UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA EM MATEMÁTICA

ROBSON ALVES SOARES

TEOREMA DE LAGRANGE E ALGUMAS DE SUAS APLICAÇÕES

PATOS – PB
2022

ROBSON ALVES SOARES

TEOREMA DE LAGRANGE E ALGUMAS DE SUAS APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Matemática.

Área de concentração: Algebra.

Orientador: José Ginaldo de Souza Farias.

PATOS – PB

2022

S676t Soares, Robson Alves.
Teorema de lagrange e algumas de suas aplicações [manuscrito] / Robson Alves Soares. - 2022.
42 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas , 2022.
"Orientação : Prof. Me. José Ginaldo de Souza Farias , Coordenação do Curso de Matemática - CCEA."

1. Matemática. 2. Teorema de Lagrange. 3. Algebra. 4. Teoria dos grupos. I. Título

21. ed. CDD 510.7

Elaborada por Edson M. Almeida - CRB - CRB 15/743 BSC7/UEPB

ROBSON ALVES SOARES

TEOREMA DE LAGRANGE E ALGUMAS DE SUAS APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Matemática.

Área de concentração: Algebra.

Aprovada em: 10/05/2022

BANCA EXAMINADORA

Prof. José Ginaldo de Souza Farias (Orientador)

Universidade Estadual da Paraíba (UEPB)

Prof. Marcelo da Silva Vieira

Universidade Estadual da Paraíba (UEPB)

Prof. Geovane de Souza Ferreira Júnior

Universidade Estadual da Paraíba (UEPB)

A minha esposa, pela dedicação, companheirismo e amor, DEDICO.

AGRADECIMENTOS

Ao professor Ginaldo pelas leituras sugeridas ao longo dessa orientação e pela dedicação, paciência e incentivo.

Aos meu pais, a minha avó, as minhas tias e toda minha família, pela compreensão por minha ausência nas reuniões familiares.

Aos funcionários da UEPB, pela presteza e atendimento quando nos foi necessário.

Aos colegas de classe pelos momentos de amizade e apoio.

Resumo

Neste trabalho, vamos estudar um dos teoremas centrais da teoria de grupos finitos conhecido como Teorema de Lagrange. Tal teorema trás em essência a relação entre a ordem de um subgrupo e a ordem de um grupo. Com base nessa relação, é possível realizar algumas aplicações importantes dentro da Teoria dos Números, por exemplo, a prova do pequeno Teorema de Fermat. A metodologia empregada neste trabalho consiste na revisão da literatura matemática que versa sobre o Teorema de Lagrange.

Palavras – chaves: Grupos. Algebra. Teorema de Lagrange.

ABSTRACT

In this job we are going to study one of the central theorems related to mathematical finite groups, known as Lagrange Theorem. Such theorem talks about the relation between a subgroup order and a group order. Based in this relation, it is shown that it is possible to perform some important applications within Number Theory, for example, the proof of Fermat's Little Theorem. The methodology used in this work consists of a review of the mathematical literature that deals with Lagrange's Theorem.

Keywords: Groups. Algebra. Lagrange Theorem.

SUMÁRIO

1 INTRODUÇÃO

A essência de número é algo incrível no sentido de poder representar diversas situações ou problemas com o mesmo valor simbólico, como por exemplo o número 3, que pode representar três casas, três batatas, três motos, etc. Partindo dessa ideia, em matemática, quando resolvemos uma equação, essa mesma pode representar um problema de física, um problema de engenharia ou simplesmente um problema do nosso cotidiano. No entanto, para a mesma ser resolvida não é necessário saber o problema que a originou onde vemos a álgebra e sua forma de generalização das coisas. Assim, a álgebra, vem sendo desenvolvida a partir de problemas dentro da própria matemática, o que é algo muito interessante e prazeroso de se observar. Esses fatos, são facilmente vistos quando estudamos um pouco de sua história.

Euclides de Alexandria foi um dos matemáticos mais conhecidos de sua época, que no reinado de Ptolomeu I (306 A.C) foi chamado para Alexandria no Egito. Sua obra publicada na época chamada de "Os elementos" trouxe conhecimentos matemáticos que ainda não tinha sido explorado em publicações. No "Os Elementos" vemos nos volumes II, V, VI, VII, VIII e IX, muitos teoremas e proposições representados de forma geométrica, que hoje foram reestruturados e aplicamos na Álgebra e Teoria dos números, que na época era vista como os inteiros positivos ($\mathbb{N}$).

Apolônio de Perga (262 a 190 A.C.) foi outro grande matemático da mesma época. Precursor da geometria analítica de Fermat, em sua obra restaurada de "Lugares Planos", já utilizava problemas envolvendo as equações quadráticas do tipo $ax - x^2 = bc$. Em sua obra "As cônicas" deu uma nova perspectiva sobre os trabalhos de Euclides, modernizando no método e indo além em algumas demonstrações.

