Universidade Tecnológica Federal do Paraná

Programa de Mestrado em Matemática em Rede Nacional – PROFMAT

Guilherme Elias Egg Monteiro

CONTANDO AS SIMETRIAS ROTACIONAIS DOS POLIEDROS REGULARES

Dissertação – Mestrado

Curitiba

2013

GUILHERME ELIAS EGG MONTEIRO

CONTANDO AS SIMETRIAS ROTACIONAIS DOS POLIEDROS REGULARES

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de "Mestre em Matemática".

Orientadora: Mari Sano, Dra.

CURITIBA

2013

Dados Internacionais de Catalogação na Publicação

M775 Monteiro, Guilherme Elias Egg
Contando as simetrias rotacionais dos poliedros regulares / Guilherme Elias Egg Monteiro. – 2013.
72 f. : il. ; 30 cm

Orientadora: Mari Sano.
Dissertação (Mestrado) – Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional. Curitiba, 2013.
Bibliografia: f. 72.

1. Matemática – Estudo e ensino. 2. Teoria dos grupos. 3. Demonstração automática de teoremas. 4. Poliedros. 5. Simetria (Matemática) – Contagem. 6. Professores de matemática – Formação. 7. Matemática – Dissertações. I. Sano, Mari orient. II. Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional. III. Título.

CDD (22. ed.) 510

Biblioteca Central da UTFPR, Campus Curitiba

Título da Dissertação No. 003

"Contando as simetrias rotacionais dos poliedros regulares"

por

Guilherme Elias Egg Monteiro

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de Mestre em Matemática, pelo Programa de Mestrado em Matemática em Rede Nacional - PROFMAT - da Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Curitiba, às 14h do dia 12 de julho de 2013. O trabalho foi aprovado pela Banca Examinadora, composta pelos doutores:

Profa. Mari Sano, Dra.
(Presidente - UTFPR/Curitiba)

Prof. Marcelo Muniz Silva Alvez, Dr.
(UFPR)

Profa. Patricia Massae Kitani, Dra.
(UTFPR/Curitiba)

Visto da coordenação:

Prof. Ronie Peterson Dario, Dr.
(Coordenador do PROFMAT/UTFPR)

"A Folha de Aprovação assinada encontra-se na Coordenação do PROFMAT/UTFPR"

Aos meus professores que, ao longo de minha vida, me ensinam a ser alguém melhor.

AGRADECIMENTOS

- À minha mãe Soraya pelo amor sincero e pelo apoio nos momentos difíceis da vida.
- Às minhas tias Samira e Leila e à minha madrinha Jussara pela presença constante, pelos conselhos e pela torcida.
- À minha namorada e companheira Estela Vicentim que esteve presente durante toda esta trajetória.
- Aos amigos Lucas Pelissari, Jean Kukla, Alexandre Florão, Rosana Oliveira, Maira Batista e Edson Joly pelos constantes incentivos.
- Aos amigos do mestrado William Bruginski e Daniel Almeida pelo companheirismo e pelos conselhos em todo o período de nossa amizade.
- Aos amigos do trabalho Jonathan Silva, Noslen Borges, Gerson Carassai, Eder Miotto, Edgar Stelle e Flávio Sandi por acreditarem em meu conhecimento e minha capacidade.
- À CAPES pela recomendação do PROFMAT por meio do parecer do Conselho Técnico Científico da Educação Superior e pelo incentivo financeiro.
- À Sociedade Brasileira de Matemática que, na busca da melhoria do ensino de Matemática na Educação Básica, viabilizou a implementação do PROFMAT.
- À minha orientadora Mari Sano que, com sua infinita paciência e seu incrível conhecimento, tornou possível a realização deste trabalho.

RESUMO

MONTEIRO, Guilherme Elias Egg. CONTANDO AS SIMETRIAS ROTACIONAIS DOS POLIEDROS REGULARES. 72 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Esta dissertação está dividida em duas partes. A primeira parte é uma introdução da teoria básica de grupos necessária para o desenvolvimento do teorema da órbita-estabilizador, que permite fazer as contagens das simetrias dos poliedros regulares. A segunda parte é a descrição de uma atividade aplicada em sala de aula.

Palavras-chave: Poliedros regulares, Teorema da órbita - estabilizador, Contagem de simetrias

ABSTRACT

MONTEIRO, Guilherme Elias Egg. COUNTING THE ROTATIONAL SYMMETRIES OF THE REGULAR POLYEDRA. 72 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

This dissertation is divided in two parts. The first part is an introduction to basic group theory required for the development of the orbit-stabilizer theorem, that allows the counts of symmetries of the regular polyhedra. The second part is the description of an activity applied in classroom.

Keywords: Regular Polyhedra , Orbit-stabilizer theorem, Count of symmetries.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Ensinar simetria para os alunos das séries básicas não é tarefa fácil. O motivo não é a dificuldade do conteúdo nem a relação do aluno com o objeto, mas sim o fato de tratar a matemática como ciência abstrata ser cada vez mais raro, devido às demandas educacionais das aplicações da matemática em situações-problema. Essas demandas são constantes nos livros didáticos do ensino fundamental, médio e nos planejamentos escolares, de modo que os professores usufruem de bons materiais de trabalho. De certo modo, a matemática das aplicações no cotidiano representa um grande avanço do ensino da educação básica, por se tratar de relacionar a teoria e a prática.

Este trabalho é uma tentativa de mesclar a álgebra e a geometria em sala de aula e contribuir com o aperfeiçoamento dos professores da educação básica. Nos currículos dos cursos de licenciatura em matemática, o grupo das simetrias, estudado em um curso semestral de álgebra moderna ou de teoria de grupos, dificilmente é aplicado. A importância desta aplicação está na escassez do ensino da simetria na educação básica.

O professor de matemática do ensino fundamental e médio, com seus cronogramas apertados e ementas exageradas, tem deixado a essência da investigação matemática e das conclusões abstratas de lado. O aluno que cresce sem estas, dificilmente estará apto a enxergar a verdadeira natureza da “Rainha das Ciências”.

Apesar deste trabalho conter conceitos que os alunos do ensino médio não estão aptos a entender, é um bom material de estudo para o professor que vai ensinar a simetria na educação básica. De fato, os conceitos relacionados à álgebra moderna, como teoria de grupos e seus teoremas, podem ser aplicados na educação básica mesmo que o aluno não entenda a natureza das quais estas ideias surgiram.

A origem da teoria de grupos está na teoria de equações polinomiais que foi desenvolvida por Évariste Galois e na geometria descrevendo simetria de objetos.

Um dos objetivos deste trabalho é desenvolver toda a base algébrica para que se possa demonstrar um importante teorema da teoria de grupos, com o qual é possível estudar a contagem de simetrias. Outro objetivo é descrever uma atividade de simetria realizada em sala de aula, com o intuito de poder observar se os alunos do 9° ano do ensino fundamental e 1° ano do ensino médio conseguem identificar e operar as simetrias de alguns objetos geométricos.

No capítulo 2 (Preliminares) abordaremos, de maneira sucinta, parte dos pré-requisitos para este trabalho como o princípio de indução, relações de equivalência e classes de equivalência. Em seguida, uma breve explicação dos conceitos básicos que envolvem função, sendo o conceito de permutação o mais importante para este trabalho. No capítulo 3 (Poliedros Regulares) apresentaremos os poliedros regulares e provaremos as proposições que permitem concluir que existem somente cinco desses. No capítulo 4 (Grupos) faremos o desenvolvimento da teoria de grupos, necessário para o entendimento deste trabalho. Alguns conceitos apresentados serão subgrupos, classes laterais, homomorfismo e ação. Também será apresentada a demonstração do importante teorema de Cayley. No capítulo 5 (Órbitas e Estabilizadores) daremos a definição de órbitas e estabilizadores e demonstraremos o teorema que é responsável pela contagem dos elementos de um grupo, o teorema da órbita-estabilizador. No capítulo 6 aplicaremos o resultado deste mesmo teorema para fazer a contagem das simetrias rotacionais dos poliedros regulares. O capítulo 7 apresentará a descrição de uma atividade prática realizada em sala de aula. Por fim, no capítulo 8 apresentaremos as conclusões acerca deste trabalho.

2 PRELIMINARES

Alguns pré-requisitos são necessários para o estudo da teoria de grupos. A maioria desses não faz parte do currículo de ensino médio, porém devem estar ao alcance do professor da educação básica, uma vez que são definições importantes, estudadas nos cursos de licenciatura em matemática.

2.1 PRINCÍPIO DE INDUÇÃO

Em algumas demonstrações, precisamos mostrar que uma propriedade é válida para todo número natural $n \geq a$. Para tal tarefa, usamos um axioma dos números naturais chamado princípio de indução, enunciado a seguir:

Seja $P(n)$ uma propriedade no universo dos números naturais $\mathbb{N}$. Suponha que

1. $P(a)$ é verdadeira;
2. se $P(n)$ é verdadeira para algum $n \geq a$, então $P(n+1)$ é verdadeira.

Deste modo, $P(n)$ é verdadeira para todo número natural $n \geq a$.

De acordo com (ROSEN, 2009), o funcionamento deste princípio pode ser comparado a brincadeira de equilibrar as peças do jogo de dominó, umas ao lado das outras, para que, derrubando a primeira peça, todas caiam em seguida. Imagine uma carreira infinita de peças de dominó equilibradas. Para que todas as peças caiam, devemos ter duas garantias: a primeira é a garantia que a primeira peça cai, e a segunda é que, se uma peça aleatória cai, a peça seguinte também cai. Deste modo, todas as infinitas peças cairão.

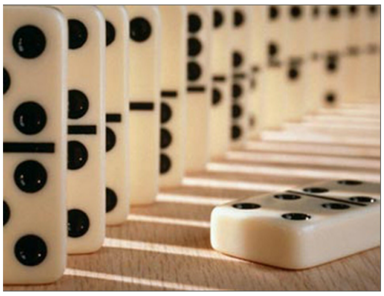

Figura 1: Peças equilibradas de dominó

Fonte: ***Disponível em http://clickeaprenda.uol.com.br/portal/mostrarConteudo.php?idPagina=30093. Acessado em 04/05/2013.***

Exemplo 2.1. *Vamos mostrar que, para todo $n \in \mathbb{N}^*$, é válida a afirmação*

$$P(n) : 1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6},$$

ou seja, que a soma dos n primeiros quadrados pode ser calculada pela fórmula $\frac{n(n+1)(2n+1)}{6}$.

1. *Para $n = 1$ temos $1^2 = \frac{1 \cdot 2 \cdot 3}{6}$. Logo $P(1)$ é verdadeira.*

2. *Suponha $P(n)$ verdadeira para algum $n \geq 1$, isto é,*

$$1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Queremos mostrar que $P(n+1)$ é verdadeira, ou seja, deve valer a igualdade

$$1^2 + 2^2 + ... + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

De fato, adicionando $(n+1)^2$ em ambos os membros da igualdade da hipótese, temos:

$$\begin{aligned}
\overbrace{1^2 + 2^2 + ... + n^2}^{\frac{n(n+1)(2n+1)}{6}} + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\
&= \frac{(n+1)(2n^2 + 4n + 3n + 6)}{6} \\
&= \frac{(n+1)[2n(n+2) + 3(n+2)]}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6}
\end{aligned}$$

Portanto, segue pelo princípio de indução de $P(n)$ é verdadeira para $n \in \mathbb{N}^*$.

2.2 RELAÇÕES E CLASSES DE EQUIVALÊNCIA

Nesta seção veremos as noções básicas de relações e classes de equivalência.

Definição 2.2. *Sejam E e F conjuntos não-vazios. Chamamos de relação binária de E em F todo subconjunto R de $E \times F$. Se $E = F$, dizemos que R é uma relação sobre E. Se $(a,b) \in R$, denotamos como aRb.*

Exemplo 2.3. *Se $E = \{1,2,3\}$ e $F = \{2,4\}$, temos que*

$$E \times F = \{(1,2),(1,4),(2,2),(2,4),(3,2),(3,4)\}.$$

Sabemos da análise combinatória que existem $2^6 = 64$ subconjuntos de $E \times F$, ou seja, 64 relações binárias de E em F. Algumas delas são:

1. *$R_1 = \{(1,2),(1,4)\}$. Deste modo, $1R_12$ e $1R_14$.*
2. *$R_2 = \{(2,2),(3,2);(3,4)\}$. Deste modo, $2R_22$, $3R_22$ e $3R_24$.*
3. *$R_3 = \emptyset$.*

Definição 2.4. *Uma relação R sobre um conjunto não-vazio E é chamada de relação de equivalência sobre E se as seguintes condições forem satisfeitas:*

1. *(reflexiva) se $x \in E$ então xRx;*
2. *(simétrica) se $x,y \in E$ e xRy então yRx;*
3. *(transitiva) se $x,y,z \in E$, xRy e yRz então xRz.*

Exemplo 2.5. *Se $E = \{a,b,c,d\}$ e R é uma relação sobre E definida por*

$$R = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,c)\},$$

temos que:

1. *R é reflexiva, pois xRx para todo $x \in E$.*
2. *R não é simétrica, pois $(a,b) \in R$, porém $(b,a) \notin R$.*

3. *R não é transitiva, pois $(a,b) \in R$ e $(b,c) \in R$, porém $(a,c) \notin R$.*

Concluímos que R não é de equivalência.

