UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE EDUCAÇÃO E SAÚDE

UNIDADE ACADÊMICA DE FÍSICA E MATEMÁTICA

LICENCIATURA PLENA EM MATEMÁTICA

MARCIEL SANTIAGO DE OLIVEIRA

GRUPOS FINITOS E O TEOREMA DE LAGRANGE

Cuité - PB

2016

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE EDUCAÇÃO E SAÚDE

UNIDADE ACADÊMICA DE FÍSICA E MATEMÁTICA

LICENCIATURA PLENA EM MATEMÁTICA

MARCIEL SANTIAGO DE OLIVEIRA

GRUPOS FINITOS E O TEOREMA DE LAGRANGE

Cuité - PB

2016

FICHA CATALOGRÁFICA ELABORADA NA FONTE
Responsabilidade Jesiel Ferreira Gomes – CRB 15 – 256

O48g Oliveira, Marciel Santiago de.

Grupos finitos e o teorema de Lagrange. / Marciel Santiago de Oliveira. – Cuité: CES, 2016.

46 fl.

Monografia (Curso de Licenciatura em Matemática) – Centro de Educação e Saúde / UFCG, 2016.

Orientador: Msc. Jussiê Ubaldo da Silva.

1. Teorema de Lagrange. 2. Grupos. 3. Ciclos de permutações. I. Título.

Biblioteca do CES - UFCG CDU 512

MARCIEL SANTIAGO DE OLIVEIRA

GRUPOS FINITOS E O TEOREMA DE LAGRANGE

TCC apresentado ao curso de Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande em cumprimento às exigências do Componente Curricular Trabalho Acadêmico Orientado, para obtenção do grau de Licenciado em Matemática.

Comissão Examinadora:

Prof.Ms. Jussiê Ubaldo da Silva.

(Orientador)

Prof. Dr.Aluízio Freire da Silva Junior

(Examinador)

Prof. Ms. Marciel Medeiros de Oliveira

(Examinador)

Aprovado em: ___/___/___

Agradecimentos

A Deus, por permitir concretização deste Trabalho.

Aos meus pais, acolher e encorajar - me.

As Pessoas Especiais, que fazem parte da nossa vida.

Ao Meu filho: por ser ponte reflexão na minha vida.

A Toda Família, que apoiaram nesta luta.

Ao Meu orientador, Professor Jussiê Ubaldo da Silva, pela paciência e incetivo.

Aos Meus amigos, que apoiaram, incentivando e caminharam ao meu lado.

Aos Meus Mestres, que ajudaram a encarar as dificuldades, dados seus princípios éticos, didáticos e enriquecendo nosso conhecimento.

A todos Aqueles, que testemunharam esta caminhada e auxiliaram na conclusão deste curso.

Aos meus pais pela perspectiva, apoio e paciência,
além de sempre incentiva para esse momento chegasse.

"Quem quer que imagine que a álgebra é um artifício para achar quantidades desconhecidas pensou em vão. Não se deve dar atenção ao fato da álgebra e a geometria serem diferentes na aparência. As álgebras são fatos geométricos que são provados "

Omar khayyam

Resumo

Neste trabalho, vamos falar de grupos finitos e provar o Teorema de Lagrange, dando algumas de suas aplicações. No capitulo 1, definimos Grupos, com suas propriedades, e subgrupos. Construirmos os grupos das classes residuais $\mathbb{Z}_n$ e o grupo das permutações S_n. No capitulo 2, Definimos as classes laterais, e provamos o Teorema de Lagrange. No Capitulo 3, damos algumas das aplicações do Teorema de lagrange e falamos um pouco sobre sua recíproca, que não é válida.

Palavras-chave: Grupos. Subgrupos gerados. Classes Laterais. Teorema Lagrange. Permutações. Ciclos de permutações.

Abstract

In this work, let's talk about finite groups and prove the Lagrange's Theorem, giving some of its applications. In Chapter 1, we define Groups, with their properties, and subgroups. We building the groups of the residual classes Z_n and the group of the permutations S_n. At the Chapter 2, we define the cosets, and we proved the Lagrange's Theorem. At the Chapter 3, we give some of the Theorem applications lagrange and we talked a little bit about their reciprocal, that is not valid.

Keywords: Groups. Generated subgroups. Cosets. Lagrange theorem. Permutations, Permutations cycles.

Sumário

Introdução

O conceito de número é algo fascinante no sentido de poder representar diversas situações ou problemas, como por exemplo o número 2, que pode representar dois celulares, duas laranjas, dois navios, duas pessoas, etc. Assim, partindo dessa ideia, em matemática, quando resolvemos uma equação, essa mesma pode representar um problema de economia, um problema da área biológica, um problema da área de engenharia ou simplesmente um problema do cotidiano das pessoas comuns. No entanto, esta equação para ser resolvida, não é necessário saber qual problema a originou. Assim, a matemática, como também a álgebra em particular, foi sendo desenvolvida a partir de problemas dentro da própria matemática, e isso é algo extraordinário. Esses fatos, são facilmente percebido quando estudamos um pouco seu desenvolvimento.

Euclides de Alexandria foi um dos matemáticos mais notório, que no reinado de Ptolomeu I, por volta 306 A.C. foi chamado para Alexandria no Egito. Sua Obra "Os elementos"nos traz todos conhecimentos matemáticos até então não visto em publicações. No "os Elementos"temos nos volumes II,V,VI,VII,VIII e IX, muitas proposições e teoremas representados de forma geométrica, que hoje foram reformulados e utilizamos na Álgebra e Teoria dos Números, que para época era os inteiros positivos ($\mathbb{N}$).

Um outro matemático importante da mesma época foi Apolônio de Perga (262 a 190 A.C.), precursor da geométrica analítica de Fermat, na sua obra restaurada de "Lugares Planos", já utilizava problemas envolvendo equações quadráticas do tipo $ax - x^2 = bc$. Ele na sua obra "As cônicas"deu um nova visão sobre os trabalhos de Euclides, inovando no método e indo além em algumas demonstrações.

No período que vai até 500 D.C. surgiram alguns algebristas, como o sírio Nicômaco de Gerasa (100 D.C.) com a obra "A Introduction arithmetica", neopitagórico. O maior algebrista grego foi Diofante de Alexandria, chamado pai da álgebra, com sua

obra "Arithmetica"uma coleção de aplicações algébricas, na sua maioria envolvendo equações quadrática. Foi uma ruptura aos padrões gregos, que achavam mais próximo a álgebra dos babilônios. Por volta de 320 D.C., Papus de Alexandria lança a obra "Coleção"com oito volumes onde faz relatos históricos e revisão das obras de Euclides, Arquimedes, Apolônio, Ptolomeu e entre outros matemáticos. Dando novos resultados e apresentando fatos não conhecidos das obras clássicas.

No período chamado de Idade média do século VI à XVI D.C. o ocidente estagnou para na produção dos estudos matemático, pois os reinos europeus focaram em se defender das invasões dos povos inimigos e a religião ganhou destaque e promoveu uma desvalorização dos conhecimentos que não fosse religiosos. Os principais matemáticos se sentidos perseguidos foram se exilando no oriente e boa parte foi para Pérsia, e dela para Índia e China, com essa mistura de conhecimentos, por volta de 628 D.C., Brahmagupta da Índia Central contribuiu para álgebra com soluções gerais para equações quadráticas, incluído solução negativa e zero, até mesmo de todas soluções inteiras das equações lineares diofantina $ax + by = c$, onde o próprio Diofante tinha se contentado em mostrar uma particular e outra indeterminada. Outro Matemático indiano foi mais importante do século doze, Bhaskara, preenchendo lacunas na obra Brahmagupta com a divisão por zero, o qual afirmou de que tal quociente é infinito e deu uma solução final para a equação de Pell, suas obras foram "Vija-Ganita"e "Lilavati "que contém vários problemas de equações lineares e quadráticas.

Já no século IX, surgiu o matemático, Al-Khowarizmi, que deu origem a palavra "álgebra"que é a tradução de uma das palavras de suas obra, a "Al-jabr wa'l muqabalah ". O ocidente, além de adotar como um ramo da matemática, ainda lhe homenageou com seu nome o sistema numérico indo-arábico, Algorismo ou algoritmo. Outro árabe que contribuiu no desenvolvimento da Álgebra foi Omar Khayyam que em sua obra "a Álgebra ", deu os primeiros passos para generalização do método par solução das equações cúbicas.

O ocidente passou vários séculos sem produzir matemática, devido as restrições dos governantes da chamada Idade média, e depois a religião por não aceitar outras culturas religiosas em seus domínios. No século doze, houve o primeiro contato com os árabes, principalmente na Espanha onde os árabes dominaram por alguns anos, deixando grande influencia, e começaram as traduções das obras para o latim dando um novo impulso no conhecimento matemático. Em 1202, Leonardo Fibonacci com

sua obra "Liber abaci", trata de método e problemas algébricos usando os numerais indo-arábicos.

No século XIV, Nicolas Chuquet, na sua obra "Triparty en la science des nombres", da uma nova visão nos termos matemáticos, entre eles chama a álgebra de regras da incógnita, deu nome as quarto operações fundamentais, inventor notações importantes para exponenciais. Foi nesta obra que apareceu uma equação igual a um número negativo, $4x = -2$, e se deparou nas solução das equações da forma $ax^m + bx^{m+n} = cx^{m+2n}$, com os números imaginários, os quais não os reconheciam e quanto ao zero. ele rejeitava.

No início do século XVI e num processo de rivalidade entre grandes matemático houve um grande impulsou na álgebra, um exemplo disso foi a disputa pela resolução das equações de grau 3, tendo um dos precursores o matemático italiano Scipione del Ferro (1465-1526) com a resolução das equações cubicas $x^3 + px = q, (p, q > 0)$, onde ele tinha um método para solução como raízes cúbicas, hoje nós expressamos pela fórmula

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2}^2) + (\frac{p}{3})^3}} - \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}.$$

Teve como grande rival o matemático Nicallo Fontana (1500-1557), também conhecido por Tartaglia, o mesmo lançou um desafio dos métodos para resolver todas equações algébrica e se era resolúvel por radicais, coube o discípulos de del Ferro, Antônio Maria Fior, aceita o desafio e perdeu.