Na Idade Média do século VI à XVI D.C. o ocidente impediu o progresso da produção de estudos matemáticos devido as invasões dos povos inimigos levando os reinos europeus a focarem em se defender e fazendo com que a religião ganhasse destaque e desvalorizando os conhecimentos que não fosse religioso. Com isso, os principais matemáticos se sentiram perseguidos e foram se exilando no oriente e boa parte foi para Pérsia, e de lá para Índia e China, com essa mistura de conhecimentos, por volta de 628 D.C., Brahmagupta da Ìndia 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. Bhaskara foi outro matemático indiano mais importante do século, preenchendo lacunas na obra Brahmagupta com a divisão por

zero, o qual afirmou de que tal quociente é infinito e mostrou uma solução final para a equação de Pell, suas obras foram “Vija-Ganita” e “LIlavati” que contém vários problemas de equações lineares e quadráticas.

No século IX, surgiu o matemático, AI-Khowarizmi, que deu origem a palavra “álgebra” sendo essa palavra uma tradução das palavras de sua obra, “Al-jabr’lmuqabalah”. O ocidente ainda lhe homenageou com o seu nome o sistema numérico indo-arábico, Algarismo ou Algoritmo, além de adotar também como um ramo da matemática. Omar Khayyam foi outro árabe que contribuiu para o desenvolvemento da Álgebra que em sua obra “a Álgebra”, deu os primeiros passos para generalização do método para a soluão das equações cúbicas. Em 1202, Leonardo Fibonacci com sua obra “Liber abaci”, aborda os métodos e problemas algébricos usando os numerais indo-arábicos.

Nicolas Chuquet (século XIV), em sua obra “Triparfty em la Science des nombres”, dá uma nova visão nos termos matemáticos, entre eles chama a “álgebra” de regras da incógnita, deu nome as quatro operações básicas, inventou 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 houve um grande impulso na álgebra por causa de um processo de rivalidade entre grandes matemáticos, um exemplo disso foi a disputa pela resolução das equações de 3° grau, tendo um dos precursores o matemático italiano Scipione del Ferro (1465-1526) com a resolução das equações cúbicas da forma $x^3 + px = q, (p, q > 0)$, onde ele tinha um método para solução com raízes cúbicas, atualmente conhecido pela fórmula

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

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 algébricas e se resolúvel por radicais, coube o discípulo de del Ferro, Antônio Maria Fior, aceita o desafio e perdeu.

Ainda no mesmo século (em 1545), o italiano Geônimo Cardano (1501-1576), na obra “Ars magna” divulgou os métodos de Tartaglia para equações cúbicas e quádricas e Ludovico de Ferrari

(1522-15645) para redução de uma equação do 4° para uma de 3° grau. Geônimo utilizou os métodos de Del Ferro e Tartaglia para provar que todas as equações de 4° para uma equação é solucionável por radicais nos racionais. Na mesma época, o italiano Rafael Bombelli (1526-1573), criou um método para equações que Geônimo chamava resolúveis, as que apresentavam soluções com números racionais ou negativos. Porem a mesma só funcionava para equações já solucionadas, sem perceber, construiu os primeiros elementos para os Números Complexos, criando a ideia de imaginário conjugado.

O francês François Viéte (1540-1603), também deu uma grande colaboração para a álgebra, instituiu o ouso 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 generalizada. Ele defendia que a análise 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 está na sua obra de 1591, Isagoge (ou Introdução).

René Descartes (1596-1650) foi outro importante matemático que em sua época fez uma grande inovação no modo de pensar, 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 indicar incógnitas, e adotou os símbolos de $+$ e $-$. Em sua obra "La géométrie" dá origem a um dos ramos da matemática (a geometria analítica), onde ele conseguiu mostrar resultados geométricos através da álgebra, desprendendo das construções de diagramas e dando significado às operações da álgebra por meio de interpolações geométricas. Mesmo simplificando as equações, Descartes só conseguiu apresentar métodos para resoluções de equações até o quarto grau.

O francês Pierre de Fermat (1601 – 1665), um outro notório matemático, nunca se interessou em publicar suas descobertas em matemática e apreciava a matemática como uma diversão porem depois de sua morte seu filho reuniu seus escritos e foi feito a obra "Introdução aos lugares de Fermat", onde tinha vários teoremas da teoria dos números e uma geometria analítica similar à de Descartes, que partia das equações indeterminadas, mas se tivesse sido publicada teria ofuscado a de Descartes por ser de uma 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 mesmo século, 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 $(=)$, semelhança $(\sim)$, congruência a $(\simeq)$. Trabalhou com um conceito de álgebra da lógica, porém não foi muito apreciado pelos seus contemporâneos.

O britânico Conde Ehrenfried Walter Von Tschirnhaus (1651-1708), deu uma importante contribuição para a álgebra moderna que ficou conhecido como as Transformações de Tschirnhaus onde o mesmo desejava achar uma forma para resolver as equações de grau n. Sua obra "Acta Eruditorum", mostrou que polinômios de grau $n > 2$ poderia ser reduzido em $n-1, n-2$ e $n-3$, no entanto o alcance do método foi limitado pois as equações de grau superior ou igual a cinco em geral não são resolúveis algebricamente, mas foi um grande avanço para a álgebra da época.

