgrupo de $\mathbb{Z}$,então existe $n \in \mathbb{Z}$ tal que

$$H = nZ = \{nk : k \in \mathbb{Z}\}.$$

Exemplos 1.2.5 Seja G um grupo qualquer. Considere o subconjunto $\mathcal{Z}(G) = \{x \in G; xg = gx, \forall g \in G\}$. Pode-se mostrar que $\mathcal{Z}(G)$ é um subgrupo de G, chamado *centro* de G. Observe ainda que G é abeliano se, e somente se, $\mathcal{Z}(G) = G$.

Proposição 1.2.1 *Seja H um subconjunto não vazio de um do grupo G. Então H é um subgrupo de G se, e somente se as duas condições seguintes são satisfeitas:*

1. $h_1.h_2 \in H$, $\forall$ h_1,$h_2 \in H$.
2. $h^{-1} \in H$, $\forall$ $h \in H$.

Se S é um subconjunto não-vazio do grupo G, o conjunto $\langle S\rangle = \{a_1a_2...a_n,\ n \in \mathbb{N};\ a_i \in S$ ou $a_i \in S^{-1}\}$ é o subgrupo gerado por S. Quando $S = \{\alpha_1, \alpha_2, ..., \alpha_r\}$ é finito, denotaremos $\langle\{\alpha_1, \alpha_2, ..., \alpha_r\}\rangle$ por $\langle\alpha_1, \alpha_2, ..., \alpha_r\rangle$. Observe que se $g \in G$, então $\langle g\rangle = \{..., (g^{-1})^2, g^{-1}, e, g, g^2, ...\}$. Escreveremos $\langle g\rangle = \{g^t; t \in \mathbb{Z}\}$ para denotar que o grupo é *gerado pelo elemento g*. Quando existe $g \in G$ tal que $\langle g\rangle = G$, então dizemos que G é *cíclico*.

O grupos aditivos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$ são exemplos clássicos de grupos cíclicos.

Definição 1.2.2 *A* ordem de um grupo *G é o número de elementos em G; denotaremos por $|G|$. Se a é um elemento do grupo G, a* ordem de *a é a ordem do subgrupo gerado por a, ela será denotada por $\mathcal{O}(a)$.*

Exemplos 1.2.6 $|\mathbb{Z}_n| = n$ *e* $|S_n| = n!$.

1.3 Classes laterais e Teorema de Lagrange

Seja G um grupo e seja H um subgrupo de G. Definindo sobre G a relação de equivalência:

$$y \sim x \Leftrightarrow \exists\ h \in H \textit{ tal que } y = xh.$$

O conjunto $xH = \{y \in G;\ y \sim x\} = \{xh;\ h \in H\}$ é chamado *classe lateral à esquerda de H em G*. Em particular, H é a classe lateral do elemento neutro e à esquerda. Além disso, observe que $y \in xH \Leftrightarrow yH = xH$.

Analogamente, podemos definir a classe lateral à direita de H em G como $Hx = \{hx; h \in H\}$.

Definição 1.3.1 *O* índice *n de H em G é a cardinalidade do conjunto das classes laterais à esquerda; anotamos $(G : H) = n$.*

Proposição 1.3.1 *Para todo $x \in G$ tem-se $|xH| = |H|$.*

Demonstração: Veja que, ao definirmos uma aplicação

$$\begin{array}{rccc} f: & H & \longrightarrow & xH \\ & h & \longmapsto & xh \end{array}$$

claramente temos uma bijeção. ■

O teorema a seguir é o principal teorema sobre grupos finitos.

Teorema 1.3.1 (Teorema de Lagrange) *Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |H| \cdot (G : H)$.*

Demonstração: Tomaremos a relação de equivalência $\sim$ em G. Particionando G em classes de equivalência cujo número de elementos em cada umas delas e $|H|$ (garantido pela proposição anterior). Ao passo que definimos o índice de H em G como o número de classes de equivalência, donde

$$|G| = |H| \cdot (G : H)$$

■

Como consequências do Teorema de Lagrande, destacamos:

Corolário 1.3.1 *Sejam G um grupo finito e $\alpha \in G$. Então a ordem de α divide a ordem de G. Em particular,*

$$\alpha^{|G|} = e.$$

Demonstração: Por definição, $\mathcal{O}(\alpha) = |\langle\alpha\rangle|$ e pelo Teorema de Lagrange, temos que $\mathcal{O}(\alpha)$ divide $|G|$. Façamos então $|G| = n$ e $\mathcal{O}(\alpha) = r$. Dai, $n = r \cdot k$ para algum $k \in \mathbb{Z}$ e

$$\alpha^{|G|} = \alpha^{r \cdot k} = \alpha^{r \cdot k} = (\alpha^r)^k = e^k = e \Rightarrow \alpha^{|G|} = e.$$

■

Corolário 1.3.2 *Todo grupo G de ordem prima é cíclico. Em particular, G é abeliano.*

Demonstração: Seja G um grupo tal que $|G| = p$, em que p é um número primo. Desse modo, existe $x \in G - \{e\}$. Pelo Teorema de Lagrange, $|\langle\alpha\rangle|$ divide p. Mas, sendo p primo, temos $|\langle x\rangle| = p$, pois $|\langle x\rangle| \neq 1$. Por isso, $|\langle x\rangle| = G$ e, por conseguinte, G é cíclico. ■

Corolário 1.3.3 *Se G é um grupo finito tal que $|G| \leq 5$, então G é abeliano.*

Demonstração: Se $|G| = 1 \Rightarrow G = \{e\}$ e, desse modo, G é cíclico. Se $|G| = 2, 3$ ou 5, então G tem ordem prima e pelo Corolário 1.3.2, G é abeliano. Só nos resta considerar o caso em que $|G| = 4$.

Suponhamos que $|G| = 4$. Se existe $x \in G - \{e\}$ tal que $\langle x \rangle = G$, então G é cíclico e, portanto, abeliano. Suponhamos então

$$\langle x \rangle \neq G, \quad \forall \quad x \in G.$$

Assim, pelo Teorema de Lagrange, temos $|\langle x \rangle| = 2$ para todo $x \in G - \{e\}$. Assim, para todo $x \in G$,

$$x^2 = e \Leftrightarrow x = x^{-1}.$$

Daí, para $x, y \in G$,

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

Portanto, G é abeliano.

■

1.4 Subgrupos normais e grupos quocientes

Definição 1.4.1 *Um subgrupo N de G se diz um* subgrupo normal *de G se para todo $g \in G$ e para todo $n \in N$ temos $gng^{-1} \in N$ (e anotamos $N \lhd G$).*

Os subgrupos normais têm a particularidade de que as classes laterais à esquerda são iguais as classes laterais à direita, neste caso, iremos chamá-las apenas de *classes laterais* de N.

Exemplos 1.4.1

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

2) $Z(G) \lhd G$;

3) $G' = \langle \{xyx^{-1}y^{-1}; x, y \in aG\} \rangle$ é um subgrupo normal de G;

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

5) Se G é um grupo abeliano, então todo subgrupo de G é normal em G.