Em 1545, o também italiano Geônimo Cardano (1501-1576), na obra "Ars magna" divulgou os métodos de Tartaglia para equações cúbicas e quádricas e Ludovico de Ferrari (1522-1565) para redução de uma equação polinomial de $4^{\underline{o}}$ grau a uma equação de $3^{\underline{o}}$ grau. Cardano utilizou os métodos de Del Ferro e Tartaglia para provar que todas as equações de $4^{\underline{o}}$ grau para uma equação é solúveis por radicais nos racionais. Na mesma época, o italiano Rafael Bombelli (1526-1573), criou um método para equações que Cardano chamava resolúveis, as que apresentavam soluções com números racionais ou negativos. Mas só funcionava para equações já resolvida, sem perceber, construiu os primeiros elementos para os Números Complexos, cunhando o conceito de imaginário conjugado.

Ainda na mesma época, o francês François Viéte (1540 - 1603), também deu uma grande contribuição para álgebra, introduziu o uso de vogais para representar uma quantidade supostamente desconhecida ou indeterminada, e uma consoante para

representar uma grandeza ou números supostamente conhecidos ou dado, a qual mudou a visão de mostrar algo particular para dar uma informação mais geral. Defendia que a analise lógica deveria ser seguida da demonstração sintética, a qual chamou de "a arte analítica ". Além de apresenta um método mais simplificado para equações cúbicas entre outras contribuições que esta na sua obra de 1591, Isagoge (ou Introdução).

Um outro matemático que merece destaque por suas obras é o francês René Descartes (1596 -1650), que fez uma revolução no modo de pensar na sua época, na álgebra reformulou a maneira de representar as equações determinadas, simplificando a utilização das letras iniciais do alfabeto para indicar coeficientes e as finais para incógnitas, e adotou os símbolos de $+$ e $-$. Na sua obra "La géométrie"dá origem a um no ramos da matemática, a geometria analítica, onde ele conseguiu mostrar resultados geométricos através da álgebra, libertando das construções de diagramas e dando significado às operações da álgebra por meio de interpolações geométricas. Descartes mesmo simplificando as equações só apresentou métodos para resolução de equações até quarto grau.

O francês Pierre de Fermat (1601 - 1665), um outro notório matemático, por apreciar a matemática como um lazer, nunca se interessou em publicar suas descobertas em matemática, mas após sua morte seu filho reuniu seus escritos e foi feito a obra "Introdução aos lugares de Fermat ", onde tinha vários teorema da teoria dos números e uma geometria analítica parecida com a de Descartes, que partia das equações indeterminadas, mas se tivesse sido publicada teria ofuscado a de Descartes por ter data anterior. Em vida o que se conhecia das descobertas de Fermat foram os que seus amigos publicaram e deram créditos a ele.

Ainda no século XVII o matemático Gottfried Wilhelm Leibniz (1646-1716) foi um dos maiores formadores de notações, entre eles o ponto ($\cdot$) para multiplicação, dois pontos (:) para divisão de proporções, o símbolo de igualdade ($=$), semelhança ($\sim$), congruência a ($\simeq$). Trabalhou com um conceito de álgebra da lógica, mais o não foi muito apreciado pelo seu contemporâneos.

O britânico Conde Ehrenfried Walter Von Tschirnhaus (1651-1708), deu uma contribuição muito importante para álgebra moderna, que ficou conhecido como as Transformações de Tschirnhaus onde ele esperava achar o método para resolver as equações de grau n. Sua obra "Acta Eruditorum ", mostrou que polinômios grau $n > 2$ poderia ser reduzindo $n-1, n-2$ e $n-3$, mas o alcance do método foi limitado pois

as equação de grau superior ou igual cinco em geral não são resolúveis algebricamente, mas fui um avanço para álgebra da época.

Na segunda metade do século XVII o matemático ítalo - fancês Joseph - Louis Lagrange (1736 - 1813), lançou a obra Réflexions la résolution algébrique des équations (Reflexões sobre a resolução algébrica de equação)(1770 - 1771) que abordou a resolução de problema utilizado a "teoria das permutações"para resolução de equações.

Niels Henrik Abel (1802-1829), matemático norueguês, teve grande contribuição no desenvolvimento dos conceitos de grupo. Em 1824, ele provou que para a equação polinomial $x^5 - 6x + 3 = 0$ não é solúvel por radicais sobre os racionais, daí veio outro duvida para quais equações de $5^{\underline{o}}$ grau seria solúveis nos radicais sobre os racionais. Esse foi dos grandes feitos provou uma suspeita do próprio Lagrange que não haveria nenhuma formula geral por radicais para resolver equações de grau $\geqslant 5$ e ainda, a palavra "abeliano"é uma referência ao seu nome.

Foi dada por Evarist Galois (1811-1832), a introdução do conceito de grupo, que associou a cada equação polinomial de grau n, um grupo formado por permutações de raízes da equação. Depois provou que a equação é solúvel por radicais sobre $\mathbb{Q}$ se, e somente se, este grupo tem certas propriedades específicas. Outro grande matemático que contribui bastante para o desenvolvimento dos grupos algébricos foi inglês Artur Cayley (1821- 1899), que tem como principais contribuições as tabua de operação de grupo, introdução das matrizes na matemática, além de valoriza os aspectos formais da matemática, considerando o percursor do estudo da teoria dos grupos.

Neste trabalho vamos falar o teorema de Lagrange, garantindo para qualquer grupo finito G que a ordem de qualquer subgrupo de G divide sua ordem.

Para provar o Teorema de Lagrange vamos precisar de alguns conceitos e resultados, que serão tratados no capítulo I, onde iremos ver alguns grupos finitos importantes e também definir subgrupos, alguns resultados importantes e a noção de grupo finito e ordem de um elemento do grupo.

No capítulo II , vamos falar sobre classes laterais e provar o teorema de Lagrange. E no capítulo III, apresentaremos algumas consequências do teorema de Lagrange e falaremos sobre a recíproca do Teorema de Lagrange.

Capítulo 1

GRUPOS

Neste capítulo iremos mostrar as principais definições e resultados sobre Grupos e subgrupos, para garantir os elementos básicos na construção do Teorema de Lagrange.

1.1 Grupos

Nesta seção apresentaremos a definição de grupo e algumas propriedades básicas.

Definição 1.1. *Um conjunto não vazio G, munido de uma operação $*$ é chamado $(G, *)$ de* ***grupo****, se satisfaz as seguintes propriedades:*

1. *Associatividade:*

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

2. *Elemento neutro:*

   $\exists\ e \in G$ *tal que* $e * a = a * e = a$, $\exists\ a \in G$

3. *Inverso:* $\forall\ a \in G, \exists\ a' \in G$ *tal que* $a * a' = a' * a = e$

   Um elemento $a' \in G$ chama - se ***inverso*** *de a com relação à operação $*$. O conjunto dos elementos invertíveis em G será indicado por $\mathcal{U}(G)$, ou seja,*

$$\mathcal{U}(G) = \{a \in G \mid \exists\ a' \in G \text{ com } a * a' = a' * a = e\}.$$

Assim, denotaremos por $(G, *)$, o conjunto G com a operação " $*$ " satisfazendo as condições acima.

Observação 1.1. *:*

1 - *O grupo $(G, *)$ será abeliano ou comutativo se valer $a * b = b * a$; $\forall a, b \in G$*

2 - *A partir daqui, por questões de simplificação, adotaremos a notação multiplicativa para a operação do grupo G. Assim, em vez de $(G, *)$, usaremos $(G, \cdot)$ e $a * b$ por $a \cdot b$ ou simplesmente por ab. E por fim, para o inverso de $a \in G$ usaremos a^{-1}.*

3 - *Se não houver confusão quanto a operação de $(G, *)$, denotaremos apenas por G.*

1.1.1 Propriedades Básicas de Grupo

1. O elemento neutro é único .

   De fato, supondo que existem $e, e' \in G$ elementos neutros de G, temos que

   $$e = e \cdot e' = e',$$

   portanto, podemos concluir que $e^{'} = e$.

2. O elemento inverso é único em G.

   De fato, sejam $a \in G$, e b, $b' \in G$ dois elementos inversos de a. Daí temos que $a \cdot b = e = a \cdot b'$, mas

   $$b = b \cdot e = b(a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'.$$

   Portanto, $b = b'$ e denotamos por o elemento inverso a^{-1} .

3. Para todo $a, x \in G$, se $a \cdot x = a \cdot y$, então $x = y$.

4. Seja G é um Grupo. Se $a, b \in G$, então $(ab)^{-1} = b^{-1}a^{-1}$.

   Temos que $(ab)^{-1} \cdot (ab) = e$. Agora multiplicamos por b^{-1} os dois lados da igualdade e teremos:

   $$(ab)^{-1} \cdot (ab) \cdot (b^{-1}) = eb^{-1} \Rightarrow$$

   $$\Rightarrow (ab)^{-1}(abb^{-1}) = b^{-1} \Rightarrow$$

   $$\Rightarrow (ab)^{-1}(ae) = b^{-1} \Rightarrow$$

   $$\Rightarrow (ab)^{-1}a = b^{-1}$$

   Agora multiplicamos por a^{-1} os dois lados da igualdade teremos:

   $$(ab)^{-1}aa^{-1} = b^{-1}a^{-1} \Rightarrow$$

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

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

5. $(a^{-1})^{-1} = a$, $\forall a \in G$.

   Por definição sabemos que $a^{-1} \cdot a = e$, então $(a^{-1})^{-1} = a$, temos

   $a^{-1} \cdot (a^{-1})^{-1} = (a^{-1} \cdot a)^{-1} = e$,

   Como o inverso é único satisfazendo essa condição, podemos dizer que $a = (a^{-1})^{-1}$.

6. Seja G um grupo, com a e b dois elementos de G. Temos que as equações $ax = b$ e $ya = b$, tem uma única solução em G.

   Primeiro mostraremo a existência de solução para $ax = b$.