O matemático ítalo – francês 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, contribuiu bastante para o desenvolvimento dos conceitos de grupo. Em 1824, ele provou que para a equação polinomial $x^5 - 6x + 3 = 0$ não é resolvível por radicais sobre os racionais, daí veio outra dúvida para quais equações do 5° grau seria resolvível nos radicais sobre os racionais. Esse foi um dos grandes feitos que provou uma suspeita do próprio Lagrange que não haveria nenhuma formula geral por radicais para resolver equações de grau ≥ 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 gral n, um grupo formado por permutações de raízes da equação. Depois provou que a equação é resolvível por radicais sobre $\mathbb{Q}$ se , e somente se, este grupo tem certas propriedades específicas. Outro grande matemático que contribuiu muito para o desenvolvimento dos grupos algébricos foi o inglês Artur Cayley (1821 – 1899), que tem como principais contribuições a tabua de operação de grupo, introdução das matrizes na matemática, além de valorizar os aspectos formais da matemática, considerando o percursor do estudo da teoria dos grupos.

Neste trabalho falaremos sobre 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 algumas definições e consequências que serão vistas no capítulo II, onde iremos ver alguns grupos finitos importantes e também definir subgrupos, algumas consequências importantes e a ideia de grupo finito e ordem de um grupo.

No capítulo III, vamos falar sobre as classes laterais e provar o teorema de Lagrange. E no capítulo IV, veremos algumas aplicações do teorema de Lagrange.

2 GRUPOS

Neste capítulo, estudaremos alguns princípios básicos da teoria de grupos finitos, o capítulo resume-se em estabelecer uma base adequada para os capítulos seguintes.

2.1 Grupos

Definição 2.1. Uma operação binária em um conjunto G é uma operação onde para cada par ordenado (x, y) de elementos de G, $x * y$ existe, é único e pertence a G.

Definição 2.2. Seja $G = \{a, b, c, ...\}$ um conjunto não vazio munido de uma operação

$$*: G \times G \to G$$

$$(a, b) \mapsto a * b$$

Dizemos que $(\boldsymbol{G}, *)$ é um grupo se o mesmo satisfaz as seguintes propriedades:

i) Associativa

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

ii) Existência do Elemento Neutro

Existe $e \in G$ tal que $e * a = a * e = a$, para todo $a \in G$

iii) Existência do Inverso

Para todo $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$

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

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

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

Exemplo 2.1.1. O conjunto dos números inteiros ℤ munido com a operação de adição é um grupo. Em notação $(\mathbb{Z}, +)$. De fato, dados $a, b, c \in \mathbb{Z}$, temos que

i) $(a + b) + c = a + (b + c)$;

ii) Existe $0 \in \mathbb{Z}$, tal que $a + 0 = 0 + a = a$;

iii) Para todo $a \in \mathbb{Z}$, com $a \neq 0$, existe $(-a) \in \mathbb{Z}$ tal que $a + (-a) = -a + a = 0$. Portanto, $(\mathbb{Z}, +)$ é um grupo.

Observações:

1. O grupo $(G,*)$ será Abeliano ou Cumultativo se valer $a * b = b * a$ para todo $a, b \in G$;
2. No objetivo de simplificar as notações, a partir daqui, utilizaremos a notação multiplicativa para a operação do grupo em G. Desse modo, em vez de $(G,*)$ usaremos $(G,\cdot)$ e $a * b$ por $a \cdot b$ ou simplesmente por ab. E para o inverso de $a \in G$ colocamos a^{-1}.
3. Quando não houver mistura na notação $(G,*)$, denotaremos apenas por G.

2.1.1 Propriedades básicas de um Grupo

1. O elemento neutro é único.

De fato, supondo que exista $e, e' \in G$ elementos neutros de G, daí temos que;

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

Logo, podemos concluir que $e = e'$.

2. O elemento inverso é único.

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

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

Logo,$b = b'$e denotamos pôr 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 um grupo. Se $a, b \in G$, então $(ab)^{-1} = b^{-1}a^{-1}$.

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

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

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

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

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

Agora, vamos multiplicar por a^{-1} os dois lados da igualdade tendo assim:

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

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

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

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

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

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

   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.

   Primeiramente vamos mostrar a existência da solução para $ax = b$.

   De fato, pelo inverso de a, temos que

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

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

Agora, mostrando a existência para $ya = b$

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

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

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 2.1.2.

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{C}, +), (\mathbb{R}, +)$, são grupos abelianos, pois quaisquer elementos a e b pertencentes a um desses grupos, teremos sempre $a + b = b + a$.
2. $(\mathbb{Q}^*, \cdot)$ é um grupo. De fato, dados $x, y, z \in \mathbb{Q}^*$, temos que

   i) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

   ii) $\exists\, 1 \in \mathbb{Q}^* \mid x \cdot 1 = 1 \cdot x = x$

   iii) $\forall\, x \in \mathbb{Q}^*$, com $x \neq 1$, $\exists\, x^{-1} \mid x^{-1} \cdot x = x \cdot x^{-1} = 1$.

   Portanto, $(\mathbb{Q}^*, \cdot)$ é um grupo

3. $(\mathbb{Q}, \cdot)$ Não é um grupo pois o 0 não tem inverso.