Definição 1.4.2 *Sejam G um grupo e N um subgrupo normal de G. O conjunto das classes laterais com a operação induzida de G por N é o grupo quociente de G por N. Denotaremos por G/N ou $\frac{G}{N}$.*

1.5 Homomorfismo de grupos

Definição 1.5.1 *Sejam $(G_1, \cdot)$ e $(G_2, *)$ dois grupos. Uma função $f : G_1 \to G_2$ é um homomorfismo se ela é compatível com as estruturas dos grupos, isto é, se*

$$f(a \cdot b) = f(a) * f(b), \text{ para todo } a, b \in G.$$

Exemplos 1.5.1
1) $Id : (G, \cdot) \to (G, \cdot)$, $Id(g) = g$, é um homomorfismo chamado *identidade*;
2) $e : G_1 \to G_2$, $e(g) = eg$, para todo $g \in G$, é um homomorfismo chamado *trivial*.
3) Se $(G, \cdot)$ é um grupo abeliano, então $f_n : G \to G$, $f_n(g) = g^n$, é um homomorfismo;
4) Seja $H \lhd G$, então $f : G \to G/H$, $f(g) = gH$, é um homomorfismo chamado de *projeção canônica*.

Definição 1.5.2 *Se φ é um homomorfismo de G_1 em G_2, definimos* núcleo *de φ (e denotamos por $ker\varphi$) como sendo o conjunto $ker\varphi = \{x \in G; \varphi(x) = e_g\}$.*

Definição 1.5.3 *Um homomorfismo φ é de G_1 em G_2 é dito um* isomorfismo *se φ é bijetivo. Dizemos então que G_1 e G_2 são* isomorfos *(anotamos $G_1 \approx G_2$).*

Algumas propriedades elementares de um homomorfismo $f : (G_1, \cdot) \to (G_2, *)$ são: Seja $f : (G1, \cdot) \to (G2, *)$ um homomorfismo de grupos. Então:

1. $f(e_{G_1}) = e_{G_2}$.
2. $f(x^{-1}) = f(x)^{-1}$.
3. $kerf$ é um subgrupo normal de G_1.
4. A imagem $Im\ f$ de f,
$$Im\ f = \{f(x) : x \in G_1\}$$
é um subgrupo de G_2.
5. $\ker f = \{e_{G_1}\} \Leftrightarrow f$ é injetiva, em que e_{G_1} é a identidade de G_1.
6. Se a ordem de $x \in G_1$ é finita, isto é, se $\mathcal{O}(x) < \infty$, então $\mathcal{O}(f(x))$ divide $\mathcal{O}(x)$.

Teorema 1.5.1 (Fundamental dos Homomorfismos) *Seja $f : G \to K$ um homomorfismo de grupos. Então,*

$$\frac{G}{kerf} \simeq Imf.$$

1.6 Grupo de Permutações

A maior parte dos grupos finitos surgiu como permutações, os grupos S_n. Arthur Cayley, em 1878, afirmou que *todo grupo pode ser escrito como subgrupo do grupo das permutações* S_n, resultado conhecido como *Teorema de Cayley.*

Definição 1.6.1 *Um grupo G é dito* simples *quando possui apenas dois subgrupos normais distintos entre si.*

Observação 1.6.1 *Se G é um grupo simples, necessariamente temos que $G \neq \{e\}$ e os únicos subgrupos normais de G são G e $\{e\}$.*

Proposição 1.6.1 *Seja G um grupo de ordem prima. Então G é um grupo simples.*

Demonstração: Seja G tal que $|G| = p$, com p primo. Pelo Teorema de Lagrange, se H é um subgrupo próprio de G, isto é, $H \neq G$ então

$$p = (G : H) \cdot |H| \Rightarrow (G : H) = \frac{p}{|H|} \Rightarrow H = \{e\} \Rightarrow (G : H) = |G| = p$$

■

Teorema 1.6.1 (Teorema de Cayley) *Todo grupo é isomorfo a um subgrupo de um grupo de permutações.*

Devido ao resultado do último teorema, também conhecido como Teorema da Representação, podemos perceber que é de extrema importância estudar os grupos S_n e seus subgrupos. Por isso o faremos com mais detalhes nessa seção.

Definição 1.6.2 *Uma permutação $\alpha \in S_n$ é chamada de* r-ciclo *se existem elementos distintos $\alpha_1, ..., \alpha_n$ em $\{1, ..., n\}$ tais que $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$, ..., $\alpha(a_{r-1}) = a_r$, $\alpha(a_r) = a_1$, e tais que $\alpha(j) = j$, para todo $j \in \{1, ..., n\} - \{a_1, ..., a_r\}$; tal r-ciclo será denotado por $(a_1...a_r)$; o número r é chamado comprimento do ciclo. Os 2-ciclos são também chamados de transposições.*

Exemplos 1.6.1 *Consideremos o grupo S_4. Temos que:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

é um 4-ciclo denotado por (1234). *Podemos também representá-lo por* (2341), (3412) *ou* (4123).
Já a permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

é um 2-ciclo, representado por (13) *ou* (31).

Definição 1.6.3 *Seja $\alpha \in S_n$ um r-ciclo e seja $\beta \in S_n$ um s-ciclo. As permutações α e β são* disjuntas *se, $\forall a \in \{1, 2, ..., n\}$, temos $\alpha(a) = a$ ou $\beta(a) = a$.*

Exemplos 1.6.2
1) Os ciclos (13) e (24) são disjuntos.
2) Os ciclos (1234) e (234), por sua vez, não são disjuntos visto que 2, 3 e 4 são "movidos" por ambos.

Proposição 1.6.2 *Toda permutação pode ser expressa de forma única como um produto de ciclos disjuntos.*

Com o intuito de restringir o número de elementos do conjunto com o qual se irá trabalhar, apresentamos um teorema que gen- eraliza o Teorema de Cayley epermite-nos reduzir o número de elementos ao encontrarmos um grupo isomorfo "menor":

Teorema 1.6.2 *Sejam G um grupo, H um subgrupo de G e $X = \{gH : g \in G\}$. Então existe um homomorfismo de G em S_X tal que o núcleo deste homomorfismo é o maior subgrupo normal de G que está contido em H, onde S_X é o grupo de permutações do conjunto X.*

Demonstração: Considere a aplicação

$$\begin{aligned} \phi : \ G &\to S_X \\ g &\mapsto f_g, \end{aligned}$$

onde $f_g(xH) = gxH$ e seja $g \in ker\phi$. Assim, $f_g(xH) = gxH = xH$, para todo $x \in G$. Se, em particular, $x = e$ temos que $gH = H$. Daí, $g \in ker\phi$ nos diz que $g \in H$, isto é, $ker\phi \subset H$. Para tanto, se N é um subgrupo normal de G, $N \subset H$ e $n \in \mathbb{N}$, temos então que $g^{-1}ngN \subset H$,$\forall g \in G$. Logo, $g^{-1}ng \in H$ e isso nos dá $ngH = gH$, donde $n \in ker\phi$. Portanto, se $N \lhd G$ e $N \subset H$ então $N \subset ker\phi$. ∎