Exemplo 2.6. *Na geometria euclidana plana, a relação de perpendicularismo $a \sim b \iff a \perp b$ sobre o conjunto das retas do plano é reflexiva e simétrica, porém não é transitiva, pois se $r \perp s$ e $s \perp t$, temos $r//t$ e não $r \perp t$. Portanto $\sim$ não é de equivalência.*

Definição 2.7. *Sejam $a,b \in \mathbb{Z}$. Se existir $k \in \mathbb{Z}$ tal que $b = ka$, dizemos que a é divisor de b (ou b é múltiplo de a) e representamos por $a|b$.*

Exemplo 2.8. $17|51$, *pois existe $k \in \mathbb{Z}$ tal que $51 = 17k$, a saber, $k = 3$.*

Exemplo 2.9. *A relação de divisibilidade $a \sim b \iff a|b$ sobre $\mathbb{Z}$ é reflexiva e transitiva, porém não é simétrica, pois $2|4$, mas $4 \nmid 2$. Portanto $\sim$ não é de equivalência.*

Definição 2.10. *Seja $m > 1$ um número inteiro. Dados $a,b \in \mathbb{Z}$, dizemos que a é congruente a b, módulo m, quando $m|(a-b)$, ou seja, se existe $k \in \mathbb{Z}$ tal que $a - b = km$. Representamos por $a \equiv b(mod m)$.*

Exemplo 2.11. $-3 \equiv 24(mod 3)$, *pois existe $k \in \mathbb{Z}$ tal que $-3-24 = 3k$, a saber, $k = -9$.*

Exemplo 2.12. *A relação de congruência módulo m definida por $a \sim b \iff a \equiv b(mod m)$ sobre $\mathbb{Z}$ é uma relação de equivalência. De fato:*

1. *(reflexiva) $a \sim a$, pois $m|a-a$, ou seja, $a \equiv a(mod m)$.*

2. *(simétrica) se $a \sim b$ então $a \equiv b(mod m)$. Logo, existe $k \in \mathbb{Z}$ tal que $a - b = km$, ou seja, $b - a = (-k)m$. Deste modo, $b \equiv a(mod m)$ de onde concluímos que $b \sim a$.*

3. *(transitiva) se $a \sim b$ e $b \sim c$ então $a \equiv b(mod m)$ e $b \equiv c(mod m)$. Logo, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a - b = k_1 m$ e $b - c = k_2 m$. Somando estas igualdades temos $a - c = (k_1 + k_2)m$ de onde concluímos que $a \sim c$.*

Uma relação de equivalência sobre E divide o conjunto E nas chamadas classes de equivalência.

Definição 2.13. *Seja R uma relação de equivalência sobre um conjunto não-vazio E. Dado $a \in E$, chama-se classe de equivalência determinada por a, e representamos por $\overline{a}$, o subconjunto de E constituído pelos elementos $x \in E$ que estão relacionados com a, por meio de R. Mais precisamente,*

$$\overline{a} = \{x \in E | xRa\}.$$

Definição 2.14. *O conjunto das classes de equivalência de uma determinada relação R sobre E será chamado conjunto quociente de E por R, e representaremos por E/R. Mais precisamente:*

$$E/R = \{\overline{a} | a \in E\}.$$

Exemplo 2.15. *Considere a relação $\sim$ de equivalência sobre $\mathbb{R}^2$ definida por*

$$(x_1, y_1) \sim (x_2, y_2) \iff x_1 - y_1 = x_2 - y_2.$$

Deste modo:

1. *a classe de equivalência determinada por $(1,1) \in \mathbb{R}^2$ é definida pelo conjunto de todos os pares ordenados que estão relacionados com $(1,1)$ por meio de $\sim$. Logo:*

$$\begin{aligned} \overline{(1,1)} &= \{(a,b) \in \mathbb{R}^2 | (a,b) \sim (1,1)\} \\ &= \{(a,b) \in \mathbb{R}^2 | a - b = 0\} \\ &= \{(a,b) \in \mathbb{R}^2 | a = b\} \\ &= \{(a,a) | a \in \mathbb{R}\}. \end{aligned}$$

2. *a classe de equivalência determinada por $(3,1) \in \mathbb{R}^2$ é definida pelo conjunto de todos os pares ordenados que estão relacionados com $(3,1)$ por meio de $\sim$. Logo:*

$$\begin{aligned} \overline{(3,1)} &= \{(a,b) \in \mathbb{R}^2 | (a,b) \sim (3,1)\} \\ &= \{(a,b) \in \mathbb{R}^2 | a - b = 2\} \\ &= \{(a,b) \in \mathbb{R}^2 | b = a - 2\} \\ &= \{(a,a-2) | a \in \mathbb{R}\}. \end{aligned}$$

3. *o conjunto quociente de $\mathbb{R}^2$ por $\sim$ é dado pelo conjunto de todas as classes de equivalência $\overline{(x_1, y_1)}$ tais que $(x_1, y_1) \in \mathbb{R}^2$. Note que*

$$\begin{aligned} \overline{(x_1,y_1)} &= \{(a,b) \in \mathbb{R}^2 | (a,b) \sim (x_1,y_1)\} \\ &= \{(a,b) \in \mathbb{R}^2 | a - b = x_1 - y_1\}. \end{aligned}$$

   Fazendo $x_1 - y_1 = k$, temos:

$$\begin{aligned}\overline{(x_1,y_1)} &= \{(a,b)\in\mathbb{R}^2|b=a-k\}\\ &= \{(a,a-k)|a\in\mathbb{R}\}.\end{aligned}$$

Logo, uma classe de equivalência genérica é o conjunto de pontos que pertencem à retas paralelas a reta $y=x$ do plano $\mathbb{R}^2$. Isso nos leva a concluir que o conjunto quociente $\mathbb{R}^2/\sim$ é o conjunto de todas as retas paralelas a $\{(x,y)|y=x\}$.

Proposição 2.16. *Seja R uma relação de equivalência sobre E e sejam $a,b\in E$. São equivalentes as afirmações:*

$$I.\ aRb \qquad II.\ a\in\overline{b} \qquad III.\ b\in\overline{a} \qquad IV.\ \overline{a}=\overline{b}$$

Demonstração:

1. $(I \Longrightarrow II)$ Sabemos que $\overline{b}=\{x\in E|xRb\}$. Como, por hipótese, aRb, concluímos que $a\in\overline{b}$.

2. $(II \Longrightarrow III)$ Se $a\in\overline{b}$, então aRb. Pela propriedade simétrica temos bRa. Como $\overline{a}=\{x\in E|xRa\}$ segue que $b\in\overline{a}$.

3. $(III \Longrightarrow IV)$ Temos como hipótese que $b\in\overline{a}$, ou seja, bRa e, consequentemente, aRb. Devemos mostrar que valem as duas continências $\overline{a}\subset\overline{b}$ e $\overline{b}\subset\overline{a}$. Para mostrar a primeira continência considere $x\in\overline{a}$, ou seja, xRa. Como, por hipótese, aRb, pela propriedade transitiva segue que xRb, ou seja, $x\in\overline{b}$. A segunda continência tem demonstração análoga. Deste modo $\overline{a}=\overline{b}$.

4. $(IV \Longrightarrow I)$ Sabemos que $a\in\overline{a}$ e $b\in\overline{b}$, ou seja, $\overline{a}\neq\emptyset$ e $\overline{b}\neq\emptyset$. Deste modo, considere $x\in\overline{a}=\overline{b}$. Logo xRa e xRb. Pela propriedade simétrica temos aRx e pela propriedade transitiva segue que aRb.

□

Exemplo 2.17. *Seja $a\in\mathbb{Z}$ e considere a relação de equivalência de congruência módulo m, do exemplo 2.12. Para encontrar a classe de equivalência determinada por a, consideramos o seguinte conjunto:*

$$
\begin{aligned}
\overline{a} &= \{x \in \mathbb{Z} | x \sim a\} \\
&= \{x \in \mathbb{Z} | x \equiv a(modm)\} \\
&= \{x \in \mathbb{Z} | x - a = km, \textit{ para algum } k \in \mathbb{Z})\} \\
&= \{x \in \mathbb{Z} | x = a + km, \textit{ para algum } k \in \mathbb{Z})\}.
\end{aligned}
$$

Para $0 \leq a < m$, temos que a é o resto da divisão de x por m, em que k é o quociente. A divisão de a por m garante que existem $q, r \in \mathbb{Z}$ tais que $a = qm + r$ com $0 \leq r \leq m - 1$. Logo $\overline{a} = \overline{r}$, pois $a - r = qm$, ou seja, $a \equiv r(modm)$. Deste modo $a \in \{0, 1, 2, ..., m - 1\}$, ou seja, $\overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$.

Assim $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ é um candidato a conjunto quociente da relação de congruência. Basta mostrarmos que as classes $\overline{0}, \overline{1}, ..., \overline{m-1}$ são disjuntas. Para isso, suponha que existam duas classes, $\overline{r}$ e $\overline{s}$ iguais em $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$, determinadas por r e s, ambos menores que m, com $r < s < m$. Como $\overline{r} = \overline{s}$, temos pela Proposição 2.16 que $s \equiv r(modm)$ e, assim, $m | s - r$. Porém isso é impossível, pois $m > 1$ e $s - r < m$. Logo $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ é composto por m elementos distintos. Portanto

$$\mathbb{Z}/ \sim = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}.$$

Mais comumente usaremos a notação $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ e chamaremos de conjunto de classes de restos.

Agora exploraremos a ligação entre relações de equivalência e partições em um conjunto não vazio E, a qual será usada na demonstração do importante Teorema de Lagrange.

Definição 2.18. *Seja E um conjunto não-vazio. Diz-se que um conjunto F formado por subconjuntos de E é uma partição de E se forem satisfeitas as seguintes condições:*

1. *dois membros de F ou são iguais, ou são disjuntos;*
2. *a união dos membros de F é igual a E.*

Exemplo 2.19. *Uma partição natural do conjunto $\mathbb{Z}$ é $F = \{P, I\}$, em que P e I representam os conjuntos dos números pares e ímpares, respectivamente. Note que P e I são disjuntos e $P \cup I = \mathbb{Z}$.*

Proposição 2.20. *Se R é uma relação de equivalência sobre um conjunto E, então E/R é uma partição de E.*

Demonstração:

Primeiramente, note que $E/R \neq \emptyset$, pois $E \neq \emptyset$. De fato, como R é reflexiva, se $a \in E$ então $\overline{a} \in E/R$. Portanto, falta verificar as condições da definição 2.18:

1. (as classes de E/R ou são iguais ou são disjuntas) Considere $\overline{a}$ e $\overline{b}$ tais que $\overline{a} \cap \overline{b} \neq \emptyset$. Vamos mostrar que $\overline{a} = \overline{b}$. Suponha $x \in \overline{a} \cap \overline{b}$. Deste modo $x \in \overline{a}$ e $x \in \overline{b}$, ou seja, xRa e xRb. Pela propriedade simétrica temos aRx e pela propriedade transitiva segue que aRb. A Proposição 2.16 garante que $\overline{a} = \overline{b}$.

2. (a união das classes de E/R deve ser igual a E) Como $\overline{a} \subset E$ para todo $a \in E$, temos que a união de todas as classes de E/R está contida em E. Por outro lado, um elemento de E sempre pertence a classe representada por ele, isto é, este elemento pertence a união de todas as classes de E/R. Logo E está contido na união de todas as classes de E/R. Deste modo, mostramos a igualdade entre E e a união das classes de E/R.

$\square$

2.3 FUNÇÃO

O conceito de função é um dos mais importantes (senão o mais importante) estudado no ensino médio e é a base do desenvolvimento de grandes áreas como a álgebra moderna e a análise matemática.

Definição 2.21. *Uma função f de um conjunto A em um conjunto B é uma regra que associa a cada elemento do conjunto A um único elemento do conjunto B. Usaremos a notação $f(a) = b$ para representar que o elemento $a \in A$ está associado com $b \in B$ por meio de f. Também dizemos que b é a imagem de a pela f. O conjunto A é chamado de domínio de f, representado por $D(f)$, e o conjunto B é chamado de contradomínio de f, representado por $CD(f)$. Para indicar que uma função tem domínio A e contradomínio B, usamos a notação $f : A \longrightarrow B$. O conjunto das imagens de cada elemento do domínio é chamado conjunto imagem, e denotado por $Im(f)$.*

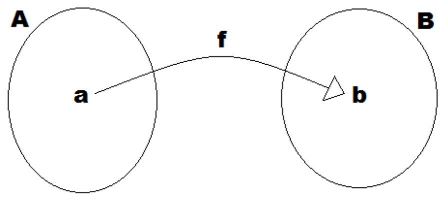

Figura 2: Função de A em B

De especial interesse para o nosso estudo são as funções bijetoras.

Definição 2.22. *Uma função $f : A \longrightarrow B$ é dita injetora se, para todo $a_1, a_2 \in A$, temos que $f(a_1) = f(a_2)$ implica $a_1 = a_2$.*

Definição 2.23. *Uma função $f : A \longrightarrow B$ é dita sobrejetora se $Im(f) = CD(f)$. Mais precisamente, para todo $y \in B$ deve existir $x \in A$ tal que $f(x) = y$.*

Exemplo 2.24. *A função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = 3x - 1$ é uma função injetora. De fato:*

$$\begin{aligned} f(a_1) = f(a_2) &\implies 3(a_1) - 1 = 3(a_2) - 1. \\ &\implies a_1 = a_2 \end{aligned}$$

Esta função também é sobrejetora, pois dado $y \in \mathbb{R}$ existe $x \in \mathbb{R}$ tal que $3x - 1 = y$, a saber, $x = \frac{y+1}{3}$.

Exemplo 2.25. *A função $g : \mathbb{R}_+ \longrightarrow \mathbb{R}$ definida por $g(x) = \sqrt{x}$ é injetora. De fato:*

$$\begin{aligned} g(a_1) = g(a_2) &\implies \sqrt{a_1} = \sqrt{a_2}. \\ &\implies a_1 = a_2 \end{aligned}$$

Porém, g não é sobrejetora, pois existe $y \in \mathbb{R}$ tal que $\sqrt{x} \neq y$, para todo $x \in \mathbb{R}_+$, a saber, qualquer $y < 0$.