2.1.2 Potências Múltiplos em um Grupo

- **Potência**

Definição 2.3. 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 2.1. 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) $a^{-n} = (a^n)^{-1}$.

Demonstração: Para detalhes da prova, o leitor pode consultar a referência [2] (DOMINGUES, 2003, p. 174).

- **Adição**

Definição 2.4. Seja G um Grupo, $a \in G$ *e* $n \in \mathbb{Z}$. Definimos

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

Proposição 2.2. Se G é um grupo e $a \in G$ então:

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

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

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

Demonstração: Para detalhes da prova, o leitor pode consultar a referência [2] (DOMINGUES, 2003, P.176)

Observação 2.1. 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.

2.1.3 Grupo Finito

Definição 2.5. 1. Dado um grupo G. Chama-se ordem de G a sua quantidade de elementos. Em símbolos, denotamos a ordem de G por $|G|$.

2. Se G é um conjunto finito de n elementos, dizemos que G é um grupo finito de ordem n. Caso G tenha números de elementos infinito dizemos que G é um grupo infinito.

Exemplo 2.1.3. O conjunto $G = \{-1, 1\} \sqsubseteq \mathbb{Z}$; 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 $\mathcal{U}(\mathbb{z})$, cujas operações são descritas na seguinte tabela.

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

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

Definição 2.6. (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, $n|(c-a)$. Portanto, $n|(a-c)$. Logo, temos que $a \equiv c(mod\ n)$.

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

$x \equiv y(mod\ n) \Leftrightarrow n|(x-y)$.

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

$$\bar{a} = \{x \in \mathbb{z} \mid x \equiv a(mod\ n)\}$$

Assim,

$$x \in \bar{a} \Leftrightarrow x \equiv a(mod\ n) \Leftrightarrow n \mid (x - a).$$

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

$$a - r = qn \Longrightarrow n \mid (a - r) \Longrightarrow a \equiv r(mod\ n) \qquad (1.1)$$

Assim por definição $a \in \bar{r}$.

Considere $x \in \bar{a}, então\ x \equiv a(mod\ n)$, por (1.1) e usando transitividade temos $x \equiv r(mod\ n)$, então $x \in \bar{r}$ e assim $\bar{a} \sqsubset \bar{r}$.

Por outro lado, se $x \in \bar{r}$, 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, $x \in \bar{a}$ e dai $\bar{r} \sqsubset \bar{a}$, portanto $\bar{a} = \bar{r}$, onde $r \in \{0,1,2,..,n-1\}$.

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

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

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

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

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

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

Exemplo 2.2.1. Para $n = 2$, temos $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. Deste modo,

$\bar{0} = \{x \mid x \equiv 0(mod\ 2)\} \Leftrightarrow 2|x \Leftrightarrow x = 2q, q \in \mathbb{z}$, logo

$$\bar{0} = \{x \in \mathbb{z} \mid x = 2q, q \in \mathbb{z}\}$$

$$\bar{1} = \{x \in \mathbb{z} \mid x \equiv 1(mod\ 2)\} \Leftrightarrow 2 \mid (x - 1) \Leftrightarrow x - 1 = 2q \Leftrightarrow x = 2q + 1, q \in \mathbb{z}, logo$$

$$\bar{1} = \{x \in \mathbb{z} \mid x = 2q + 1, q \in \mathbb{z}\}$$

Exemplo 2.2.2. Para $n = 4$, temos $\mathbb{z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Temos que,

$\bar{0} = \{x \mid x \equiv 0(mod\ 4)\} \Leftrightarrow 4|x \Leftrightarrow x = 4q, q \in \mathbb{z}$. Logo,

$$\bar{0} = \{x \in \mathbb{z} \mid x = 4q, q \in \mathbb{z}\}$$

$\bar{1} = \{x \mid x \equiv 1(mod\ 4)\} \Leftrightarrow 4 \mid (x-1) \Leftrightarrow x - 1 = 4q \Leftrightarrow x = 4q + 1, q \in \mathbb{z}$. Portanto,

$$\bar{1} = \{x \in \mathbb{z} \mid x = 4q + 1, q \in \mathbb{z}\}$$

$\bar{2} = \{x \mid x \equiv 2(mod\ 4)\} \Leftrightarrow 4 \mid (x-2) \Leftrightarrow x - 2 = 4q \Leftrightarrow x = 4q + 2, q \in \mathbb{z}$. Logo,

$$\bar{2} = \{x \in \mathbb{z} \mid x = 4q + 2, q \in \mathbb{z}\}$$

$\bar{3} = \{x \mid x \equiv 3(mod\ 4)\} \Leftrightarrow 4 \mid (x-3) \Leftrightarrow x - 3 = 4q \Leftrightarrow x = 4q + 3, q \in \mathbb{z}$. Logo,

$$\bar{3} = \{x \in \mathbb{z} \mid x = 4q + 3, q \in \mathbb{z}\}$$

2.2.1 Adição em $\mathbb{Z}_n$

Em $\mathbb{z}_n$ podemos definir as operações de adição e multiplicação

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

$$\oplus: \quad \mathbb{z}_n \times \mathbb{z}_n \longrightarrow \mathbb{z}_n$$

$$(\bar{a}, \bar{b}) \longrightarrow \bar{a} \oplus \bar{b} = \overline{a + b}$$

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

1. **Associatividade**

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

2. **Existência do elemento neutro.**

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

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

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

3. **Existência do elemento inverso.**

   Sejam $\bar{a}, \bar{c} \in \mathbb{z}_n$, tais que $\bar{a} \oplus \bar{c} = \bar{0}$, temos