Corolário 1.6.1 *Seja G um grupo finito e $H \neq G$ um subgrupo tal que $|G| \nmid (G : H)!$, então H contém um subgrupo normal não trivial.*

Demonstração: Como $|G|$ não divide $(G : H)!$, pelo Teorema de Lagrange temos que S_G não possui nenhum subgrupo de ordem $|G|$, portanto nenhum subgrupo isomorfo a G. No entanto, temos que $S_G \supset \phi(G)$, assim $\phi(G)$ não pode ser isomorfo a G. Daí, $ker\ \phi \neq \{e\}$. Portanto, pelo resultado precedente $ker\ \phi \lhd H$ e $ker\ \phi \neq \{e\}$ nos leva a concluir que existe um subgrupo normal não trivial de H. ∎

Corolário 1.6.2 *Seja G um grupo finito, $H < G$ tal que $(G : H) = p$, onde p é o menor primo que divide $|G|$. Então $H \lhd G$.*

Demonstração: Sabemos que $ker\ \phi \lhd G$ e, pelos teoremas de Lagrange e do Homomorfismo, $|G/ker\ \phi|$ é um divisor de $|S_X| = p!$; voltando a aplicar o Teorema de Lagrange deduzimos, como p é o menor primo divisor de $|G|$, segue que p é o menor divisor primo de $|G/ker\ \phi|$, já que $|G| = (G : H)|H| = (G : H)(H : ker\ \phi)|\ker\ \phi|$. Resta-nos inferir que se $|G/ker\ \phi|$ divide $p!$, então $|G/ker\ \phi| = p$. Portanto,

$$\frac{|G|}{|ker\ \phi|} = p = \frac{|G|}{|H|} \Rightarrow |ker\ \phi| = |H|,$$

ou seja, $ker\ \phi = H \lhd G$. ■

APLICAÇÃO: Seja G um grupo de ordem 99 e suponha H um subgrupo de ordem 11 (é possível provar essa existência usando um resultado conhecido como "Teorema de Cauchy"). Mostraremos que este subgrupo é normal. De fato, seja H um subgrupo, pelo Teorema de Lagrange $(G : H) = 9$. Por outro lado, como $99 \nmid 9!$ segue do *Corolário 2.1* que H contém um subgrupo normal não trivial N de G em H. Mas $|H| = 11$, como a ordem de H é número primo, segue que H é um grupo simples, logo $N = H$. Portanto, H é um subgrupo normal de G.

Proposição 1.6.3
a) Todo elemento de S_n é um produto de transposições, isto é, $S_n = \langle\{transposições\}\rangle$;
b) $S_n = \langle\{(12), (13), ..., (1n)\}\rangle$;
c) $S_n = \langle(12), (23), ..., ((n-1)n)\rangle$.

Observação 1.6.2 A decomposição de um elemento $\alpha \in S_n$ como um produto de transposições não é única, mesmo se exigirmos um número mínimo de transposições; por exemplo, $(123) = (13)(12) = (23)(13)$.

Proposição 1.6.4 *Seja $\alpha \in S_n$ e seja $\alpha = \tau_t \circ ... \circ \tau_1$ uma fatoração qualquer de α como um produto de transposições. Se $X_1, ..., X_n$ são indeterminadas sobre $\mathbb{Z}$, então*

$$\prod_{1 \leq i < j \leq n} (X_{\alpha(j)} - X_{\alpha(i)}) = (-1)^t \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

Em particular, se $\alpha = \tau_t \circ ... \circ \tau_1 = \mu_u \circ ... \circ \mu_1$ são duas fatorações de α como produto de transposições, então $t \equiv u\ mod\ 2$.

Não apresentamos as demonstrações das duas proposições apresentadas anteriormente devido ao seu caráter bastante independente em relação aos nossos resultados principais.

Definição 1.6.4 *Um elemento $\alpha \in S_n$ é uma* permutação par *quando é possível escrevê-lo como um produto de um número par de transposições, isto é*

$$\prod_{1\leq i<j\leq n}(X_{\alpha(j)} - X_{\alpha(i)}) = \prod_{1\leq i<j\leq n}(X_j - X_i).$$

Analogamente, podemos definir permutação ímpar *como um elemento $\alpha \in S_n$ que pode ser escrito como o produto de um número ímpar de transposições. Equivalentemente*

$$\prod_{1\leq i<j\leq n}(X_{\alpha(j)} - X_{\alpha(i)}) = -\prod_{1\leq i<j\leq n}(X_j - X_i).$$

Proposição 1.6.5 *Seja $A_n = \{\alpha \in S_n; \alpha$ é uma permutação par$\}$. Então A_n é um subgrupo de S_n de índice 2; o denominamos* grupo alternado *ou* grupo das permutações pares.

Demonstração: Seja $\psi : S_n \to W = \{-1, 1\}$ dada por

$$\psi(\beta) = \begin{cases} 1 & se \quad \beta \text{ é par}, \\ -1 & se \quad \beta \text{ é ímpar}. \end{cases}$$

Como ψ é um homomorfismo e seu núcleo é A_n, que é normal em S_n, então $\frac{S_n}{A_n} \approx W$. Portanto,

$$2 = \mathcal{O}(W) = \mathcal{O}\left(\frac{S_n}{A_n}\right) = \mathcal{O}(S_n)/\mathcal{O}(A_n).$$

■

Definição 1.6.5 *Seja $n \geq 2$. Se $\rho \in S_n$ e se $\rho = (a_{11}...a_{1r_1})...(a_{t1}...a_{tr_t})$ é a sua decomposição em ciclos disjuntos com $r_1 \leq r_2 \leq ... \leq r_t$, dizemos que $\{r_1, ..., r_t\}$ é o tipo de decomposição de ρ.*

Exemplos 1.6.3 $\rho := (123)(45)(67)$ e $\rho' := (15)(36)(247)$ têm o mesmo tipo de decomposição, a saber $\{2, 2, 3\}$.

Proposição 1.6.6 *Sejam σ e ρ permutações disjuntas. Então $\sigma\rho = \rho\sigma$, e para todos os k inteiros positivos, $(\sigma\rho)^k = \sigma^k\rho^k$. Seja π um produto de ciclos disjuntos de comprimentos $k_1, k_2, ..., k_r$, então a ordem de π é o mínimo múltiplo comum dos inteiros $k_1, k_2, ..., k_r$.*

Demonstração: Inicialmente, iremos comutar permutações disjuntas. Se ρ fixa i, então $\sigma\rho(i) = \sigma(i)$, considerando $\rho\sigma(i) = \rho(\sigma(i))$. Como ρ e σ são disjuntos, ρ deve fixar $\sigma(i)$ e assim por $\sigma\rho(i) = \rho\sigma(i)$. Por outro lado, se ρ não fixar i então o fato de ρ e σ serem disjuntas nos dá que σ deve fixar i, e novamente segue que $\sigma\rho(i) = \rho\sigma(i)$. Uma vez que *sigma* e ρ comutam, uma prova indutiva mostra que, para todos os k inteiros positivos, $(\sigma\rho)^k = \sigma^k\rho^k$. Faremos em duas etapas. Primeiro mostraremos por indução sobre k que

se $\sigma\rho = \rho\sigma$, então $\sigma\rho^k = \rho^k\sigma$:
Quando $k = 1$, a veracidade decorre da hipótese. Se supusermos que $\sigma\rho^k = \sigma\rho^k = \rho^k\sigma$, então

$$\sigma\rho^{k+1} = \sigma\rho^k\rho = \rho^k\sigma\rho = \rho^k\rho\sigma = \rho^{k+1}\sigma.$$