   De fato, pelo inverso de a, temos que

   $$a^{-1} \cdot a \cdot x = a^{-1} \cdot b \Longrightarrow$$
   $$\Longrightarrow x = a^{-1} \cdot b$$

   De modo semelhante temos para $y \cdot a = b$

   $$y \cdot a \cdot a^{-1} = b \cdot a^{-1} \Longrightarrow$$
   $$\Longrightarrow y = b \cdot a^{-1}$$

   Como o inverso de a é único, concluímos que as soluções $x = a^{-1} \cdot b$ e $y = b \cdot a^{-1}$ são únicas para essas equações.

Exemplo 1.1.1. *:*

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *, são grupos abelianos, pois quaisquer elementos a e b pertencente a um desses grupos, teremos* $a + b = b + a$.

2. $(\mathbb{Q}^*, \cdot)$ *é um grupo. Seja* $a, b, c \in \mathbb{Q}^*$*, como o zero não faz parte do conjunto, vale a associatividade, existe um elemento neutro e inverso.* $(\mathbb{Q}, \cdot)$ *não é grupo,* 0 *não tem inverso em* $(\mathbb{Q}, \cdot)$. $(\{1; -1\}, \cdot), (\mathbb{R}^*, \cdot)$.

3. *Dados* $n \in \mathbb{Z}, n > 0$*, considere o conjunto* $C_n = \{z \in \mathbb{C} | z^n = 1\}$, . $z_1, z_2 \in \mathbb{C}$.

   $$z_1^n = z_2^n = 1 \Longrightarrow (z_1 \cdot z_2)^n = z_1^n \cdot z_2^n = 1.1 = 1.$$

   C_n*, munido do produto usual dos números complexos é um grupo abeliano chamado* **grupo das raízes unitárias da unidade de** $\mathbb{C}$.

4. *Considere* $n \in \mathbb{Z}, n \geqslant 1$ *e tomemos o conjunto*

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid detA \neq 0\}$$

que, munido do produto usual de matrizes é um grupo, chamado **grupo linear de grau** n *sobre* $\mathbb{R}$.

5. *Sejam* H_1 *e* H_2 *subgrupos de* G *então* $H_1 \cap H_2$ *é um subgrupo de* G. *Em geral uma união qualquer de subgrupos é um subgrupo de* G.

1.1.2 Potências Múltiplos em um Grupo

- **Potência**

Definição 1.2. *Seja* G *um Grupo,* $a \in G$ *e* $n \in \mathbb{Z}$. *Definimos*

$$a^n = \begin{cases} e\ , & se\ n{=}0 \\ \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n\ vezes} & se\ n > 0 \\ (a^n)^{-1} & se\ n < 0 \end{cases},$$

Proposição 1.1. *Se* G *é um grupo e* $a \in G$ *então:*

a) $a^{n+m} = a^n \cdot a^m, \forall\ m, n \in \mathbb{Z}$.

b) $(a^n)^m = a^{n \cdot m}, \forall\ n, m \in \mathbb{Z}$.

c) $a^{-n} = (a^n)^{-1}$.

A demonstração [2] (DOMINGUES, 2003, p.174)

- **Soma**

Definição 1.3. *Seja* G *um Grupo,* $a \in G$ *e* $n \in \mathbb{Z}$. *Definimos*

$$na = \begin{cases} e\ , & se\ n{=}0 \\ \underbrace{a + a + a + \ldots + a}_{n\ vezes} & se\ n > 0 \\ (-1)(na) & se\ n < 0 \end{cases},$$

Proposição 1.2. *Se* G *é um grupo e* $a \in G$ *então:*

a) $(m + n)a = na + ma, \forall\ m, n \in \mathbb{Z}$.

b) $n(ma) = (nm)a, \forall\ n, m \in \mathbb{Z}$.

c) $(-n)a = (-1)na$.

A demonstração [2] (DOMINGUES, 2003, p.176)

Observação 1.2. *Note que em $m+n$ e mn, temos a soma e o produto usual dos inteiros respectivamente. E, em $na+ma$ e $a^n \cdot a^m$ temos a operação do grupo G.*

1.1.3 Grupo Finito

Definição 1.4. *1. Definimos a* **ordem** *de um grupo, como sendo a sua cardinalidade.*

2. Se G é um conjunto finito com n elementos, dizemos que grupo G é ***grupo finito*** *de ordem n, denotaremos sua ordem por $|G| = n$. Caso G tem número de elementos infinitos G é um* ***grupo infinito****.*

Observação 1.3. *A notação $|G|$ é usada apenas quando G é finito.*

Exemplo 1.1.2. *O conjunto $G = \{-1, 1\} \subseteq \mathbb{Z}$; é um grupo abeliano multiplicativo, Note ainda que o elemento neutro é 1, o inverso de 1 é -1, e o inverso de -1 é 1, denotaremos $\mathcal{U}(\mathbb{Z})$ [6](JANESCH, 2008, p.28), cujas operações são descritas na seguinte tabela.*

$\cdot$	*1*	*-1*
1	*1*	*-1*
-1	*-1*	*1*

A tabela acima é chamada de ***tábua do Grupo*** *G.*

1.2 A Classe Residual $\mathbb{Z}_n$

Definição 1.5 (**Congruência**). *Sejam $a, b, q \in \mathbb{Z}$ e $n \in \mathbb{Z}_+^*$. Dizemos que a é congruente a b módulo n se $n|(a-b)$, isto é $a-b = nq$. Denotaremos essa congruência usando a notação $a \equiv b \ (mod\ n)$.*

Propriedades básicas de congruência

- ***Reflexividade*** $a \equiv a(mod\ n)$

  De fato, $a - a = 0$ é divisível por n

- ***Simétrica*** *Se $a \equiv b(mod\ n)$, então $b \equiv a(mod\ n)$.*

  Se $a \equiv b(mod\ n)$, então $n|(b-a)$, ou seja, $a - b = nq$ para algum q. Daí $b - a = n(-q)$, portanto, $n|b-a$. Logo, $b \equiv a(mod\ n)$.

- ***Transitividade*** *Se $a \equiv b(mod\ n)$ e $b \equiv c(mod\ n)$, então $a \equiv c(mod\ n)$.*

  Por hipótese, temos que $n|(b-a)$ e $n|(c-b)$. Daí, $n|[(b-a)+(c-b)]$, ou seja, $n|(c-a)$. Logo, $n|(a-c)$. Portanto, temos que $a \equiv c(mod\ n)$.

Observação 1.4. *As demais propriedades podem serem vistas em [2] (DOMINGUES, 2003, p.54)*

Considere sobre $\mathbb{Z}$ a congruência "$\equiv (mod\ n)$", com $n \geq 2$, ou seja, dados $x, y \in \mathbb{Z}$ temos que

$x \equiv y(mod\ n) \iff n \mid (x-y)$.

Considere agora $a \in \mathbb{Z}$, chamaremos de classe residual módulo n ou classe de resíduos, denotado por $\overline{a}$, o conjunto

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a(mod\ n)\}$$

Assim

$x \in \overline{a} \iff x \equiv a(mod\ n) \iff n \mid (x-a)$.

Agora dividindo a por n, pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$, tais que $a = qn + r$, com $0 \leq r \leq n-1$, daí

$$a - r = qn \Longrightarrow n \mid (a-r) \Longrightarrow a \equiv r(mod\ n) \tag{1.1}$$

.

Assim por definição $a \in \overline{r}$.

Considerando $x \in \overline{a}$, então $x \equiv a(mod\ n)$, por (1.1) e usando transitividade temos $x \equiv r(mod\ n)$, então $x \in \overline{r}$ e assim $\overline{a} \subset \overline{r}$.

Por outro lado, se $x \in \overline{r}$, então $x \equiv r(mod\ n)$, e de (1.1), temos $r \equiv a(mod\ n)$, por transitividade $x \equiv a(mod\ n)$, ou seja, $x \in \overline{a}$ e dai $\overline{r} \subset \overline{a}$, portanto $\overline{a} = \overline{r}$, onde $r \in \{0, 1, 2, \ldots, n-1\}$.

Mostremos agora que as classes $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ são todas distintas. Para isso consideremos $\overline{r}, \overline{s} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ tal que $\overline{r} = \overline{s}$. Daí,

$\overline{r} = \overline{s} \Longrightarrow r \in \overline{s} \Longrightarrow r \equiv s(mod\ n) \Longrightarrow n \mid (r-s)$, mas,

$r - s < n$, logo $n \nmid (r-s)$,

portanto $\overline{r} \neq \overline{s}$.

Então, denotaremos por $\mathbb{Z}_n$ todas as classes residuais módulo n, ou seja,

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Exemplo 1.2.1. *Para $n = 2, temos\ \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. Assim,*

$\overline{0} = \{x \mid x \equiv 0(mod\ 2)\} \iff 2|x \iff x = 2q,\ q \in \mathbb{Z}$, *logo*

$$\overline{0} = \{x \in \mathbb{Z} \mid x = 2q, q \in \mathbb{Z}\}$$

.

$\overline{1} = \{x \in \mathbb{Z} \mid x \equiv 1(mod\ 2)\} \iff 2 \mid (x-1) \iff x - 1 = 2q \iff$
$x = 2q + 1, \quad q \in \mathbb{Z}$, *logo*

$$\overline{1} = \{x \in \mathbb{Z} \mid x = 2q + 1,\ q \in \mathbb{Z}\}$$

Exemplo 1.2.2. *Considere $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Temos que:*

$\overline{0} = \{x \mid x \equiv 0(mod\ 3)\} \iff 3 \mid x \Longrightarrow x = 3q,\ q \in \mathbb{Z}$.

Logo,

$$\overline{0} = \{x \in \mathbb{Z} \mid x = 3q, \quad q \in \mathbb{Z}\}$$

$\overline{1} = \{x \mid x \equiv 1(mod\ 3)\} \iff 3 \mid x - 1 \iff x - 1 = 3q \iff x = 3q + 1$. *Logo,*

$$\overline{1} = \{x \in \mathbb{Z} \mid x = 3q + 1, \quad q \in \mathbb{Z}\}$$

.

$\overline{2} = \{x \mid x \equiv 2(mod\ 3)\} \iff 3 \mid x - 2 \iff x - 2 = 3q \iff x = 3q + 2,\ q \in \mathbb{Z}$.

