Universidade Estadual da Paraíba
Centro de Ciências e Tecnologia
Departamento de Matemática

O Teorema de Lagrange

Joel Gilvandro de Freitas

Trabalho de Conclusão de Curso

Orientador: **Prof. Dr. Vandenberg Lopes Vieira**

Banca Examinadora:

Prof. Dr. Vandenberg Lopes Vieira - DM/UEPB

Prof. Dra. Maria Isabelle Silva - DM/UFEB

Prof. Msc. Fernando Luiz T. da Silva - DM/UEPB

Trabalho de Conclusão de Curso apresentado na Universidade Estadual da Paraíba, como parte dos requisitos exigidos para a obtenção do título de Licenciado em Matemática.

03 de Outubro 2012
Campina Grande - PB

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

F866t Freitas, Joel Gilvandro de.

O Teorema de Lagrange [manuscrito] / Joel Gilvandro de Freitas. – 2012.

55 f.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2012.

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

1. Teoria dos grupos. 2. Álgebra. 3. Classes laterais. I. Título.

21. ed. CDD 512.5

JOEL GILVANDRO DE FREITAS

O TEOREMA DE LAGRANGE

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

BANCA EXAMINADORA

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

Profª. Drª. Maria Isabelle Silva
Departamento de Matemática – CCT/UEPB
Examinadora

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

Campina Grande, 03 de Outubro de 2012

A toda minha família e em especial

aos meus pais por todo o incentivo.

DEDICO

Agradecimentos

Neste momento tão especial para mim, não poderia deixar de direcionar os meus sinceros agradecimentos a todos que contribuíram para que este evento se realize hoje.

Ao meu eterno Deus por ter me dado saúde, coragem e sabedoria;

Aos meus familiares que colaboraram de forma direta e indiretamente, especialmente aos meus pais;

Ao meu orientador, Vandenberg Lopes por ter me dado a oportunidade de começar uma caminhada no estudo da álgebra e pela força dada durante o curso;

Ao meu estimado ex-professor de matemática do ensino fundamental, mestre e professor da UFCG, Fernando Leite Aires que tanto me incentivou para estudar;

A UEPB por ter oferecido o curso de matemática;

A todos os meus ex – professores por ter, cada um, dado a sua contribuição para minha formação;

A minha turma por toda amizade

Agradeço a todos.

Resumo

Neste trabalho abordamos o Teorema de Lagrange que é o principal teorema sobre grupos finitos. São muitas as aplicações desse importante resultado. Entretanto, por se tratar de um trabalho de conclusão de curso, o texto foi basicamente planejado para servir de suporte a alunos de graduação. Por isso, focalizamos os resultados básicos os quais, em geral, são vistos em um curso de Licenciatura em Matemática. Assim, após uma breve introdução, apresentamos inicialmente o conceito de operação binária e, em seguida, consideramos o conceito de grupo. Destacamos os resultados necessários relacionados a esse conceito com o objetivo de apresentar e demonstrar o Teorema de Lagrange.

Palavras-chave: Grupo, Classes Laterais, Teorema de Lagrange.

Sumário

Introdução

Desde os tempos antigos, o homem sempre viveu fazendo suas descobertas nas mais variadas áreas do conhecimento, e isto não foi diferente com os números. Tais descobertas surgiram da necessidade de se resolver problemas do seu cotidiano. Essas descobertas deram - se também com os números: naturais $\mathbb{N}$, inteiros $\mathbb{Z}$, reais $\mathbb{R}$, racionais $\mathbb{Q}$ e irracionais $\mathbb{I}$.

Era comum trabalhar com situações em que faltavam dados, mas tinham conhecimento do resultado final. A esse tipo de problema deram o nome de equações algébricas por empregarem letras no lugar do número desconhecido. Até então, tinham conhecimentos de meios de resolução de equações até o quarto grau por meio de radicais, ou seja, toda equação de grau inferior ou igual a quatro era resolvida empregando radicais. Para equações que apresentavam graus superiores a quatro, não se conheciam meios de resolução empregando radicais.

Na busca de obter meios para resolução de equações de graus superiores a quatro, no ano 1777, Joseph Louis Lagrange estudando solução de equações pelo método já existente (utilizando radical na resolução), utilizou a permutação de raízes, (e foi o primeiro matemático a compreender que utilizando as permutações, conseguiria provar a sua tese), verificou a impossibilidade de se encontrar solução para essas equações empregando radicais. Deixou assim, um caminho para o matemático Paolo Ruffini, de origem italiana, (considerado o seu discípulo), trilhar na busca de soluções para

essas equações. Mais uma vez, a permutação foi empregada por Paolo Ruffini nessas resoluções de equações e concluiu também que equações de graus superiores a quatro eram insolúveis por radicais.

Sabe - se que muitos matemáticos pesquisavam a cerca de encontrar meios para resolver equações de graus superiores a quatro. Assim, no início do século XIX, Niels Henrik Abel mostrou a impossibilidade de resolução dessas equações por meios de radicais.

Outro importante matemático a trabalhar com equações foi Evariste Galois que continuou o trabalho de Abel. Foi atribuído a ele (Galois), o primeiro matemático a desenvolver a ideia de grupo, (mas a definição formal de grupos foi dado por Augustin – Louis Cauchy em suas publicações acerca das permutações), reunindo equações de grau qualquer em um conjunto fechado em relação à multiplicação, formado pelas permutações de raízes de equações que eram solúveis por radical. A esse tipo de conjunto foi chamado de grupo de Galois. Com isso, Galois contribuiu com a identificação de equações polinomiais que são solúveis por radical quando definiu que uma equação é resolúvel por radical se, e somente se, o grupo formado pelas permutações de suas raízes é igual ao grupo formado pelo quociente de dois corpos é solúvel.

A ideia de grupos surgiu do trabalho de vários matemáticos, tais como: Euler, Gauss, Lagrange, Abel e Galois. Vale ressaltar, que a teoria dos grupos surgiu por três vias. São elas: a teoria das equações, a teoria dos números e geometria, ou seja, estes três itens foram a base para chegar a conceito de grupo.

Depois que foi estabelecida a ideia e o conceito de grupo, muitos matemáticos passaram a empregar os grupos nos seus trabalhos. Exemplo disso, foi o matemático norueguês Sophus Lie. Por esta razão, o seu trabalho nos estudos de equações diferenciais usando permutações, foi chamado de grupos de Lie.

Évariste Galois (1811-1832) foi um matemático Francês que basicamente deu início ao estudo dos grupos, obtendo resultados relevantes para o estudo de soluções de equações algébricas. O estudo deste ramo da matemática é realizado pela teoria que leva seu nome — a Teoria de Galois.

Essa teoria é a interação entre polinômios e as estruturas algébricas de grupos e corpos. Galois associou um grupo a cada polinômio e usou propriedades desse grupo para dar condições para que a equação algébrica associada ao polinômio seja solúvel por radicais. Na realidade, Galois mostrou que uma equação algébrica é solúvel por radicais se, e somente se, o grupo de automorfismo associado à equação é solúvel. Talvez essa teoria se constitua em uma das mais importantes aplicações da teoria dos grupos e seja um dos mais belos ramos da matemática, pois sintetiza resultados clássicos da teoria dos grupos e da teoria dos corpos, de modo a fornecer uma resposta completa ao problema da solubilidade de polinômios por radicais.

Capítulo 1

Operações Binárias e Grupos

Dentre as estruturas algébricas de interesse, um grupo é relativamente a mais simples quando comparada com outras tais como anel e corpo, pois é uma estrutura dotada de apenas uma operação. Por isso, essa relativa simplicidade deve-se principalmente a esse fato.

Vale à pena ressaltar que a teoria dedicada ao estudo dos grupos — Teoria dos Grupos —, abrange tópicos de complexidade considerável. Nela, há vários problemas que ainda não foram resolvidos (os chamados problemas em aberto) que desafiam pesquisadores da área. Por essa razão, é razoável que o leitor tenha bastante cuidado em interpretar a palavra simples mencionada acima.

O que iremos fazer neste capítulo é iniciar o estudo de grupos, destacando os resultados necessários de modo a considerar os conceitos que cercam o Teorema de Lagrange, que é a essência deste trabalho.

Inicialmente, apresentaremos o conceito de operação binária. Após esse, o conceito de grupo surge naturalmente.

Definio 1.1 *Seja A um conjunto não-vazio. Uma função $f : A \times A \to A$ chama-se* ***operação binária*** *sobre A.*

Chamaremos uma operação binária simplesmente de *operação*.

Observa-se que uma operação sobre A associa cada par ordenado (a, b) de elementos de A num único elemento $f(a, b) \in A$. É comum usar outros símbolos para representar a operação f, tais como $\star$, $+$, $\cdot$, $\circ$, entre outros. Por exemplo, escolhendo o símbolo $\star$, temos que $f(a, b) = \star(a, b)$. Essa notação não tem praticidade para o desenvolvimento de alguns resultados. Por isso, denotaremos o elemento $\star(a, b)$ por $a \star b$, de modo que

$$f(a, b) = \star(a, b) = a \star b.$$

O elemento $a \star b$ chama-se **composto** de a e b pela operação $\star$, sendo a e b o primeiro e segundo termos do composto, respectivamente.

Dois casos particulares de símbolos serão frequentemente usados no decorrer do texto, a saber a operação de **adição** ou **soma** " $+$ " e a operação de **multiplicação** ou **produto** " $\cdot$ ". Nestes casos, os elementos do composto $a + b$ são as **parcelas**; enquanto que no composto $a \cdot b$ são os **fatores**.

Exemplo 1.1 As funções $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ e $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dadas por $f(a, b) = a + b$ e $g(a, b) = a \cdot b$ são as operações de adição e multiplicação sobre $\mathbb{N}$. Por exemplo, $f(2, 3) = 2 + 3 = 5$ e $g(2, 3) = 2 \cdot 3 = 6$. Estas operações podem ser estendidas aos conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

Exemplo 1.2 A função $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por $f(a, b) = a + 3$ é uma operação de adição sobre $\mathbb{Z}$ diferente da usual. Temos $f(3, 5) = 3 + 3 = 6$ e $f(5, 3) = 5 + 3 = 8$. ♣

Exemplo 1.3 Consideremos $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $g(a, b) = a^b$; esta é a operação de potenciação sobre $\mathbb{N}$. Ela pode ser estendida a $\mathbb{Z}$? Observamos primeiramente que uma operação binária sobre um conjunto A é definida para todo par ordenado $(a, b) \in A^2$. Como $(2, -3) \in \mathbb{Z}^2$ e $f(2, -3) = 2^{-3} = \frac{1}{8} \notin \mathbb{Z}$, então f não pode ser estendida a $\mathbb{Z}$.

Exemplo 1.4 Denotemos por $M_{n\times m}(\mathbb{R})$ o conjunto de todas as matrizes reais (ou com entradas reais) de ordem $n \times m$. A adição F e a subtração de matrizes G,

$$\begin{array}{rccc} F: & M_{n\times m}(\mathbb{R}) \times M_{n\times m}(\mathbb{R}) & \to & M_{n\times m}(\mathbb{R}) \\ & (A, B) & \mapsto & A + B, \end{array}$$

e

$$\begin{array}{rccc} G: & M_{n\times m}(\mathbb{R}) \times M_{n\times m}(\mathbb{R}) & \to & M_{n\times m}(\mathbb{R}) \\ & (A, B) & \mapsto & A - B, \end{array}$$

são operações sobre $M_{n\times m}(\mathbb{R})$. Também são operações sobre $M_{n\times m}(\mathbb{C})$ (com entradas complexas). Agora, e quanto ao produto de matrizes? Bem, dados $A, B \in M_{n\times m}(\mathbb{R})$, o produto $A \cdot B$ só é definido quando o número de colunas de A for igual ao número de linhas de B, isto é, quando $n = m$. Por isso, o produto de matrizes não é uma operação sobre $M_{n\times m}(\mathbb{R})$ se $n \neq m$. Entretanto, ele é uma operação sobre o conjunto $M_n(\mathbb{R})$ de todas as matrizes reais de ordem n. ♣

Exemplo 1.5 Seja A um conjunto não-vazio. Para funções $f : A \to A$ e $g : A \to A$, tem-se a composta $g \circ f : A \to A$. Portanto, a composição de funções,

$$\begin{array}{rccc} H: & A^A \times A^A & \to & A^A \\ & (f, g) & \mapsto & g \circ f, \end{array}$$

é uma operação sobre o conjunto $A^A = \{f : A \to A\}$ de todas as funções de A em A.