Segue-se então, também por indução sobre k, que $(\sigma\rho)^k = \sigma^k\rho^k$: Quando $k = 1$, segue claramente. Ao passo que, se $(\sigma\rho)^k = \sigma^k\rho^k$,

$$(\sigma\rho)^{k+1} = (\sigma\rho)^k\sigma\rho = \sigma^k\rho^k\sigma\rho = \sigma^k\sigma\rho^k\rho = \sigma^{k+1}\rho^{k+1},$$

conforme queríamos. E assim $\pi^m = 1$. A ordem de π, portanto, divide m. No entanto, se $\pi^s = 1$, então os ciclos são disjuntos, cada um $\rho_i^s = 1$ e assim s é divisível por cada k_i, e então s é divisível por m. Logo, a ordem de π é m. ■

Proposição 1.6.7 *Seja $n \geq 3$.*
a) Todo elemento de A_n é um produto de 3-ciclos, isto é, temos $A_n = \langle\{3\text{-}ciclos\}\rangle$.
b) Sejam $a, b \in \{1, 2, ..., n\}$,$a \neq b$. Então

$$A_n = \langle\{(abl); l = 1, 2, ..., l, \ com \ l \neq a, b\}\rangle$$

2 Representação por Permutação e Teoremas de Sylow

Até o momento, tratamos de noções básicas de grupos, alguns exemplos e seus elementos. Observe, no entanto, que tudo o que foi feito se resume a um 'estudo interno ao grupo', como o de certas propriedades, elementos, subgrupos, entre outros conceitos.

Por sua vez, nesta parte do trabalho iremos proceder uma abordagem diferente ao utilizarmos um homomorfismo de grupos para transportar certas características de grupo ao outro por meio do que chamamos representações por permutações.

Outro tipo de representação historicamente bastante utilizado é do tipo $\rho : G \to GL(n, K)$, onde K é um corpo e n um inteiro positivo, a chamada *representação matricial* ou *linear* de G de grau n.

Nosso interesse aqui são as representações por permutações de um conjunto, visando máximo de informações possíveis sobre o grupo. Nesse sentido, examinaremos a existência de subgrupos de certa ordem dada bem como, em caso positivo, o número destes e quais relações ocorrem entre eles.

2.1 Representações por permutações

Definição 2.1.1 *Sejam G um grupo, C um conjunto e $\mathcal{P}(C)$ o grupo das permutações de C. Uma representação de G no grupo de permutações de C é um homomorfismo $\rho : G \to \mathcal{P}(C)$, isto é, uma função tal que $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$. Diz-se também que o grupo G* opera sobre o conjunto *C.*

Em algumas situações poderemos usar o conjunto G sem a estrutura de grupo, neste caso usaremos a notação G_0 (e dizemos que G_0 é o conjunto subjacente ao grupo G).

Exemplos 2.1.1
1) Seja G um grupo e seja $C = G_0$. Considere

$$\begin{array}{rcl} T: G & \to & \mathcal{P}(G_0) \\ g & \mapsto & \mathcal{I}_g: \begin{array}{rcl} G_0 & \to & G_0 \\ a & \mapsto & gag^{-1} \end{array} \end{array}$$

Sabemos que T é um homomorfismo, logo uma representação de G no grupo de permutações do conjunto G_0.
2) Sem maiores dificuldades, podemos verificar que

$$\begin{array}{rcl} T: G & \to & \mathcal{P}(G_0) \\ g & \mapsto & T_g: \begin{array}{rcl} G_0 & \to & G_0 \\ a & \mapsto & ga \end{array} \end{array}$$

é um homomorfismo, segue que T é uma representação de G no grupo de permutações de G_0.
3) Sejam G um grupo, H e K subgrupos de G e seja $C = \{aH; a \in G\}$ o conjunto das classes laterais à esquerda de H em G. Considere

$$\begin{array}{rcl} T: K & \to & \mathcal{P}(C) \\ k & \mapsto & T_k: \begin{array}{rcl} C & \to & C \\ aH & \mapsto & kaH \end{array} \end{array}$$

Assim, T é uma representação de K no grupo de permutações do conjunto das classes laterais à esquerda de H em G.

Observação 2.1.1 Utilizaremos somente representações definidas a partir de uma função "automorfismo interno" $\mathcal{I} : g \mapsto \mathcal{I}_g$ e representações definidas a partir da função "translação" $T : g \mapsto T_g$; as primeiras chamaremos representações *por conjugação*, enquanto as últimas chamaremos representações por *translação* ou *representações regulares*. Veja que nos exemplos anteriores em 1) temos uma representação por conjugação, já em 2) e 3) temos representações por translações.

Sejam G um grupo, C um conjunto e seja $\rho : G \to \mathcal{P}(C)$ uma representação de G. Sobre o conjunto C, definimos uma relação de equivalência do seguinte modo:

$$\forall x, y \in C, x \backsim y \Leftrightarrow \exists\ g \in G \quad tal\ que \quad \rho(g)(x) = y.$$

Definição 2.1.2 *Seja $x \in C$. A* órbita *de x é o conjunto*

$$\mathfrak{O}(x) := \{y \in C; y \sim x\} = \{\rho(g)(x); g \in G\}.$$

O estabilizador *de x é o conjunto dos elementos de G que deixam o elemento x fixo, isto é,*

$$E(x) := \{g \in G; \rho(g)(x) = x\}.$$

Observação 2.1.2 Quando existe apenas uma órbita, dizemos que a representação é *transitiva.*

Teorema 2.1.1 (Órbita-estabilizador) *Sejam G um grupo, C um conjunto e $\psi : G \to \mathcal{P}(C)$ uma representação de G. Seja $x \in C$. Então a aplicação ψ abaixo é uma bijeção:*

$$\begin{array}{rccc} \phi: & \mathfrak{O}(x) & \longrightarrow & \{gE(x); g \in G\} \\ & \rho(g)(x) & \longmapsto & gE(x) \end{array}$$

Em particular, no caso de G ser um grupo finito, temos que $|\mathfrak{O}(x)| = (G : E(x))$ e que $|\mathfrak{O}(x)|$ divide $|G|$.