   $\overline{a+c} = \bar{0} \Longrightarrow a + c \in \bar{0}, a + c \equiv 0 (mod\ n) \Longrightarrow \mid a + c$

   $\Longrightarrow \exists\ q \in \mathbb{z};\ \ a + c = nq \Longrightarrow c = nq - a \Longrightarrow \bar{c} = \overline{nq} + \overline{-a} \Longrightarrow \bar{c} = \bar{0} + \overline{-a} \Longrightarrow$

   $\bar{c} = \bar{n} + \overline{-a} \Longrightarrow \bar{c} = \overline{n-a}.$

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

Exemplo 2.2.3. Considere o grupo $\mathbb{z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, e sua tábua de operação

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

2.2.2 Multiplicação em $\mathbb{Z}_n$

Definamos em $\mathbb{z}_n$ a operação **Multiplicação** como sendo

$$\odot : \qquad \mathbb{z}_n \times \mathbb{z}_n \longrightarrow \mathbb{z}_n$$
$$(\bar{a}, \bar{b}) \longrightarrow \bar{a} \odot \bar{b} = \overline{a \cdot b}$$

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

Exemplo 2.2.4. Aqui, temos a tábua de operação de $\mathbb{Z}_3$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

A multiplicação em $\mathbb{Z}_n$ satisfaz as seguintes propriedades:

1. **Associatividade**

   Dados $\bar{a}, \bar{b}, \bar{c} \in \mathbb{z}$ temos,

$$\begin{aligned}\bar{a} \odot (\bar{b} \odot \bar{c}) &= \bar{a} \odot (\overline{b \cdot c}) \\ &= \overline{a \cdot (b \cdot c)} \\ &= \overline{(a \cdot b) \cdot c} \\ &= \overline{(a \cdot b)} \odot \bar{c} \\ &= (\bar{a} \odot \bar{b}) \odot \bar{c}\end{aligned}$$

2. **Elemento Neutro**

   Dados $a \in \mathbb{z}_n$ temos,

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

   Logo, $\bar{1}$ é o elemento neutro.

3. **Inverso Multiplicativo**

   Dado $\bar{a} \in \mathbb{z}_n$, vamos procurar um critério para saber se $\bar{a}$ é inversível em $\mathbb{Z}_n$. Para isso, suponhamos que exista $\bar{b} \in \mathbb{z}_n$ tal que $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} = \bar{1}$. Logo, se $\bar{a} \cdot \bar{b} = \bar{1}$, segue que $\overline{a \cdot b} = \bar{1}$, daí, $a \cdot b \in \bar{1}$, 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 $mdc(a, n) = 1$, pela identidade Bezout [6] (JANESCH, 2008, p.118), existem $x, y \in \mathbb{z}$ tal que $ax + ny = 1$, porem,

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

$\Longrightarrow \bar{a} \cdot \bar{x} + \bar{0} \cdot \bar{y} = \bar{1} \Longrightarrow \bar{a} \cdot \bar{x} = \bar{1}.$

Portanto, existe $\bar{b} \in \mathbb{z}_n$ tal que

$$\bar{a} \cdot \bar{b} = 1 \Leftrightarrow mdc(a, n) = 1 \qquad (1.2)$$

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

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

2.3 O Grupo das Permutações

A permutação é o termo específico usado na teoria dos grupos para designa uma bijeção de um conjunto nele mesmo. Seja 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*). De fato, sendo $f, g \; e \; h \in S_X$, vemos que a operação de composição está bem definida em S_X pois a composição de duas bijeções também será uma bijeção. Se $f: S_X \longrightarrow S_X$ e $g: S_X \longrightarrow S_X$ são bijeções, então $g \circ f: S_X \longrightarrow S_X$ também é uma bijeção. Como a composição de funções é associativa em seu conjunto universo, a mesma será válida para um subconjunto particular S_X. Logo, para todo $f, g \; e \; h \in S_X$, $(f \circ g) \circ h = f \circ (g \circ h)$. Ademais, dado $f \in S_X$, e e a identidade $e(x) = x, \forall x \in X$ temos;

$(\Longrightarrow) \; f \circ e(x) = f\big(e(x)\big) = f(x)$

$(\Longleftarrow) \; e \circ f(x) = e\big(f(x)\big) = f(x)$

Portanto, e elemento neutro da operação $\circ$ em S_X.E por fim, f é uma bijeção de S_X então f^{-1}(aplicação inversa) também será, pois a inversa de uma bijeção também é uma bijeção, e esta será o elemento inverso de f para composição de aplicações, visto que $f \circ f^{-1} = f^{-1} \circ f = i_e$.