Exemplo 1.6 *Através dos resultados clássicos sobre o conjunto $\mathbb{Z}_n$, sabe-se que para cada número natural n,*

$$\begin{array}{rccc} +: & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} + \overline{b} = \overline{a + b} \end{array} \quad e \quad \begin{array}{rccc} \cdot: & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \cdot \overline{b} = \overline{a \cdot b} \end{array}$$

definem duas operações de adição e multiplicação sobre $\mathbb{Z}_n$. ♣

Definio 1.2 *Uma **estrutura algébrica** é um conjunto A não-vazio munido de uma ou mais operações.*

Uma estrutura algébrica A com uma operação $\star$ é frequentemente indicada por $(A, \star)$. Além disso, se $\triangle$ é outra operação em A, então $(A, \star, \triangle)$ indica a estrutura algébrica A munido dessas operações. Assim, são exemplos de estruturas algébricas

$$(\mathbb{N}, +), \quad (\mathbb{Z}, +, \cdot), \quad (\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot) \quad \text{e} \quad (\mathbb{C}, +, \cdot).$$

Em nosso trabalho, vamos considerar estrutura algébrica com uma operação.

1.1 Propriedades Elementares das Operações

Destacaremos algumas propriedades relativas às operações. Essas serão utilizadas no próximo capítulo.

Definio 1.3 *Sejam $\star$ e $\triangle$ duas operações sobre um conjunto A. Diz-se que:*

(a) $\star$ *é* ***associativa*** *quando*

$$a \star (b \star c) = (a \star b) \star c, \quad \forall\ a, b, c \in A.$$

(b) $\star$ *é* ***comutativa*** *quando*

$$a \star b = b \star a, \quad \forall\ a, b \in A.$$

(c) $\star$ *é* ***distributiva à esquerda*** *sobre* $\triangle$ *quando*

$$a \star (b \triangle c) = (a \star b) \triangle (a \star c), \quad \forall\ a, b, c \in A.$$

(d) $\star$ *é* ***distributiva à direita*** *sobre* $\triangle$ *quando*

$$(b \triangle c) \star a = (b \star a) \triangle (c \star a) \quad \forall\ a, b, c \in A.$$

Se $\star$ é distributiva à esquerda tanto à direita sobre $\triangle$, diz-se que $\star$ é ***distributiva sobre*** $\triangle$.

Verifica-se que se a operação $\star$ é comutativa, então $\star$ é distributiva à esquerda sobre $\triangle$ se, e somente se, é distributiva à direita sobre $\triangle$.

Exemplo 1.7 As adições e multiplicações sobre os conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são comutativas e associativas. Além disso, as multiplicações são distributivas sobre as adições.♣

Exemplo 1.8 A operação $\star$ sobre $\mathbb{N}$ dada por

$$a \star b = b, \quad \forall\ a, b \in \mathbb{N},$$

não é comutativa, pois $2 \star 3 = 3$ e $3 \star 2 = 2$, isto é, $2 \star 3 \neq 3 \star 2$. Entretanto, para $a, b, c \in \mathbb{N}$,

$$a \star (b \star c) = a \star c = c$$

e

$$(a \star b) \star c = b \star c = c,$$

ou seja, $\star$ é associativa. ♣

Exemplo 1.9 Consideremos um conjunto não-vazio X. Sabe-se que a operação de composição de funções sobre $A = X^X = \{f : X \to X\}$ não é comutativa. Entretanto, é associativa. ♣

Exemplo 1.10 A soma usual de matrizes sobre $A = M_{n\times m}(\mathbb{R})$ é comutativa e associativa. Sobre $B = M_n(\mathbb{R})$, o produto de matrizes é associativo, mas não é comutativo. Por exemplo, em $A = M_2(\mathbb{R})$,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 8 & 15 \end{pmatrix}$$

e

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 11 & 16 \end{pmatrix}.$$

♣

Quando $\star$ for uma operação sobre A associativa, então $a \star (b \star c) = (a \star b) \star c$ para quaisquer $a, b, c \in A$. Desse modo, pode-se omitir o parêntese da expressão $a \star (b \star c)$ e escrevê-la simplesmente como $a \star b \star c$, sem que haja ambiguidade. Assim, na expressão $a \star b \star c \star d$ em A, pode-se inserir o parêntese para efeito de cálculo em qualquer composto e, ainda assim, obtém-se o mesmo resultado. Desse modo,

$$a \star b \star c \star d = (a \star b) \star c \star d = a \star (b \star c) \star d = a \star b \star (c \star d)\,.$$

Este resultado pode ser generalizado para n elementos $a_1, a_2, \ldots, a_n \in A$.

Definio 1.4 *Seja $\star$ uma operação sobre A. Um elemento $e \in A$ chama-se* ***neutro à esquerda*** *de $\star$ quando*

$$e \star a = a, \quad \forall\ a \in A; \tag{1.1}$$

e dito ***neutro à direita*** *de $\star$ se*

$$a \star e = a \quad \forall\ a \in A. \tag{1.2}$$

Valendo (1.1) *e* (1.2)*, diz-se simplesmente que $e \in A$ é* ***elemento neutro*** *da operação $\star$.*

Seja $\star$ uma operação sobre A com elemento neutro $e \in A$. Diremos que $a \in A$ é **invertível**[1] com relação à operação $\star$, quando existir $a' \in A$ tal que

$$a \star a' = a' \star a = e.$$

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

$$\mathcal{U}_\star(A) = \{a \in A : \exists\ a' \in A \quad \text{com} \quad a \star a' = a' \star a = e\}.$$

[1] Alguns autores usam a palavra *inversível* ou *simetrizável*.

Proposio 1.1 *Uma estrutura algébrica $(A, \star)$ tem no máximo um elemento neutro. Isto é, se $\star$ tem elemento neutro, então ele é único.*

Demonstração: Se e_1 e e_2 são elementos neutros de $\star$, então

$$\begin{aligned} e_1 \star e_2 &= e_2, \quad \text{(pois } e_1 \text{ é neutro)} \\ e_1 \star e_2 &= e_1. \quad \text{(pois } e_2 \text{ é neutro)} \end{aligned}$$

Logo, $e_1 = e_2$. ■

Exemplo 1.11 As adições usuais em $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm o número $e = 0$ como elemento neutro. Já em relação às multiplicações, todas têm o número $e = 1$ como neutro. ♣

Exemplo 1.12 A operação de divisão $\star$ sobre $\mathbb{Q}^*$ é tal que $a \star 1 = a$, para todo $a \in \mathbb{Q}^*$. Isto nos diz que o número $e = 1$ é neutro à direita. Por outro lado, não existe $e \in \mathbb{Q}^*$ tal que $e \star a = a$, para todo $a \in \mathbb{Q}^*$. Por isso, essa operação não tem neutro à esquerda e, assim, não admite neutro. ♣

Exemplo 1.13 Para a estrutura algébrica $(\mathbb{R}^{\mathbb{R}}, \circ)$, a função identidade $id_{\mathbb{R}^{\mathbb{R}}}$ é o elemento neutro da operação de composição de funções, um vez que $f \circ id_{\mathbb{R}^{\mathbb{R}}} = id_{\mathbb{R}^{\mathbb{R}}} \circ f = f$, para qualquer $f \in \mathbb{R}^{\mathbb{R}}$.

Proposio 1.2 *Seja $\star$ uma operação sobre A que é associativa e com elemento neutro e. Se $a \in A$ é invertível, então seu inverso é único.*

Demonstração: Sejam b_1 e b_2 inversos de a. Logo, $a \star b_1 = b_1 \star a = e$ e $a \star b_2 = b_2 \star a = e$; desse modo,

$$\begin{aligned} b_1 &= e \star b_1 &&= (b_2 \star a) \star b_1 \\ &= b_2 \star (a \star b_1) &&= b_2 \star e \\ & &&= b_2, \end{aligned}$$

isto é, $b_1 = b_2$. ■

Exemplo 1.14 No conjunto dos números inteiros, todo elemento tem inverso no que dizer respeito à adição; por isso, $\mathcal{U}_+(\mathbb{Z}) = \mathbb{Z}$. Da mesma forma, $\mathcal{U}_+(\mathbb{Q}) = \mathbb{Q}, \mathcal{U}_+(\mathbb{R}) = \mathbb{R}$ e $\mathcal{U}_+(\mathbb{C}) = \mathbb{C}$. Por outro lado, com respeito à multiplicação, os únicos elementos invertíveis de $\mathbb{Z}$ são ± 1 e, assim, $\mathcal{U}_\bullet(\mathbb{Z}) = \{1, -1\}$. Tem-se também $\mathcal{U}_\bullet(\mathbb{Q}) = \mathbb{Q}^*$, $\mathcal{U}_\bullet(\mathbb{R}) = \mathbb{R}^*$ e $\mathcal{U}_\bullet(\mathbb{C}) = \mathbb{C}^*$. ♣

Exemplo 1.15 Para os conjuntos $A = M_{n\times m}(\mathbb{R})$ e $B = M_n(\mathbb{R})$, tem-se $\mathcal{U}_+(A) = A$ e $\mathcal{U}_\bullet(B) = \{X \in B : \det X \neq 0\}$. ♣

Exemplo 1.16 Sob a composição de funções, para o conjunto $\mathbb{R}^\mathbb{R} = \{f : \mathbb{R} \to \mathbb{R}\}$, tem-se que $\mathcal{U}_\circ(\mathbb{R}^\mathbb{R}) = \{f \in \mathbb{R}^\mathbb{R} : f \text{ é bijetora}\}$. ♣

Definio 1.5 *Seja $\star$ uma operação sobre A. Um elemento $a \in A$ chama-se* ***regular*** *em relação à operação $\star$ quando*

$$a \star x = a \star y \Rightarrow x = y \tag{1.3}$$

e

$$x \star a = y \star a \Rightarrow x = y, \tag{1.4}$$

para todos $x, y \in A$.

Quando ocorrer (1.3), diz-se que $a \in A$ é **regular à esquerda**; e ocorrendo (1.4), a é dito **regular à direita**. É claro que se $\star$ for comutativa, então $a \in A$ é regular à esquerda se, e somente se, a é regular à direita.

Para um conjunto A dotado de uma operação $\star$, o conjunto dos elementos regulares em A será indicado por $\mathcal{R}_\star(A)$.

Exemplo 1.17 No que concerne à adição, todo elemento $a \in \mathbb{Z}$ é regular, pois

$$a + x = a + y \Rightarrow x = y, \quad \forall\, x, y \in \mathbb{Z}.$$

Com relação à multiplicação, o único elemento não-regular em $\mathbb{Z}$ é o número zero. Com efeito,

$$0 = 0 \cdot 5 = 0 \cdot 6 \quad \text{e} \quad 5 \neq 6.$$

Para qualquer elemento $a \in \mathbb{Z} - \{0\}$, tem-se sempre

$$a \cdot x = a \cdot y \Rightarrow x = y, \quad \forall x, y \in \mathbb{Z},$$

pois em $\mathbb{Z}$ vale a lei de cancelamento da multiplicação. Resultados similares são válidos para os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, com suas respectivas adições e multiplicações. ♣

Exemplo 1.18 Toda matriz $A \in M_{n\times m}(\mathbb{Z})$ é regular com respeito à adição. Isso ocorre com o conjunto $M_n(\mathbb{Z})$ no que se refere-se à multiplicação? Certamente não; para $n = 2$, o elemento

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_{n\times m}(\mathbb{Z})$$

é tal que

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix},$$

mas

$$\begin{pmatrix} 0 & 0 \\ 3 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix},$$

isto é, A não é regular. ♣

Exemplo 1.19 *Considere o conjunto* $G = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}$. *Sobre* G *considere a seguinte operação*

$$(a, b) \star (c, d) = (ac, ad + b), \quad \forall\ (a, b), (c, d) \in G.$$

Verificar se:

(a) *A operação* $\star$ *é comutativa.*

(b) *A operação $\star$ tem elemento neutro.*

(c) *Todo elemento de G é invertível em relação à operação $\star$.*

Solução: (a) Sejam $(a,b),(c,d) \in G$. Assim,

$$(a,b) \star (c,d) = (ac, ad+b)$$

e

$$(c,d) \star (a,b) = (ca, cb+d).$$

Nota-se que, em geral, $(a,b) \star (c,d) \neq (c,d) \star (a,b)$. Portanto, a operação não é comutativa.