Demonstração: Sejam $g_1, g_2 \in G$ tais que $\rho(g_1)(x) = \rho(g_2)(x)$, aplicando $\rho(g_2^{-1})$ em ambos os lados, como ρ é um homomorfismo, tem-se $\rho(g_2^{-1}g_1)(x) = x$. Assim, temos $g_2^{-1}g_1 \in E(x)$, logo $g_1 \in g_2E(x)$ e $g_1E(x) = g_2E(x)$.
Verificaremos agora a injetividade de ψ. Sejam $y_1 = \rho(g_1)(x)$ e $y_2 = \rho(g_2)(x)$ elementos de $\mathfrak{O}(x)$ tais que $\psi(y_1) = \psi(y_2)$, isto é, tais que $g_1E(x) = g_2E(x)$. Então temos $g_2^{-1}g_1 \in E(x)$, logo $\rho(g_1^{-1}g_2)(x) = x$, ou seja, $\rho(g_1^{-1}) \circ \rho(g_2)(x) = x$ e, portanto,

$$y_2 = \rho(g_2)(x) = \rho(g_1) \circ \rho(g_1^{-1})(x) \circ \rho(g_2)(x) = \rho(g_1)(x) = y_1.$$

Por sua vez, a sobrejetividade é direta, pois se $gE(x)$ é uma classe lateral á esquerda de $E(x)$ em G, então temos que $E(x) = \psi(y)$, com $y = \rho(g)(x)$. ∎

2.1.1 Equação das Classes

Exibiremos uma relação, provaremos que é uma relação de equivalência, e em seguida, iremos encontrar uma descrição algébrica clara do "tamanho" de cada classe de equivalência. A partir desta simples descrição, virá uma bela e poderosa série de resultados sobre grupos finitos.

Definição 2.1.3 *Se $a, b \in G$, então b se diz um* conjugado *de a em G se existe um elemento $c \in G$ tal que $b = c^{-1}ac$.*

Escrevemos então $a \sim b$ e nos referimos a esta relação como *conjugação.*

Lema 2.1.2 *A conjugação é uma relação de equivalência sobre G.*

Demonstração: Devemos agora mostrar que a relação é reflexiva, simétrica e transitiva.
a) Como $a = e^{-1}ae$, $a \sim a$, assim $c = e$ pela definição de conjugação;
b) Se $a \sim b$, então $b = x^{-1}ax$ para algum $x \in G$, donde $a = (x^{-1})^{-1}b(x^{-1})$. Como $y = x^{-1} \in G$ e $a = y^{-1}by$, segue que $b \sim a$;
c) Suponhamos que $a \sim b$ e $b \sim c$ com $a, b, c \in G$. Então $b = x^{-1}ax$ e $c = y^{-1}by$ para algum b e algum c em G. Substituindo a expressão de b na expressão de c, obtemos $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$. Como $xy \in G$, tem-se que $a \in c$.
Logo a relação é de equivalência. ■

Para $x \in G_0$ seja $\mathcal{C}l(x) = \{a \in G; a \sim x\}$, a classe de equivalência de x em G_0 no que diz respeito a relação acima estudada, usualmente chamamos de *classe de conjugação* de x. Veja que $\mathcal{C}l(x)$ consiste no conjunto de elementos da forma $g^{-1}xg$ quando x toma valores em G. Além disso, observe que temos $\mathcal{C}l(x) = \{x\} \Leftrightarrow gxg^{-1} = x, \forall\ g \in G \Leftrightarrow x \in Z(G)$.

Definição 2.1.4 *Se $x \in G_0$, então o* centralizador *de x em G é o conjunto $Z(x) = \{g \in G; gx = xg\}$, isto é, são os elementos de G que comutam com x.*

Lema 2.1.3 *$Z(x)$ é um subgrupo de G.*

Demonstração: Aqui não podemos fazer restrições quanto a ordem de G, devido ao fato deste ser finito ou infinito.
Suponhamos que $g, h \in Z(x)$. Teremos pois $gx = xg$ e $hx = xh$. Portanto $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$, logo $gh \in Z(x)$.
De $gx = xg$ segue que $g^{-1}x = g^{-1}(xg)g^{-1} = g^{-1}(gx)g^{-1} = xg^{-1}$, logo também temos $g^{-1} \in Z(x)$. ■

Agora, estamos prontos para enunciar o nosso princípio de contagem.

Teorema 2.1.4 *Se G é um grupo finito e c_x o número de elementos de $Z(x)$, então $c_x = \frac{\mathfrak{O}(G)}{\mathfrak{O}(N(x))}$; isto é, o número de elementos conjugados x em G é o índice do normalizador de x em G. Em símbolos,*

$$|\mathcal{C}l(x)| = (G : Z(x)).$$

Demonstração: Inicialmente, veja que a classe de conjugados de x em G é exatamente o elementos da forma $g^{-1}xg$ com g em G, e c_x mede o número de $g^{-1}xg$ distintos. Mostraremos que os elementos de mesma classe lateral à esquerda de $Z(x)$ em G dão lugar a um mesmo conjugado de x, enquanto os elementos de diferentes classes laterais à esquerda de $Z(x)$ em G dão lugar a diferentes conjugados de x. Desta forma, teremos uma correspondência bijetiva entre os conjugados de x e classes laterais a esquerda de $Z(x)$ em G.
Suponhamos que $g, h \in G$ estão em uma mesma classe lateral à esquerda de $Z(x)$ em G. Então $h = ng$ donde $n \in Z(x)$ e então $nx = xn$. Portanto, como $h^{-1} = (ng)^{-1} = g^{-1}n^{-1}$

e $h^{-1}xh = g^{-1}n^{-1}xng = g^{-1}n^{-1}nxg = g^{-1}xg$, temos que g e h dão lugar a um mesmo conjugado de x.
Por outro lado, se x e y pertencem a classes laterais à esquerda distintas de $Z(x)$ em G, afirmamos que $g^{-1}xg \neq h^{-1}xh$. Caso contrário, $g^{-1}xg = h^{-1}xh$ nos daria $hg^{-1}x = xhg^{-1}$, que por sua vez implicaria que $hg^{-1} \in Z(x)$. Isto nos diz que x e y estão na mesma classe lateral à esquerda de $Z(x)$ em G, o que contradiz o fato de estarem em diferentes classes laterais. E isto encerra a demonstração. ■

Naturalmente, o conjunto G_0 é igual à união disjunta das classes de conjugação. Em cada classe de conjugação escolhemos um representante x_α. Então, temos $|G| = \sum_\alpha |\mathcal{C}l(x_\alpha)|$, logo

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |\mathcal{C}l(x_\alpha)|$$

Esta igualdade se chama a *equação das classes de conjugação.*

Seja G um grupo e seja $C = \{\text{subgrupos de G}\}$. Considere a aplicação

$$\begin{array}{rcl} T: K & \to & \mathcal{P}(C) \\ g & \mapsto & T_g: \begin{array}{rcl} C & \to & C \\ H & \mapsto & gHg^{-1} \end{array} \end{array}$$

Seja $H \in C$. A órbita $\mathfrak{O}(H) = \{T_g(H); g \in G\} = \{gHg^{-1}; g \in G\}$ de um subgrupo H se chama a *classe de conjugação* de H. Os elementos de $\mathfrak{O}(H)$ se chamam os *subgrupos conjugados* de H. Observe que $\mathfrak{O}(H) = \{H\} \Leftrightarrow H \lhd G$. O estabilizador $E(H) = \{g \in G; T_g(H) = H\} = \{g \in G; gHg^{-1} = H\}$ se chama o *normalizador* de H em G (denota-se $N_G(H)$).