Exemplo 2.26. *A função $h : \mathbb{R} \longrightarrow \mathbb{R}_+$ definida por $h(x) = x^2$ é sobrejetora, pois $Im(h) = \mathbb{R}_+$, e não é injetora, pois $h(2) = h(-2) = 4$.*

Definição 2.27. *Uma função $f : A \longrightarrow B$ é chamada bijetora se for injetora e sobrejetora. Quando $f : S \longrightarrow S$ for bijetora, dizemos que f é uma permutação de S.*

A teoria das permutações tem papel fundamental na história da teoria de grupos e foi usada por Évariste Galois (1811 - 1832) para caracterizar matematicamente as equações de grau maior do que ou igual a 5, que não são resolúveis por radicais. Este fato foi provado anteriormente por Niels Abel (1802 - 1829), porém não se sabia o que diferenciava estas equações das equações de grau menor que 5, que são resolúveis por radicais.

Exemplo 2.28. *A função do exemplo 2.24 é bijetora e também é uma permutação do conjunto dos números reais.*

Exemplo 2.29. *Seja $S = \{1,2\}$. Podemos associar duas permutações $f : S \longrightarrow S$:*

$$f_1(1) = 1 \quad , \quad f_1(2) = 2 \qquad ; \qquad f_2(1) = 2 \quad , \quad f_2(2) = 1$$

Estas permutações podem ser representadas por meio da notação a seguir:

$$f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad ; \quad f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Exemplo 2.30. *Seja $S = \{1,2,3\}$. Podemos associar seis permutações $f : S \longrightarrow S$:*

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \; ; \; f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \; ; \; f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \; ; \; f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \; ; \; f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Definição 2.31. *Sejam $f : A \longrightarrow B$ e $g : B \longrightarrow C$ duas funções. Uma função h chama-se composta de g e f, e representa-se por $h = g \circ f$, se $h(x) = (g \circ f)(x) = g(f(x))$, para todo $x \in A$.*

Exemplo 2.32. *Considere as funções*

$$\begin{array}{c} g : \mathbb{R}_+ \longrightarrow \mathbb{R} \\ x \mapsto \sqrt{x} \end{array} \qquad ; \qquad \begin{array}{c} h : \mathbb{R} \longrightarrow \mathbb{R}_+ \\ x \mapsto x^2 \end{array}$$

definidas nos exemplos 2.25 e 2.26. Há uma composição natural de h e g. Para calcularmos $(h \circ g)(5)$, fazemos:

$$(h \circ g)(5) = h(g(5)) = h(\sqrt{5}) = (\sqrt{5})^2 = 5.$$

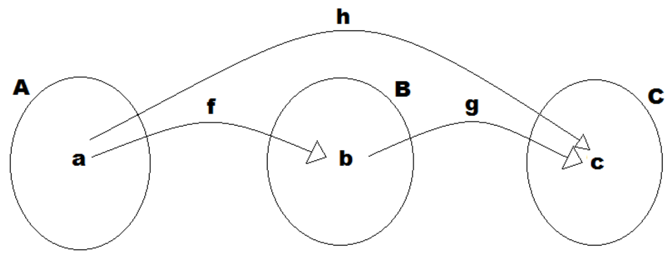

Figura 3: Função composta $h(a) = g(f(a))$

Proposição 2.33. *A composta de duas funções bijetoras é uma função bijetora.*

Demonstração:

Sejam $f : A \longrightarrow B$ e $g : B \longrightarrow C$ duas funções bijetoras e considere $g \circ f : A \longrightarrow C$ a função composta de g e f. Devemos mostrar que $g \circ f$ satisfaz as condições da definição 2.27:

1. ($g \circ f$ é injetora) Sejam $a_1, a_2 \in A$ tais que $(g \circ f)(a_1) = (g \circ f)(a_2)$. Então $g(f(a_1)) = g(f(a_2))$ e como g é injetora segue $f(a_1) = f(a_2)$. Como f também é injetora concluímos que $a_1 = a_2$.

2. ($g \circ f$ é sobrejetora) Seja $c \in C$. Como g é sobrejetora, existe $b \in B$ tal que $g(b) = c$. Como f também é sobrejetora, existe $a \in A$ tal que $f(a) = b$. Deste modo $c = g(b) = g(f(a)) = (g \circ f)(a)$.

$\square$

Exemplo 2.34. *Para fazer a composição das permutações f_1 e f_2 do exemplo 2.29, observe que:*

$$(f_2 \circ f_1)(1) = f_2(f_1(1)) = f_2(1) = 2 \quad ; \quad (f_2 \circ f_1)(2) = f_2(f_1(2)) = f_2(2) = 1$$

Usando outra notação, temos:

$$f_2 \circ f_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Note que a composição de permutações pode ser calculada rapidamente se usarmos a notação anterior. Para isso, procedemos da permutação da direita para a permutação de esquerda, do seguinte modo:

$$1 \mapsto 1 \mapsto 2 \quad ; \quad 2 \mapsto 2 \mapsto 1$$

Exemplo 2.35. *Seguem algumas composições de permutações do exemplo 2.30:*

$$f_3 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_5 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$f_2 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Encerramos esta seção com a definição de função inversa.

Definição 2.36. *Seja $f : A \longrightarrow B$ uma função. Definimos a inversa de f, se existir, a função $f^{-1} : B \longrightarrow A$ tal que $f \circ f^{-1} = id_B$ e $f^{-1} \circ f = id_A$.*

Exemplo 2.37. *Note que no exemplo 2.35, a permutação inversa de f_2 é a própria f_2, pois $f_2 \circ f_2 = id_A = f_1$. Denotamos por $f_2 = {f_2}^{-1}$.*

Exemplo 2.38. *A inversa da função $f(x) = 3x - 1$ definida no exemplo 2.24 é $f^{-1}(x) = \frac{x+1}{3}$, pois $f \circ f^{-1} = f^{-1} \circ f = id_{\mathbb{R}}$. De fato,*

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f\left(\frac{x+1}{3}\right) = 3\left(\frac{x+1}{3}\right) - 1 = x;$$

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(3x-1) = \frac{(3x-1)+1}{3} = x.$$

Exemplo 2.39. *As funções dos exemplos 2.25 e 2.26 não admitem inversa. A proposição seguinte fornece uma condição necessária e suficiente para que a inversa exista.*

Proposição 2.40. *Seja $f : A \longrightarrow B$ uma função. A função inversa $f^{-1} : B \longrightarrow A$ de f existirá se, e somente se, f for bijetora.*

Demonstração:
($\Longrightarrow$) Vamos mostrar que, se f^{-1} existe então f é bijetora.

1. (f é injetora) Sejam $a_1, a_2 \in A$ tais que $f(a_1) = f(a_2) = b$. Então $a_1 = f^{-1}(b)$ e $a_2 = f^{-1}(b)$. Como f^{-1} é função, temos que $f^{-1}(b)$ é único, ou seja, $a_1 = a_2$.

2. (f é sobrejetora) Seja $b \in B$. Como f^{-1} é função de B em A, existe $a \in A$ tal que $f^{-1}(b) = a$, e assim, $f(a) = b$.

($\Longleftarrow$) Vamos mostrar que, se f é bijetora então f^{-1} existe.

1. Como f é sobrejetora, dado $b \in B$, existe $a \in A$ tal que $f(a) = b$. Deste modo, defina $f^{-1}(b) = a$. Concluímos que $D(f^{-1}) = B$.

2. Vejamos que f^{-1} está bem definida. Seja $b \in B$ e suponhamos $f^{-1}(b) = a_1$ e $f^{-1}(b) = a_2$. Então $f(a_1) = f(a_2) = b$. Como f é injetora, segue que $a_1 = a_2$. Isso nos mostra que para cada $b \in B$ existe um único $a \in A$ tal que $b = f^{-1}(a)$.

$\square$

3 POLIEDROS REGULARES

Há uma gama muito grande de definições de poliedros. Todas elas nos remetem a pensar em uma reunião de um número finito de polígonos planos com algumas determinadas condições. Cada uma tem o seu propósito de estudo e o seu nível de ensino. A definição a seguir, proposta por (LIMA et al., 2006), é a mais adequada para os alunos de ensino médio, por se tratar da primeira visão sobre o assunto.

Definição 3.1. *Poliedro é uma reunião de um número finito de polígonos planos, chamados faces, em que:*

1. *cada lado de um desses polígonos é também lado de um, e apenas um, outro polígono;*
2. *a interseção de duas faces quaisquer ou é um lado comum, ou é um vértice ou é vazia. Cada lado de um polígono, comum a exatamente duas faces, é chamado de aresta do poliedro e cada vértice de uma face é um vértice do poliedro;*
3. *é sempre possível ir de um ponto de uma face a um ponto de qualquer outra, sem passar por nenhum vértice (ou seja, cruzando apenas arestas).*

Definição 3.2. *Um poliedro diz-se convexo quando qualquer segmento de reta, não paralela a nenhuma das faces deste poliedro, o corta em, no máximo, dois pontos.*

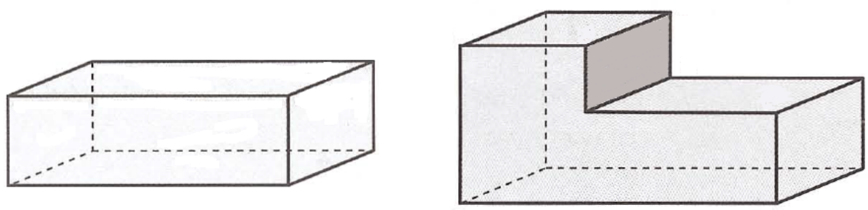

Figura 4: Um poliedro convexo e um poliedro não-convexo

Fonte: (PAIVA, 1995)

3.1 A RELAÇÃO DE EULER

Em todo poliedro convexo, e alguns não convexos, é válida uma importante relação entre o número de faces, arestas e vértices. Esta é chamada relação de Euler.

Proposição 3.3. *Representando por V o número de vértices, por F o número de faces e por A o número de arestas de um poliedro convexo, é válida a relação de Euler:*

$$V+F=A+2.$$

Demonstração:
Vamos considerar um polígono P_1 em que o número de lados seja A_1 e o número de vértices seja V_1, como na figura 5. Representamos a única face de P_1 por F_1. Deste modo, como $A_1 = V_1$, este polígono satisfaz a relação $V_1 + F_1 - A_1 = 1$.

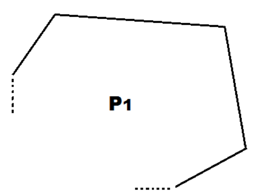

Figura 5: Superfície P_1 com $A_1 = V_1$

Seja P_2 um polígono com k lados, não coplanar a P_1, com um lado comum a P_1, como na figura 6. Então, para a superfície $P_1 \cup P_2$ temos

1. número de vértices $V_2 = V_1 + k - 2$
2. número de arestas $A_2 = A_1 + k - 1$
3. número de faces $F_2 = F_1 + 1$

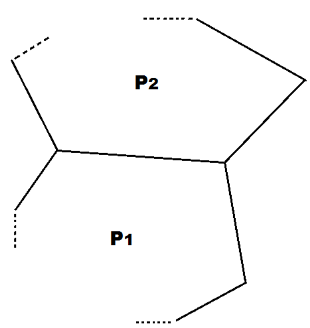

Figura 6: Superfície $P_1 \cup P_2$

Note que

$$V_2 + F_2 - A_2 = (V_1 + k - 2) + (F_1 + 1) - (A_1 + k - 1) = V_1 + F_1 - A_1 = 1.$$

Assim por diante, vamos acrescentando regiões poligonais com o intuito de construir um poliedro convexo aberto, ou seja, um poliedro sem alguma face (ou sem algumas de suas faces).

Vamos mostrar por indução que um poliedro convexo aberto de F_n faces, V_n vértices e A_n arestas satisfaz a relação $V_n + F_n - A_n = 1$:

1. Já vimos que para $n = 1$, vale $V_1 + F_1 - A_1 = 1$;

2. Suponha que $V_n + F_n - A_n = 1$ seja verdadeira para $n \geq 1$, ou seja, temos uma superfície aberta que é formada por $P_1 \cup P_2 \cup P_3 \cup \ldots \cup P_n$. Vamos acrescentar a essa superfície um polígono P_{n+1} com p lados, sendo que q destes lados coincidem com arestas já existentes ($q < p$). Deste modo, obtemos um novo poliedro convexo aberto

$$P_1 \cup P_2 \cup P_3 \cup \ldots \cup P_n \cup P_{n+1}$$

tal que:

(a) $V_{n+1} = V_n + p - (q+1)$, pois $q+1$ vértices coincidem;

(b) $A_{n+1} = A_n + p - q$, pois q arestas coincidem;

(c) $F_{n+1} = F_n + 1$.