(b) O elemento $e = (1,0)$ é tal que

$$(1,0) \star (a,b) = (a,b) = (a,b) \star (1,0).$$

Por isso, $e = (1,0)$ é o neutro da operação.

(c) Dado $(a,b) \in G$, vamos verificar se existe $(c,d) \in G$, de modo que

$$(a,b) \star (c,d) = (c,d) \star (a,b) = e = (1,0).$$

Bem,

$$(a,b) \star (c,d) = (1,0) \Rightarrow (ac, ad+b) = (1,0).$$

Logo,

$$ac = 1 \quad \text{e} \quad ad + b = 0 \Rightarrow c = \tfrac{1}{a} \quad \text{e} \quad d = \tfrac{-b}{a}.$$

A igualdade $(c,d) \star (a,b) = (1,0)$ também nos conduz a $c = \frac{1}{a}$ e $d = \frac{-b}{a}$. Portanto, $(c,d) = (\frac{1}{a}, \frac{-b}{a})$ é o inverso de (a,b). Isso mostra que todo elemento de G é invertível em relação à operação $\star$. ♣

Exemplo 1.20 *Seja E um conjunto sobre o qual está definida uma operação associativa $\star$. Mostrar que:*

(a) *$a \in E$ é regular à esquerda se, e somente se, a função $f : E \to E$ dada por $f(x) = a \star x$ é injetora.*

(b) *$\mathcal{R}_\star(E)$ é fechado em relação à operação $\star$.*

Solução: (a) Vamos supor que $a \in E$ é regular à esquerda. Sejam $x, y \in E$ tais que $f(x) = f(y)$. Assim,

$$f(x) = f(y) \Rightarrow a \star x = a \star y \Rightarrow x = y,$$

ou seja, f é injetora. Reciprocamente, se f é injetora e $x, y \in E$ são tais que $a \star x = a \star y$, então

$$a \star x = a \star y \Rightarrow f(x) = f(y) \Rightarrow x = y,$$

isto é, a é regular.

(b) Consideremos $a, b \in R_\star(E)$ e $x, y \in E$. Vamos mostrar que se $(a \star b) \star x = (a \star b) \star y$ e $x \star (a \star b) = y \star (a \star b)$ implicam que $x = y$. Temos que

$$\begin{array}{lcll} (a \star b) \star x & = & (a \star b) \star y & \Rightarrow \\ a \star (b \star x) & = & a \star (b \star y) & \Rightarrow \\ b \star x & = & b \star y, & \Rightarrow \text{ (pois } a \text{ é regular)} \end{array}$$

de modo que $x = y$, pois b também é regular. Portanto, $a \star b$ é regular. O outro caso é tratado similarmente. ♣

Proposio 1.3 *Seja A um conjunto munido de uma operação $\star$ associativa com elemento neutro $e \in A$. Então, todo elemento $a \in A$ invertível é regular, ou seja, $\mathcal{U}_\star(A) \subset \mathcal{R}_\star(A)$.*

Demonstração: Se $a \in \mathcal{U}_\star(A)$, então por definição, existe $a' \in A$ tal que $a \star a' = a' \star a = e$. Consideremos agora $x, y \in A$ com

$$a \star x = a \star y \quad \text{e} \quad x \star a = y \star a.$$

Assim, operando à esquerda da igualdade $a \star x = a \star y$ com a',

$$\begin{array}{rcrcrcl} a \star x & = & a \star y & \Rightarrow & a' \star (a \star x) & = & a' \star (a \star y) \\ & & & \Rightarrow & (a' \star a) \star x & = & (a' \star a) \star y \\ & & & \Rightarrow & e \star x & = & e \star y \\ & & & \Rightarrow & x & = & y. \end{array}$$

Do modo análogo,

$$x \star a = y \star a \Rightarrow x = y.$$

Isso mostra que $\mathcal{U}_\star(A) \subset \mathcal{R}_\star(A)$. ■

As operações sobre $\mathbb{Z}_n$ dadas na Proposição gozam de importantes propriedades conforme destacamos no próximo teorema.

Teorema 1.1 *As operações de adição e multiplicação sobre $\mathbb{Z}_n$ têm as propriedades:*

(1) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}, \quad \forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n.$ (a adição é associativa)

(2) $\overline{a} + \overline{b} = \overline{b} + \overline{a}, \quad \forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n.$ (a adição é comutativa)

(3) $\overline{a} + \overline{0} = \overline{0} + \overline{a}, \quad \forall\ \overline{a} \in \mathbb{Z}_n.$ (existência de elemento neutro da adição)

(4) *Dado $\overline{a} \in \mathbb{Z}_n$, existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} + \overline{b} = \overline{0}$.* (existência de inverso aditivo de cada elemento em $\mathbb{Z}_n$)

(5) $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}, \quad \forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n.$ (a multiplicação é associativa)

(6) $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{b}, \quad \forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n.$ (a multiplicação é comutativa)

(7) $\overline{a} \cdot \overline{1} = \overline{a}, \quad \forall\ \overline{a} \in \mathbb{Z}_n.$ (existência de elemento neutro da multiplicação)

(8) *Dado $\overline{a} \in \mathbb{Z}_n$, existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$ se, e somente se, $mdc(a, n) = 1$.* ($\overline{a}$ tem inverso multiplicativo)

Demonstração: Demonstraremos apenas os itens (1), (4) e (8).

(1) Considerando $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ e o fato de a adição em $\mathbb{Z}$ ser associativa, obtemos

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{(b + c)} = \overline{a + (b + c)} = \overline{(a + b) + c}$$

$$= \overline{a + b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c},$$

ou seja, a adição é associativa.

(4) Dado $\overline{a} \in \mathbb{Z}_n$, existe $\overline{x} \in \mathbb{Z}$ tal que $\overline{a} + \overline{x} = \overline{0}$ se, e somente se, $\overline{a + x} = \overline{0}$. Ou seja,

$$\overline{a} + \overline{x} = \overline{0} \Leftrightarrow \overline{a + x} = \overline{0} = \overline{n},$$

pois $n \equiv 0 (\mathrm{mod}\, n)$. Logo,

$$a + x \in \overline{n} \Leftrightarrow a + x = nk \quad \text{para algum } k \in \mathbb{Z}.$$

Em particular, para $k = 1$, $x = n - a$. Portanto, $\overline{x} = \overline{n - a} \in \mathbb{Z}_n$ é o inverso aditivo de $\overline{a}$.

(8) Dado $\overline{a} \in \mathbb{Z}_n$, suponhamos que existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Logo,

$$\begin{aligned} \overline{a} \cdot \overline{b} = \overline{1} &\Leftrightarrow \overline{a \cdot b} = \overline{1} \Leftrightarrow a \cdot b \equiv 1 (\mathrm{mod}\, n) \\ &\Leftrightarrow a \cdot b - k \cdot n = 1 \quad \text{com} \quad k \in \mathbb{Z}. \end{aligned}$$

Portanto, concluímos que $mdc(a, n) = 1$. Reciprocamente, seja $a \in \mathbb{Z}$ com $mdc(a, n) = 1$. Pela Identidade de Bézout[2], existem $x, y \in \mathbb{Z}$ tais que $a \cdot x + n \cdot y = 1$. Assim,

$$\begin{aligned} a \cdot x + n \cdot y = 1 &\Rightarrow \overline{a \cdot x + n \cdot y} = \overline{1} \Rightarrow \overline{a \cdot x} + \overline{n \cdot y} = \overline{1} \\ &\Rightarrow \overline{a} \cdot \overline{b} + \overline{n} \cdot \overline{y} = \overline{1} \Rightarrow \overline{a} \cdot \overline{b} + \overline{0} \cdot \overline{y} = \overline{1} \\ &\Rightarrow \overline{a} \cdot \overline{b} = \overline{1}, \end{aligned}$$

isto é, $\overline{a}$ tem inverso multiplicativo. ■

[2]A Identidade de Bézout assegura que se a e b são dois inteiros e $d = mdc(a, b)$, então existem inteiros x e y de modo que $d = ax + by$.

1.2 Tábua de uma Operação

Para um conjunto finito A, digamos $A = \{a_1, a_2, \ldots, a_n\}$, uma operação $\star$ sobre A pode ser definida por meio de uma tábua (ou tabela), da seguinte forma: sendo $\star : A \times A \to A$, consideremos

$$a_i \star a_j = a_{ij}, \quad \forall\, i, j \in \{1, 2, \ldots, n\},$$

em que a_i e a_j são os primeiros elementos da i-ésima linha e j-ésima coluna, respectivamente. Portanto, a operação $\star$ faz corresponder, para cada par $(a_i, a_j) \in A^2$, o elemento a_{ij} que está na i-ésima linha e j-ésima coluna. Nestas condições, dispondo os elementos de A na primeira linha e primeira coluna, obtemos a seguinte tábua:

$\star$	a_1	a_2	$\ldots$	a_i	$\ldots$	a_j	$\ldots$	a_n
a_1	a_{11}	a_{12}	$\ldots$	a_{1i}	$\ldots$	a_{ij}	$\ldots$	a_{1n}
a_2	a_{21}	a_{21}	$\ldots$	a_{2i}	$\ldots$	a_{2j}	$\ldots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_i	a_{i1}	a_{i2}	$\ldots$	a_{ii}	$\ldots$	a_{ij}	$\ldots$	a_{in}
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
a_j	a_{j1}	a_{j2}	$\ldots$	a_{ji}	$\ldots$	a_{jj}	$\ldots$	a_{jn}
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
a_n	a_{n1}	a_{n2}	$\ldots$	a_{n3}	$\ldots$	a_{nj}	$\ldots$	a_{nn}

Tábua da operação $\star$

Os elementos $a_{11}, a_{22}, \ldots, a_{nn}$ constituem a **diagonal principal** da tábua de $\star$. A linha

a_{i1}	a_{i2}	$\ldots$	a_{ii}	$\ldots$	a_{ij}	$\ldots$	a_{in}

é a **linha correspondente** ao elemento a_i. Da mesma forma,

a_{1i}
a_{2i}
$\vdots$
a_{ii}
$\vdots$
a_{ji}
$\vdots$
a_{n3}

é a **coluna correspondente** ao elemento a_i. A primeira linha,

a_1	a_2	$\ldots$	a_i	$\ldots$	a_j	$\ldots$	a_n

,

e primeira coluna,

a_1
a_2
$\vdots$
a_i
$\vdots$
a_j
$\vdots$
a_n

da tábua de $\star$ são ditas **fundamentais**.

Exemplo 1.21 A tábua da multiplicação sobre $A = \{1, -1, i, -i\}$ é

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

Exemplo 1.22 Consideremos o conjunto $A = \{1, 2, 3, 4, 6\}$. Temos que $\star$ dada por $a \star b = mdc(a, b)$ é uma operação sobre A. Sua tábua é

$\star$	1	2	3	4	6
1	1	1	1	1	1
2	1	2	1	2	2
3	1	1	3	1	3
4	1	2	1	4	2
6	1	2	3	2	6

.