Logo,

$$\overline{2} = \{x \in \mathbb{Z} \mid x = 3q + 2, \quad q \in \mathbb{Z}\}.$$

1.2.1 Soma em $\mathbb{Z}_n$

Definamos em $\mathbb{Z}_n$ a operação **Soma** como sendo

$$\begin{aligned} \oplus : \qquad & \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) \longrightarrow \overline{a} \oplus \overline{b} = \overline{a + b} \end{aligned}$$

onde "+ "abaixo dos traços é a soma usual dos inteiros. Note que em $(\mathbb{Z}_n, \oplus)$ valem:

1. **Associatividade**

$$\begin{aligned} (\overline{a} \oplus \overline{b}) \oplus \overline{c} &= (\overline{a + b}) \oplus \overline{c} \\ &= \overline{(a + b) + c} \\ &= \overline{a + (b + c)} \\ &= \overline{a} \oplus \overline{b + c} \\ &= \overline{a} \oplus (\overline{b} \oplus \overline{c}) \end{aligned}$$

2. Existe elemento neutro.

   Dado $\overline{a}, \overline{e} \in \mathbb{Z}_n$ tais que $\overline{a} + \overline{e} = \overline{a}$, temos

   $\overline{a} \oplus \overline{e} = \overline{a} \Longrightarrow \overline{a+e} = \overline{a} \Longrightarrow a + e \in \overline{a} \Longrightarrow a + e \equiv a(mod\ n)$,

   então $n \mid (a+e) - a \Longrightarrow n \mid e$. Como $e < n$, tem-se $e = 0$. Facilmente verifica-se que $\overline{a} \oplus \overline{0} = \overline{0} \oplus \overline{a} = \overline{a}$. Portanto, $\overline{0}$ é o elemento neutro de $(\mathbb{Z}_n, \oplus)$

3. Sejam $\overline{a}, \overline{c} \in \mathbb{Z}_n$, tais que $\overline{a} \oplus \overline{c} = \overline{0}$, temos

   $\overline{a+c} = \overline{0} \Longrightarrow a + c \in \overline{0},\ a + c \equiv 0(mod\ n) \Longrightarrow n \mid a + c$
   $\Longrightarrow \exists\ q \in \mathbb{Z};\ a + c = nq \Longrightarrow c = nq - a \Longrightarrow \overline{c} = \overline{nq} + \overline{-a} \Longrightarrow \overline{c} = \overline{0} + \overline{-a} \Longrightarrow$
   $\overline{c} = \overline{n} + \overline{-a} \Longrightarrow \overline{c} = \overline{n-a}$.

Portanto, dado $\overline{a} \in \mathbb{Z}_n$, $\overline{n-a}$ é o simétrico de $\overline{a}$ e assim $(\mathbb{Z}_n, \oplus)$ é um grupo com a operação "$\oplus$".

Exemplo 1.2.3. *Considere o grupo* $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$*, e sua* **tábua** *de operação*

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

1.2.2 Produto em $\mathbb{Z}_n$

Definamos em $\mathbb{Z}_n$ a operação **Produto** como sendo

$$\begin{aligned} \odot: \qquad & \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) \longrightarrow \overline{a} \odot \overline{b} = \overline{a \cdot b} \end{aligned}$$

onde "$\cdot$ "abaixo dos traços é o produto usual dos inteiros.

Exemplo 1.2.4. *Aqui, temos a tábua de operação de* $\mathbb{Z}_4$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}_n$ com o produto "$\odot$"vale:

1. **Associatividade**

   Dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ temos,

   $\overline{a} \odot (\overline{b} \odot \overline{c}) = \overline{a} \odot (\overline{b \cdot c}) = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot b} \odot \overline{c} = (\overline{a} \odot \overline{b}) \odot \overline{c}$

2. **Elemento Neutro**

   $\overline{1} \odot \overline{a} = \overline{1 \cdot a} = \overline{a}$

   $\overline{a} \odot \overline{1} = \overline{a \cdot 1} = \overline{a}$

   Portanto $\overline{1}$ é o elemento neutro.

3. **Inverso Multiplicativo**

   Dado $\overline{a} \in \mathbb{Z}_n$, vamos procurar uma critério para saber se $\overline{a}$ é inversível em $\mathbb{Z}_n$. Para isso, suponhamos que exista $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1}$. Logo, se $\overline{a} \cdot \overline{b} = \overline{1}$, segue que $\overline{a \cdot b} = \overline{1}$, daí, $a \cdot b \in \overline{1}$, então

   $a \cdot b \equiv 1 \ (mod\ n) \Longrightarrow n \mid (ab - 1)$,

   logo existe $k \in \mathbb{Z}$ tal que

   $ab - 1 = nk \Longrightarrow ab - nk = 1 \Longrightarrow ab + n(-k) = 1 \Longrightarrow mdc(a, n) = 1.$

   Reciprocamente, se o $madc(a, n) = 1$, pela identidade de Bezout [6] (JANESCH, 2008, p.118), existem $x, y \in \mathbb{Z}$ tal que $ax + ny = 1$, mas,

   $ax + ny = 1 \Longrightarrow \overline{ax + ny} = \overline{1} \Longrightarrow \overline{ax} + \overline{ny} = \overline{1} \Longrightarrow \overline{a} \cdot \overline{x} + \overline{n} \cdot \overline{y} = \overline{1} \Longrightarrow$
   $\Longrightarrow \overline{a} \cdot \overline{x} + \overline{0} \cdot \overline{y} = \overline{1} \Longrightarrow \overline{a} \cdot \overline{x} = \overline{1}.$

   Portanto, Existe $\overline{b} \in \mathbb{Z}_n$ tal que

$$\overline{a} \cdot \overline{b} = 1 \Longleftrightarrow mdc(a, n) = 1 \tag{1.2}$$

Assim, com base em (1.2) para obter um grupo multiplicativo em $\mathbb{Z}_n$, temos que excluir a classe $\overline{0}$ e exigir que n seja primo, ou seja, sendo $\mathbb{Z}_n^* = \mathbb{Z}_n - \{\overline{0}\}$

$(\mathbb{Z}_p^*, \odot)$ é um grupo, se, e somente se, p é primo.

1.3 O Grupo das Permutações

A permutação é o termo específico usado na teoria dos grupos para designa um bijeção de um conjunto nele mesmo. Se X um conjunto não vazio, e denotamos por S_X o conjunto das permutações dos elementos de X. A composição de aplicação, isto é, $S_X = \{f : X \longrightarrow X \mid f \text{ é } bijetora\}$ sendo " $\circ$ " a composição de função , temos que $(S_X, \circ)$ é um grupo, chamado de grupo simétrico sobre X (ou grupo das permutações sobre X).

Se X é finito, então S_X é finito e $|S_X| = n(X)!$, onde $n(X)$ é o número de elementos de X.

Provaremos essa afirmação por indução.

i)Note que, para $n = 1$ é verdadeira, pois se X possui um elemento, então só existe um função que associa esse elemento a ele mesmo, daí $|S_n| = 1 = 1!$

ii) Supondo verdade para $n = k$, ou seja, supondo que X possui k elementos, então $|S_X| = k!$. Agora, considerando $X = \{1, 2, \ldots k, k+1\}$, seja $f \in S_X$, para que f seja bijetiva, temos que:

- 1 possui $k + 1$ possibilidades para associar os elementos de X.
- 2 possui k possibilidades para associar com os elementos de X.
- $\vdots$
- k possui2 possibilidades para associara com os elementos de X.
- $k + 1$ possui 1 possibilidade para associar com os elementos de X.

Desse modo, pelo princípio da contagem, existe $(k + 1) \cdot k \ldots 3 \cdot 2 \cdot 1 = (k + 1)!$ possibilidades para a função f, logo, $|S_X|!$.

Exemplo 1.3.1. *Se S_X é abeliano se, e somente se $|X| \leq 2$. De fato, se $|X| > 2$, considere $a, b, c \in X$ e $f, g \in S_X$*

Definimos f como sendo,

$f(a) = b$

$f(b) = a$

$f(x) = x \ \forall x \ \in X - \{a, b\}$

e definimos g como sendo,

$g(b) = c$

$g(c) = b$

$g(x) = x \ \forall x \in X - \{b, c\}$. *Note que,*

$f \circ g(a) = f(g(a)) = f(a) = b$ *e* $g \circ f(a) = g(f(a)) = g(b) = c$

Logo $f \circ g \neq g \circ f$ *Portanto* S_X *não é abeliano para* $|X| > 2$.

Exemplo 1.3.2. *Sendo* $I_n = \{1, 2, \cdots, n\}$, *denotamos* S_{I_n} *simplesmente por* S_n, *assim,* $|S_n| = n!$, *se* $\sigma \in S_n$, *denotamos* σ *por*

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \in S_n$$

.

Sejam $\sigma, \theta, \pi \in S_n$, a composição com essa notação é feita da seguinte forma:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ \theta(1) & \theta(2) & \cdots & \theta(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$

Onde $\pi(i) = (\sigma\theta)(i) = \sigma(\theta(i))$, com $i \in \{1, 2, \ldots n\}$

Para $n = 3$, temos o grupo S_3 cujas permutações são:

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

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

Considerando os elementos

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

temos

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

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

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

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

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, como foi visto antes.

1.4 Subgrupos

Definição 1.6. *Sejam G um Grupo e H um subconjunto não vazio de G. Então H é subgrupo de G (denotado $H < G$) , se, e somente se, as condições seguintes são satisfeitas:*

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

Observação 1.5. *:*

1. *Note que* **associatividade** *é válida para todos elementos de G.*
2. *O elemento neutro e_H de H é igual ao elemento neutro e em G.*

   De fato, se $a \in H$, temos $e_H \cdot a = a$, ao multiplicamos os dois lado a^{-1}, obtemos:

   $$e_H \cdot a \cdot a^{-1} = a \cdot a^{-1}$$

   $$e_H \cdot e = e, \text{ então } e_H = e.$$

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

   De fato, se k é o inverso de h em H, então $h \cdot k = k \cdot h = e_H$ como $e_H = e$, tem-se $hk = kh = e$ e por definição k é inverso também em G.