Deste modo:

$$V_{n+1} + F_{n+1} - A_{n+1} = [V_n + p - (q+1)] + [F_n + 1] - [A_n + p - q] = 1.$$

Para concluírmos a demonstração da relação de Euler, basta retirar uma face de um poliedro convexo com V vértices, F faces e A arestas. Deste modo, obtemos um poliedro convexo aberto com $A_n = A$, $V_n = V$ e $F_n = F - 1$. Portanto:

$$V_n + F_n - A_n = 1 \Longrightarrow V + F - 1 - A = 1 \Longrightarrow V + F = A + 2.$$

$\square$

3.2 OS CINCO POLIEDROS DE PLATÃO

Definição 3.4. *Um poliedro é chamado poliedro de Platão se, e somente se:*

1. *todas as faces têm o mesmo número n de arestas;*

2. *todos os ângulos poliédricos têm o mesmo número m de arestas (ou seja, m arestas concorrem em cada vértice);*

3. *vale a relação de Euler, $V+F=A+2$.*

Teorema 3.5. *Existem somente cinco classes de poliedros de Platão.*

Demonstração:
Como cada aresta é comum a duas faces, temos $2A = nF = mV$, ou seja, $F = \frac{2A}{n}$ e $V = \frac{2A}{m}$. Substituindo na relação de Euler, obtemos:

$$V+F=A+2 \Longrightarrow \frac{2A}{m}+\frac{2A}{n}=A+2 \Longrightarrow 2A\left(\frac{1}{m}+\frac{1}{n}-\frac{1}{2}\right)=2 \Longrightarrow \frac{1}{m}+\frac{1}{n}-\frac{1}{2}=\frac{1}{A},$$

com $m \geq 3$ e $n \geq 3$. Observe que m,n não podem ser simultaneamente maiores que 3. Do contrário teríamos $m \geq 4 \Rightarrow \frac{1}{m} \leq \frac{1}{4}$ e $n \geq 4 \Rightarrow \frac{1}{n} \leq \frac{1}{4}$, e assim,

$$\frac{1}{m}+\frac{1}{n} \leq \frac{1}{2} \Longrightarrow \frac{1}{m}+\frac{1}{n}-\frac{1}{2} \leq 0 \longrightarrow \frac{1}{A} \leq 0,$$

o que é absurdo, pois $\frac{1}{A} > 0$. Concluímos que um poliedro de Platão possui ângulo triédrico (3 arestas concorrendo em cada vértice) e/ou faces triangulares.

1. $m=3 \Rightarrow \frac{1}{m}+\frac{1}{n}-\frac{1}{2}=\frac{1}{A} \Rightarrow \frac{1}{n}-\frac{1}{6}=\frac{1}{A} \Rightarrow \frac{1}{n}>\frac{1}{6} \Rightarrow n<6$. Deste modo, $m=3$ (ângulo triédrico) implica

    - $n=3$ (faces triangulares);
    - $n=4$ (faces quadrangulares);
    - $n=5$ (faces pentagonais).

2. $n=3 \Rightarrow \frac{1}{m}+\frac{1}{n}-\frac{1}{2}=\frac{1}{A} \Rightarrow \frac{1}{m}-\frac{1}{6}=\frac{1}{A} \Rightarrow \frac{1}{m}>\frac{1}{6} \Rightarrow m<6$. Deste modo, $n=3$ (faces triangulares) implica

    - $m=3$ (ângulos triédricos);
    - $m=4$ (ângulos tetraédricos);

- $m = 5$ (ângulos pentaédricos).

□

Resumimos as cinco classes de poliedros de Platão na Tabela 1:

m	n	A	V	F	poliedro de Platão
3	3	6	4	4	Tetraedro
3	4	12	8	6	Hexaedro
4	3	12	6	8	Octaedro
3	5	30	20	12	Dodecaedro
5	3	30	12	20	Icosaedro

Tabela 1: Poliedros de Platão

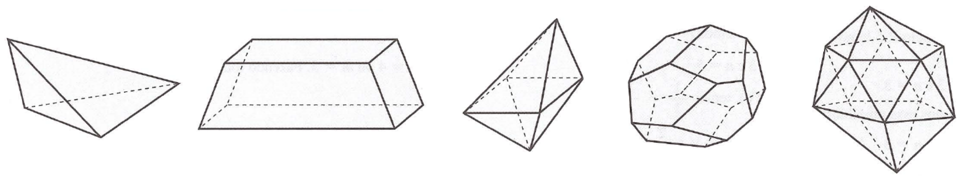

Figura 7: Os cinco poliedros de Platão

Fonte: (PAIVA, 1995)

3.3 POLIEDROS REGULARES

Definição 3.6. *Diz-se que um poliedro convexo é regular se, e somente se,*

1. *todas as suas faces são polígonos regulares e congruentes entre si (implica que as faces têm o mesmo número de lados);*
2. *todos os seus ângulos poliédricos são congruentes entre si (implica que têm o mesmo número de arestas).*

Deste modo, todo poliedro regular é poliedro de Platão.

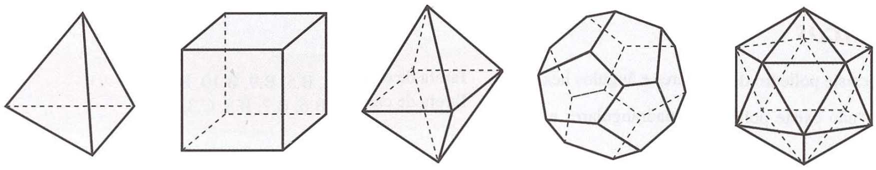

Figura 8: Os cinco poliedros regulares

Fonte: (PAIVA, 1995)

3.4 POLIEDROS DUAIS

Definição 3.7. *Considere P um poliedro regular. O poliedro dual de P é o poliedro cujos vértices são os centros de cada uma das faces de P.*

Exemplo 3.8. *O dual de um tetraedro regular é um tetraedro regular. Dizemos que o tetraedro regular é auto-dual.*

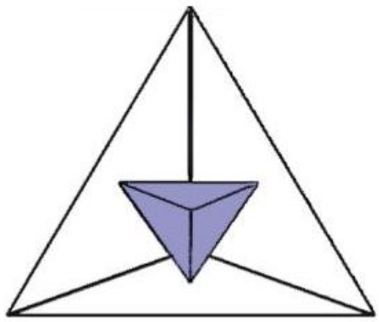

Figura 9: A dualidade do tetraedro regular

Fonte: (*Disponível em http://www.es.iff.edu.br/poliedros/poli_duais.html. Acessado em 04/05/2013*)

Exemplo 3.9. *O hexaedro regular e o octaedro regular são duais.*

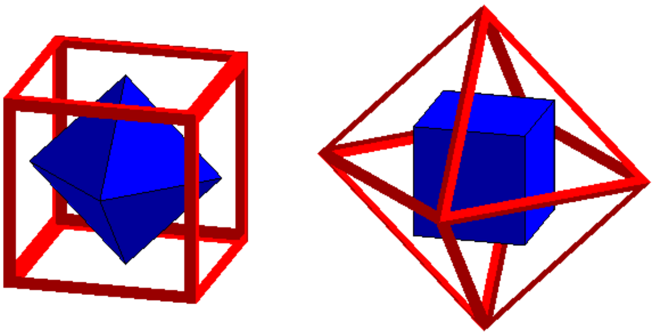

Figura 10: A dualidade do hexaedro regular e do octaedro regular

Fonte: (*Disponível em http://pt.wikipedia.org/wiki/S%C3%B3lido_plat%C3%B3nico. Acessado em 04/05/2013*)

Exemplo 3.10. *O icosaedro regular e o dodecaedro regular são duais.*

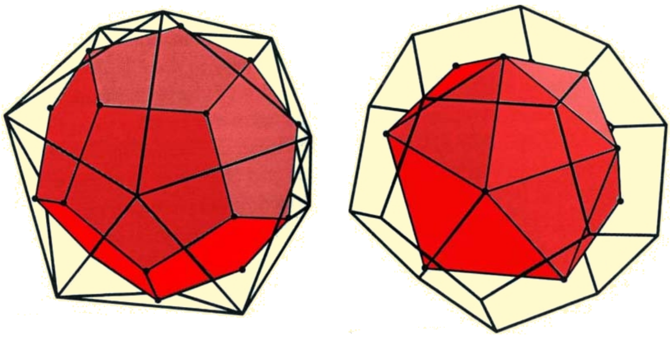

Figura 11: A dualidade do icosaedro regular e do dodecaedro regular

Fonte: (*Disponível em http://www.educadores.diaadia.pr.gov.br/arquivos/File/tvmultimidia/imagens/5matematica/8_dodecaedro_e_icosaedro_2.jpg. Acessado em 04/05/2013*)

4 GRUPOS

Observe o relógio analógico da figura 12. Suponha que o ponteiro se movimenta no sentido horário e retorna ao ponto inicial (representado na figura) depois de sessenta minutos. Chamaremos de “horário”o número inteiro entre 0 e 59 (inclusive) que o ponteiro estará marcando.

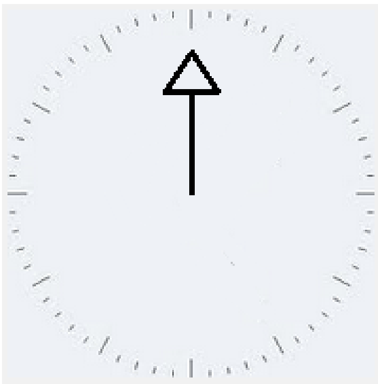

Figura 12: Relógio Analógico apenas com o ponteiro dos minutos

Definimos uma operação sobre $I = \{i \in \mathbb{Z} | 0 \leq i < 60\}$ da seguinte forma: a soma de dois horários $x, y \in I$, denotada por $x + y$, é a movimentação do ponteiro para o horário x e, em seguida, a movimentação do ponteiro em y horários. Observe que:

1. $x + (y + z) = (x + y) + z$ para todo $x, y, z \in I$, pois a soma de horários em I obedece as leis da adição de números inteiros, entre elas, a associatividade.

2. $x + 0 = 0 + x = x$, para todo $x \in I$, pois somar 0 a um horário significa não deslocar o ponteiro. Deste modo, existe um horário $0 \in I$ que somado com qualquer horário $x \in I$ resulta o próprio $x \in I$.

3. $x + (60 - x) = (60 - x) + x = 0$, para todo $x \in I$, ou seja, sempre existe um horário $(60 - x) \in I$ que somado com $x \in I$ resultará $0 \in I$. Esta soma faz com que o ponteiro retorne ao ponto inicial.

Essas observações nos motivam para a definição de grupo.

4.1 DEFINIÇÃO DE GRUPO

Definição 4.1. *Um conjunto G, não-vazio, munido de uma operação binária*

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (a,b) &\mapsto ab \end{aligned}$$

é chamado de grupo se as seguintes condições são satisfeitas:

1. *A operação binária é associativa, isto é,* $(ab)c = a(bc)$ *para todo* $a,b,c \in G$*;*

2. *Existe um elemento e em G tal que* $ae = ea = a$*, para todo* $a \in G$*;*

3. *Para cada* $a \in G$ *existe um elemento* $a^{-1} \in G$ *tal que* $aa^{-1} = a^{-1}a = e$*.*

O elemento $e \in G$ com a propriedade do item 2 é chamado elemento neutro do grupo G. O elemento $a^{-1} \in G$ com a propriedade do item 3 é chamado de elemento simétrico do elemento $a \in G$.

A operação de multiplicação citada na definição de grupo é apenas um símbolo que usaremos para representar a operação com a qual o grupo está munido. Esta operação vai depender da natureza de seus elementos.

Definição 4.2. *Um grupo é denominado abeliano se a operação do grupo é comutativa, ou seja, para todo* $a,b \in G$ *vale que* $ab = ba$*.*

Exemplo 4.3. *Os conjuntos dos números inteiros* $\mathbb{Z}$*, dos números racionais* $\mathbb{Q}$ *e dos números reais* $\mathbb{R}$ *são grupos abelianos munidos da operação de adição usual, pois esta operação é associativa e comutativa em* $\mathbb{R}$ *(consequentemente em* $\mathbb{Z}$ *e* $\mathbb{Q}$*), o* 0 *é o elemento neutro e todos os elementos têm simétricos aditivos (opostos).*

Exemplo 4.4. *O conjunto dos números naturais* $\mathbb{N} = \{0,1,2,3,...\}$ *com a operação de adição usual não tem estrutura de grupo, pois os elementos deste conjunto não tem simétricos aditivos. Observe que* $2 \in \mathbb{N}$*, porém* $-2 \notin \mathbb{N}$*.*

Exemplo 4.5. *Os conjuntos* $\mathbb{Q}^*$ *e* $\mathbb{R}^*$ *são grupos abelianos munidos da operação de multiplicação usual, pois esta operação é associativa e comutativa em* $\mathbb{R}$ *(consequentemente em* $\mathbb{Q}$*), o 1 é o elemento neutro e todos os elementos têm simétricos multiplicativos (inversos). O conjunto dos números inteiros* $\mathbb{Z}^*$ *não tem estrutura de grupo com a operação de multiplicação pela inexistência de elementos simétricos para todos os seus elementos.*

Exemplo 4.6. *Denotamos por $M_{m\times n}(\mathbb{R})$ o conjunto das matrizes do tipo $m\times n$ com entradas reais. Este conjunto tem estrutura de grupo munido da operação usual de adição de matrizes. Sabemos que esta operação é associativa, a matriz nula $O_{m\times n}$ é o elemento neutro e dado $A\in M_{m\times n}(\mathbb{R})$, temos a matriz oposta $-A\in M_{m\times n}(\mathbb{R})$ como seu elemento simétrico.*

Exemplo 4.7. *Considere o conjunto das classes dos restos, definido no exemplo 2.17. Para $m>1$, definimos a adição em $\mathbb{Z}_m=\{\overline{0},\overline{1},\overline{2},...,\overline{m-1}\}$ por*

$$\overline{a}+\overline{b}=\overline{a+b}$$

para todo $\overline{a},\overline{b}\in\mathbb{Z}_m$. Note que esta operação assim definida tem as seguintes propriedades:

1. *(associativa)*
$$\begin{aligned}(\overline{a}+\overline{b})+\overline{c} &= \overline{a+b}+\overline{c}\\ &= \overline{a+b+c}\\ &= \overline{a}+\overline{b+c}\\ &= \overline{a}+(\overline{b}+\overline{c})\end{aligned}$$

2. *(comutativa)* $\overline{a}+\overline{b}=\overline{a+b}=\overline{b+a}=\overline{b}+\overline{a}$

3. *(existência de elemento neutro)* $\overline{a}+\overline{0}=\overline{a+0}=\overline{a}$

4. *(existência de elementos simétricos)* $\overline{a}+\overline{m-a}=\overline{a+m-a}=\overline{m}=\overline{0}$

Deste modo, o conjunto $\mathbb{Z}_m$ munido da operação de adição de classes de restos definida acima tem estrutura de grupo abeliano.