♣

1.3 Definições e Exemplos de Grupos

Consideremos agora as estruturas algébricas $(\mathbb{Z}, +)$ e $(M_2(\mathbb{R}), +)$. A soma usual em $\mathbb{Z}$ atende as propriedades:

1. $x + (y + z) = (x + y) + z, \quad \forall\ x, y, z \in \mathbb{Z}$. (a adição é associativa)

2. Existe um elemento em $\mathbb{Z}$, indicado por 0, tal que $x + 0 = +x = x$, para todo $x \in \mathbb{Z}$. (existe neutro para a adição)

3. Dado $x \in \mathbb{Z}$, existe um elemento $-x \in \mathbb{Z}$, tal que $x + (-x) = (-x) + x = 0$. (todo elemento em $\mathbb{Z}$ tem inverso aditivo)

No conjunto $M_2(\mathbb{R})$, a adição usual de matrizes goza das mesmas três propriedades da adição em $\mathbb{Z}$. Considerando esse fato, tem-se que os conjuntos $\mathbb{Z}$ e $M_2(\mathbb{R})$ têm a mesma estrutura, no que se refere às respectivas operações neles definidas. Por que então não estudar as estruturas $(\mathbb{Z}, +)$ e $(M_2(\mathbb{R}), +)$ e todas as outras cujas operações tenham essas mesmas propriedades? É isso que faremos a seguir, ao considerarmos o conceito de grupo.

Definio 1.6 *Um conjunto não-vazio G munido da operação $\star$ é um* ***grupo*** *quando as propriedades seguintes são satisfeitas:*

$(\mathcal{G}_1)$ *A operação é associativa, isto é,*

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

$(\mathcal{G}_2)$ *Existe elemento neutro para $\star$, ou seja,*

$$\exists\ e \in G \ \mid\ a \star e = e \star a = a, \quad \forall\ a \in G.$$

$(\mathcal{G}_3)$ *Todo elemento em G é invertível em relação à operação $\star$, em outras palavras,*

$$\forall\ a \in G, \quad \exists\ b \in G \ \mid\ a \star b = b \star a = e.$$

Chama-se frequentemente a operação $\star$ de **produto**. Entretanto, isso não tem, em princípio, relação com os produtos que conhecemos sobre os conjuntos numéricos clássicos. Assim, usa-se $a \cdot b$ ou ab (notação multiplicativa) ao invés de $a \star b$. Neste caso, diz-se que o grupo G é **multiplicativo**. Especificamente, vamos considerar exemplos de grupos com operações indicadas por $+$, — os **grupos aditivos**.

Definio 1.7 *Um grupo G é* ***comutativo*** *ou* ***abeliano***[3] *quando*

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

ou seja, quando a operação em G for comutativa.

Daremos a seguir alguns exemplos e contra-exemplos de grupos.

Exemplo 1.23 Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ munidos das adições usuais são exemplos clássicos de grupos aditivos abelianos. ♣

[3]Os grupos comutativos são chamados *abelianos* em homenagem ao matemático Norueguês Niels Henrik Abel (1802-1829).

Exemplo 1.24 Para cada $n \in \mathbb{N}$, o conjunto $\mathbb{Z}_n$ dotado da adição descrita no Exemplo 1.6 é um grupo abeliano. As propriedades que fazem de $(\mathbb{Z}_n, +)$ um grupo abeliano foram apresentadas no Teorema 1.1.

Exemplo 1.25 O conjunto dos números reais não é um grupo multiplicativo, pois $a = 0 \in \mathbb{R}$ não tem inverso sob a multiplicação. Fora isso, tem-se claramente que $(\mathbb{R}^*, \cdot)$ é um grupo abeliano. Da mesma forma, $(\mathbb{Q}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$ são grupos abelianos.♣

Exemplo 1.26 O conjunto $G = M_{n\times m}(\mathbb{R})$ de todas as matrizes reais de ordem $n \times m$ é um grupo abeliano sob a adição usual. De fato,

a) $X + (Y + Z) = (X + Y) + Z, \quad \forall\ X, Y, Z \in G.$

b) $X + \mathbf{0} = \mathbf{0} + X$, $\forall\ X \in G$, em que

$$\mathbf{0} = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

é a matriz nula.

c) Para

$$X = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in G,$$

a matriz

$$Y = \begin{pmatrix} -a_{11} & \dots & -a_{1m} \\ \vdots & \dots & \vdots \\ -a_{n1} & \dots & -a_{nm} \end{pmatrix} \in G$$

é tal que $X + Y = Y + X = \mathbf{0}$. Isso mostra que G é um grupo. A comutatividade da adição em G é imediata. ♣

Exemplo 1.27 Consideremos o conjunto $G = M_n(\mathbb{R})$ de todas as matrizes reais de ordem n. Sabe-se que o produto usual de matrizes é associativo, ou seja, dadas as matrizes $X, Y, Z \in G$,

$$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z.$$

Além disso, a matriz identidade de ordem n,

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \vdots & 0 \\ \vdots & \dots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

é o neutro do produto, pois

$$X \cdot I_n = I_n \cdot X = X, \quad \forall\ X \in G.$$

Agora, certamente existe em G uma matriz tal que $\det X = 0$. Para tal matriz, não existe uma matriz $Y \in G$ com $X \cdot Y = I_n$, pois uma matriz X em G é invertível se, e somente se, $\det X \neq 0$. Por conseguinte, $G = M_n(\mathbb{R})$ não é um grupo multiplicativo.♣

Exemplo 1.28 No exemplo anterior, observamos que em $G = M_n(\mathbb{R})$ a propriedade da existência de inverso para cada elemento não é satisfeita. Consideremos então

$$GL_n(\mathbb{R}) = \{X \in M_n(\mathbb{R}) : \det X \neq 0\}.$$

Vamos mostrar que $GL_n(\mathbb{R})$ é um grupo multiplicativo. Pelo que vimos até agora, é suficiente mostrar que $GL_n(\mathbb{R})$ é fechado sob o produto. Se $X, Y \in GL_n(\mathbb{R})$, então $\det X \neq 0$ e $\det Y \neq 0$; como o determinante do produto de duas matrizes é o produto de seus determinantes,

$$\det(X \cdot Y) = \det X \cdot \det Y \neq 0 \Rightarrow X \cdot Y \in GL_n(\mathbb{R}),$$

ou seja, $GL_n(\mathbb{R})$ é fechado sob o produto e, assim, é um grupo. Chama-se $GL_n(\mathbb{R})$ ***grupo linear geral de grau*** n ***sobre*** $\mathbb{R}$.

Exemplo 1.29 Sobre o conjunto $\mathbb{Z}$, vamos considerar a operação $\star$ obtida a partir da adição usual, dada por

$$a \star b = a + b + 3.$$

Vamos mostrar que $(\mathbb{Z}, \star)$ é um grupo abeliano. Para $a, b, c \in \mathbb{Z}$,

$$\begin{aligned} a \star (b \star c) = a \star (b + c + 3) &= a + b + c + 3 + 3 \\ &= (a + b + 3) + c + 3 = (a \star b) + c + 3 \\ &= (a \star b) \star c, \end{aligned}$$

ou seja, $\star$ é associativa. Vamos agora determinar $e \in \mathbb{Z}$ tal que

$$a \star e = e \star a = a, \quad \forall\ a \in \mathbb{Z}.$$

Mas,

$$a \star e = a \Rightarrow a + e + 3 = a \Leftrightarrow e = -3.$$

Da mesma forma, $e \star a = a$ implica que $e = -3$. Desse modo, $e = -3$ é o elemento neutro de $\mathbb{Z}$ sob a operação $\star$. Por fim, dado $a \in \mathbb{Z}$, vamos determinar $b \in \mathbb{Z}$ para o qual $a \star b = -3 = b \star a$. Assim,

$$a \star b = -3 \Leftrightarrow a + b + 3 = -3 \Leftrightarrow b = -a - 6.$$

A igualdade $-3 = b \star a$ também implica em $b = -a - 6$. Portanto, $(\mathbb{Z}, \star)$ é um grupo, e como

$$a \star b = a + b + 3 = b + a + 3 = b \star a, \quad \forall\ a, b \in \mathbb{Z},$$

segue que $(\mathbb{Z}, \star)$ é abeliano. ♣

Exemplo 1.30 Consideremos os grupos $(G_1, \star)$ e $(G_2, \triangle)$. Então o produto cartesiano $G_1 \times G_2$ dotado da operação " $\cdot$ " dada por

$$(a, b) \cdot (c, d) = (a \star c, b \triangle d),$$

para quaisquer (a, b) e (c, d) em $G_1 \times G_2$ é um grupo.

Solução: Como as operações em G_1 e G_2 são associativas, então a operação em $G_1 \times G_2$ também é associativa. Agora, se $e_1 \in G_1$ e $e_2 \in G_2$ são os elementos neutros das operações $\star$ e $\triangle$, respectivamente, então $e = (e_1, e_2) \in G_1 \times G_2$ satisfaz

$$(a, b) \cdot (e_1, e_2) = (a, b) = (e_1, e_2) \cdot (a, b), \quad \forall\ (a, b) \in G_1 \times G_2,$$

isto é, $e = (e_1, e_2)$ é o elemento neutro da operação em $G_1 \times G_2$. Por fim, dado $(a, b) \in G_1 \times G_2$, existem $a_1 \in G_1$ e $b_1 \in G_2$ tais que $a \star a_1 = e_1 = a_1 \star a$ e $b \star b_1 = e_2 = b_1 \star b$. Por isso,

$$(a, b) \cdot (a_1, b_1) = (e_1, e_2) = (a_1, b_1) \cdot (a, b),$$

ou seja, (a_1, b_1) é o inverso de (a, b) em $G_1 \times G_2$. Por conseguinte, $(G_1 \times G_2, \cdot)$ é um grupo. ♣

Vale observar que:

1. O produto direto $G_1 \times G_2$ é abeliano se, e somente se, G_i é abeliano, para cada $i = 1, 2$.

2. Quando a operação em G_i for aditiva para cada $i = 1, 2$, então a operação em $G = G_1 \times G_2$ também será aditiva. Assim, para os elementos $(x_1, x_2, \ldots, x_n)$ e $(y_1, y_2, \ldots, y_n)$ em G,

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2).$$

1.3.1 Grupos de Permutações

Vamos nesta seção apresentar os grupos de permutações, os quais são de muita importância em teoria dos grupos. Conforme veremos mais adiante, todo grupo G é idêntico (tem as mesmas propriedades algébricas) a algum grupo de permutação (isso

é o que afirma o Teorema de Cayley). Isso já é motivo mais do que suficiente para destacar esses grupos em uma seção à parte.

Sejam A um conjunto não-vazio e S_A o conjunto de todas as permutações de A, isto é,

$$S_A = \{f : A \to A : f \quad \text{é} \quad \text{bijetora}\}.$$

Vamos mostrar que S_A com a composição de funções é um grupo. Primeiramente, mostremos que S_A é fechado sob essa operação. Sejam $f, g \in S_A$ e $x_1, x_2 \in A$ tais que $(f \circ g)(x_1) = (f \circ g)(x_2)$. Logo,

$$(f \circ g)(x_1) = (f \circ g)(x_2) \Rightarrow f(g(x_1)) = f(g(x_2)).$$

Desde que f é injetora, segue que $g(x_1) = g(x_2)$. Mas, como g também é injetora, então $x_1 = x_2$. Desse modo, $f \circ g$ é injetora. Agora, seja $y \in A$. Como f é sobrejetora, existe $x \in A$ tal que $f(x) = y$. Por outro lado, sendo g também sobrejetora, existe $z \in A$ de maneira que $x = g(z)$. Assim,

$$y = f(x) = f(g(z)) = (f \circ g)(z).$$

Por isso, $f \circ g$ é sobrejetora e, por conseguinte, $f \circ g$ é uma permutação de A. Portanto,

$$f \circ g \in S_A, \quad \forall\ f, g \in S_A.$$

Sabe-se que a composição de funções é associativa. A permutação $id_A : A \to A$ (a identidade sobre A) é tal que $id_A \circ f = f \circ id_A = f$ para qualquer $f \in S_A$. Por fim, cada $f \in S_A$ tem inversa em S_A. Portanto, as propriedades $\mathcal{G}_1$, $\mathcal{G}_2$ e $\mathcal{G}_3$ são satisfeitas. Desse modo, $(S_A, \circ)$ é um grupo, não-abeliano em geral (pois a composição de funções não é comutativa). Chama-se $(S_A, \circ)$ **grupo das permutações sobre** A.