Exemplo 1.4.1. *Seja G um grupo. $Z(G) = \{a \in G | ax = xa; \forall x \in G\}$ é um subgrupo de G, chamado de* ***centro de G****. Temos que $e \in Z(G)$, logo $Z(G)$ é não vazio. Agora, seja $b \in Z(G)$, dado $x \in G$, tem-se $bx = xb$ e assim,*

$$b^{-1}(bx) = b^{-1}(xb) \Rightarrow$$
$$\Rightarrow (b^{-1}b)x = (b^{-1}x)b \Rightarrow$$
$$\Rightarrow x = (b^{-1}x)b \Rightarrow$$
$$\Rightarrow xb^{-1} = [(b^{-1}x)b]b^{-1} \Rightarrow$$
$$\Rightarrow xb^{-1} = (b^{-1}x)(bb^{-1}) \Rightarrow$$
$$\Rightarrow xb^{-1} = b^{-1}x$$

Portanto, $b^{-1} \in Z(G)$. *Seja* $a, b \in Z(G)$, *então* $ax = xa$ *e* $bx = xb$, $\forall x \in G$. *Assim,*

$$(ab)x = a(bx) \Rightarrow$$
$$\Rightarrow (ab)x = a(xb) \Rightarrow$$
$$\Rightarrow (ab)x = (ax)b \Rightarrow$$
$$\Rightarrow (ab)x = (xa)b \Rightarrow$$
$$\Rightarrow (ab)x = x(ab),\ \forall x \in G.$$

Assim $ab \in Z(G)$. *Pela proposição 1.3,* $Z(G)$ *é subgrupo de* G.

Exemplo 1.4.2. *Considere o conjunto* $H = m\mathbb{Z} = \{mr,\ r \in \mathbb{Z}, m \in \mathbb{N}\}$. $m\mathbb{Z}$ *é subgrupo aditivo dos inteiros. De fato,*
Note que $0 = m0 \in H$. *Assim ,* $H \neq \emptyset$.
Sejam $a, b \in H$, *então* $a = mr_1$ *e* $b = mr_2$, *para algum* r_1 *e algum* r_2 *em* $\mathbb{Z}$.
Note que
(i) $a + b = mr_1 + mr_2 \Rightarrow a + b = m(r_1 + r_2) \in H$
(ii) *Dado* $b \in H$, *Daí,*

$$ab^{-1} = mr_1 + m(-r_2)$$
$$ab^{-1} = m(r_1 - r_2) \in H$$

Portanto, $m\mathbb{Z}$ *é um subgrupo de* $\mathbb{Z}$.

Exemplo 1.4.3. *Todos os subgrupos de* H *de* $\mathbb{Z}$ *são da forma* $H = n\mathbb{Z}$, *com* $n \in \mathbb{Z}$.

De fato, se $H = \{0\}$, *então* $H = 0\mathbb{Z}$. *Suponha agora* $H \neq \{0\}$, *então existe* $a \in H$ *com* $a \neq 0$, *como* $H < \mathbb{Z}$, *temos* $-a \in H$. *Agora considere* $W = \{x \in H \mid x > 0\}$. *Pelo parágrafo anterior* $W \neq \varnothing$, *então pelo principio da boa ordenação,* W *possui elemento minimo, assim sendo* $n = min\{W\}$, *vamos provar que* $H = n\mathbb{Z}$. *Como* $n \in H$, *pois* $n \in W \subset H$, *temos* $n \cdot k \in H, \forall k \in \mathbb{Z}$, *pois,*

$$n \cdot k = \begin{cases} n + \ldots + n\ , & se\ k > 0 \\ -n - \ldots - n & se\ k < 0 \end{cases},$$

assim $n\mathbb{Z} \subset H$.

Por outro lado, pelo algoritmo da divisão, dado $h \in H$, *existem* $q, r \in \mathbb{Z}$ *tais que* $h = n \cdot q + r$, *com* $0 \leqslant r < n$. *Logo* $r = \underbrace{h}_{\in H} - \underbrace{n \cdot q}_{\in H} \in H$, *pela minimalidade de* $n, r = 0$. *Daí, temos* $h = nq \in n\mathbb{Z}$, *ou seja,* $H \subset n\mathbb{Z}$ *e portanto* $H = n\mathbb{Z}$.

1.5 Subgrupos Finitamente Gerados

Definição 1.7. *Sejam* G *um grupo e* S *um subconjunto de* G. *Definimos o subgrupo de* G *gerado por* S, *denotado por* $\langle S \rangle$, *como sendo*

$$\langle S \rangle = \bigcap_{S \subseteq H < G} H$$

Consequências imediatas da definição

1. $S \subseteq \langle S \rangle$.
2. Se $H \leq G$ *e* $S \subseteq H$ então $\langle S \rangle \subseteq H$.
3. $S_1 \subseteq S_2 \subseteq G$, então $\langle S_1 \rangle \subseteq \langle S_2 \rangle$.
4. $H = \langle S \rangle$, dizemos que S gera H.
5. Se H é subgrupo de G então $\langle H \rangle = H$.
6. Se $S = \{x_1, \ldots, x_n\}$, usamos a notação $\langle x_1, x_2, \ldots, x_n \rangle$ ao invés de $\langle \{x_1, \ldots, x_n\} \rangle$.
7. $\langle S \rangle$ **é o menor subgrupo de** G **contendo** S, ou seja, qualquer outro subgrupo que conter S, deve também conter $\langle S \rangle$. Para ver isso, suponha $K < G$ tal que $S \subset K$. Por definição, $\langle S \rangle = \bigcap H$, para todo $H < G$ que contem S, em particular $\langle S \rangle \subset K$.

Definição 1.8. *Sejam* G *um grupo e* H *um subgrupo de* G.

1. *Dizemos que* H *é* **finitamente gerado**, *se existe* S *finito tal que* $H = \langle S \rangle$.
2. *Dados* $H < G$ *e* $S = \{a\}$ *tal que* $H = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$, *dizemos que* H *é um* **Subgrupo cíclico**.

3. *Se existe $a \in G$ tal que $\langle a \rangle = G$, dizemos que G é um* **grupo cíclico**.

Observação 1.6. $\langle \varnothing \rangle = \{e\}$

De fato, o conjunto $\varnothing$ está em todos os subgrupos de G, em particular o grupo $\{e\}$, então $\langle \varnothing \rangle \cap H = \{e\}$, com $H < G$.

Exemplo 1.5.1. 1. *Sendo $P = \{x \in \mathbb{Z} | x > 0\}$, temos $\langle P \rangle = \mathbb{Z}$ e ainda $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.*

2. *Considere o grupo S_4 e os conjuntos de dois elementos*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

temos $\alpha^2 = \alpha = Id$ e $\beta^2 = \beta = Id$, daí, $\langle \alpha, \beta \rangle = \{Id, \alpha, \beta, \alpha\beta\}$

3. *O grupo $(\mathbb{Z}_n, \oplus)$ é cíclico, pois $\mathbb{Z}_n = \langle 1 \rangle$.*

4. *o grupo aditivo dos inteiros é cíclico. Observe que $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$*

5. *, Seja $G = \{e, a, b, c\}$, o grupo onde cada elemento é o seu próprio simétrico, é chamamos de* ***Grupo de Klein*** *[6] (JANESCH, 2008, p.93), não é cíclico, no entanto possui subgrupos cíclicos.*

6. *O Grupo $(\mathbb{Q}, +)$ não é cíclico .*

   Suponha que existe $a \in G - \{0\}$ tal que

$$\mathbb{Q} = \langle a \rangle = \{n \cdot a \mid n \in \mathbb{Z}\}$$

   ,

   Note que $\frac{a}{2} \in \mathbb{Q}$, então existe $m \in \mathbb{Z}$ tal que $\frac{a}{2} = m \cdot a$. Assim,

$$\frac{a}{2} = m \cdot a \Longrightarrow m = \frac{1}{2},$$

   absurdo! pois, $m \in \mathbb{Z}$. Logo $(\mathbb{Q}, +)$ não é cíclico.

7. *$\mathbb{Q}$ não é finitamente gerado.*

   De fato, considere

$$\mathbb{Q} = \langle \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} \rangle \ e \ \alpha = \frac{1}{q_1, \ldots, q_n} \in \mathbb{Q}.$$

Note que $\frac{p_i}{q_i} \in \langle \alpha \rangle$, *pois,*

$$\frac{p_i}{q_i} = (p_i q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n) \cdot \alpha, \ com \ \ i = \{1, \ldots, n\}.$$

E daí,

$\mathbb{Q} = \langle \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} \rangle \subseteq \langle \alpha \rangle$. *Por outro lado,* $\langle a \rangle \subseteq \mathbb{Q}$, *e assim* $\langle a \rangle = \mathbb{Q}$.

Mas, como já vimos acima, $\mathbb{Q}$ *não é cíclico e portanto, não é finitamente gerado.*

8. *O grupo multiplicativo* $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1, n \geq 1\}$. *é um grupo cíclico. De fato, tome* $w_n = cos\frac{2\pi}{n} + i \ sen\frac{2\pi}{n}$. *Então*

$$\mathbb{C}_n = \{w_n \mid k \in \mathbb{Z}\} = \{w_n^k \mid k = 0, 1, 2, \ldots n-1\}$$

.

1.5.1 Ordem de um Elemento do Grupo

Definição 1.9. *Dado* $a \in G$.

1. *Definimos a* **ordem** *de a, denotado por* $O(a)$, *como sendo ordem de* $\langle a \rangle$, *ou seja,* $O(a) = |\langle a \rangle|$.

2. *Se existe* $m \in \mathbb{N}$ *tal que* $a^m = e$, *dizemos que a tem* **ordem finita**. *Neste caso, o menor inteiro positivo n que satisfaz* $a^n = e$, *é a ordem de a, ou seja,* $O(a) = min\{n \in \mathbb{N} \mid a^m = e\}$.

Exemplo 1.5.2. 1. *Dados* $-1, 1 \in (\mathbb{Z}, +)$, *temos* $O(-1) = O(1) = \infty$.