Exemplo 4.8. *Seja S um conjunto não-vazio e indiquemos por $A(S)$ o conjunto das permutações de S, como na definição 2.27. Note que a operação de composição de funções tem as seguintes propriedades:*

1. *(associativa)*
$$\begin{aligned}((f\circ g)\circ h)(x) &= (f\circ g)(h(x))\\ &= f(g(h(x)))\\ &= f((g\circ h)(x))\\ &= (f\circ(g\circ h))(x)\end{aligned}$$

2. *(existência de elemento neutro)*

$$(f\circ i)(x)=f(i(x))=f(x) \quad ; \quad (i\circ f)(x)=i(f(x))=f(x)$$

3. *(existência de elementos simétricos)*

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = x \quad ; \quad (f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$$

Portanto, o conjunto $A(S)$ das permutações de S munido da operação de composição de funções tem estrutura de grupo, chamado grupo das permutações.

Exemplo 4.9. *Um caso particular do exemplo 4.8 é quando $S = \{1,2,3,...,n\}$. Neste caso, a notação $A(S)$ passa a ser indicada por S_n e é denominado grupo simétrico de grau n. Nos exemplos 2.29 e 2.30 foram mostrados todos os elementos de S_2 e S_3. Note que S_n não é abeliano, pois, por exemplo, em S_4:*

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

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

4.2 ALGUMAS PROPRIEDADES

O resultado a seguir nos fornece algumas das propriedades elementares de grupo.

Proposição 4.10. *Seja G um grupo. Então:*

1. *O elemento neutro de G é único;*
2. *O elemento simétrico de $a \in G$ é único;*
3. *Para todo $a \in G$ vale que $(a^{-1})^{-1} = a$;*
4. *Sejam $a, b \in G$. Então $(ab)^{-1} = b^{-1}a^{-1}$.*

Demonstração:

1. Considere $e, e' \in G$ elementos neutros tais que $e \neq e'$. Deste modo, temos $ae = ea = a$ e $ae' = e'a = a$ para todo $a \in G$. Então:

$$e = ee = ee' = e'.$$

Contradição.

2. Seja $e \in G$ o elemento neutro de G e considere $a', a'' \in G$ simétricos de $a \in G$, tal que $a' \neq a''$. Deste modo, temos $aa' = a'a = e$ e $aa'' = a''a = e$. Então:

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

Contradição.

3. Sendo $e \in G$ o elemento neutro de G, basta mostrar que $a^{-1}a = e$ e $aa^{-1} = e$. Estas igualdades fazem parte da definição de grupo.

4. Basta mostrar que $(ab)(b^{-1}a^{-1}) = e$ e $(b^{-1}a^{-1})(ab) = e$.

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = (ae)a^{-1} = aa^{-1} = e;$$

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

□

Definiremos agora uma operação importante para os elementos de um grupo.

Definição 4.11 (Potência de um elemento)**.** *Seja $a \in G$ e $n \in \mathbb{Z}$. A potência n-ésima de a é definida como:*

$$a^n = \begin{cases} a^{n-1}a & se\ n \geq 1 \\ a^0 = 1 & \\ \left(a^{-1}\right)^{-n} & se\ n \leq -1 \end{cases}$$

Proposição 4.12. *Seja G um grupo. Se $a \in G$, e $m, n \in \mathbb{Z}$ então $a^m a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$.*

Demonstração:
Sejam $m, n \in \mathbb{Z}$. Separamos a demonstração de $a^m a^n = a^{m+n}$ em duas partes:

1. $n \geq 0$: Procedemos por indução sobre n. Para $n = 0$, temos $a^m a^0 = a^m e = a^m = a^{m+0}$. Suponha que $a^m a^n = a^{m+n}$, para algum $n \in \mathbb{Z}$. Devemos mostrar que $a^m a^{n+1} = a^{m+n+1}$. Logo:

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

Portanto, segue pelo princípio de indução que $a^m a^n = a^{m+n}$, para todo $n \geq 0$.

2. $n < 0$: Se $n < 0$ então $-n > 0$. Deste modo:

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

A demonstração de $(a^m)^n = a^{mn}$ é análoga.

$\square$

4.3 SUBGRUPOS

Definição 4.13. *Se $(G,\cdot)$ é um grupo e $H \subseteq G$, dizemos que H é um subgrupo de G se $(H,\cdot)$ é também um grupo. Pela proposição 4.10, o elemento neutro de qualquer subgrupo H é o elemento neutro de G e o elemento simétrico de $a \in H$ é o simétrico a^{-1} de $a \in G$.*

Uma caracterização de subgrupos é a seguinte:

Proposição 4.14. *Seja G um grupo e H um subconjunto não-vazio de G. Então H é um subgrupo de G se, e somente se, as seguintes condições são satisfeitas:*

1. *para todo $a,b \in H$, temos $ab \in H$;*
2. *para todo $a \in H$, temos $a^{-1} \in H$.*

Para demonstração, ver (GARCIA; LEQUAIN, 2003).

Exemplo 4.15. *Para qualquer grupo G, os subconjuntos $\{e\}$ e G são grupos, chamados subgrupos triviais.*

Exemplo 4.16. *No grupo $(\mathbb{Q}^*,\cdot)$ citado no exemplo 4.5, o subconjunto $S = \{1,-1\} \subset \mathbb{Q}^*$ é um subgrupo. Note que $ab \in S$, para todo $a,b \in S$ e $a^{-1} \in S$ para todo $a \in S$.*

Definição 4.17. *Seja G um grupo e considere H e K subconjuntos de G. Definimos os seguintes conjuntos:*

$$HK = \{hk | h \in H, k \in K\} \qquad e \qquad H^{-1} = \{h^{-1} | h \in H\}.$$

Em geral, HK não é subgrupo de G, mesmo quando H e K são subgrupos de G. Observe o exemplo 4.18.

Exemplo 4.18. *Sejam $G = S_3$, $H = \{e, \beta\}$ e $K = \{e, \beta\alpha\}$ subgrupos de G, em que*

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

Lembramos que, neste caso, a operação é a composição de funções, e que a notação multiplicativa é usada apenas para simplificar a escrita. Note que

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

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e \,;$$

$$(\beta\alpha)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Deste modo, temos $HK = \{e, \beta, \beta\alpha, \beta^2\alpha\} = \{e, \beta, \beta\alpha, \alpha\}$, porém

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

Como $\alpha^2 \notin HK$, temos que HK não é subgrupo de S_3.

4.4 GRUPO CÍCLICO

Definição 4.19. *Seja S um subconjunto qualquer do grupo G. O conjunto*

$$\{a_1 a_2 ... a_n | n \in \mathbb{N}, a_i \in S\}$$

denotado por $< S >$ é um subgrupo de G, chamado subgrupo gerado por S.

Definição 4.20. *Seja G um grupo. Definimos o conjunto das potências de $g \in G$ como*

$$< g >= \{g^t | t \in \mathbb{Z}\}.$$

Definição 4.21. *Seja G um grupo. Se existir $g \in G$ tal que $G =< g >= \{g^t | t \in \mathbb{Z}\}$, dizemos que o grupo G é cíclico. Dizemos também que g gera G ou que G é gerado por g.*

Exemplo 4.22. *São cíclicos os grupos:*

1. $\mathbb{Z} = <1> = <-1>$

2. $\mathbb{Z}_4 = <\bar{1}> = <\bar{3}>$

Não são cíclicos os grupos aditivos $\mathbb{Q}$ e $\mathbb{R}$.

Proposição 4.23. *Se um grupo G é cíclico então G é abeliano.*

Demonstração:
Sejam a,b pertencentes a um um grupo cíclico G, gerado por g. Então, existem t_1 e t_2 tais que $a = g^{t_1}$ e $b = g^{t_2}$. Logo:

$$ab = g^{t_1}g^{t_2} = g^{t_2}g^{t_1} = ba.$$

□

Observe no exemplo 4.24 que a recíproca da proposição 4.23 é falsa.

Exemplo 4.24. *Consideremos $(G,\cdot)$ e $(H,\circ)$ dois grupos cujos elementos neutros são, respectivamente, e_G e e_H. Seja*

$$G \times H = \{(g,h) | g \in G, h \in H\}$$

o produto cartesiano de G e H. No conjunto $G \times H$ definimos a operação

$$(g,h) \star (g',h') = (g \cdot g', h \circ h')$$

para todo $g, g' \in G$ e $h, h' \in H$. O grupo $(G \times H, \star)$ é chamado produto direto de G com H, com elemento neutro (e_G, e_H). Observe que, quando consideramos o grupo $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, temos que:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0},\overline{0}), (\overline{0},\overline{1}), (\overline{1},\overline{0}), (\overline{1},\overline{1})\};$$

$$(\overline{0},\overline{0})^2 = (\overline{0},\overline{0}) + (\overline{0},\overline{0}) = (\overline{0},\overline{0});$$

$$(\overline{0},\overline{1})^2 = (\overline{0},\overline{1}) + (\overline{0},\overline{1}) = (\overline{0},\overline{0});$$

$$(\overline{1},\overline{0})^2 = (\overline{1},\overline{0}) + (\overline{1},\overline{0}) = (\overline{0},\overline{0});$$

$$(\overline{1},\overline{1})^2 = (\overline{1},\overline{1}) + (\overline{1},\overline{1}) = (\overline{0},\overline{0}).$$

Deste modo, $(G \times H, \star)$ é abeliano não cíclico.

Definição 4.25. *Chamamos de ordem do grupo G o número de elementos de G, e denotamos $|G|$. Se $a \in G$, a ordem de a, denotada por $O(a)$ é a ordem do subgrupo cíclico $< a >$.*

4.5 CLASSES LATERAIS

Agora podemos voltar a considerar um subgrupo H de um grupo G. A relação definida no exemplo a seguir é de extrema importância no estudo dos subgrupos.

Exemplo 4.26. *Sobre G, definimos a seguinte relação:*

$$\forall a, b \in G,\ a \sim b \iff ab^{-1} \in H.$$

Proposição 4.27. *A relação definida acima é uma relação de equivalência.*

Demonstração:
Devemos mostrar que a relação é reflexiva, simétrica e transitiva:

1. (reflexiva) Seja $a \in G$ e e o elemento neutro de G. Então existe $a^{-1} \in G$ tal que $aa^{-1} = e$. Como H é subgrupo de G, temos $e \in H$, e assim, $aa^{-1} \in H$. Portanto $a \sim a$, ou seja, a relação é reflexiva.

2. (simétrica) Suponhamos $a \sim b$, isto é, $ab^{-1} \in H$. Como H é subgrupo de G, temos $(ab^{-1})^{-1} \in H$. Como $(ab^{-1})^{-1} = ba^{-1}$, temos que $b \sim a$, ou seja, a relação é simétrica.

3. (transitiva) Suponhamos que $a \sim b$ e $b \sim c$, isto é, $ab^{-1} \in H$ e $bc^{-1} \in H$. Como H é subgrupo de G, temos que $ac^{-1} = a(b^{-1}b)c^{-1} = (ab^{-1})(bc^{-1}) \in H$. Logo, $a \sim c$, ou seja, a relação é transitiva.

$\square$

Proposição 4.28. *A classe de equivalência determinada por $a \in G$ da relação anterior é o conjunto $\overline{a} = \{b \in G | a \sim b\} = \{ha | h \in H\} = Ha$.*

Demonstração:

Mostraremos as duas continências:

1. ($\supset$) Seja $x \in Ha$, ou seja, $x = ha$, para algum $h \in H$. Daí, $ax^{-1} = h^{-1} \in H$, isto é $a \sim x$. Portanto $[a] \supset Ha$.

2. ($\subset$) Seja $x \in [a]$, ou seja, $a \sim x$, e assim, $ax^{-1} \in H$. Logo, $ax^{-1} = h$, para um conveniente $h \in H$. Daí, $x = h^{-1}a \in Ha$, uma vez que $h^{-1} \in H$. Portanto, $[a] \subset Ha$.

□

Chamamos o conjunto Ha de classe lateral à direita.

Analogamente, podemos definir a relação $\forall a, b \in G$, $a \sim b \iff a^{-1}b \in H$ que também é uma relação de equivalência, da qual obteríamos classes laterais à esquerda de H em G. A classe lateral de a, à esquerda, é $aH = \{ah | h \in H\}$.

Exemplo 4.29. *No grupo aditivo $\mathbb{Z}_4$, temos o subgrupo $H = \{\overline{0}, \overline{2}\}$. As classes laterais são:*

$$
\begin{array}{lcl}
\overline{0} + H = \{\overline{0}+\overline{0}, \overline{0}+\overline{2}\} = \{\overline{0},\overline{2}\} & ; & H + \overline{0} = \{\overline{0}+\overline{0}, \overline{2}+\overline{0}\} = \{\overline{0},\overline{2}\} \\
\overline{1} + H = \{\overline{1}+\overline{0}, \overline{1}+\overline{2}\} = \{\overline{1},\overline{3}\} & ; & H + \overline{1} = \{\overline{0}+\overline{1}, \overline{2}+\overline{1}\} = \{\overline{1},\overline{3}\} \\
\overline{2} + H = \{\overline{2}+\overline{0}, \overline{2}+\overline{2}\} = \{\overline{2},\overline{0}\} & ; & H + \overline{2} = \{\overline{0}+\overline{2}, \overline{2}+\overline{2}\} = \{\overline{2},\overline{0}\} \\
\overline{3} + H = \{\overline{3}+\overline{0}, \overline{3}+\overline{2}\} = \{\overline{3},\overline{1}\} & ; & H + \overline{3} = \{\overline{0}+\overline{3}, \overline{2}+\overline{3}\} = \{\overline{3},\overline{1}\}
\end{array}
$$

Observe no exemplo anterior que o número de classes laterais à esquerda é o mesmo que o número de classes laterais à direita. E ainda, para classes diferentes, o número de elementos é o mesmo, igual ao número de elementos de H. Essas conclusões serão provadas nas duas proposições que seguem.