De modo particular, quando o conjunto A tem um número finito de elementos, digamos $A = \{1, 2, \ldots, n\}$, então S_A tem uma representação e nome especial. Neste

caso, denota-se S_A por S_n e chama-se **grupo simétrico** ou **grupo das permutações de n letras**. Observa-se que S_n só é abeliano quando $A = \{1\}$ ou $A = \{1, 2\}$.

É comum representar uma permutação $\alpha \in S_n$ por

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}. \tag{1.5}$$

Sob esta notação, não importa a ordem das colunas. Por exemplo,

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix} = \begin{pmatrix} 2 & 1 & \dots & n \\ \alpha(2) & \alpha(1) & \dots & \alpha(n) \end{pmatrix}.$$

Além disso, para efetuar a composição dos elementos

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \beta(2) & \beta(1) & \dots & \beta(n) \end{pmatrix}$$

em S_n, procede-se como[4]:

$$\begin{aligned} \alpha \cdot \beta &= \begin{pmatrix} 1 & \dots & \beta(r) & \dots & n \\ \alpha(1) & \dots & \alpha(\beta(r)) & \dots & \alpha(n) \end{pmatrix} \cdot \begin{pmatrix} 1 & \dots & r & \dots & n \\ \beta(1) & \dots & \beta(r) & \dots & \beta(n) \end{pmatrix} \\ &= \begin{pmatrix} \dots & \dots & r & \dots & \dots \\ \dots & \dots & \alpha(\beta(r)) & \dots & \dots \end{pmatrix}. \end{aligned}$$

Pela análise combinatória, verifica-se que o grupo S_3 tem $n!$ elementos.

O Grupo S_3

Vamos considerar o caso em que $A = \{1, 2, 3\}$ e efetuar alguns produtos $\alpha \cdot \beta$, com $\alpha, \beta \in S_3$. As permutações de $A = \{1, 2, 3\}$ são:

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

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

[4]Estamos representando o elemento $\alpha \circ \beta$ por $\alpha \cdot \beta$.

ou seja,

$$S_3 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}.$$

Façamos $\alpha = \alpha_6$ e $\beta = \alpha_2$. Assim,

$$\begin{aligned}
\alpha^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha_5, \\
\alpha^3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e \\
\beta^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e, \\
\beta\alpha &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha_3 \\
\alpha\beta &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \alpha_4.
\end{aligned}$$

Nota-se que o cálculo de $\alpha\beta$ usando a notação em (1.5) é mais prático do que o método tradicional.

Verificamos que os elementos do grupo S_3 foram obtidos por meio de produtos com fatores α ou β (considerando que $\alpha = e \cdot \alpha$ e $\beta = e \cdot \beta$). Isso se traduz dizendo que os elementos α e β geram S_3.

1.3.2 Ordem de um Grupo

Um grupo $(G, \cdot)$ é dito **finito** quando o conjunto G for finito. Neste caso, o número de elementos de G chama-se **ordem** de G, a qual indicaremos[5] por $|G|$. Caso contrário, diz-se que G é **infinito** ou que tem **ordem infinita.**

Assim, temos

$$|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4, \quad |\mathbb{Z}_n| = n, \quad |S_n| = n!.$$

[5]Esta notação já foi usada para indicar a cardinalidade de um conjunto S.

Observao 1.1 A decisão de não indicar a ordem infinita de um grupo G por $|G|$ é apenas para não causar confusão com a definição de igualdade entre cardinalidades de conjuntos (equivalência entre conjuntos). Essa é atribuída ao matemático Alemão Georg Cantor (1845-1918), e que revolucionou a Teoria dos Conjuntos. Sob essa definição, prova-se que os conjuntos $\mathbb{Z}$ e $\mathbb{R}$, apesar de serem infinitos, não têm a mesma cardinalidade, pois não existe nenhuma bijeção entre $\mathbb{Z}$ e $\mathbb{R}$. Entretanto, os grupos $(\mathbb{Z}, +)$ e $(\mathbb{R}, +)$ têm ordem infinita. Por isso, quando G for um conjunto infinito, diremos apenas que o grupo $(G, \star)$ é de ordem infinita.

Definio 1.8 *A **tábua** de um grupo finito $(G, \star)$ é a tábua da operação $\star$.*

Exemplo 1.31 As tábuas do grupo aditivo $(\mathbb{Z}_5, +)$ e do grupo multiplicativo $(U(\mathbb{Z}_5), \cdot)$, em que $U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, são

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

e

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

.

♣

Em uma tábua de um grupo finito $(G, \star)$ não pode haver repetição entre os elementos de suas linhas ou colunas, não considerando é claro linha e coluna nas quais

os elementos de G estão dispostos. Por exemplo, vamos supor que na i-ésima ocorra $a_{ij} = a_{ir}$. Logo,

$$a_i \star a_j = a_i \star a_r \Rightarrow a_j = a_r.$$

1.4 Propriedades Elementares de um Grupo

Vamos considerar nesta seção algumas propriedades de um grupo, as quais são obtidas diretamente da definição.

Seja $(G, \star)$ um grupo. Então as leis do cancelamento à esquerda e à direita são válidas em G, isto é, dados $a, b, c \in G$,

$$a \star b = a \star c \Rightarrow b = c \quad \text{e} \quad b \star a = c \star a \Rightarrow b = c.$$

Demonstração: Suponhamos que $a \star b = a \star c$. Como existe $a_1 \in G$ tal que

$$a_1 \star a = e = a \star a_1,$$

temos que

$$\begin{aligned}
a \star b = a \star c &\Rightarrow a_1 \star (a \star b) = a_1 \star (a \star c) && \text{(operando à esquerda com } a_1) \\
&\Rightarrow (a_1 \star a) \star b = (a_1 \star a) \star c && \text{(pois } \star \text{ é associativa)} \\
&\Rightarrow e \star b = e \star c && \text{(pois } a_1 \star a = e) \\
&\Rightarrow b = c. && \text{(pois } e \text{ é neutro de } \star)
\end{aligned}$$

Da mesma forma, pode-se mostrar que se $b \star a = c \star a$, então $b = c$. ■

Proposio 1.4 *Seja $(G, \star)$ um grupo. Dados $a, b \in G$, as equações lineares $a \star x = b$ e $x \star a = b$ têm únicas soluções em G.*

Demonstração: Vamos mostrar a existência e unicidade de solução apenas para equação $a \star x = b$, pois o outro caso é tratado similarmente. Seja $a_1 \in G$ tal que $a_1 \star a = e$. Logo, o elemento $x = a_1 \star b \in G$ é tal que

$$a \star (a_1 \star b) = (a \star a_1) \star b = e \star b = b,$$

isto é, $x = a_1 \star b$ é uma solução de $a \star x = b$. Suponhamos que $x_1, x_2 \in G$ sejam duas soluções de $a \star x = b$. Por isso, $a \star x_1 = b$ e $a \star x_2 = b$, e pela Proposição 1.4, tem-se

$$a \star x_1 = a \star x_2 \Rightarrow x_1 = x_2,$$

o que mostra a unicidade de solução. ■

Os resultados da proposição são obtidos diretamente do que foi estudado sobre operações.

Proposio 1.5 *Seja $(G, \star)$ um grupo. Então,*

(1) *Existe único elemento $e \in G$ tal que*

$$e \star a = a \star e = a, \quad \forall\ a \in G.$$

(2) *Para cada $a \in G$, existe único $a' \in G$ tal que*

$$a' \star a = a \star a' = e.$$

Definio 1.9 *Seja $(G, \cdot)$ um grupo. Dados $a \in G$ e $n \in \mathbb{Z}$, define-se a n-ésima potência de a, em símbolo a^n, da seguinte forma:*

$$a^n = \begin{cases} e & se \quad n = 0, \\ a^{n-1} \cdot a & se \quad n > 0, \\ (a^{-n})^{-1} & se \quad n < 0. \end{cases}$$

De acordo com a definição, dado $n \in \mathbb{N}$,

$$a^n = a \cdot a \cdot \cdots \cdot a \quad (n \text{ fatores})$$

e

$$a^{-n} = a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1} \quad (n \text{ fatores}).$$

Se a operação em G for aditiva, então define-se múltiplo de a, $n \cdot a$, ao invés de potência de a. Assim,

$$n \cdot a = \begin{cases} e & \text{se} \quad n = 0, \\ (n-1)a + a & \text{se} \quad n > 0, \\ (-n)(-a) & \text{se} \quad n < 0. \end{cases}$$

Da mesma forma, para $n \in \mathbb{N}$,

$$n \cdot a = a + a + \cdots + a \quad (n \text{ parcela})$$

e

$$n \cdot (-a) = (-a) + (-a) + \cdots + (-a) \quad (n \text{ parcela})$$

Exemplo 1.32 No grupo multiplicativo $(\mathbb{Q}^*, \cdot)$,

$$\left(\frac{1}{2}\right)^3 = \left(\frac{1}{2}\right)^2 \cdot \frac{1}{2} = \frac{1}{8} \quad \text{e} \quad \left(\frac{1}{2}\right)^{-3} = \left(\left(\frac{1}{2}\right)^3\right)^{-1} = 8$$

Já para os grupos aditivos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_6, +)$,

$$2 \cdot 3 = 3 + 3 = 6 \quad \text{e} \quad (-2) \cdot 3 = 2 \cdot (-3) = -6$$

e

$$4 \cdot \overline{2} = \overline{2} + \overline{2} + \overline{2} + \overline{2} = \overline{2} \quad \text{e} \quad (-3) \cdot \overline{2} = 3 \cdot \left(-\overline{2}\right) = 3 \cdot \overline{4} = \overline{0}.$$

♣

Proposio 1.6 *Seja $(G, \cdot)$ um grupo. Dados $a \in G$ e $n, m \in \mathbb{Z}$, então*

(1) $a^n \cdot a^m = a^{n+m}$.

(2) $(a^n)^m = a^{nm}$.

Demonstração: Vamos demonstrar apenas a propriedade (1). Consideremos dois casos separadamente.

Caso 1: Se $n \geq 0$ e $n + m \geq 0$.

Vamos usar indução sobre n. Se $n = 0$,

$$a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}.$$

Suponhamos agora que o resultado seja válido para n, ou seja, $a^n \cdot a^m = a^{n+m}$. Assim, como $a^n \cdot a = a^{(n+1)-1} \cdot a = a^{n+1}$,

$$\begin{aligned} a^m \cdot a^{n+1} &= a^m \cdot a^n \cdot a = a^{n+m} \cdot a \\ &= a^{(n+m+1)-1} \cdot a = a^{n+m+1}. \end{aligned}$$

Caso 2: Suponhamos agora que m e n sejam quaisquer inteiros. Vamos considerar um inteiro $r > 0$ de maneira que $r+m > 0$, $r+n > 0$ e $r+m+n > 0$. Logo, considerando o fato que $a^r \cdot a^{-r} = a^r \cdot (a^r)^{-1} = e$, obtém-se usando a primeira parte da demosntração,

$$\begin{aligned} a^{m+n} &= a^{m+n} \cdot \left(a^r \cdot a^{-r}\right) = \left(a^{m+n} \cdot a^r\right) \cdot a^{-r} \\ &= a^{m+n+r} \cdot a^{-r} = a^{m+(n+r)} \cdot a^{-r} \\ &= a^m \cdot (a^n \cdot a^r) \cdot a^{-r} = a^n \cdot a^m. \end{aligned}$$

■

Observao 1.2 Se na Proposição 1.6, a operação do grupo for " + ", então para quaisquer inteiros n e m, os itens (1) e (2) são reescritos da forma:

(a) $n \cdot a + m \cdot a = (n+m) \cdot a$.

(b) $m(n \cdot a) = (mn) \cdot a$.

1.5 Subgrupos

Consideremos agora subconjuntos especiais de um grupo G, no sentido da definição seguinte.