2.2 p-Grupos e Teoremas de Sylow

A recíproca do Teorema de Lagrange, de modo geral, não é válida. No entanto, nesta seção iremos enunciar dois resultados, um dos quais está mais próximo dessa recíproca. Os Teoremas de Sylow se apresentam como ferramentas básicas para verificar se um determinado grupo possui subgrupos normais próprios, um problema de grande importância na Teoria dos Grupos Finitos, especialmente no século XX. Antes de apresentá-los, introduziremos algumas noções sobre p-Grupos.

2.2.1 p-Grupos

Definição 2.2.1 *Seja G um grupo (finito ou não), p um primo, então G é um p-Grupo se todo elemento de G tem ordem correspondente a uma potência de p, isto é,*

$$G \ \ um\ p-Grupo \ \Leftrightarrow g \in G \Rightarrow \mathcal{O}(g) = p^n, \ para\ algum\ n \in \mathbb{Z}.$$

É possível observar que G pode ser finito. Neste caso, se G tem ordem par então G deve ter elementos de ordem 2. A seguir, apresentaremos a generalização deste fato, caso tenhamos a cardinalidade de G divisível por um primo.

Teorema 2.2.1 (Cauchy-Frobenius) *Sejam G um grupo finito e p um número primo tal que $p||G|$. Então*

$$\#\{g \in G; \mathcal{O}(g) = p\} \equiv (-1) \ \ mod\ p.$$

Demonstração: Definindo o produto cartesiano de G por ele mesmo p vezes como:

$$X = \{(x_1, ..., x_p); x_i \in G \ e \ x_1...x_p = e_G\} - \{(e_G, ..., e_G)\} = \{e_X\},$$

a componente x_p dos elementos de X fica determinada pelos primeiros $p-1$ elementos, ou seja, $x_p = (x_1...x_{p-1})^{-1}$ de modo que $|X| \equiv |G|^{p-1} - 1$. Particularmente, $|X| \equiv (-1) \ \ mod\ p$. Tomando $\langle\psi\rangle$ um grupo tal que $\mathcal{O}(\psi) = p$, definiremos ϕ uma aplicação

$$\begin{array}{rccc} \phi: & \langle\psi\rangle & \to & S_x \\ & \psi^i & \mapsto & f_{\psi^i} \end{array},$$

onde

$$f_{\psi^i}(x_1, ..., x_p) := (x_{i+1}, ..., x_p, x_1, ..., x_i).$$

Por outro lado,

$$x_1...x_p = e_G \Rightarrow x_1^{-1}x_1...x_px_1 = e_G \Rightarrow x_2x_3...x_px_1 = e_G,$$

Usando indução matemática, obtemos

$$\underbrace{x_{i+1}...x_px_1...x_i}_{p \ fatores} = e_G,$$

assim concluímos que ϕ é um homomorfismo, e assim $\langle\psi\rangle$ opera sobre X. Logo, as órbitas de X sobre a representação definida por ϕ possui 1 ou p elementos. Seja $\mathcal{X} = (x_1, ..., x_p) \in X$, então $|\mathcal{O}(\mathcal{X})| = 1 \Leftrightarrow \mathcal{X} = (x, ..., x) \Leftrightarrow x^p = e_G$. Por sua vez, definiremos o conjunto

$$X' = \{\mathcal{X} \in X; |\mathfrak{O}(\mathcal{X})| = 1\},$$

de forma que a cardinalidade de X' é igual ao número de elementos em G de ordem p e $|X| = |G|^{p-1} - 1 \equiv |X'| \ \ mod\ p$, como queríamos. ∎

Corolário 2.2.1 *Se G é um grupo finito, então G é um p-Grupo se, e somente se, $|G| = p^n$ para algum n.*

Demonstração: Seja G um p-grupo, por definição, todo elemento de G tem ordem igual a uma potência de p.

Suponha, por absurdo, que a ordem de G não é uma potência de p, assim existe um primo $q \neq p$ tal que $q||G|$. Mas se G é um grupo finito e q é um número primo nessas condições, tem-se que existe $x \in G$ com ordem q, o que contradiz a hipótese.
Reciprocamente, seja $|G| = p^n$ e seja $x \in G$, então $\mathcal{O}(x)|p^n$, isto é, a ordem de x é uma potência de p, e isto encerra nossa prova. ■

Corolário 2.2.2 *Se $G \neq \{e_G\}$ é um p-grupo finito, então $|Z(G)| > 1$.*

Demonstração: De acordo com a Equação das Classes,

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

e com o corolário anterior, temos que:
1) Se $G = Z(G)$, é direto.
2) Se $G \neq Z(G)$, então para cada $x_\alpha Z(G)$ tem-se $Z(x_\beta) \neq Z(x_\gamma)$. Logo, $\sum_{x_\alpha \notin Z(G)}(G : Z(x_\alpha))$ é um múltiplo de p. Daí, obtemos que $|Z(G)| > 1$. ■

Definição 2.2.2 *Seja 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-subgrupo de Sylow.

2.2.2 Teoremas de Sylow

Teorema 2.2.2 (1º Teorema de Sylow) *Seja G um grupo finito e P um p-subgrupo de Sylow e seja n_p o número de p-subgrupos de Sylow de G. Então*

$$n_p \mid |G| \text{ e } n_p \equiv 1 \mod p.$$

Além disso, os p-subgrupos de Sylow são conjugados.

Demonstração: Inicialmente, consideremos a representação de G em seus subgrupos por conjugação. Se P é um p-subgrupo de Sylow, consideraremos $X = \{P = P_1, P_2, ..., P_r\}$, o conjunto dos subgrupos conjugados de P. É direto que se um subgrupo é maximal seus conjugados também o são, assim os elementos de X são subgrupos de Sylow. Como X é uma órbita sobre a representação descrita, então G opera em X e, por restrição, P opera em X. Dado $Q \in X$, $(P : E|_P(Q)) = p^s$, para algum s. Temos então que $s = 0 \Leftrightarrow P = E|_P(Q) = N_G(Q) \cap P$, e este último quando $P \subset N_G(Q)$. Como Q é um subgrupo normal de seu normalizador, então $P \otimes Q$ é um p-subgrupo de G tal que $P \otimes Q \supset P$ e $P \otimes Q \supset Q$. Devido à maximalidade destes, devemos ter $P = Q$. Logo, P é o único elemento de X que tem órbita com um só elemento quando é opera em X. Daí, $|X| = r = \sum | \mathfrak{O} |_P(Q)| = 1 + pl$, para algum $l \in \mathbb{N}$, ou seja, $|X| \equiv 1 \mod p$. Por outro

lado, ao considerarmos X como a órbita de P sobre a representação de G obtemos que $|X| = (G : N_G(P))$ e este é um divisor da ordem de G.
Nos preocuparemos agora em provar que os p-subgrupos de Sylow são conjugados. Para tanto, suponhamos que Q é um p-subgrupo de Sylow e que $Q \notin X$, em particular, $Q \neq P_i$. Pelo mesmo motivo, temos que Q opera sobre X e suas órbitas sobre esta representação tem cardinalidade múltipla de p, o que contradiz o fato anterior. Deste modo, deduzimos que todo p-subgrupo de Sylow é conjugado a P e, portanto, $\#\{p-subgrupos\ de\ Sylow\} = n_p = r$. ■