Vamos mostrar que a cardinalidade da classe lateral à direita de $a \in G$ é a mesma que a da classe lateral à esquerda de $a \in G$, permitindo-nos, desse modo, dar um nome para essa cardinalidade, independente da classe que adotamos.

Proposição 4.30. *É bijetora a aplicação*

$$
\begin{aligned}
\varphi : X = \{\textit{Classes laterais à esquerda}\} &\longrightarrow Y = \{\textit{ Classes laterais à direita}\} \\
aH &\longmapsto Ha^{-1}
\end{aligned}
$$

Demonstração:

1. (sobrejetora) Dada uma classe $Hc \in Y$ queremos mostrar que existe $bH \in X$ tal que $\varphi(bH) = Hc$. Seja $b = c^{-1}$. Logo $\varphi(bH) = \varphi(c^{-1}H) = H(c^{-1})^{-1} = Hc$.

2. (injetora) Suponha $Ha^{-1} = Hb^{-1}$. Então existem h, h' tais que $ha^{-1} = h'b^{-1}$, ou seja, $(h')^{-1}ha^{-1} = b^{-1}$, e assim $(h')^{-1}h = b^{-1}a$, o que implica $(b^{-1}a) \in H$. Queremos mostrar que $aH = bH$.

   $(\subset)$ Considere $ah_1 \in aH$. Então:

$$ah_1 = (bb^{-1})ah_1 = b\underbrace{(b^{-1}a)h_1}_{h_2} = bh_2 \in bH$$

($\supset$) Análogo, com $a^{-1}b \in H$.

$\square$

Chamaremos de índice de H em G o número de classes laterais módulo H em G. Notação: $(G : H)$.

Proposição 4.31. *Todas as classes laterais de H em G têm a mesma cardinalidade de H.*

Demonstração:

A maneira mais natural de definir uma função de H em aH é

$$\begin{aligned} \Phi : H &\longrightarrow aH \\ h &\longmapsto ah. \end{aligned}$$

Precisamos verificar se esta função é uma bijeção.

1. (sobrejetora) Dado $ah \in aH$, sempre existe $h \in H$ tal que $\Phi(h) = ah$.
2. (injetora) Sejam $h_1, h_2 \in H$ tais que $\Phi(h_1) = \Phi(h_2)$. Então $ah_1 = ah_2$. Como $a \in G$, temos $a^{-1} \in G$. Logo $a^{-1}(ah_1) = a^{-1}(ah_2)$, e assim, $h_1 = h_2$.

$\square$

Provaremos agora o teorema de Lagrange.

Teorema 4.32 (Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então*

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

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

Demonstração:
Suponhamos $(G : H) = r$ e seja $\{a_1H, a_2H, ..., a_rH\}$ o conjunto de todas as classes laterais à

esquerda, módulo H. A Proposição 2.18 garante que esse conjunto determina uma partição de G. Deste modo, temos

$$a_1H \cup a_2H \cup ... \cup a_rH = G.$$

Como as classes laterais são todas disjuntas, temos

$$|a_1H| + |a_2H| + ... + |a_rH| = |G|.$$

Da Proposição 4.31 , segue que

$$\underbrace{|H| + |H| + ... + |H|}_{r \text{ vezes}} = |G|.$$

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

$\square$

Seguem algumas das consequências imediatas do Teorema de Lagrange:

Corolário 4.33. *Todo grupo finito de ordem prima é cíclico.*

Demonstração:
Seja $p > 1$ um número primo. Se p é a ordem de um grupo G então existe $a \in G$ tal que $a \neq e$. Logo $H =< a >$ é um subgrupo de G de ordem, no mínimo, igual a 2. Como $|H|$ divide $|G|$ e $|G|$ é um número primo, concluímos que $|H| = p$. Logo $H =< a >= G$ e, portanto, G é cíclico.

$\square$

Deste corolário, podemos concluir que, neste caso, G só comporta os subgrupos triviais, pois os únicos valores possíveis para $|H|$ são 1 e p.

Corolário 4.34. *Se G é um grupo tal que $|G| \leq 5$ então G é abeliano.*

Demonstração:

1. Se $|G| = 1$ então $G = \{e\}$.
2. Se $|G| = 2, 3$ ou 5 então $|G| = p$, com p primo e, pelo corolário anterior, G é cíclico. Portanto G é abeliano.

3. Se $|G| = 4$, separamos em dois casos:

   (a) Se existe $a \neq e$ com $a \in G$ tal que $< a >= G$, então G é cíclico e, portanto, abeliano.

   (b) Suponhamos que para todo $a \in G$ com $a \neq e$ se tem $< a > \neq G$. Pelo Teorema de Lagrange segue que $| < a > | = 2$. Assim, $a^2 = e$ para todo $a \in G$. Portanto G é abeliano.

$\square$

Observação 4.35. *Se G é um grupo finito e se m é um divisor da ordem de G, não podemos garantir que G contém um subgrupo de ordem m. Porém podemos afirmar que se p é um primo divisor da ordem de G, então G contém um subgrupo de ordem p. Esta conclusão é o teorema de Cauchy (cuja demonstração está fora dos limites deste trabalho).*

4.6 SUBGRUPOS NORMAIS E GRUPOS QUOCIENTES

Queremos determinar para quais subgrupos H de um grupo G, as classes laterais à esquerda (direita) formam um grupo sob a operação induzida por G.

Primeiro, vejamos que a operação induzida por G sobre o conjunto das classes laterais à esquerda de H em G está bem definida, isto é, que a operação $(aH, bH) \mapsto abH$ está bem definida, ou seja, que não depende da escolha dos representantes a e b.

Sejam $a, b \in G$ e $h, k \in H$. Os elementos a e ah são representantes da mesma classe aH. Da mesma forma, b e bk são representantes da mesma classe bH. A operação induzida sobre as classes laterais à esquerda está bem definida se, e somente se, $(ab)H = (ahbk)H$, para todo $a, b \in G$ e $h, k \in H$. Deste modo:

$$\begin{aligned}
(ab)H = (ahbk)H \quad &\iff \quad (b^{-1}a^{-1}ab)H = (b^{-1}a^{-1}ahbk)H \\
&\iff \quad H = (b^{-1}hbk)H \\
&\iff \quad H = (b^{-1}hb)H \\
&\iff \quad b^{-1}hb \in H
\end{aligned}$$

Precisamos que H satisfaça a seguinte propriedade: se $h \in H$ e $x \in G$ então $xhx^{-1} \in H$. Isto nem sempre é verdade, pois como veremos a seguir, esta propriedade equivale a valer que $xH = Hx$ para cada $x \in G$.

Proposição 4.36. *Seja H um subgrupo de um grupo G. As afirmações seguintes são equivalentes:*

1. *a operação induzida sobre as classes laterais à esquerda de H em G é bem definida;*
2. $gHg^{-1} \subseteq H$, $\forall g \in G$;
3. $gHg^{-1} = H$, $\forall g \in G$;
4. $gH = Hg$, $\forall g \in G$.

Demonstração:

- $(1 \iff 2)$ Foi feito anteriormente.
- $(2 \Longrightarrow 3)$ Suponhamos que $gHg^{-1} \subseteq H, \forall g \in G$. Queremos mostrar que $H \subseteq gHg^{-1}$, $\forall g \in G$. Para isso, sejam $h \in H$ e $g \in G$. Logo

$$h = g(g^{-1}hg)g^{-1} \in g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}.$$

- $(2 \Longleftarrow 3)$ Definição de igualdade de conjuntos.
- $(3 \iff 4)$ Definição de classe lateral.

□

Definição 4.37. *Um subgrupo H é um subgrupo normal de G, e denotamos por $H \lhd G$, se ele satisfaz as afirmações equivalentes da Proposição 4.36. Nesse caso, as classes laterais à esquerda de H são iguais às classes laterais à direita de H.*

Exemplo 4.38. *Se G é um grupo abeliano, então todo subgrupo de G é normal.*

Proposição 4.39. *Todo subgrupo de índice dois de um grupo é subgrupo normal.*

Demonstração:
Queremos mostrar que $aH = Ha$ para todo $a \in G$. Se $a \in H$, então $aH = H = Ha$. Se $a \notin H$, então $aH \neq H$ e $Ha \neq H$. Como $(G : H) = 2$ existem duas classes laterais à esquerda: aH e H. As classes de equivalência decompõem o espaço em uma união disjunta de classes. Então $aH = G \setminus H$ e $Ha = G \setminus H$. Portanto $aH = G \setminus H = Ha$.

□

Definição 4.40. *Sejam G um grupo e H um subgrupo normal de G. O grupo de suas classes laterais com a operação induzida de G é o grupo quociente de G por H. Denotaremos por G/H.*

Exemplo 4.41. *Considere o grupo $G = \mathbb{Z}_6$ e $H = \{\overline{0}, \overline{3}\}$ um subgrupo de G. Então*

$$G/H = \{H, \overline{1} + H, \overline{2} + H\}$$

é um grupo com a operação induzida de G sobre as classes laterais.

4.7 HOMOMORFISMO DE GRUPOS

Para qualquer classe de objetos algébricos é essencial o estudo das funções que preservam a estrutura algébrica.

Definição 4.42. *Sejam $(G, \cdot)$ e $(G', \times)$ dois grupos. Uma função $\Psi : G \longrightarrow G'$ é um homomorfismo de grupos se ela é compatível com as estruturas dos grupos, ou seja,*

$$\Psi(x \cdot y) = \Psi(x) \times \Psi(y),$$

para todo $x, y \in G$. Se o homomorfismo $\Psi : G \longrightarrow G'$ for injetivo, dizemos que Ψ é um monomorfismo, se for sobrejetivo dizemos que é um epimorfismo, se for bijetivo dizemos que ψ é um isomorfismo e, neste caso dizemos que G é isomorfo a G', e denotamos por $G \cong G'$. Um isomorfismo $\Psi : G \longrightarrow G$ diz-se um automorfismo de G.

Exemplo 4.43. *$e : G \longrightarrow G'$, dada por $e(g) = e_{G'}$, para todo $g \in G$, é um homomorfismo chamado homomorfismo trivial.*

Exemplo 4.44. *$f : \mathbb{R}^*_+ \longrightarrow \mathbb{R}$ dada por $f(x) = log x$ é um homomorfismo de $(\mathbb{R}^*_+, \cdot)$ em $(\mathbb{R}, +)$, uma vez que*

$$f(ab) = log(ab) = log(a) + log(b) = f(a) + f(b), \forall a, b \in \mathbb{R}^*_+.$$

Exemplo 4.45. *Seja $g \in G$ fixo. Então $I_g : G \longrightarrow G$ dada por $I_g(x) = gxg^{-1}$ é um homomorfismo bijetivo.*

Proposição 4.46. *Seja $f : (G, \cdot) \longrightarrow (G', \times)$ um homomorfismo de grupos. Então:*

1. *$f(e_G) = e_{G'}$;*
2. *$f(x^{-1}) = (f(x))^{-1}$.*

Demonstração:

1. $f(e_G) \times e_{G'} = f(e_G) = f(e_G e_G) = f(e_G) \times f(e_G)$;
2. $e_{G'} = f(e_G) = f(xx^{-1}) = f(x) \times f(x^{-1})$.

$\square$

Definição 4.47. *Seja $f : G \longrightarrow G'$ um homomorfismo de grupos. Denominamos de conjunto imagem de Ψ, e representamos por $Im\Psi$, o conjunto*

$$Im\Psi = \Psi(G) = \{\Psi(g) | g \in G\}.$$

Definição 4.48. *Seja $f : G \longrightarrow G'$ um homomorfismo de grupos em que e' é o elemento neutro de G. Denominamos de núcleo de Ψ, e representamos por $ker(\Psi)$, o conjunto*

$$ker(\Psi) = \{g \in G | \Psi(g) = e'\}.$$

Proposição 4.49. *Sejam G e G' grupos com elementos neutros e e e', respectivamente e $\Psi : G \longrightarrow G'$ um homomorfismo. Então:*

(1) $Im\Psi$ é um subgrupo de G' ;

(2) $ker(\Psi)$ é um subgrupo normal de G;

(3) Ψ é injetiva se, e somente se, $ker(\Psi) = \{e\}$;

(4) $G/Ker(\Psi) \cong Im\Psi$.

Demonstração:

1. Sejam $x, y \in Im\Psi$, ou seja, existem $g_1, g_2 \in G$ tais que $x = \Psi(g_1)$ e $y = \Psi(g_2)$. Devemos mostrar que $xy^{-1} \in Im\Psi$. Então:

$$xy^{-1} = \Psi(g_1)(\Psi(g_2))^{-1} = \Psi(g_1(g_2)^{-1}).$$

Como $(g_1(g_2)^{-1}) \in G$, temos que $xy^{-1} \in Im\Psi$. Portanto $Im\Psi$ é um subgrupo de G'.

2. Primeiro verificaremos que $ker(\Psi)$ é um subgrupo de G. Considere $a, b \in ker(\Psi)$, ou seja, $\Psi(a) = e'$ e $\Psi(b) = e'$. Devemos mostrar que $ab^{-1} \in Ker(\Psi)$. Temos:

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

Portanto $ab^{-1} \in ker(\Psi)$.

Finalmente, vamos mostrar que ker(Ψ) é normal. Considere $g \in G$ e $n \in ker(\Psi)$, ou seja, $\Psi(n) = e'$. Devemos mostrar que $g^{-1}ng \in ker(\Psi)$. Temos:

$$\Psi(g^{-1}ng) = \Psi(g^{-1})\Psi(n)\Psi(g) = (\Psi(g))^{-1}e'\Psi(g) = (\Psi(g))^{-1}\Psi(g) = e'.$$

Portanto $Ker\Psi$ é um subgrupo normal de G.