Definio 1.10 *Consideremos um grupo $(G, \star)$. Um subconjunto não-vazio H de G é um* ***subgrupo*** *de G quando H, com a operação induzida de G, também é um grupo.*

Usaremos a notação $H < G$ para indicar que H é um subgrupo de G. Assim,

$$H < G \Leftrightarrow H \quad \text{é} \quad \text{subgrupo de } G.$$

Para um grupo G qualquer, tem-se que $H_1 = \{e\}$ e $H_2 = G$ são subgrupos de G, os quais chamam-se **subgrupos triviais** de G. Um subgrupo H de G é dito **subgrupo próprio** quando $H \neq G$ e $H \neq \{e\}$.

Exemplo 1.33 Para um grupo G qualquer, tem-se que $H_1 = \{e\}$ e $H_2 = G$ são subgrupos de G, os quais chamam-se subgrupos triviais de G. Um subgrupo H de G é dito subgrupo próprio quando $H \neq G$ e $H \neq \{e\}$.

Exemplo 1.34 Sob as adições usuais, temos os exemplos clássicos de subgrupos

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

E sob as multiplicações usuais,

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

♣

Exemplo 1.35 Como conjunto, sabe-se que $\mathbb{Q}^* \subset \mathbb{R}$. Entretanto, $(\mathbb{Q}^*, \cdot)$ não é subgrupo de $(\mathbb{R}, +)$, pois a operação em $\mathbb{Q}^*$ não é a operação induzida da operação em $\mathbb{R}$. ♣

Vale ressaltar que se $H < G$, então:

1. A identidade de H, e_H, é igual a identidade de G.

2. Dado $h \in H$, o inverso de h em H coincide com o inverso de h em G.

Entretanto, o próximo teorema estabelece um critério que caracteriza os subgrupos de um grupo.

Teorema 1.2 *Seja H um subconjunto não-vazio de um grupo G. Então H é um subgrupo de G se, e somente se, uma das seguintes condições são satisfeitas:*

(1) $h_1 \cdot h_2 \in H \quad e \quad h_1^{-1} \in H, \forall\ h_1, h_2 \in H.$

(2) $h_1 \cdot h_2^{-1} \in H, \quad \forall\ h_1, h_2 \in H.$

Demonstração: Se H é um subgrupo de G, então H também é um grupo e por isso as condições 1 e 2 são claramente satisfeitas. Reciprocamente, suponhamos que H satisfaz a Condição (1). Logo, para qualquer $h \in H$, $h^{-1} \in H$. Assim, $e = h \cdot h^{-1}$ e, por conseguinte, $H < G$. Finalmente, se H satisfaz a Condição (2), então dados $h_1, h_2 \in H$,

$$e = h_2 \cdot h_2^{-1} \in H \Rightarrow h_2^{-1} = e \cdot h_2^{-1} \in H.$$

Com isso,

$$h_1 \cdot h_2 = h_1 \cdot \left(h_2^{-1}\right)^{-1} \in H.$$

Portanto, H é subgrupo de G. ■

Quando H for um subconjunto finito de um grupo G, então o processo de caracterização é mais simples, De fato, neste caso temos que:

$$H < G \Leftrightarrow h_1 \cdot h_2 \in H, \quad \forall\ h_1, h_2 \in H.$$

Exemplo 1.36 Para cada $n \in \mathbb{Z}$, o conjunto $H = n \cdot \mathbb{Z}$ de todos os múltiplos de n,

$$n \cdot \mathbb{Z} = \{nk : k \in \mathbb{Z}\},$$

é um subgrupo de $\mathbb{Z}$. A recíproca deste resultado é verdadeira, ou seja, se H é um subgrupo de $\mathbb{Z}$, então existe $n \in \mathbb{Z}$ tal que $H = n \cdot \mathbb{Z}$.

Exemplo 1.37 O conjunto S^1 de todos os números complexos de norma 1 (S^1é o círculo trigonométrico),

$$S^1 = \{z \in \mathbb{C} : ||z|| = 1\},$$

é um subgrupo de $(\mathbb{C}^*, \cdot)$. Com efeito, dados z_1, z_2, então $||z_1|| = 1$ e $||z_2|| = 1$. Além disso, o inverso de um complexo não-nulo z é $z^{-1} = \frac{\overline{z}}{||z||^2}$. Por isso,

$$\left|\left|z_1 \cdot z_2^{-1}\right|\right| = ||z_1|| \cdot \left|\left|z_2^{-1}\right|\right| = ||z_1|| \cdot ||z_2||^{-1} = 1.$$

Portanto, S^1 é um subgrupo de $\mathbb{C}^*$. ♣

Exemplo 1.38 Sejam $G = S_3$ e H_1 e H_2 subconjuntos de S_3 dados por

$$H_1 = \{e, \alpha\} \quad \text{e} \quad H_2 = \{e, \alpha, \beta\},$$

em que

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

Assim, $H_1 < S_3$, pois $\alpha \cdot \alpha = e \in H_1$. Entretanto, para H_2,

$$\alpha \cdot \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \notin H_2.$$

Desse modo, H_2 não é subgrupo de S_3. ♣

Exemplo 1.39 Sejam G um grupo qualquer e $Z(G)$ o subconjunto de G cujos elementos comutam com todo elemento de G, ou seja,

$$Z(G) = \{a \in G : xa = ax, \ \forall \ x \in G\}.$$

Vamos mostrar que $Z(G)$ é um subgrupo de G, o qual chama-se **centro** de G. Primeiramente, tem-se que $Z(G) \neq \emptyset$, pois claramente $e \in Z(G)$. Sejam $a, b \in Z(G)$ e $x \in G$.

Assim,

$$\begin{aligned}(ab^{-1})x &= (ab^{-1})xe &&= ab^{-1}xbb^{-1} \\ &&&= ab^{-1}bxb^{-1} \qquad (\text{pois } b \in Z(G)) \\ &&&= aexb^{-1} \\ &&&= axb^{-1} \\ &&&= x(ab^{-1}), \qquad (\text{pois } a \in Z(G))\end{aligned}$$

ou seja, $(ab^{-1})x = x(ab^{-1})$, o que mostra que $ab^{-1} \in Z(G)$ e assim $Z(G) < G$. Nota-se que G é abeliano se, e somente se, $Z(G) = G$. ♣

1.6 Grupos Cíclicos

Sejam G um grupo e $a \in G$. Consideremos H o conjunto de todas as potências de a (ou múltiplos, se a operação for uma adição), ou seja,

$$H = \{a^n : n \in \mathbb{Z}\}.$$

Vamos mostrar que $H < G$. É claro que $H \neq \emptyset$; agora, para $h_1, h_2 \in H$, digamos $h_1 = a^{n_1}$ e $h_2 = a^{n_2}$ com $n_1, n_2 \in \mathbb{Z}$,

$$h_1 h_2 = a^{n_1} a^{n_2} = a^{n_1+n_2} \in H.$$

Por outro lado,

$$h_1^{-1} = (a^{n_1})^{-1} = a^{-n_1} \in H.$$

Isso mostra que H é um subgrupo de G. Chama-se H **subgrupo cíclico gerado por** a. Diz-se também que o elemento a é um **gerador** de H. Vamos denotar este subgrupo por $H = \langle a \rangle$.

Exemplo 1.40 Para o grupo aditivo $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, tem-se para qualquer $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$,

$$a + a = 2 \cdot a = (\overline{0}, \overline{0}).$$

Por isso, $\langle a \rangle = \{e, a\}$ para todo $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$. ♣

Exemplo 1.41 No grupo multiplicativo $G = \{1, -1, i, -i\}$, então $i^2 = -1$, $i^3 = -i$ e $i^4 = 1$. Por conseguinte, $\langle i \rangle = \{1, -1, i, -i\} = G$. Da mesma forma, $\langle -i \rangle = G$. ♣

Definio 1.11 *Um grupo G é dito* ***cíclico*** *quando existe $a \in G$ de maneira que*

$$G = \langle a \rangle .$$

Observao 1.3 Para um grupo cíclico $G = \langle a \rangle$ há duas possibilidades:

(a) $a^n = e$ para algum $n \in \mathbb{N}$. Neste caso, G tem ordem finita. Ou,

(b) $a^n \neq e$ para todo $n \in \mathbb{N}$. Neste caso, todas as potências de a são distintas e G tem ordem infinita.

Exemplo 1.42 Pelo que vimos o grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ não é cíclico, enquanto o grupo $G = \{1, -1, i, -i\}$ é cíclico gerado por i e também por $-i$. ♣

Exemplo 1.43 O grupo $G = (\mathbb{Z}, +)$ é cíclico. Com efeito, para todo[6] $n \in \mathbb{Z}$,

$$b = b \cdot 1 \Rightarrow b \in \langle 1 \rangle .$$

Portanto, $\mathbb{Z} = \langle 1 \rangle$. Pode-se verificar isso observando que

$$\langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\} = \{n : n \in \mathbb{Z}\} = \mathbb{Z}.$$

♣

Proposio 1.7 *Todo grupo cíclico é abeliano.*

Demonstração: Sejam G um grupo cíclico e $a \in G$ tal que

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

[6] Aqui estamos usando múltiplo ao invés de potência, já que o grupo é aditivo.

Dados, $x_1, x_2 \in G$, digamos $x_1 = a^{n_1}$ e $x_2 = a^{n_2}$,

$$x_1 x_2 = a^{n_1} a^{n_2} = a^{n_1+n_2} = a^{n_2+n_1} = a^{n_2} a^{n_1} = x_2 x_1,$$

ou seja, G é abeliano. ■

Teorema 1.3 *Todo subgrupo de um grupo cíclico é cíclico.*

Definio 1.12 *Sejam G um grupo e $a \in G$. Se existe $n \in \mathbb{N}$ tal que $a^n = e$, diz-se que o elemento a tem* ***ordem finita*** *(ou é de ordem finita). Neste caso, o menor inteiro positvo m tal que $a^m = e$ chama-se* ***ordem*** *de a, a qual denotaremos por $O(a)$. Caso não exista nenhum $n \in \mathbb{N}$ satisfazendo $a^n = e$, então o elemento a é dito ser de* ***ordem infinita****.*

Em um grupo G, tem-se sempre

$$O(a) = 1 \Leftrightarrow a = e.$$

Exemplo 1.44 No grupo multiplicativo $G = \{1, -1, i, -i\}$, por definição $O(-1) = 2$, pois $-1^2 = 1 = e$. Além disso, $O(i) = O(-i) = 4$. ♣

Exemplo 1.45 Qualquer elemento não-nulo no grupo aditivo $\mathbb{Z}$ é de ordem infinita. De fato, para $a \in \mathbb{Z}$ com $a \neq 0$ e $n \in \mathbb{Z}$,

$$n \cdot a = 0 \Rightarrow n = 0.$$

♣

Proposio 1.8 *Seja G um grupo.*

(1) *Dado $a \in G$, $a \neq e$, tem-se que $O(a) = 2$ se, e somente se, $a = a^{-1}$.*

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

(3) *Se* $O(a) = 2$ *para todo* $a \in G - \{e\}$*, então* G *é abeliano.*

(4) *Se* $O(a) = nm$*, então* $O(a^m) = n$*.*

Demonstração: (1) Se $O(a) = 2$, então

$$a^2 = e \Rightarrow a^{-1}a^2 = a^{-1} \Rightarrow a = a^{-1}.$$

Reciprocamente, se $a = a^{-1}$, então $aa = aa^{-1}$, ou seja, $a^2 = e$, o que implica que $O(a) = 2$.

(2) Se $a \in G$ tem ordem finita, então existe $n \in \mathbb{N}$ tal que $a^n = e$. Logo

$$a^n = e \Leftrightarrow a^{-n} = e \Leftrightarrow \left(a^{-1}\right)^n = e. \tag{1.6}$$

Por isso, o menor $m \in \mathbb{N}$ satisfazendo $a^m = e$ é o menor que satisfaz $(a^{-1})^n = e$. Portanto, $O(a) = O(a^{-1})$. Se $a \in G$ tem ordem infinita, então por (1.6) a ordem de a^{-1} também é infinita.