Portanto $(S_X, \circ)$ é um grupo, o grupo das permutações sobre S_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) Notemos que, para $n = 1$ é verdadeira, pois se X possui um elemento, então só existe uma 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 $X = \{1, 2, \dots, k, k+1\}$, 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.
- ⋮
- k possui 2 possibilidades para associar com os elementos de X.
- $k + 1$ possui 1 possibilidade para associar com os elementos de X.

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

Exemplo 2.3.1. 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,

$g(b) = c$

$g(c) = b$

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

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

2.4 Subgrupos

Definição 2.7. Seja 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 2.2.

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 lados por a^{-1}, temos:

$$e_H \cdot a \cdot a^{-1} = a \cdot a^{-1}$$
$$e_H \cdot e = e, então\ e_H = e.$$

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 2.4.1. 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,

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

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

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

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

Exemplo 2.4.2. 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

$(i)\ a + b = mr_1 + mr_2 \Rightarrow a + b = m(r_1 + r_2) \in H$

$(ii)\ Dado\ a \in H, Daí,$

$$a^{-1} = -mr_1 = m(-r_1) \in H$$

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

Exemplo 2.4.3. 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 $a \neq 0$, com $H < \mathbb{Z}$, temos $-a \in H$. Agora considere $W = \{x \in H \mid x > 0\}$. Pelo parágrafo anterior $W \neq \emptyset$, então pelo princípio da boa ordenação, W possui elemento mínimo, assim sendo $n = \min\{W\}$, vamos provar que $H = n\mathbb{Z}$. Como $n \in H$, pois $n \in W \subset H$, temos $n \cdot k \in H, \forall k \in \mathbb{Z}, pois,$

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

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 $0 \leq r < n$. 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 $H = n\mathbb{Z}$.

2.5 Subgrupos Finitamente Gerados

Definição 2.8. 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. Se $S_1 \subseteq S_2 \subseteq G$, então $\langle S_1 \rangle \sqsubseteq \langle S_2 \rangle$.
4. $H = \langle S \rangle$,dizemos que S gera H.
5. Se H é subgrupo de G então $\langle H \rangle = H$.
6. Se $S = \{x_1, \dots, x_n\}$, usamos a notação $\langle x_1, x_2, \dots, x_n \rangle$ ao invés de $\langle \{x_1, \dots, x_n\} \rangle$.
7. $\langle S \rangle$ **é 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 $\langle S \rangle \subseteq K$.

Definição 2.9. 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.**

Exemplo 2.5.1. 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 $\beta^2 = \beta = Id$, dai, $\langle \alpha, \beta \rangle = \{Id, \alpha, \beta, \alpha\beta\}$

3. O grupo $(\mathbb{Z}_n, \bigoplus)$ 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 exista $a \in G - \{0\}$ 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, $m \in \mathbb{Z}$. Portanto $(\mathbb{Q}, +)$ não é cíclico.

7. $\mathbb{Q}$ não é finitamente gerado.
   De fato, considere

$$\mathbb{Q} = \langle \frac{p_1}{q_2}, \cdots, \frac{p_n}{q_n} \rangle \ e \ \alpha = \frac{1}{q_1, \cdots, q_n} \in \mathbb{Q}.$$

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

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

   Daí,

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

Mas, como já vimos acima, $\mathbb{Q}$ 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 $w_n = \cos\frac{2\pi}{n} + i \ \text{sen}\frac{2\pi}{2}$. Então

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

2.5.1 Ordem de um Elemento do Grupo

Definição 2.10. 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 $O(a) = \min\{n \in \mathbb{N} \mid a^n = e\}$.

Exemplo 2.5.2. 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

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

   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 2.3. Seja g um grupo.

1. Dado $a \in g$, e $a \neq 0$, tem $O(a) = 2 \Leftrightarrow a = a^{-1}$.
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. $O(a) = 2 \Leftrightarrow a^2 = e$.

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

$(\Longleftarrow)$ 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, $a^r(a^{-1})^r = a^r \Longrightarrow e = a^r$, 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 $(a^m)^n = e$, segue que $a^{m\cdot n} = e$, mas, como $m \cdot r < m \cdot n$, isso contradiz a minimalidade de $m \cdot n$. Logo, $O(a^m) = n$.

Teorema 2.1. Seja 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

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

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 $p, r \in \mathbb{Z}$ 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 2.5.3. Vamos determinar $\langle \alpha \rangle \in S_e$ 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 2.5.4. 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,

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

Teorema 2.2. Se os únicos subgrupos de um grupo são $\{e\}$ e G, então G é cíclico de ordem prima.

Demonstração. Dado $a \in G$, se $a = \{e\}$, temos $\langle \alpha \rangle = \{e\}$. Se $a \neq e$, temos $\langle a \rangle \neq \{e\}$.

Por hipótese $\langle \alpha \rangle = G$.

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 $p, q \in \mathbb{N}$.

Como $1 < p, q < n$, com $n = p \cdot q$. Considere o subgrupo $K = \langle a^{\frac{n}{p}} \rangle$ e pela proposição 2.3 K tem ordem p. Portanto, $K \neq \{e\}$ e também $K \neq G$, mas isso contradiz a hipótese.