$O(e) = 1$, *pois,* $\langle e \rangle = \{e\}$.

2. *No grupo Multiplicativo* $G = \{1, -1, i, -i\} \subset (\mathbb{C}^*, \cdot)$, *temos*

$O(-1) = 2$ *e* $O(i) = (-i) = 4$

3. *Seja* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix} \in S_6$

Note que,

$$\alpha^2 = \alpha\cdot\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 4 & 6 \end{pmatrix},$$

e

$$\alpha^3 = \alpha^2\cdot\alpha \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 4 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} =$$

$= Id.$

Então $O(\alpha) = 3$.

4. *Se* $a \in (\mathbb{Z}, +)$ *com* $a \neq 0$

   Note que $O(a) = \infty$, *pois se* $n \cdot a = 0$, *não existem,* $n \in \mathbb{N}^*$ *tal que* $n \cdot a = 0$. *Logo* $O(a) = \infty$.

Proposição 1.3. *Seja g um grupo .*

1. *Dado* $a \in g$, *e* $a \neq 0$, *tem-se* $O(a) = 2 \iff a = a^{-1}$.
2. $O(a) = O(a^{-1}), \forall a \in G$.
3. *Se* $O(a) = 2, \forall a \in G - \{e\}$, *então G é abeliano.*
4. *Se* $O(a) = m \cdot n$, *então* $O(a^m) = n$.

Demonstração. 1. $O(a) = 2 \iff a^2 = e$.

($\Longrightarrow$) $a \cdot a = e \Longrightarrow a \cdot a^{-1} \cdot a = a^{-1} \cdot e \Longrightarrow ea = a^{-1} \Longrightarrow a = a^{-1}$

($\Longleftarrow$) Temos $a = a^{-1}$

$a \cdot a = a \cdot a^{-1} \Longrightarrow a^2 = e$

2. Seja $n = O(a)$, então $a^n = e$, segue que $(a^n)^{-1} \cdot a^n = (a^n)^{-1} \cdot e$ e daí temos

   $a^{-n} \cdot a^n = (a^n)^{-1} \Longrightarrow e = a^{n\cdot(-1)} \Longrightarrow e = (a^{-1})^n$.

   Suponha que exista $0 < r < n$, tal que $(a^{-1})^r = e$. Daí, $a^r \cdot (a^{-1})^r = a^r \Longrightarrow e = a^r$, contradição! pois, n é o menor inteiro positivo satisfazendo essa condição. Assim $O(a^{-1}) = O(a)$

3. Sendo $O(a) = 2$ então $a^2 = e \Longrightarrow a = a^{-1}$. Considere agora $a, b \in G$ temos,

   $a \cdot b = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a$.

4. Temos, que $a^{m\cdot n} = e \Longrightarrow (a^m)^n = e$. Agora, considerando $r < n$ tal que $(a^m)^r = e$, segue que $a^{m\cdot r} = e$, mas, como $m \cdot r < m \cdot n$, isso contradiz a minimalidade de $m \cdot n$. Portanto, $O(a^m) = n$.

□

Teorema 1.1. *Sejam G um grupo e $a \in G$.*

1. *Se $a^n = e$ para algum $n \in \mathbb{N}$ então $O(a)$ divide n.*
2. *Se $O(a) = m$, então $a^k = a^r, \forall k \in \mathbb{Z}$ e r como sendo o resto da divisão de k por m.*

Demonstração. 1. Dividindo n por $O(a)$, pelo algoritmo da divisão existe $q, r \in \mathbb{Z}$ tais que,

$n = O(a) \cdot q + r,\ 0 \leq r < O(a)$, então temos

$e = a^n = a^{o(a)\cdot q+r} = (a^{o(a)})^q \cdot a^r \Longrightarrow e \cdot a^r = a^r \Longrightarrow a^r = e,$

logo só podemos ter $r = 0$.

Assim $n = O(a) \cdot q$. Portanto $O(a)$ divide n.

2. Dividindo k por m, pelo algoritmo da divisão existem $q, r \in \mathbb{Z}$ tais que,

$k = m \cdot q + r,\ 0 \leq r < m$, então temos

$a^k = a^{m\cdot q+r} = (a^m)^q.a^r = e.a^r = a^r.$

□

Exemplo 1.5.3. *Vamos determina $\langle\alpha\rangle \in S_3$ onde* $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

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

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

$\langle\alpha\rangle = \{Id, \alpha, \alpha^2\} \in S_3$

Exemplo 1.5.4. *Dado $A \in GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid det\ A \neq 0\}$, vamos determinar $\langle A\rangle$ tal que* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$$A^2 = A \cdot A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$A^3 = A^2 \cdot A \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

$$A^4 = A^3 \cdot A \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$$

De modo indutivo, então suponhamos que seja verdade para $n = k$*, então* $A^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$*, daí,*

$$A^{k+1} = A^k \cdot A \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}.$$

Logo para $n = k + 1$ *é verdade , portanto é verdade* $\forall n \in \mathbb{N}$*. Assim,*

$\langle A \rangle = \{I, A^1, A^2, \ldots, A^n\}$.

Teorema 1.2. *Se os únicos subgrupos de um grupo são* $\{e\}$ *e* G*, então* G *é cíclico de ordem prima.*

Demonstração. Dodo $a \in G$, se $a = \{e\}$, temos $\langle a \rangle = \{e\}$. Se $a \neq e$, temos $\langle a \rangle \neq \{e\}$. Por hipótese $\langle a \rangle = G$.

Mostremos que G tem ordem finita. Dado $a \in G - \{e\}$, temos $\langle a^2 \rangle < G$. Segue que $\langle a^2 \rangle \neq \{e\}$, então $\langle a \rangle = G$.

Sendo $\langle a^2 \rangle = G$, com $a \in G$ existe $k \in \mathbb{Z}$ tal que $a = (a^2)^k = a^{2k}$ ou seja, $a = a^{2k} \Longrightarrow e = a^{2k-1}, 2k - 1 \in \mathbb{N}$, então $o(a)$ é finita.

Supondo agora que $|G| = n$, e considerando n composto, então existe $p, q \in \mathbb{N}$. Com $1 < p, q < n$, com $n = p \cdot q$, Considere o subgrupo $K = \langle a^{\frac{n}{p}} \rangle$ e pela proposição 1.3 K tem ordem p. Portanto, $K \neq \{e\}$ e também $K \neq G$, mas isso contradiz a hipótese.

□

Proposição 1.4. *Sejam* α *um elemento do grupo* G *e* $\langle \alpha \rangle$ *o subgrupo gerado por* α*. Então as seguintes condições são equivalentes:*

1. *A ordem* $|\langle \alpha \rangle|$ *é finita.*

2. *Existem* $t \geq 1$ *tal que* $a^t = e$

   Neste caso denotaremos por n *a ordem de* α*, daí,*

   $\{t \geq 0; \alpha^t = e\} = \{0, n, 2n, ...\}$ *e* $\langle \alpha \rangle = \{e, \alpha, ..., \alpha^{n-1}\}$.

Demonstração. (1) $\Longrightarrow$ (2) como $\langle \alpha \rangle = \{\alpha^m | m \in \mathbb{Z}\}$, e como por hipótese, o grupo $\langle \alpha \rangle$ é finito, existem $p, q \in \mathbb{Z}, p \neq q$ tais que $\alpha^p = \alpha^q$. Sem perda de generalidade, podemos supor que $p > q$. Mas $\alpha^p = \alpha^q$, então $\alpha^{p-q} = e$, e portanto existe $t > 0$ tal que $\alpha^t = e$.

(2) $\Longrightarrow$(1). Vamos considerar o inteiro $r = min\{t \geq 1; \alpha^t = e\}$. Podemos afirmar que $\langle\alpha\rangle = \{e, \alpha, \alpha^2, ..., \alpha^{r-1}\}$ e os elementos $e, \alpha, \alpha^2, ..., \alpha^{r-1}$ são todos distintos.

Para isso vamos supor que $\alpha^p = \alpha^q$ com $0 \leq p, q \leq r-1, p \neq q$; podemos ainda supor que $p > q$. Daí temos $\alpha^{p-q} = e$ com $0 < p-q < r$, pela minimalidade de r não é possível. Portanto $e, \alpha, \alpha^2, ..., \alpha^{r-1}$ são elementos distintos de G. Mas para provar que $\langle\alpha\rangle = \{e, \alpha, \alpha^2, ..., \alpha^{r-1}\}$, mostremos que $\forall\ m \in \mathbb{Z}, \alpha^m = \alpha^l$ para alguns $0 \leq l < r$. Pelo Algoritmo de Euclides, existem $q, l \in \mathbb{Z}$ tais que $m = qr + l$ com $0 \leq l < r$, e portanto $\alpha^m = \alpha^{qr+l} = (\alpha^r)^q \cdot \alpha^l = e^q \cdot \alpha^l = \alpha^l$. □

Capítulo 2

Classes Laterais e Teorema Lagrange

Neste capítulo vamos estudar as classe laterais e demonstrar o Teorema de Lagrange

2.1 Classes Laterais

Seja G um grupo e H um subgrupo de G. Sobre G, defina a relação " $\sim_E$ " da seguinte forma:

$$y \sim_E x \Leftrightarrow \exists h \in H \text{ tal que } x^{-1}y \in H$$

é uma relação equivalência. De fato,

i) **Reflexiva**: $x^{-1}x = e \in H \Longrightarrow x \sim x$.

ii) **Simétrica**: $y \sim x \Longrightarrow x^{-1}y \in H \Longrightarrow (y^{-1}x)^{-1} \in H \Longrightarrow y^{-1}x \in H \Longrightarrow x \sim y$.

iii)**Transitiva**: $y \sim x$ e $x \sim z \Longrightarrow x^{-1}y \in H$ e $z^{-1}x \in H \Longrightarrow$

$$\Longrightarrow (z^{-1}x)(x^{-1}y) \in H \Longrightarrow z^{-1}y \in H \Longrightarrow y \sim z.$$

Agora sendo G um grupo , $H \leqslant G$ e $x, y \in G$ a temos

$$\begin{aligned} y \sim_E x \quad &\Longleftrightarrow x^{-1}y \in H \quad \Longleftrightarrow \exists\ h \in H; x^{-1} = H \\ &\Longleftrightarrow y = xh, para\ algum\ h \in H \\ &\Longleftrightarrow y \in xH. \end{aligned}$$

Daí, por definição, a classe de equivalência que contém x é o conjunto

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

denotaremos esse conjunto por xH e será chamado de **classe lateral à esquerda de H em G que contém x**. Em particular, H è a classe lateral do elemento neutro e à esquerda.