(3) Por hipótese, $O(a) = 2$ para todo $a \in G - \{e\}$. Logo, pelo item (1),

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

Para $a, b \in G$, $ab \in G$. Logo, $ab = (ab)^{-1}$ e

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

o que mostra que G é abeliano.

(4) Inicialmente,

$$O(a) = nm \Rightarrow a^{nm} = e \Rightarrow (a^m)^n = e.$$

Só nos resta mostrar que n é o menor inteiro positivo satisfazendo $(a^m)^n = e$. Se $r \in \mathbb{N}$ e $r < n$ é tal que $(a^m)^r = e$, então

$$\begin{cases} a^{mr} &= e, \\ mr &< mn. \end{cases}$$

Isso contradiz o fato de mn ser a ordem de a. ■

Teorema 1.4 *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 para qualquer $k \in \mathbb{Z}$, $a^k = a^r$, sendo r o resto da divisão de k por m.*

(3) *$O(a) = m$ se, e somente se, $\langle a \rangle$ tem ordem m.*

Observao 1.4 O item (3) do Teorema anterior mostra que a ordem de um elemento a de um grupo G é a ordem do subgrupo cíclico por ele gerado. No caso de a ter ordem finita, $O(a) = |\langle a \rangle|$. Em virtude disto, concluímos que se G é um grupo finito, então todo elemento $a \in G$ tem ordem finita.

Capítulo 2

Classes Laterais e o Teorema de Lagrange

O Teorema de Lagrange é a base da teoria dos grupos finitos. Antes de apresentá-lo, deve-se falar do conceito de classe lateral. A partir deste, esse teorema surge naturalmente.

2.1 Classes Laterais

Sejam G um grupo e H um subgrupo de G. Sobre G, vamos considerar a relação[1] " $\equiv_E \pmod{H}$ " ou " $\equiv_E$ " dada, para quaisquer $a, b \in G$, por

$$a \equiv_E b (\mathrm{mod}\, H) \Leftrightarrow a^{-1}b \in H. \tag{2.1}$$

Proposio 2.1 *A relação* $\equiv_E \pmod{H}$ *em* (2.1) *é de equivalência. Além disso, a classe de equivalência de um elemento* $g \in G$*, relativa a esta relação é dada por* $\{g \cdot h : h \in H\}$.

Demonstração: Consideremos $a, b, c \in G$.

($\equiv_E$ **é reflexiva)** Como $a^{-1}a = e \in H$, então $a \equiv_E a (\mathrm{mod}\, H)$, ou seja, $\equiv_E$ é reflexiva.

($\equiv_E$ **é simétrica)** Se $a \equiv_E b (\mathrm{mod}\, H)$, então $a^{-1}b \in H$. Mas,

$$a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow b \equiv_E a (\mathrm{mod}\, H),$$

[1] A letra E aqui deriva-se da palavra *esquerda.*

de modo que $\equiv_E \pmod{H}$ é simétrica.

($\equiv_E$ **é transitiva)** Se $a \equiv_E b \pmod{H}$ e $b \equiv_E c \pmod{H}$, então $a^{-1}b = h_1 \in H$ e $b^{-1}c = h_2 \in H$. Como $H < G$,

$$(a^{-1}b)\left(b^{-1}c\right) = h_1h_2 \in H \Rightarrow a^{-1}c \in H \Rightarrow a \equiv_E c \pmod{H}.$$

Assim, $\equiv_E \pmod{H}$ é transitiva e, por isso, é de equivalência.

Por outro lado, dado $g \in G$, seja $\overline{g}$ a classe de equivalência de g relativa à relação $\equiv_E \pmod{H}$. Por definição, $\overline{g} = \{x \in G : g \equiv_E x\}$. Logo, para $x \in G$,

$$x \in \overline{g} \Leftrightarrow g \equiv_E x \Leftrightarrow g^{-1}x \in H,$$

ou seja, $g^{-1}x = h \in H$, ou melhor, $x = gh \in \{gh : h \in H\}$. Isso nos diz que $\overline{g} \subset \{gh : h \in H\}$. Por outro lado, se $x \in \{gh : h \in H\}$, então, existe $h \in H$ tal que $x = gh$, isto é, $g^{-1}x = h$. Por conseguinte, $g \equiv_E x \pmod{H}$ e, assim, $x \in \overline{g}$. Logo, $\{gh : h \in H\} \subset \overline{g}$, mostrando que $\overline{g} = \{gh : h \in H\}$. ■

Conforme o lema anterior, a classe de equivalência de um dado $g \in G$ segundo a relação $\equiv_E \pmod{H}$ em (2.1) é o conjunto $\overline{g} = \{gh : h \in H\}$. Em geral, denota-se a classe $\overline{g}$ por gH, algo que é bem sugestivo. Assim,

$$gH = \{gh : h \in H\}.$$

Para cada $g \in G$, a classe gH recebe um nome especial. Chama-se **classe lateral de** g à **esqueda.**

Analogamente, prova-se que a relação $\equiv_D \pmod{H}$ sobre G dada, para quaisquer $a, b \in G$, por

$$a \equiv_D b \pmod{H} \Leftrightarrow ab^{-1} \in H$$

é de equivalência. Mais ainda, para cada $g \in G$, a classe de equivalência de g segundo $\equiv_D \pmod{H}$ é $\overline{g} = \{hg : h \in H\}$, a qual denota-se por

$$Hg = \{hg : h \in H\}$$

e chama-se **classe lateral de** g à **direita.** O uso da palavra *direita* é justificada similarmente ao da palavra *esquerda.*

Como as classes à esquerda são classe de equivalência decorrem duas coisas importantes. Primeiramente,

$$G = \bigcup_{g \in G} gH,$$

e depois observa-se ainda pelo mesmo teorema que para $x, y \in G$, $x \neq y$,

$$xH = yH \quad \text{ou} \quad xH \cap yH = \emptyset,$$

isto é, duas classes laterais são iguais ou disjuntas. Desse modo, denotando por H_E o conjunto de todas as classes laterais à esquerda de H,

$$H_E = \{gH : g \in G\} = G/\equiv_E,$$

tem-se que H_E constitui uma partição de G.

Considerações similares podem ser feitas para as classes laterais à direita. Especificamente, se H_D é o conjunto das classes laterais à direita,

$$H_D = \{Hg : g \in G\} = G/\equiv_D,$$

então H_D é uma partição de G.

Observao 2.1 É importante ressaltar que:

(a) Se G é um grupo abeliano, então para cada $g \in G$,

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg.$$

Portanto, a classe lateral à direita de g coincide com sua classe lateral à esquerda. Retirando-se a hipótese de comutatividade de G, não se pode mais afirmar que as classes à esquerda e à direita de algum subgrupo H coincidem. Por isso, em geral, $H_E \neq H_D$.

(b) O subgrupo H é ele próprio uma classe lateral de H tanto à esquerda quanto à direita, pois

$$eH = \{eh : h \in H\} = H = \{he : h \in H\} = He.$$

(c) Para $g \in G$,

$$gH = H \Leftrightarrow gH = eH \Leftrightarrow g \equiv_E e \Leftrightarrow g^{-1}e \in H \Leftrightarrow g \in H.$$

Similarmente,

$$Hg = H \Leftrightarrow g \in H.$$

Exemplo 2.1 Sejam o grupo multiplicativo abeliano $G = \{1, -1, i, -i\}$ e o subgrupo $H = \{1, -1\}$ de G. Como 1 e -1 pertencem a H, então $1H = H = (-1)H$. Além disso,

$$iH = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\} = (-i)H, \quad \text{pois} \quad -i \in iH.$$

Portanto, H e $\{i, -i\}$ são as únicas classes laterais à esquerda (à direita) de H. Desse modo, $H_E = H_D = \{H, \{i, -i\}\}$. ♣

Exemplo 2.2 Consideremos $G = (\mathbb{Z}_6, +)$ e o subgrupo $H = \{\overline{0}, \overline{2}, \overline{4}\}$. Assim,

$$\overline{0} + H = \overline{2} + H = \overline{4} + H, \quad \text{pois} \quad \overline{0}, \overline{2}, \overline{4} \in H.$$

Agora,

$$\overline{1} + H = \{\overline{1}, \overline{3}, \overline{5}\} = \overline{3} + H = \overline{5} + H.$$

Por isso, há duas classes laterais à esquerda (à direita) de H, que são H e $\{\overline{1}, \overline{3}, \overline{5}\}$. ♣

Exemplo 2.3 Sejam $G = (\mathbb{Z}, +)$ e $H = 3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$. Como G é abeliano, então o conjunto H_E é igual a H_D. Sendo G infinito, vamos considerar um elemento arbitrário $n \in \mathbb{Z}$ e analisar as possíveis classes $n + 3\mathbb{Z}$. Não há mais nada natural do

que fazer uso do Algoritmo da Divisão e considerar os resultados sobre classes laterais (de equivalência) vistos até aqui. Por esse algoritmo, existem $q, r \in \mathbb{Z}$ tais que

$$n = 3q + r \quad \text{com} \quad r \in \{0, 1, 2\}.$$

Dessa forma,

$$n - r = 3q \in H \Leftrightarrow n \equiv_E r.$$

Portanto, sendo $\equiv_E$ uma relação de equivalência sobre G, tem-se

$$n + 3\mathbb{Z} = r + 3\mathbb{Z}.$$

Mas, como $r = 0$, $r = 1$ ou $r = 2$, então $0 + 3\mathbb{Z} = 3\mathbb{Z}$, $1 + 3\mathbb{Z} = \{1 + 3\lambda : \lambda \in \mathbb{Z}\}$ e $2 + 3\mathbb{Z} = \{2 + 3\lambda : \lambda \in \mathbb{Z}\}$ são as únicas classes à esquerda (à direita) de H. Consequentemente, $H_E = H_D = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$. ♣

Teorema 2.1 *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 têm a mesma cardinalidade.*

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

$$\begin{array}{rccc} f: & H & \to & gH \\ & h & \mapsto & gh. \end{array}$$

É claro que f é sobrejetora. Para $h_1, h_2 \in H$ obtemos pela Proposição 1.4,

$$f(h_1) = f(h_2) \Rightarrow gh_1 = gh_2 \Rightarrow h_1 = h_2.$$

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

$$\begin{array}{rccc} f: & H & \to & Hg \\ & h & \mapsto & hg \end{array}$$

é bijetora. Para outra parte,

$$\begin{array}{rccc} \varphi: & H_E & \to & H_D \\ & gH & \mapsto & Hg^{-1} \end{array}$$

define um 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,

$$\begin{array}{rcccccl} \varphi(g_1H) & = & Hg_1^{-1} & = & Hhg_2^{-1} & = & Hg_2^{-1} \quad (\text{pois } h \in H) \\ & & & & & = & \varphi(g_2H), \end{array}$$

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,

$$\begin{array}{rcccccl} \varphi(g_1H) & = & \varphi(g_2H) & \Leftrightarrow & Hg_1^{-1} & = & Hg_2^{-1} \\ & \Leftrightarrow & g_1^{-1} \equiv_D g_2^{-1} & \Leftrightarrow & g_1^{-1}g_2 & = & h \in H, \end{array}$$

ou seja, $g_2 = g_1h$. Desse modo,

$$g_2H = g_1hH = g_1H, \quad (\text{pois } h \in H)$$

o que mostra que φ é injetora e, assim, é bijetora. Por isso, H_E e H_D têm a mesma cardinalidade. ■

Os resultados do último teorema nos conduzem à definição seguinte, a qual é indispensável para a demonstração do Teorema de Lagrange.

Definio 2.1 *Sejam G um grupo e H um subgrupo de G. A cardinalidade do conjunto H_E (a mesma que H_D) chama-se* ***o índice*** *de H em G, o qual será indicado por $(G : H)$.*

O índice $(G : H)$ pode ser finito ou infinito. Se G é finito, então claramente $(G : H)$ é finito, pois os elementos de H_E são subconjuntos de G. Além disso, é perfeitamente

possível para um grupo infinito G possuir um subgrupo $H \neq G$, para o qual o índice $(G : H)$ é finito; também é possível que esse mesmo grupo contenha um subgrupo $K \neq G$, de maneira que $(G : K)$ é infinito. Exemplos serão dados para ambos os casos.