Teorema 2.2.3 (2º Teorema de Sylow) *Sejam G um grupo e p um número primo tal que $|G| = p^m b$ com mdc $\{p, b\} = 1$. Então, todo p-subgrupo de Sylow tem cardinalidade p^n.*

Demonstração: Concentrar-nos-emos apenas em mostrar que, para algum p-subgrupo de Sylow P, *mdc* $\{(G : P), p\} = 1$. Observe que $(G : P) = (G : N_G(P)) \cdot (N_G(P) : P)$, onde $N_G(P)$ é o normalizador de P. Para mostrar que $(G : P)$ e p são primos entre si é basta-nos mostrar que *mdc* $\{p, (G : N_G(P))\} = 1$ e *mdc* $\{p, (N_G(P) : P)\} = 1$. Como $(G : N_G(P))$ é o número de p-subgrupos de Sylow de G, pelo teorema anterior, concluímos que $(G : N_G(P)) \equiv 1 \mod p$. Por sua vez, $(N_G(P))/P$ não possui elementos de ordem p, observe que se $\overline{x} \in (N_G(P))/P$ é um elemento tal que $\overline{x}^e$ é a identidade, então o grupo $\langle x, P\rangle/P$ é um p-grupo, com efeito, este grupo é o gerado por $\overline{x}$. Ora, se um quociente é um p-grupo assim como o seu denominador, então o numerador é um p-grupo. Daí, pela maximalidade de P, deduzimos que $x \in P$. ■

2.2.3 Aplicações dos Teoremas de Sylow

Nesta seção apresentaremos alguns problemas cujos teoremas de Sylow podem ajudar-nos a resolver:

(a) Grupos de Ordem $2p$

Seja p um número ímpar primo, e seja G um grupo com $2p$ elementos. Podemos aplicar a teoria Sylow para os primos 2 e p, por sua vez. Assim, o número n_p de p-subgrupos de Sylow divide 2p e é congruente a 1 *mod* p pelo 1º Teorema de Sylow. Daí n_p é um dos l, 2, p ou $2p$. Como p e $2p$ são divisíveis por p ambos são congruentes a 0 *mod* p. Como 2 é menor de p, 2 não é congruente a 1 *mod* p, então concluímos que n_p é 1. Assim o p-subgrupo de Sylow, P, é um subgrupo normal de G. Como P tem p elementos, P é cíclico, digamos $P = \langle x\rangle$. Sabemos também que G tem pelo menos um 2-subgrupo de Sylow, então existe um elemento y de ordem 2. Os elementos de G são, portanto,

$$\{1, x, ..., x^{p-1}, y, yx, ..., yx^{p-1}\}.$$

Como P é normal, yxy^{-1} é um elemento de P e por isso é da forma x^i para alguns i. Assim, desde $y^2 = 1$,

$$(yx)^2 = yxy^{-1}x = x^{i+1}.$$

Isto significa que as potências pares de yx são iguais potências de x enquanto as potências ímpares de yx são da forma yx^j para algum j. Pelo corolário do teorema de Lagrange, a ordem de yx divide $2p$, e assim é um de 1,2, p ou $2p$. Se $i \neq -1$ na equação acima, vemos que yx não é de ordem 1 (não é o elemento de identidade), não é de ordem 2 (uma vez que $(yx)^2$ é igual a x^{i+1}) e não de ordem p (desde a sua p-ésima potência é da forma yx^j para algum j). Assim yx deve ter ordem $2p$, de modo as potências de yx incluem todos os elementos de G e G é cíclico. Isto implica que G é abeliano e, assim, de fato, $xy = yx$. Mostramos assim que quando p é um número ímpar primo, um grupo com $2p$ elementos é cíclico ou é da forma $\langle x, y \ ; \ x^p = 1 = y^2 \ e \ yx = x^{-1}y \rangle$.

(b) Grupos de Ordem 21

Há dois resultados preliminares necessários antes da discussão dos grupos com 21 elementos.

Lema 2.2.4 *Seja p e q primos com $p > q$. Um grupo de ordem pq tem um p-subgrupo normal de Sylow.*

Demonstração: Os dividores de pq são 1, p, q e pq. Destes p e pq tem resto 0 quando dividido por p, q tem resto q quando dividido por p, pois q é menor que p. Portanto, pelo resta apenas um p-subgrupo de Sylow, e assim que este subgrupo é normal. ■

Lema 2.2.5 *Sejam x, y são elementos de um grupo G tal que $xy = yx$. Então, para todo o inteiro k, $(xy)^k = x^k y^k$.*

Demonstração: Podemos provar esse resultado por permutações disjuntas quando k é um inteiro positivo, como vimos na Proposição 4 do Capítulo II. O caso quando $k = 0$ é trivial, e o caso quando $k < 0$ segue facilmente. ■

Agora, seja G um grupo com 21 elementos. O lema anterior mostra que G tem um único 7-subgrupo de Sylow $P = \langle x \ ; \ x^7 = 1 \rangle$, por exemplo, e um elemento de y ordem 3. Como P é um subgrupo normal de G, $yxy^{-1} = x^i$ para algum i com $0 \leq i \leq 6$. Assim

$$\begin{aligned} x &= y^3xy^{-3} = y^2(yxy^{-1})y^{-2} \\ &= y^2x^iy^{-2} = (y^2xy^{-2})^i \\ &= (yx^iy^{-1})^i = (yxy^{-1})^{i^2} = x^{i^3}. \end{aligned}$$

Daí, $i^3 \equiv 1 \mod 7$, assim que 7 divide i^3 - 1. Considerando os sete possíveis valores de i, por sua vez, vemos que as únicas soluções para i são $i = 1$,2 ou 4 *mod* 7. No

primeiro caso, quando $yxy^{-1} = x$, vemos que $xy = yx$. Usando o último lema, vemos que $(xy)^3 = x^3$ e $(xy)^7 = y$, então a ordem de xy, sendo um divisor de 21, deve ser igual a 21, de modo que G é cíclico.

Os casos em que $i \equiv 2$ ou 4 *mod* 7 produzem grupos isomorfos pois se y é um elemento de ordem 3 para os quais $yxy^{-1} = x^2$, então $z = y^2$ é um elemento de ordem 3 para os quais $zxz^{-1} = x^4$. Assim, via isomorfismo, existem dois grupos com 21 elementos, o grupo cíclico e que, com a apresentação

$$\langle x, y \ ; \ x^7 = 1 = y^3 \ e \ yxy^{-1} = x^2 \rangle.$$

A fim de mostrar que existe um grupo com 21 elementos com esta apresentação, considere as matrizes com entradas em $\mathbb{Z}_7$:

$$X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}.$$

É fácil de verificar que essas matrizes satisfazem as relações do grupo de ordem 21.