De forma semelhante, podemos definir a seguinte relação de equivalência,

$$y \sim_D x \Leftrightarrow \exists h \in H \text{ tal que } y = hx \text{ ou } yx^{-1} \in H$$

Seguindo mesmo raciocínio, temos que o conjunto Hx será à **classe lateral à direita de H em G**. Então a classe lateral à direita de H em G é

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

.

Observação 2.1. *1. Note que, $a = a.e \in aH$ e $a = e.a \in Ha$*

2. *As aplicações $f_a : H \longrightarrow aH$ e $g_a : H \longrightarrow Ha$, tais que $f_a(h) = ah$ e $g_a(h) = ha$ são bijetivas.*

   De fato, mostremos que f_a é bijetiva. Claramente f_a e sobrejetiva, resta provar a injetividade, ou seja, devemos mostrar que dados $h_1, h_2 \in H$ se $f(h_1) = f(h_2)$ isso implica que $h_1 = h_2$, então

   $$f(h_1) = f(h_2) \Longrightarrow ah_1 = ah_2 \Longrightarrow a^{-1}ah_1 = a^{-1}ah_2 \Longrightarrow eh_1 = eh_2 \Longrightarrow h_1 = h_2.$$

   Analogamente prova-se que g_a é bijetiva.

3. *Se H é finito então Ha e aH são finitas e $|Ha| = |H| = |Ha|$.*

4. *$a \in H \Longleftrightarrow Ha = H$ e $a \in H \Longleftrightarrow aH = H$.*

5. *Na notação aditiva, ao invés de $a \cdot H$, usamos $a + H = \{a + h | h \in H\}$.*

Exemplo 2.1.1. *:*

1) Seja $a \in G$ então $G \cdot a = a \cdot G = G$ e $a \cdot \{e\} = \{a\} = \{e\} \cdot a$.

2) Seja $n \in \mathbb{Z}$ e considere o subgrupo $H = n \cdot \mathbb{Z}$ de $(\mathbb{Z}, +)$.

Dado $a \in \mathbb{Z}$, temos

$$\begin{aligned} a + n \cdot \mathbb{Z} &= \{a + n \cdot x \mid x \in \mathbb{Z}\} \\ &= \{y = a + n \cdot x \mid x \in \mathbb{Z}\} \\ &= \{y - a = n \cdot x \mid x \in \mathbb{Z}\} \\ &= \{y \in \mathbb{Z} \mid y = a \ (mod\ n)\} \end{aligned}$$

3) Considere $\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$ *e* $H = \langle\varphi\rangle = \{Id, \varphi\}$. *Dado* $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, *temos*

$$\beta H = \{\beta, \beta\varphi\} = \left\{\beta, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right\}$$

e

$$H\beta = \{\beta, \varphi\beta\} = \left\{\beta, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}.$$

Logo $H\beta \neq \beta H$.

Proposição 2.1. *1. Todas as classes laterais de* H *em* G *têm a mesma cardinalidade, igual à de* H.

$$\begin{aligned} \varphi &= E \longrightarrow D \\ & \quad xH \longmapsto Hx^{-1} \end{aligned}$$

Onde $E = \{xH \mid x \in G\}$ *e* $D = \{Hx \mid x \in G\}$ *é bijetiva.*

2. As funções

$$\begin{aligned} \psi_1 : H &\longrightarrow xH \\ h &\longmapsto xh \end{aligned}$$

e

$$\begin{aligned} \psi_2 : H &\longrightarrow Hx \\ h &\longmapsto hx \end{aligned}$$

são bijeitvas.

Demonstração. 1. Note que φ é claramente sobrejetiva, então vamos mostrar a sobrejetividade.

Devemos mostrar que se $\varphi(x_1H) = \varphi(x_2H)$, tem -se $a \in x_1H$, exite $h \in H$, tal que $a = x_1h$, daí,

$a = x_1h \Longrightarrow h^{-1}x_1^{-1} = a^{-1} \in Hx_1^{-1}$

Então, exite $h_1 \in H$ tal que

$a^{-1} = h_1x_2^{-1} \Longrightarrow a = x_2h_1^{-1} \in x_2H$,

ou seja, $x_1H \subset x_2H$, como ambas tem a mesma cardinalidade.

2. Basta verificar que ψ_1 *e* ψ_2 são bijetivas. Considerando ψ_1, note que claramente ψ_1 é sobrejetiva. Para ver a injetividade, tememos $h, k \in H$ e se

   $\psi_1(h) = \psi_1(k) \Longrightarrow xh = xk \Longrightarrow x^{-1}xh = x^{-1}xk \Longrightarrow h = k.$

   para ψ_2 a demonstração é análoga. Assim, concluímos que

   $|H| = |xH| = |Hx|$.

□

Definição 2.1. *Sejam G um grupo e H um subgrupo de G. Definimos índice H em G , denotado por $(G : H)$ como sendo o número de classes laterais à direita ou à esquerda de H em G.*

Proposição 2.2. *1. Temos que $G = \bigcup_{x \in G} Hx$;*

2. $Hx = Hy \Longleftrightarrow x \cdot y^{-1} \in H$;

3. se $Hx \neq Hy$ então $Hx \cap Hy = \emptyset$.

Demonstração. 1. Claramente $\bigcup_{x \in G} Hx \subset G$. Agora dado $a \in G$, temos que

   $a \in Ha \subset \bigcup_{x \in G} Hx$. Assim temos a igualdade.

2. ($\Longrightarrow$). Sendo $x \in Hy$, existe $h \in H$ tal que $x = hy$ é daí $xy^{-1} = h \in H$.

   ($\Longleftarrow$). Considerando por hipótese $xy^{-1} \in Hx$, se $a \in Hx$, existem $h_1h_2 \in H$ tais que $xy^{-1} = h_1$ e $a = h_2x$, então

   $a = h_2x = h_2h_1y \in Hy$. Logo, $H \subset Hy$ e por 2.1 temos a igualdade.

3. Suponha $a \in Hx \neq Hy$, então existem $h_1h_2 \in H$ tais que $a = h_1x$ e $a = h_2y$, daí,

   $h_1x = h_2y \Longrightarrow xy^{-1} = h_1^{-1}h_2 \in H$ e por 2), temos $Hx = Hy$, contradição!.

□

Os mesmos resultados são análogos para as classes laterais a esquerda de H.

Proposição 2.3. *1. Temos que $G = \bigcup_{x \in G} xH$;*

2. $xH = yH \Longleftrightarrow y^{-1}x \in H$;

3. se $xH \neq yH$ então $xH \cap yH = \emptyset$.

Agora já temos condições suficientes para provar o Teorema de Lagrange.

2.2 Teorema de Lagrange

Teorema 2.1. *Sejam G um grupo finito e H um subgrupo de G. Então, a ordem de G divide a ordem de H, ou seja*

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

Demonstração. Sabemos que o número de classe laterais à direta e à esquerda é o mesmo, então vamos apenas considerar as classes laterais à esquerda de H. Sejam $x_1H, x_2H, \ldots, x_mH$, as m distintas classes laterais à esquerda de H em G.

Sabemos que $G = x_1H \cup x_2H \cup \ldots \cup x_mH$ e daí temos

$$\begin{aligned} |G| &= |x_1H| + |x_2H| + \ldots + |x_mH| \\ &= |H| + |H| + \ldots + |H| = m|H| \\ &= (G : H) \cdot |H| \end{aligned}$$

□

Capítulo 3

Consequências e a Recíproca do Teorema de Lagrange

Neste capítulo veremos algumas consequências do teorema de Lagrange e falaremos sobre a recíproca, que não é válida, mas podemos dar condições para que seja.

3.1 Consequências Imediatas do Teorema de Lagrange

Aplicação 3.1. *Seja G um grupo finito e de ordem prima, então G é abeliano.*

Demonstração. Seja G um grupo, tal que $|G| = p$, com p sendo um número primo, temos que existe $x \in G - \{e\}$. Pelo Teorema de Lagrange $|\langle g \rangle|$ divide p, mas p é primo, temos que $|\langle x \rangle| = p$, pois $|\langle x \rangle| \neq 1$. Daí $\langle x \rangle = G$ e por conseguinte, G é Cíclico, logo é abeliano. □

Aplicação 3.2. *Se G é um grupo finito e $g \in G$, então $O(g)$ divide $|G|$ e $g^{|G|} = e$.*

Demonstração. Por definição , $O(g) = |\langle g \rangle|$ e pelo Teorema de Lagrange, temos que $|\langle g \rangle|$ divide $|G|$. De fato se pegarmos $|G| = n$ *e* $o(g) = r$, com $n = r \cdot k$, para todo $k \in \mathbb{Z}$ e

$$g^{|G|} = g^{r \cdot k} = (g^r)^k = e^k = e \Longrightarrow g^{|G|} = e$$

□

Aplicação 3.3. *Se $H, K < G$ e G finito com $mdc(|H|, |K|) = 1$ então $H \cap K = \{e\}$.*

Demonstração. Suponha que $a \in H \cap K$, então pelo Teorema de Lagrange $O(a)|\ |H|$ e $O(a)\ |\ |K|$, Como $mdc(|K||H|) = 1$, temos que $O(a) = 1$, e daí $a = e$. □

Aplicação 3.4. *Se $|G| = 2p$, onde p é um primo impar, então G possui elemento de ordem p.*

Demonstração. Primeiramente e supondo que existe elemento $x \in G$ tal que, $O(x) = 2p$.