Exemplo 2.4 Se $G = (\mathbb{Z}_6, +)$ e $H = \{\overline{0}, \overline{2}, \overline{4}\}$,então H e $\{\overline{1}, \overline{3}, \overline{5}\}$ são as classes laterais à esquerda. Por isso, $(G : H) = 2$. ♣

Exemplo 2.5 Seja G um grupo qualquer. Para $H = G$,

$$H_E = \{xG : x \in G\}.$$

Também, $xG = \{y \in G : y \equiv_E x\}$. Assim,

$$y \in xG \Leftrightarrow y \equiv_E x \Leftrightarrow y^{-1}x \in G.$$

Mas, $y^{-1}x \in G$ é verdade para todo $y \in G$. Portanto,

$$xG = \{y \in G : y \equiv_E x\} = \{y : y \in G\} = G.$$

Isso implica que $H_E = \{G\}$ e, por conseguinte, $(G : H) = (G : G) = 1$. ♣

Exemplo 2.6 Se $G = (\mathbb{Z}, +)$ e $H = 3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$, então $0 + 3\mathbb{Z} = 3\mathbb{Z}$, $1 + 3\mathbb{Z}$ e $2 + 3\mathbb{Z}$ são as únicas classes à esquerda; desse modo, $(G : H) = 3$. Generalizando, para $n \in \mathbb{N}$ fixo e arbitrário, o subgrupo $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ é tal que $(G : H) = n$, pois pelo o algorítmo da divisão, verifica-se que

$$H_E = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, \ldots, (n-1) + \mathbb{Z}\}.$$

♣

Exemplo 2.7 Se G é um grupo de ordem infinita e $H = \{e\}$, então $(G : H)$ é infinita. Com efeito, para cada $g \in G$,

$$x \in gH \Leftrightarrow x^{-1}g \in H \Leftrightarrow x^{-1}g = e \Leftrightarrow x = g,$$

isto é, cada classe gH é composta apenas por g. Portanto,

$$H_E = \{\{g\} : g \in G\},$$

que é um conjunto infinito, pois assim o é G. ♣

2.2 O Teorema de Lagrange

Com os conceitos definidos anteriormente, já podemos apresentar o Teorema de Lagrange que, como já foi mencionado, é o principal teorema que versa sobre grupos finitos.

Teorema 2.2 (Teorema de Lagrange). *Sejam G um grupo finito e H um subgrupo de G. Então a ordem de H divide a ordem de G. Especificamente,*

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

Demonstração: Como G é finito, então $(G : H)$ também o é, digamos $(G : H) = r$. Consideremos então[2] $H_E = \{a_1H, a_2H, \ldots, a_rH\}$. Como H_E é uma partição de G,

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH,$$

e mais ainda, $a_iH \cap a_jH = \emptyset$ para $i \neq j$. Desse modo, considerando o fato de a cardinalidade de cada classe em H_E ser a igual a ordem de H (c.f. Teorema 2.1), obtemos

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{r \text{ vezes}} = |H| \cdot r,$$

ou seja,

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

■

[2] A demonstração pode ser feita considerando o conjunto H_D.

2.2.1 Algumas Consequências do Teorema de Lagrange

Vamos considerar a seguir algumas consequências elementares do Teorema de Lagrange.

Corolrio 2.1 *Sejam G um grupo finito e $g \in G$. Então, a ordem de g divide a ordem de G. Em particular,*

$$g^{|G|} = e.$$

Demonstração: Pelo item (3) do Teorema 1.4, sabemos que $O(g) = |\langle g \rangle|$. Logo, aplicando o Teorema de Lagrange ao subgrupo $\langle g \rangle$, segue que $O(g) = \lambda$ divide $|G|$. Existe portanto $k \in \mathbb{N}$ tal que $|G| = \lambda \cdot k$. Assim,

$$g^{|G|} = g^{\lambda \cdot k} = \left(g^{\lambda}\right)^{k} = e^{k} = e.$$

■

Corolrio 2.2 *Todo grupo G de ordem prima é cíclico. Em particular, G é abeliano.*

Demonstração: Seja $|G| = p$ com p primo; assim, existe $a \in G$ tal que $a \neq e$. Pelo Teorema de Lagrange, $|\langle a \rangle|$ divide $|G| = p$. Sendo p um número primo, então $|\langle a \rangle| = 1$ ou $|\langle a \rangle| = p$. Mas, como $a \neq e$, segue que $|\langle a \rangle| = p$, ou seja, $|\langle a \rangle| = G$, o que mostra que G é cíclico. Pela Proposição 1.7, tem-se que G é abeliano. ■

Corolrio 2.3 (Pequeno Teorema de Fermat). *Sejam p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então,*

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Demonstração: Sabemos que $U(\mathbb{Z}_p) = \{\overline{a} \in \mathbb{Z}_p : mdc(a, p) = 1\}$ é um grupo com a multiplicação sobre $\mathbb{Z}_p$. Mas, como p é primo, $|U(\mathbb{Z}_p)| = p - 1$. Por outro lado, se $p \nmid a$, então $\overline{a} \in U(\mathbb{Z}_p)$. Assim, pelo Corolário 2.1,

$$\overline{a}^{p-1} = \overline{1} \Rightarrow \overline{a^{p-1}} = \overline{1} \Leftrightarrow a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

■

Corolrio 2.4 *Todo grupo G tal que $|G| \leq 5$ é abeliano.*

Demonstração: Seja G um grupo com $|G| \leq 5$. Para $|G| = 1$ o resultado é imediato, pois $G = \{e\} = \langle e \rangle$. Se $|G| = 2$, $|G| = 3$ ou $|G| = 5$, então G tem ordem prima e pelo Corolário 2.2 tem-se que G é cíclico e, portanto, abeliano. Nos resta considerar o caso $|G| = 4$. Se G tem um elemento a de ordem 4, então $\langle a \rangle = G$. Caso contrário, pelo Teorema de Lagrange, todo elemento $a \in G$ com $a \neq e$ tem ordem 2. Desse modo, pelo item (1) da Proposição 1.7, tem-se que

$$a = a^{-1}, \quad \forall\ a \in G.$$

Assim, dados $a, b \in G$, o elemento $ab \in G$ e

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

o que mostra que G é abeliano. ■

O resultado a seguir também é válido quando o grupo G é infinito; entretanto, vamos considerar apenas o caso em que G tem ordem finita.

Teorema 2.3 *Seja G um grupo finito. Se H e K são subgrupos de G tais que $K < H < G$, então*

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

Demonstração: Pelo Teorema de Lagrange,

$$H < G \Rightarrow |G| = |H| \cdot (G : H),$$

$$K < H \Rightarrow |H| = |K| \cdot (H : K).$$

Dessas duas igualdades, obtém-se

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

de modo que,

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

■

Exemplo 2.8 Sejam n e m dois números naturais. Já sabemos pelo Exemplo 2.6 que $n \cdot \mathbb{Z}$ e $m \cdot \mathbb{Z}$ são subgrupos de $G = (\mathbb{Z}, +)$. Se $m \mid n$, então todo múltiplo de n é um múltiplo de m. Em outras palavras, $n \cdot \mathbb{Z} < m \cdot \mathbb{Z}$. Por isso,

$$n \cdot \mathbb{Z} < m \cdot \mathbb{Z} < \mathbb{Z}.$$

Pondo $K = n \cdot \mathbb{Z}$ e $H = m \cdot \mathbb{Z}$, obtém-se pelo Teorema 2.3,

$$(m \cdot \mathbb{Z} : n \cdot \mathbb{Z}) = \frac{(\mathbb{Z} : n \cdot \mathbb{Z})}{(\mathbb{Z} : m \cdot \mathbb{Z})}.$$

Ainda pelo mesmo exemplo, $(\mathbb{Z} : n \cdot \mathbb{Z}) = n$ e $(\mathbb{Z} : m \cdot \mathbb{Z}) = m$, de maneira que

$$(m \cdot \mathbb{Z} : n \cdot \mathbb{Z}) = \frac{n}{m}.$$

♣

A recíproca do Teorema de Lagrange não é válida. No entanto, para grupos cíclicos finitos vale o seguinte:

Teorema 2.4 *Seja $G = \langle a \rangle$ um grupo cíclico finito de ordem n. Então, para cada divisor d de n, existe único subgrupo H de G cuja ordem é d.*

Demonstração: Se $d = 1$ ou $d = n$, então basta considerar $H = \{e\}$ ou $H = G$. Suponhamos que $1 < d < n$ e seja $m \in \mathbb{N}$ tal que $n = md$. Consideremos o elemento $b = a^m$. Logo, $b^d = (a^m)^d = a^n = e$, pois $O(a) = n$. Por outro lado, se $k \in \mathbb{N}$ com $k < d$ é tal que $b^k = e$,

$$e = b^k = a^{mk}$$

e $km < dm = n$, o que não é possível, pois n é a ordem de a. Por isso, $b = a^m$ tem ordem d e, de acordo com o item (3) do Teorema 1.4, $H = \langle b \rangle$ é um subgrupo de G de ordem d.

Mostremos agora a unicidade de H. Seja K um subgrupo de G de ordem d. Pelo Teorema 1.3, K é cíclico gerado por um elemento da forma $c = a^r$. Logo, como a ordem de c é d,

$$e = c^d = a^{rd}.$$

Assim, pelo item (1) do mesmo teorema, n divide rd, ou seja, $n = md \mid rd$. Consequentemente, $m \mid r$, digamos $r = m\lambda$. Portanto, para $x \in K = \langle a^r \rangle$, existe $s \in \mathbb{Z}$ tal que

$$x = (a^r)^s = a^{rs} = a^{m\lambda s} = (a^m)^{\lambda s} \in \langle a^m \rangle = H,$$

de maneira que $K \subset H$. Mas, como cada um desses subgrupos tem ordem d, segue que $K = H$. ■

Exemplo 2.9 Determinar o subgrupo H de $(\mathbb{Z}_8, +)$ com ordem 4.

Solução: Vamos proceder usando o teorema anterior. Como $\mathbb{Z}_8 = \langle \overline{1} \rangle$, podemos considerar $a = \overline{1}$. Por outro lado, sendo $8 = 4 \cdot 2$, então $m = 2$ e $b = 2 \cdot \overline{1} = \overline{2}$, de modo que $H = \langle \overline{2} \rangle$ é o subgrupo procurado. Como $\mathbb{Z}_8$ é um grupo aditivo, então

$$H = \langle \overline{2} \rangle = \{\overline{0}, 1 \cdot \overline{2}, 2 \cdot \overline{2}, 3 \cdot \overline{2}\} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}.$$

Nota-se que $\mathbb{Z}_8 = \langle \overline{3} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle$, ou seja, poderíamos considerar $b = 2 \cdot \overline{3} = \overline{6}$ ou $b = 2 \cdot \overline{7} = \overline{6}$. Por exemplo, $\langle \overline{6} \rangle = \{\overline{0}, 1 \cdot \overline{6}, 2 \cdot \overline{6}, 3 \cdot \overline{6}\} = \{\overline{0}, \overline{6}, \overline{4}, \overline{2}\} = H$. ♣

Bibliografia

[1] GONÇALVES, A. – *Introdução à Álgebra* (5ª edição), Projeto Euclides, IMPA, Rio de Janeiro, 2006.

[2] DOMINGUES, HYGINO H. Álgebra Moderna: Volume único2215 Higino H. Domingues, Gelsom Iezzi. - 42da edição reformada, - São Paulo: Atual, 2003.

[3] FRALEIGH, JOHN B. Algebra. A First Couse in Abstract Algebra.

[4] HERSTEIN, I. N. – *Abstract Algebra* (3rd edition), John Wiley & Sons, Inc., 1999.

[5] MILIES, C. P. e COELHO, S. P. – *Números: Uma Introdução à Matemática* (3ª edição), Edusp, 2001.