Proposição 2.4. 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,
   $\{t \geq 0; \alpha^t = e\} = \{0, n, 2n, \dots\}$ e $\langle \alpha \rangle = \{e, \alpha, \dots, \alpha^{n-1}\}$

Demonstração. $(1) \Longrightarrow (2)$ como $\langle \alpha \rangle = \{\alpha^m | m \in \mathbb{Z}\}$, e com 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 $\langle \alpha \rangle = \{e, \alpha, \alpha^2, \dots, \alpha^{r-1}\}$ e os elementos $e, \alpha, \alpha^2, \dots, \alpha^{r-1}$ 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 $e, \alpha, \alpha^2, \dots, \alpha^{r-1}$ são elementos distintos de G. Mas para provar que $\langle \alpha \rangle = \{e, \alpha, \alpha^2, \dots, \alpha^{r-1}\}$, mostremos que $\forall\, m \in \mathbb{Z}, \alpha^m = \alpha^1$ para alguns $0 \leq 1 < r$. Pelo Algoritmo de Euclides, existem $q, 1 \in \mathbb{Z}$ tais que $m = qr + 1$ com $0 \leq 1 < r$, e portanto $\alpha^m = \alpha^{qr+1} = (\alpha^r)^q \cdot a^1 = e^q \cdot \alpha^1 = \alpha^1$.

3 CLASSES LATERAIS E TEOREMA LAGRANGE

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

3.1 Classes Laterais

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

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

É uma relação equivalência. De fato,

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

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

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

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

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

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 é a classe lateral do elemento neutro e a 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 o 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 3.1. 1. Note que, $a = a \cdot e \in aH$ e $a = e \cdot a \in Ha$

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_aé bijetiva.

3. Se H é finito então Ha e aH são finitas e $|Ha| = |H| = |Ha|$.
4. $a \in H \Leftrightarrow Ha = H$ e $a \in H \Leftrightarrow aH = H$.
5. Na notação aditiva, ao invés de $a \cdot H$, usamos $a + H = \{a + h | h \in H\}$.

Exemplo 3.1.

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

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

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 $H\beta \neq \beta H$.

Teorema 3.1. Sejam G um grupo e H um subgrupo de G. Então, toda classe lateral à esquerda (à direita) tem a mesma cardinalidade de H. Além disso, os conjuntos H_E e H_D tem a mesma cardinalidade.

Demonstração: Para cada $g \in G$, consideremos a função

$$f: H \longrightarrow gH$$
$$h \longmapsto gh.$$

é claro que f é sobrejetora. Por outro lado, dados $h_1, h_2 \in H$, obtemos

$$f(h_1) = f(h_2) \Longrightarrow gh_1 = gh_2 \Longrightarrow h_1 = h_2$$

logo, f é injetora e, portanto, é bijetora. Da mesma forma, prova-se que

$$f: H \longrightarrow Hg$$
$$h \longmapsto hg$$

é bijetora. Para outra parte.

$$\varphi: H_E \longrightarrow H_D$$
$$gH \longmapsto Hg^{-1}$$

define uma função de H_E em E_D. Com efeito, se g_1H e g_2H são elementos quaisquer de H_E e $g_1H = g_2H$, então

$$g_1 \equiv_E g_2 \Leftrightarrow g_1^{-1}g_2 = h \in H \Leftrightarrow g_1^{-1} = hg_2^{-1}$$

por isso,

$$\varphi(g_1H) = Hg_1^{-1} = Hhg_2^{-1} = Hg_2^{-1} \qquad (\text{pois } h \in H)$$
$$= \varphi(g_2H).$$

de modo que $\varphi(g_1H) = \varphi(g_2H)$, isto é, φ está bem definida. Agora, dado $Hg \in H_D$, o elemento $g^{-1}H \in H_E$ é tal que $\varphi(g^{-1}H) = Hg$ de modo que φ é sobrejetora. Por fim,

$$\varphi(g_1H) = \varphi(g_2H) \Leftrightarrow Hg_1^{-1} = Hg_2^{-1}$$

$$\Leftrightarrow g_1^{-1} \equiv_D g_2^{-1}$$
$$\Leftrightarrow g_1^{-1} g_2 = h \in H.$$

Ou seja, $g_2 = g_1 h$. Desse modo,

$$g_2 H = g_1 h H = g_1 H \quad \text{(pois } h \in H\text{)}.$$

O que mostra que φ é injetora e, assim, é bijetora. Por isso, H_E e H_D tem a mesma cardinalidade.

Definição 3.1. 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 3.1. 1. Temos que $G = \bigcup_{x \in G} Hx$;

2. $Hx = Hy \Leftrightarrow x \cdot y^{-1} \in H$;
3. Se $Hx \neq Hy$ então $Hx \cap Hy = \emptyset$.

Demonstração. 1. Claramente $\bigcup_{x \in G} Hx \sqsubset G$. Agora dado $a \in G$, temos que $a \in Ha \sqsubset \bigcup_{x \in G} Hx$. 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 $a \in H$, existem $h_1 h_2 \in H$ tais que $xy^{-1} = h_1$ e $a = h_2 x$, então
   $a - h_2 x = h_2 h_1 y \in Hy$. Logo, $H \subset Hy$ e por 3.1 temos a igualdade.
3. Suponha $a \in H \neq Hy$, então existem $h_1 h_2 \in H$ tais que $a = h_1 x$ e $a = h_2 y$, daí, $h_1 x = h_2 y \Longrightarrow xy^{-1} = h_1^{-1} h_2 \in H$ e por 2, temos $Hx = Hy$, contradição!.