3. A definição de injetividade nos diz que $\Psi(a) = \Psi(b)$ implica que $a = b$, para todo $a, b \in D(\Psi)$. Temos que mostrar a dupla implicação.

   ($\Rightarrow$) Suponha que Ψ é injetiva. Vamos mostrar que $ker(\Psi) = \{e\}$. Como Ψ é homomorfismo, temos $\Psi(e) = e'$. Deste modo, $ker(\Psi) \supset \{e\}$. Para mostrar que $ker(\Psi) \subset \{e\}$ considere $n \in ker(\Psi)$, ou seja, $\Psi(n) = e' = \Psi(e)$. Pela hipótese de que Ψ é injetiva, temos $n = e$.

   ($\Leftarrow$) Suponha que $ker(\Psi) = \{e\}$. Devemos mostrar que Ψ é injetiva. Para isso, considere $a, b \in G$ tais que $\Psi(a) = \Psi(b)$. Deste modo, $\Psi(a)(\Psi(b))^{-1} = e'$, ou seja, $\Psi(ab^{-1}) = e'$. Logo, $ab^{-1} = e'$, e assim, $a = b$.

4. Devemos encontrar uma função de $G/ker(\Psi)$ em $Im(\Psi)$ que cumpra as condições de isomorfismo. A maneira mais natural de definir esta função é

$$\begin{aligned} \overline{\Psi} : G/ker(\Psi) &\longrightarrow Im(\Psi) \\ aker\Psi &\mapsto \Psi(a) \end{aligned}$$

   Primeiramente, devemos verificar se $\overline{\Psi}$ está bem definida. Para facilitar a escrita fazemos $ker(\Psi) = N$. Considere duas classes $aN, bN \in G/N$ tais que $aN = bN$. Então $(a^{-1}b)N = N$ e isso implica que $a^{-1}b \in N$. Logo $\Psi(a^{-1}b) = e'$, ou seja, $(\Psi(a))^{-1}\Psi(b) = e'$. Portanto $\Psi(a) = \Psi(b)$.

   Em seguida, devemos mostrar que $\overline{\Psi}$ é um homomorfismo, ou seja, para $aN, bN \in G/ker(\Psi)$ vale que $\overline{\Psi}(aNbN) = \overline{\Psi}(aN)\overline{\Psi}(bN)$. Então:

$$\overline{\Psi}(aNbN) = \overline{\Psi}((ab)N) = \Psi(ab) = \Psi(a)\Psi(b) = \overline{\Psi}(aN)\overline{\Psi}(bN).$$

   Finalmente, devemos mostrar que $\overline{\Psi}$ é uma bijeção. De fato, $\overline{\Psi}$ é sobrejetora, pois $Im(\overline{\Psi}) = Im(\Psi)$. Para mostrar que $\overline{\Psi}$ é injetora, considere $\overline{\Psi}(aN) = e'$. Logo $a \in N$, e assim $aN = N$. Portanto $ker\overline{\Psi} = \{N\}$. Segue que Ψ é injetora.

$\square$

4.8 TEOREMA DE CAYLEY

A importância dos grupos de permutações está no seguinte resultado, devido ao matemático inglês A. Cayley:

Teorema 4.50. *Todo grupo G é isomorfo a um subgrupo de $A(S)$ para algum S apropriado, em que $A(S)$ é conjunto de todas as bijeções $S \to S$.*

Demonstração:
Primeiro devemos definir uma função bijetora que vai representar o elemento de $A(S)$ para a demonstração do Teorema de Cayley. Para isso, seja G um grupo e seja S o conjunto subjacente a G, isto é, S é o conjunto G sem a estrutura de grupo. Se $g \in G$, vamos definir $\delta_g : S \longrightarrow S$ por $\delta_g(x) = gx$. Esta função é uma bijeção.

1. Se $\delta_g(x) = \delta_g(y)$ temos $gx = gy$, o que implica $x = y$, pois g pertence a um grupo, e assim, obedece a lei do cancelamento. Mostramos que δ_g é injetora.
2. Dado $y \in S$ devemos encontrar $x \in S$ tal que $\delta_g(x) = y$, ou seja, $gx = y$. Em um grupo, esta equação tem solução $x = g^{-1}y$. Mostramos que δ_g é sobrejetora.

Agora temos que definir uma função de G em $A(S)$ de modo que seja um isomorfismo de grupos. De acordo com a definição de δ_g, a maneira mais natural de definir esta função é

$$\begin{aligned} F : G &\longrightarrow A(S) \\ g &\mapsto \delta_g \end{aligned}$$

1. (F é homomorfismo) Devemos mostrar que $F(g_1g_2) = F(g_1) \circ F(g_2)$. Observe que, para todo elemento $x \in S$, temos

$$\delta_{g_1g_2}(x) = (g_1g_2)(x) = g_1(g_2x) = \delta_{g_1}(g_2x) = \delta_{g_1}(\delta_{g_2}(x)) = (\delta_{g_1} \circ \delta_{g_2})(x).$$

   A igualdade $\delta_{g_1.g_2} = \delta_{g_1} \circ \delta_{g_2}$ nos permite calcular

$$F(g_1g_2) = \delta_{g_1g_2} = \delta_{g_1} \circ \delta_{g_2} = F(g_1) \circ F(g_2).$$

2. (F é injetora) Vamos mostrar que $ker(F) = \{e\}$. Seja $g \in ker(F)$, ou seja, $F(g) = \delta_g = id_S$. Isso implica que $x = \delta_g(x) = g.x$ para todo $x \in G$. Em particular, para $x = e$, temos $g = e$.

Assim F é um isomorfismo de G em um subgrupo de $A(S)$.

$\square$

Um grupo finito G pode ser visto como um subgrupo de S_n, onde $n = |G|$.

Exemplo 4.51. *Considere o grupo $G = \mathbb{Z}_4$. Pelo teorema de Cayley, sabemos que $\mathbb{Z}_4$ é isomorfo a um subgrupo de S_4. Por meio da função $\delta_{(\overline{a})}(\overline{x}) = \overline{a} + \overline{x}$, encontramos os elementos correspondentes em S_4:*

$\delta_{(\overline{0})}(\overline{x}) = \overline{0} + \overline{x} = \overline{x}$. *Deste modo, temos a permutação* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in S_4$.

$\delta_{(\overline{1})}(\overline{x}) = \overline{1} + \overline{x}$. *Deste modo, temos a permutação* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$.

$\delta_{(\overline{2})}(\overline{x}) = \overline{2} + \overline{x}$. *Deste modo, temos a permutação* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \in S_4$.

$\delta_{(\overline{3})}(\overline{x}) = \overline{3} + \overline{x}$. *Deste modo, temos a permutação* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$.

4.9 AÇÃO

No teorema de Cayley um grupo age sobre si mesmo, no sentido de que cada $g \in G$ produz uma permutação de G. Podemos generalizar a noção de um grupo agindo em um conjunto arbitrário.

Definição 4.52. *Seja G um grupo e X um conjunto não-vazio. Dizemos que G age em X se para cada $g \in G$ existe uma função*

$$\begin{aligned} f : G \times X &\longrightarrow X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

satisfazendo as seguintes condições:

1. *Para todo $x \in X$, temos $e \cdot x = x$, em que e é o elemento neutro de G;*

2. *Para todo $g, h \in G$ e $x \in X$ temos $g \cdot (h \cdot x) = (gh) \cdot x$.*

Exemplo 4.53. *O grupo $\mathbb{Z}$ age sobre $\mathbb{R}$ por translação:*

$$\begin{aligned} \mathbb{Z} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (n, x) &\mapsto n \cdot x = n + x \end{aligned}$$

Note que:

1. $0 \cdot x = 0 + x = x$;

2. $(n+m) \cdot x = (n+m) + x = n + (m+x) = n + (m \cdot x) = n \cdot (m \cdot x)$.

Exemplo 4.54. *O grupo $\mathbb{Z}$ age sobre $\mathbb{R}$ por*

$$\begin{aligned} \mathbb{Z} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (n,x) &\mapsto n \cdot x = (-1)^n x \end{aligned}$$

Note que:

1. $0 \cdot x = (-1)^0 x = x$;

2. $(n+m) \cdot x = (-1)^{(n+m)} x = (-1)^n [(-1)^m x] = (-1)^n (m \cdot x) = n \cdot (m \cdot x)$.

Exemplo 4.55. *(Ação regular) Todo grupo age sobre si mesmo por meio da operação usual do grupo.*

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,x) &\mapsto g \cdot x = gx \end{aligned}$$

A associatividade da operação de G e a propriedade do elemento neutro garantem a ação de G sobre X.

Exemplo 4.56. *(Ação trivial) Definimos como ação trivial a função que segue:*

$$\begin{aligned} G \times X &\longrightarrow X \\ (g,x) &\mapsto g \cdot x = x \end{aligned}$$

Exemplo 4.57. *Existe uma ação natural do grupo simétrico S_n no conjunto $X = \{1, 2, 3, ..., n\}$:*

$$\begin{aligned} S_n \times X &\longrightarrow X \\ (\sigma,x) &\mapsto \sigma \cdot x = \sigma(x) \end{aligned}$$

Exemplo 4.58. *Seja H um subgrupo de um grupo G. Uma ação de um subgrupo H no conjunto G é dada por*

$$\begin{aligned} H \times G &\longrightarrow G \\ (h,x) &\mapsto h \cdot x = hx \end{aligned}$$

Esta ação é chamada translação a esquerda em G.

Exemplo 4.59. *Seja H um subgrupo de um grupo G. Uma ação de H em G é dada por*

$$\begin{aligned} H \times G &\longrightarrow G \\ (h,x) &\mapsto h \cdot x = hxh^{-1} \end{aligned}$$

Esta ação de H em G é chamada conjugação por H e o elemento hxh^{-1} é dito conjugado de x por h.

Se um grupo G age sobre um conjunto X, então esta ação induz um homomorfismo $\Psi : G \longrightarrow A(X)$ em que $A(X)$ é o grupo de todas as permutações de X. (para demonstração, ver (HUNGERFORD, 1974)). E dado um homomorfismo $\Psi : G \longrightarrow A(X)$, a função $f : G \times X \longrightarrow X$ dada por $f(g,x) = \Psi(g)(x)$ é uma ação.

5 ÓRBITAS E ESTABILIZADORES

Seja G um grupo agindo sobre um conjunto X. Para cada $x \in X$, sua órbita é o conjunto

$$O_G(x) = \{g \cdot x | g \in G\} \subset X,$$

e seu estabilizador é o conjunto

$$G_x = Stab_G(x) = \{g \in G | g \cdot x = x\} \subset G.$$

Observação 5.1. *De acordo com (CONRAD, 2011), a órbita de um ponto é um conceito "geométrico", pois é o conjunto de lugares onde o ponto pode ser movido pela ação do grupo.*

Observação 5.2. *Ainda de acordo com (CONRAD, 2011), o estabilizador de um ponto é um conceito algébrico, isto é, o conjunto de elementos do grupo que fixam o ponto.*

Proposição 5.3. *Seja um grupo G agindo em um conjunto X. O estabilizador de $x \in X$ é um subgrupo de G.*

Demonstração:
$G_x \neq \varnothing$ já que $e \in G_x$, pois $e \cdot x = x$. Sejam $g, h \in G_x$, ou seja, $g \cdot x = h \cdot x = x$ e $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$. Se $g \in G_x$ então $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$. Isso implica que $g^{-1} \in G_x$.

□

As órbitas $O_G(x)$ são subconjuntos de X. O fato significativo sobre estes subconjuntos é que eles formam uma partição de X, como mostraremos na Proposicão 5.4.

Proposição 5.4. *Seja G um grupo agindo sobre um conjunto X. Então a relação sobre X definida por*

$$x \sim y \text{ se, e somente se, } x = g \cdot y, \text{ para algum } g \in G$$

é uma relação de equivalência. Além disso, a classe de equivalência de qualquer $x \in X$ é a órbita $O_G(x)$.

Demonstração:

1. (reflexiva) Se $x \in X$ então $x \sim x$, pois $x = e \cdot x$.
2. (simétrica) Seja $x \sim y$, ou seja, $x = g \cdot y$ para algum $g \in G$. Deste modo:

   $$g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = e \cdot y = y.$$

   Logo $y \sim x$.
3. (transitiva) Sejam $x \sim y$ e $y \sim z$. Deste modo, existem $g, g' \in G$ tais que $x = g \cdot y$ e $y = g' \cdot z$. Então

   $$x = g \cdot (g' \cdot z) = (gg') \cdot z.$$

   Logo, $x \sim z$.

Para qualquer $x \in X$, a classe de equivalência de x é o conjunto

$$\overline{x} = O_x = \{y \in X | y \sim x\} = \{y \in X | y = g \cdot x\}.$$

□

Exemplo 5.5. *Quando G age sobre si mesmo por multiplicação à esquerda:*

1. $O_G(e) = \{g \cdot e | g \in G\} = \{ge | g \in G\} = \{g | g \in G\} = G.$
2. $G_x = \{g \in G | g \cdot x = x\} = \{g \in G | gx = x\} = \{e\}.$

Exemplo 5.6. *Quando G age sobre si mesmo por conjugação:*

1. $O_G(x) = \{gxg^{-1} | g \in G\}$ *é chamada classe conjugada de x.*
2. $G_x = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$ *é chamado centralizador de x.*

5.1 TEOREMA DA ÓRBITA-ESTABILIZADOR

Este importante teorema da álgebra nos permitirá calcular as simetrias de polígonos regulares e de sólidos regulares. Apesar de sua demonstração ser muito simples, toda a teoria desenvolvida neste trabalho foi para este propósito.