(c) Grupos de Ordem 12

Em muitas situações os resultados Sylow são usados como ponto de partida para investigações mais detalhadas. Por exemplo, pode ser hábil para deduzir que um ou outro subgrupo de Sylow é normal, como consideraremos nas situações seguintes. Em geral, esses métodos não podem conduzir a uma classificação completa em si próprio. Observe que temos agora obteve algumas informações sobre a estrutura de todos os grupos com 11 elementos ou menos.

Lema 2.2.6 *Um grupo com 12 elementos ou tem um 2-subgrupo normal de Sylow normal ou um 3-subgrupo normal de Sylow.*

Demonstração: Observe que um 2-subgrupo de Sylow do grupo G de ordem 12 tem 4 elementos. O número de 3-subgrupos de Sylow é 1 ou 4. Mostramos que se este número é 4, então o número de 2-subgrupos de Sylow deve ser 1. Se G tem quatro 3-subgrupos Sylow distintos P_1, P_2, P_3, P_4, cada interseção $P_i \cap P_j (i \neq j)$ é um subgrupo próprio de P_i, um grupo com três elementos. Daqui resulta que $P_i \cap P_j = \{1\}$ para $i \neq j$. Assim, G contém a identidade, juntamente com oito elementos de ordem 3, dois deles ocorrendo em cada um dos quatro 3-subgrupos de Sylow. Apenas três elementos permanecem, e assim G tem um único 2-subgrupo de Sylow, este subgrupo de três elementos diferentes da identidade. ■

Observação 2.2.1 Uma classificação mais detalhada dos grupos com 12 elementos pode ser dada em um estudo mais aprofundado da Teoria dos Grupos Finitos. O argumento

usado para provar o lema acima é algo mais sofisticado do que um simples argumento de contagem, uma vez que olharam mais minunciosamente a possibilidade de que o grupo tinha mais de um 3-subgrupo de Sylow. Note que é importante a escolha da ordem dos números primos: se supunha que a G tinha três 2-subgrupos de Sylow T_1, T_2 e T_3, não poderíamos ter concluído que $T_1 \cap T_2 = \{1\}$, já que esta intersecção poderia conter dois elementos.

(d) Os grupos de ordem p^2q

Lema 2.2.7 *Se p e q são primos distintos, então um grupo de ordem p^2q tem um subgrupo normal de Sylow.*

Demonstração: O número de p-subgrupos de Sylow divide p^2q e não é um múltiplo de p, então é 1 ou q. Se $p > q$, então q não pode ser congruente a 1 *mod* p e assim o número de p-subgrupos de Sylow é 1, como requerido. Se, no entanto, $q > p$, poderia haver q p-subgrupos de Sylow se $q \equiv 1 \mod p$. Neste caso, o número de q-subgrupos de Sylow não é um múltiplo de q mas divide p^2q, por isso é 1, p ou p^2. Esse número não pode ser p (pois p não é congruente a 1 *mod* q). Se esse número fosse p^2, teríamos $p^2 \equiv 1 \mod q$, de modo que q iria dividir $(p-1)(p+1)$. Isso só pode ocorrer se q divide $p-1$ ou q divide $p+1$. No entanto, se $q > p$, então a única possibilidade é de $q = p+1$, que fazem p e q números primos consecutivos e por isso temos que p é 2 e q é 3. Neste caso, G tem 12 elementos, portanto o resultado segue então pelo lema anteriormente provado. ■

(e) Os grupos de ordem 24

Por fim, apresentaremos uma situação em que nem sequer é possível garantir que um p-subgrupo de Sylow é normal.

Lema 2.2.8 *Seja G um grupo com 24 elementos. Então G tem um subgrupo normal de ordem 8 ou tem um subgrupo normal de ordem 4.*

Demonstração: O número de 2-subgrupos de Sylow é 1 ou 3. Se esse número for 1, o 2-subgrupo de Sylow é um subgrupo normal de ordem 8. Por isso, suponha que G tem três 2-subgrupo de Sylow S_1, S_2, S_3 cada um dos quais tem ordem 8. Mas sabemos que se A e B são subgrupos finitos, então $|AB| = \frac{|A||B|}{|A \bigcap B|}$, donde o subconjunto S_1S_2 tem $2^3 2^3/2^r$ elementos, com $|S_1 \bigcap S_2| = 2^r$. Uma vez que S_1S_2 é um subconjunto de um grupo G com 24 elementos, segue-se que $2^3 2^3 \leq |S_1S_2| \cdot 2^r$ de modo que $64 = 2^6 \leq 24 \cdot 2^r$. Assim, $r \geq 2$. Uma vez que $S_1 \bigcap S_2$ é um subgrupo próprio de S_1, tem mais de 22 elementos, então é possível deduzir que, se G tem três 2-subgrupos de Sylow, logo a interseção de quaisquer dois deles tem ordem 4. ■

Seja $T = S_1 \bigcap S_2$ de forma que T tem 4 elementos. Como T é um subgrupo de S_1 de índice 2, T é um subgrupo normal de S_1. Do mesmo modo, T é um subgrupo normal de S_2. Assim S_1 e S_2 são os dois subgrupos de $N_G(T)$, então $H = \langle S_1, S_2 \rangle$ é um subgrupo de $N_T(G)$ e, portanto, T é um subgrupo normal de H. Como H é um subgrupo, ele contém S_1S_2. Vimos que contém S_1S_2 possui $2^6/2^2 = 16$ elementos. Uma vez que o único subgrupo de G que contém pelo menos 16 elementos é o próprio G, vemos que $H = G$ e assim T é um subgrupo normal de G de ordem 4.

Conclusão

O desenvolvimento deste estudo proporcionou o conhecimento introdutório da Teoria dos Grupos Finitos, onde podemos perceber o cumprimento de uma ordem gradual de conceitos de modo coerente com o nível de graduação. As representações de grupos por permutação são de grande importância por fundamentar conceitos de grande aplicabilidade na classificação de grupos e, portanto, no estudo dos grupos finitos em geral, tais como órbita, estabilizador, a equação das classes, p-grupos e Teoremas de Sylow. Permitindo assim a contagem de subgrupos normais algumas classes de grupos.

Referências Bibliográficas

DOURADO, Tiago. Elementos de Teoria dos Grupos. Três Lagoas: UFMS, 2009.

DURBIN, J. R. Modern Algebra (An Introduction). - New York: John Wiley & Sons, 1992.

FRALEIGH, J.B. A First Course in Abstract Algebra (7. ed). Addison Wesley , 1994.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de Álgebra. Rio de Janeiro: IMPA, 2010.

GONÇALVES, Adilson. Introdução à Álgebra. Rio de Janeiro: IMPA, 2008.

HERSTEIN, I. N. Álgebra moderna. Vera Cruz: Editorial Trillas, 1980.

HUMPHREYS, John. F. A Course in Group Theory. Oxford: Oxford University Press, 1980.

MILIES, Cesar Polcino. Breve História da Álgebra Abstrata. São Paulo: IMEUSP, 2009.

AZNAR, Enrique R. Disponível em: <http://www.ugr.es/ eaznar/sylow.htm>. Acesso em Março de 2011.

DONOSO, José Pedro. Disponível em: <http://www.ifsc.usp.br/ donoso/espectroscopia/ Simetria.pdf>. Acesso em Junho de 2011.