Os mesmos resultados são análogos para as classes laterais a esquerda de H.
Agora, temos condições suficientes para provar o Teorema de Lagrange.

3.2 Teorema de Lagrange

Teorema 3.2. Sejam G um grupo finito e H um subgrupo de G. Então, a ordem de H divide a ordem de G, ou seja,

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

Demonstração. Como G é finito, teremos finitas classes laterais distintas, consideremos $(G : H) = m$. Sabemos que o número de classe laterais à direita e à esquerda é o mesmo, então vamos apenas considerar as classes laterais à esquerda de H. Sejam $x_1H, x_2H, \dots, x_mH$, as m distintas classes laterais à esquerda de H em G.

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

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

4 ALGUMAS APLICAÇÕES DO TEOREMA DE LAGRANGE

Neste capítulo veremos algumas consequências do teorema de Lagrange.

4.1 Consequências Imediatas do Teorema de Lagrange

Aplicação 4.1.1. Seja G um grupo finito e de ondem 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 4.1.2. 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 4.1.3. 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 $O(a)\big||H|$ *e* $O(a)\big||K|$, Como $mdc(|K||H|) = 1$, temos que $O(a) = 1$, e daí $a = e$.

Aplicação 4.1.4. Se $|G| = 2p$, onde p é um primo ímpar, 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 $O(x) \leq 4$, 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 4.1.5 (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 $\mathcal{U}(\mathbb{Z}_p) = \{\bar{x} \in \mathbb{Z}_p \mid mdc(x, p) = 1\}$

É um grupo com a multiplicação de $\mathbb{Z}_p$, como $p \nmid a$. 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 $\bar{a} \in \mathcal{U}(\mathbb{Z}_p)$, e daí,

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

5 CONSIDERAÇÕES FINAIS

Ao final deste trabalho, concluímos que a importância do Teorema de Lagrange se estende para além da própria álgebra. O Teorema de Lagrange é o teorema central no estudo da teoria dos grupos finitos, no entanto para além de sua aplicabilidade na teoria dos grupos. O Teorema de Lagrange exerce um papel importante na teoria dos números como vimos, por exemplo, na demonstração do Pequeno Teorema de Fermat.

A relação entre a ordem do subgrupo e a ordem do grupo tem uma importância fundamental no entendimento de alguns resultados relacionados ao Homomorfismos de grupo em particular aos Isomorfismos que visam fazer uma identificação entre dois grupos.

Ao final desse trabalho é possível perceber o quanto a álgebra abstrata se estrutura nesses resultados centrais e com isso percebemos a sua importância no contexto geral da matemática.

REFERÊNCIAS BIBLIOGRÁFICAS

BASSALO, José Maria Filardo; CATTANI, Mauro Sérgio Dorsa. Grupo. In: BASSALO, José Maria Filardo; CATTANI, Mauro Sérgio Dorsa. **Teoria de Grupos**. São Paulo: Livraria da Física, 2008. p. 1-285. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=lang_pt&id=v54yI87xsq4C&oi=fnd&pg=PR11&dq=grupo+das+permuta%C3%A7%C3%B5es+teoria+dos+numeros&ots=DwrG5TcPWl&sig=ReFmGee_6VPXy5fZddDNa5akeXc#v=onepage&q&f=false. Acesso em: 25 set. 2021.

OLIVEIRA, Marciel Santiago de. **GRUPOS FINITOS E O TEOREMA DE LAGRANGE**. 2016. 44 f. TCC (Graduação) - Curso de Matemática, Universidade Federal de Campina Grande, Cuité, 2016.

SANTOS, Francicarlos de Medeiros. **Uma Introdução à Teoria dos Grupos**. 2018. 47 f. TCC (Graduação) - Curso de Matemática, Universidade Federal do Rio Grande do Norte, Caicó, 2018.

SOUZA, Rodrigo Luiz de (ed.). PERMUTAÇÕES, GRUPOS E SIMETRIAS. **Ciência e Natura**, [S.L.], v. 37, p. 289, 7 ago. 2015. Universidad Federal de Santa Maria. http://dx.doi.org/10.5902/2179460x14620.

VIANA, Thiago Mariano; TRAVASSO, Marco Antônio; TAMAROZZI, Antônio Carlos. GRUPOS DE PERMUTAÇÕES E ALGUMAS DE PROPOSIÇÕES. In: ENCONTRO DE ENSINO, PESQUISA E EXTENSÃO, ., 2012, Presidente Prudente. **Anais [...] .** Presidente Prudente: Especial, 2012. v. 1, p. 26-35.

VIEIRA, Vandenberg Lopes. **Álgebra Abstrata Para Licenciatura**. 2. ed. São Paulo: Livraria da Física, 2015. 670 p.

YARTEY, Joseph Nee Anyah (ed.). **Álgebra II**. Salvador: Cte-Sead, 2017. 243 p.