De fato, $x^{2p} = e \Longrightarrow (x^2)^p = e$, então, $o(x^2)|2p$, temos $o(x^2) = 2$ ou $o(x^2) = p$. Suponha então que $o(x^2) = 2$, então $(x^2)^2 = e$, daí $O(x) \leqslant 4$, contradição, pois, como $O(x) = 2p$ e p é primo ímpar, tem-se que $O(x) \geq 6$. Logo, só podemos ter $o(x^2) = p$.

Suponhamos agora que não existe elementos em G com ordem 2p. Então, dado $x \in G - \{e\}$ temos que $o(x)|2p$. Daí, $o(x) = 2$ ou $o(x) = p$, vamos supor que $o(x) = 2$, portanto, G é abeliano. Então considere $x, y \in G - \{e\}$, com $x \neq y$ e $H = \langle x, y\rangle$. Note que $H = \langle e, x, y, x \cdot y\rangle$, mas, $4 = |H| \nmid 2p$. Absurdo! Então $O(x) = p$.

□

Aplicação 3.5. *(Pequeno Teorema de Fermat)*

Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então .

$$a^{p-1} = 1\ (mod\ p)$$

Demonstração. Note que $\mathcal{U}(\mathbb{Z}_p) = \{\overline{x} \in \mathbb{Z}_p \mid mdc(x, p) = 1\}$

é um grupo com a multiplicação de $\mathbb{Z}_p$, como p é primo então $\mathcal{U}(\mathbb{Z}_p) = p - 1$.

Seja $a \in \mathbb{Z}$ tal que $p \nmid a$. Se $mdc(a, p) = x$, então $x|a$ e $x|p$. Se $x|p$, temos que $x = 1$ ou $x = P$, mas não pode ser $x = p$, pois $p \nmid a$. Logo $x = 1$, Então $\overline{a} \in \mathcal{U}(\mathbb{Z}_p)$, e daí,

$\overline{a}^{p-1} = \overline{1} \Longrightarrow \overline{a^{p-1}} = \overline{1} \Longrightarrow \overline{a^{p-1}} = \overline{1} \Longrightarrow a^{p-1} \equiv 1\ (mod\ p)$ □

3.2 A Recíproca do teorema de Lagrange

Antes de falar da reciproca do Teorema de Lagrange, vamos definir mais alguns conceitos sobre permutações, saber ciclos de permutação, necessários para uma melhor compreensão do que iremos falar mais adiante.

3.2.1 Ciclos de Permutações

Definição 3.1. *Sejam $\alpha, \beta \in S_n$ e $I_n = \{1, 2, \ldots, n\}$ conjunto de índices.*

1. *Definimos $Mov(\alpha) = \{i \in I_n \mid \alpha(i) \neq i\}$ e $Fix(\alpha) = \{i \in I_n \mid \alpha(i) = i\}$.*

2. *Definimos em I_n a seguinte relação:*

   $i \sim_\sigma j$ se existe $k \in \mathbb{Z}$ tal que $\sigma^k(i) = j$.

Definição 3.2. *Dado $\sigma \in S_n$ e $i \in I_n$. Se $\forall \in \mathbb{Z}$, tem - se $\sigma^k(i) = i$, então i é uma órbita unitário.*

Observação 3.1. *A relação "$i \sim_\sigma j$"é de equivalência e as classes determinadas por ela são chamadas de* **orbitas de σ** *ou* **σ-órbitas**. *Então:*

- *$Mov(\alpha)$ é a união das σ-órbitas não unitárias.*
- *$Fix(\alpha)$ é a união das σ-órbitas unitárias.*

Exemplo 3.2.1. *Seja*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \in S_5.$$

Temos $Mov(\alpha) = \{2, 3, 5\}$ e $Fiv(\alpha) = \{1, 4\}$.

Definição 3.3. *Dado $\sigma \in S_n$, dizemos que σ é um* **ciclo**, *se σ possui no máximo uma órbita não unitária.*

Exemplo 3.2.2. *Considere*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \in S_5$$

$\alpha(2) = 3$, $\alpha(3) = 5$, $\alpha(5) = 2$ daí $\alpha^2(2) = 5$ então $2 \sim_\alpha 3$ e $2 \sim_\alpha 5$, observe ainda que $\alpha^3(2) = 2$, daí dizemos que orbita de 2 tem 3 elementos.

Definição 3.4. *Uma* **transposição** *é um ciclo de tamanho 2, ou um 2-ciclo.*

Observação 3.2. *Seja*

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 6 & 5 & 8 & 4 & 7 \end{pmatrix} \in S_8$$

as órbitas de β não unitárias são $\{1,2\},\{4,6,7,8\}$. β não é um ciclo, pois possui duas orbitas não unitárias. Já

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix},$$

a única orbita de α é $\{2,3,4,5\}$, assim, α é um 4 - ciclo.

Nestes casos, denotamos β por (1 2)(4 6 7 8) e α por (2 5 3 4).

Em geral, se σ é um ciclo, com $Mov(\sigma) = \{\alpha_1, \ldots, \alpha_m\}$ e
$\sigma(j_1) = j_2, \ldots \sigma(j_m) = 1$, denotamos por
$\sigma = (\alpha_1\ \alpha_2\ \ldots\ \alpha_m)$.

Exemplo 3.2.3. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix} = (1\ 5)$ *é transposição*

Definição 3.5. *Dizemos que uma permutação σ é* **par***, se σ pode ser escrito como um produto de um número par de transposição. Caso contrário a permutação é* **ímpar**

Observação 3.3. *Se $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in S_n$, então $\alpha = (\alpha_1, \alpha_m) \ldots (\alpha_1, \alpha_3)(\alpha_1, \alpha_2)$ Então considerando*

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 7 & 6 & 9 & 1 & 3 & 5 & 8 \end{pmatrix} \in S_9.$$

Note que μ = (1 2 4 6) (3 7) (5 9 8) que pode ser escrito da forma $\mu =$ (1 6) (1 4) (1 2) (3 7) (5 9).

Logo μ é par.

Agora considere

$$\eta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \in S_5.$$

Note que η = (2 1)(3 4 5) = (2 1)(3 5)(3 4). Assim η é ímpar.

3.2.2 O Contra Exemplo da Recíproca

O recíproca do Teorema de Lagrange não é verdadeira, pois, o subgrupo A_4 das permutações **pares** de S_4 tem ordem 12, mas não possui um subgrupo de ordem 6. De fato, vamos supor que existe $H < A_4$, com $|H| = 6$. Note que $(A_4 : H) = 2$, então as classes laterais de H em A_4 são H e $gH, \forall \in A_4$. Note que $gH = Hg$, pois, sendo

$$G = H \cup gH \tag{3.1}$$

$$G = H \cup Hg \tag{3.2}$$

Considerando que classes distintas são desjuntas, ou seja, $H \cap gH = \varnothing$, se $x \in Hg$ então $x \in H$, mas por 3.1 $x \in H \cup gH$, logo $x \in gH$, ou seja, $Hg \subset gH$, como $|Hg| = |gH|$ temos que $Hg = gH$.

Sabe-se que existem 8 3-ciclos em A_4, então, pelo menos um deve está em H. Sem perda de generalidade suponha que $(1\ 2\ 3) \in H$, então $(123)^{-1} = (132) \in H$. Como $g^{-1}hg \in H$, para todo $g \in A_4$ e para todo $h \in H$, então temos

$$(124)(123)(124)^{-1} = (124)(123)(142) = (243) \in H$$

$$(243)(123)(243)^{-1} = (243)(123)(234) = (142) \in H$$

Assim H possui os seguintes elementos

$$(1), (123), (132), (243), (243)^{-1} = (234), (142), (142)^{-1} = (124).$$

Daí H tem 7 elementos, logo chegamos a uma Contradição. Portanto , A_4 não pode ter subgrupo de ordem 6.

Ainda em relação a recíproca, existe um alguns resultados chamados **Os Teoremas de Sylow** [3](FRALEIGH, 2002, p.324) dão condições para que seja válida a recíproca.

Capítulo 4

Conclusão

Este trabalho acadêmico finaliza o percurso de aprendizado dentro do curso de licenciatura em matemática. Onde após vários semestre de contemplando os variáveis ramos da matemática apresento pelo curso.

Fizemos abordagem de uma das partes mais complexa totalmente alheia a cotidiano da maioria das pessoa e que por sua exigência de dedicação e envolvimento pessoal, só ganhou seus fundamentos que hoje estamos a estuda a partir do século XVIII, que a Álgebra abstrata ou moderna.

Concluímos que foi enriquecedor a construção e as aplicações do Teorema de Lagrange, dentro dos estudos de grupos finitos, além de ser fácil utilização e aplicação. O mesmo nos possibilita obter resultados gerais sobre ordem e geração de subgrupos, mesmo como vimos sem sua reciproca ser verdadeira, existe resultados que nos garante condições que pode ser válido.

Referências Bibliográficas

[1] BOYER, Carl Benjamin. *História da matemática.* 11ª ed. São Paulo, Edgard Blucher., 1974.

[2] DOMINGUES, Higino H; IEZZI, Gelson. *Álgebra moderna: Volume Único.* 4ª ed. reform. São Paulo: Atual, 2003.

[3] FRALEIGH, John B.. *A Frist Course In Abstract Algebra.* 7ªed. Índia, Pearson Education, 2003.

[4] GARCIA, Arnaldo; LEQUAIN,Yves. *Elementos de Álgebra.* 4ªed. Rio de Janeiro, IMPA, 2006.

[5] GONÇALVES, Adilson. *Introdução à Álgebra.* 5ª ed. Rio de Janeiro, IMPA, 2007.

[6] JANESCH, Oscar Ricardo. *Álgebra II.* Florianópolis: UFSC/EAD/CED/CFM, 2008.

[7] JUDSON,Thomas W. *Abstract Algebra: Theory and Applications.* Stephen F. Austin States University, 2012. Disponível em http:w.w.w.abstract.ups.edu/.../aata-20130816.pdf. (Acessado em 04/01/2016.)

[8] VIEIRA, Vandenberg Lopes. *Álgebra abstrata para licenciatura.* Campina Grande: EDUEPB, 2013.

[9] VIEIRA, Vandenberg Lopes. *Um curso básico em teoria dos número* . Campina Grande: EDUEPB, São Paulo: Livraria da Física, 2015