Teorema 5.7. *Seja G um grupo que age em um conjunto X. Então, para qualquer $x \in X$, temos*

$$\sharp O_G(x) = (G : G_x).$$

Além disso, se G é finito, então

$$\sharp O_G(x) = \frac{|G|}{|G_x|}.$$

Demonstração:
Seja $H = G_x$ e definamos $\Psi : \{gH | g \in G\} \longrightarrow O_G(x)$ por $\Psi(gH) = g \cdot x$. Mostremos que Ψ é uma bijeção:

1. (Ψ está bem definida): Suponhamos que $g_1H = g_2H$. Assim, ${g_2}^{-1}g_1 \in H$, ou seja, $({g_2}^{-1}g_1) \cdot x = x$. Portanto:

$$g_1 \cdot x = (g_2{g_2}^{-1}g_1) \cdot x = g_2 \cdot ({g_2}^{-1}g_1) \cdot x = g_2 \cdot x$$

2. (Ψ é injetora): Suponhamos que $\Psi(g_1H) = \Psi(g_2H)$, ou seja, $g_1 \cdot x = g_2 \cdot x$. Logo:

$$({g_2}^{-1}g_1) \cdot x = {g_2}^{-1} \cdot (g_1 \cdot x) = {g_2}^{-1} \cdot (g_2 \cdot x) = ({g_2}^{-1}g_2) \cdot x = e \cdot x = x.$$

   Portanto, mostramos que ${g_2}^{-1}g_1 \in H$, o que implica que $g_1H = g_2H$.

3. (Ψ é sobrejetora): Trivial.

No caso de G ser finito, temos pelo teorema de Lagrange que

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

Portanto,

$$\sharp O_G(x) = \frac{|G|}{|G_x|}.$$

□

6 A CONTAGEM DAS SIMETRIAS ROTACIONAIS DOS POLIEDROS REGULARES

Antes de considerar os casos específicos, observemos em geral que os vértices, arestas (no caso dos polígonos convexos) e faces (no caso dos poliedros convexos) são determinados por sistemas de igualdades e desigualdades lineares. Assim, estes subconjuntos notáveis dos polígonos/poliedros são preservados por transformações lineares invertíveis, em particular, as isometrias.

6.1 O GRUPO DAS SIMETRIAS DE UM TRIÂNGULO EQUILÁTERO

Seja um triângulo equilátero de vértices representados por $1,2,3$ de baricentro O e medianas E_1, E_2 e E_3.

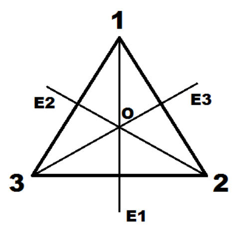

Figura 13: Triângulo equilátero

As transformações que preservam o triângulo são:

1. id: rotação plana no sentido horário centrada em O de 0°;
2. $R_{120°}$: rotação plana no sentido horário centrada em O de 120°;
3. $R_{240°}$: rotação plana no sentido horário centrada em O de 240°;
4. R_1: reflexão (rotação espacial de 180°) em torno de E_1;
5. R_2: reflexão (rotação espacial de 180°) em torno de E_2;
6. R_3: reflexão (rotação espacial de 180°) em torno de E_3.

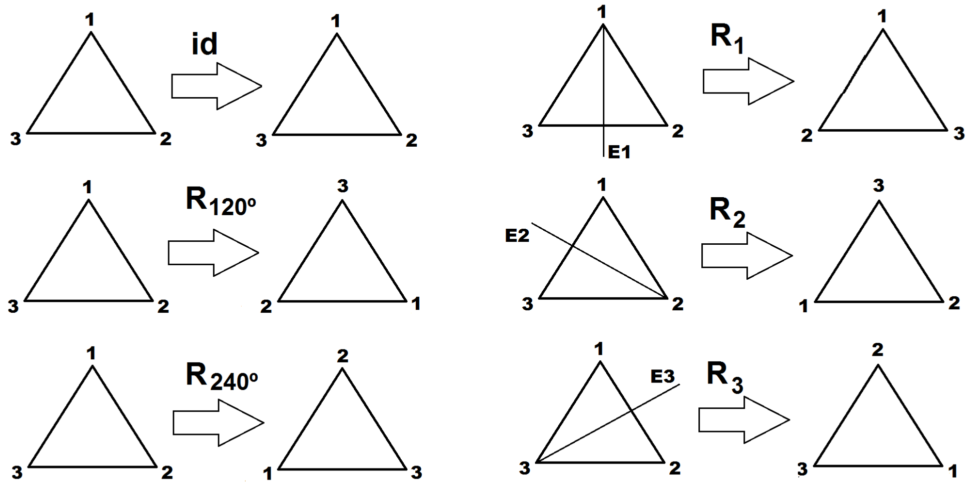

Figura 14: Simetrias do triângulo equilátero

É fácil fazer a verificação que $S_\triangle = \{id, R_{120^\circ}, R_{240^\circ}, R_1, R_2, R_3\}$ munido da operação de composição de funções é um grupo. Podemos associar $S_\triangle$ a um subgrupo das permutações dos vértices da seguinte maneira:

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad ; \quad R_{120^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad ; \quad R_{240^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad ; \quad R_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad ; \quad R_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Vamos fazer a verificação do teorema da órbita-estabilizador no grupo das simetrias do triângulo equilátero. Considere $X = \{1,2,3\}$ e $S_\triangle$ agindo sobre X como no exemplo 4.57. Note que, de acordo com a observação 5.1, o conjunto de lugares para onde o vértice 1 pode ser movido são os vértices $1,2$ e 3. Logo

$$O_{S_\triangle}(1) = \{g \cdot 1 | g \in S_\triangle\} = \{1,2,3\}.$$

Da mesma maneira, de acordo com a observação 5.2, os elementos do grupo que fixam o vértice 1 são id e R_1. Logo

$$Stab_{S_\triangle}(1) = \{g \in G | g \cdot 1 = 1\} = \{id, R_1\}.$$

De acordo com o teorema da órbita-estabilizador, a quantidade de elementos do grupo $S_\triangle$ é

$$|S_\triangle| = \sharp O_{S_\triangle}(1) \cdot |Stab_{S_\triangle}(1)| = 3 \cdot 2 = 6,$$

que são as simetrias mostradas na figura 14.

Observação 6.1. *Note que a mesma verificação anterior poderia ter sido feita com outro elemento $x \in X = \{1,2,3\}$, ou seja, usando outro vértice como base para os conjuntos $O_{S_\triangle}(x)$ e $Stab_{S_\triangle}(x)$.*

6.2 O GRUPO DAS SIMETRIAS DE UM QUADRADO

Seja um quadrado de vértices representados por 1,2,3,4 de centro O, diagonais D_I e D_P e mediatrizes M_V e M_H.

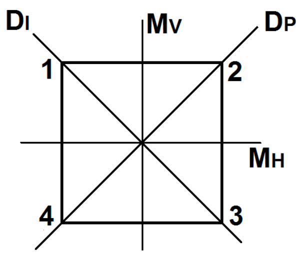

Figura 15: Quadrado

As transformações que preservam o quadrado são:

1. id: rotação plana no sentido horário centrada em O de 0°;
2. R_{90°: rotação plana no sentido horário centrada em O de 90°;
3. R_{180°: rotação plana no sentido horário centrada em O de 180°;
4. R_{270°: rotação plana no sentido horário centrada em O de 270°;
5. R_{M_v}: reflexão (rotação espacial de 180°) em torno de M_V;
6. R_{M_h}: reflexão (rotação espacial de 180°) em torno de M_H;
7. R_{D_I}: reflexão (rotação espacial de 180°) em torno de D_I;
8. R_{D_P}: reflexão (rotação espacial de 180°) em torno de D_P.

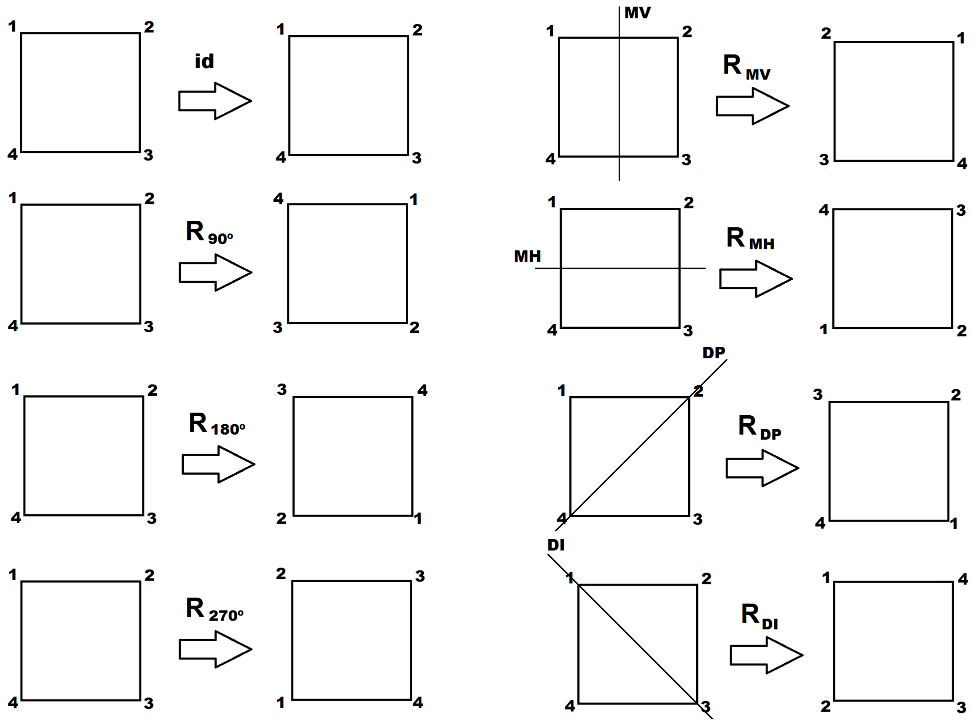

Figura 16: Simetrias do quadrado

Para fazer a verificação que $S_\square = \{id, R_{90^\circ}, R_{180^\circ}, R_{270^\circ}, R_{M_V}, R_{M_H}, R_{D_I}, R_{D_P}\}$ munido da operação de composição de funções é um grupo, associamos $S_\square$ a um subgrupo das permutações dos vértices da seguinte maneira:

$$id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad ; \quad R_{M_V} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$R_{90^\circ} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad ; \quad R_{M_H} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$R_{180^\circ} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad ; \quad R_{D_I} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$R_{270^\circ} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad ; \quad R_{D_P} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Vamos fazer a verificação do teorema da órbita-estabilizador no grupo das simetrias do quadrado, da mesma maneira que fizemos com as simetrias do triângulo equilátero. Considere $X = \{1,2,3,4\}$ e $S_\square$ agindo sobre X como no exemplo 4.57. Note que, de acordo com a observação 5.1, o conjunto de lugares para onde o vértice 1 pode ser movido são os vértices

$1, 2, 3$ e 4. Logo

$$O_{S_\square}(1) = \{g \cdot 1 | g \in S_\square\} = \{1, 2, 3, 4\}.$$

Da mesma maneira, de acordo com a observação 5.2, os elementos do grupo que fixam o vértice 1 são id e R_{D_I}. Logo

$$Stab_{S_\square}(1) = \{g \in G | g \cdot 1 = 1\} = \{id, R_{D_I}\}.$$

De acordo com o teorema da órbita-estabilizador, a quantidade de elementos do grupo $S_\square$ é

$$|S_\square| = \sharp O_{S_\square}(1) \cdot |Stab_{S_\square}(1)| = 4 \cdot 2 = 8,$$

que são as simetrias mostradas na figura 16.

Observação 6.2. *Como na observação 6.1, a mesma verificação anterior poderia ter sido feita com outro elemento $x \in X = \{1, 2, 3, 4\}$, ou seja, usando outro vértice como base para os conjuntos $O_{S_\square}(x)$ e $Stab_{S_\square}(x)$.*

6.3 OS GRUPOS DAS SIMETRIAS DOS POLIEDROS REGULARES

No caso dos polígonos regulares, a aplicação do teorema da órbita-estabilizador aparenta não ser necessária, pois, de maneira geral, a quantidade de elementos do grupo das simetrias de um polígono regular de n vértices é sempre $2n$; este grupo é chamado grupo diedral. De fato, sempre teremos n simetrias de rotações planas e n simetrias de reflexões (rotações espaciais em torno de um eixo).

Observação 6.3. *O subconjunto das simetrias rotacionais planas do grupo diedral é sempre um subgrupo, pois a composição de rotações será sempre uma rotação.*

Agora veremos como o teorema da órbita-estabilizador é útil na contagem de simetrias rotacionais dos cinco poliedros regulares (figura 8).

6.3.1 TETRAEDRO REGULAR

Seja G_T o grupo das simetrias rotacionais do tetraedro regular e $X = \{1, 2, 3, 4\}$ o conjunto dos vértices deste tetraedro. Cada rotação induz uma permutação sobre X, ou seja, G_T pode ser visto como um subgrupo de S_4.

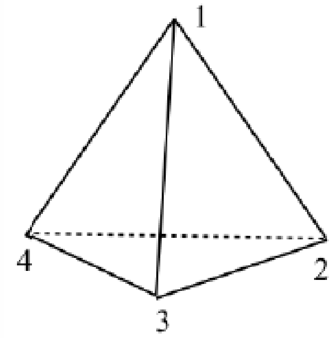

Figura 17: Tetraedro regular de vértices 1,2,3 e 4

Fonte: (MULHOLLAND, 2011)

Note que:

1. os lugares para onde o vértice 1 pode ser movido são os vértices $1,2,3$ e 4. Logo $\sharp O_{G_T}(1) = 4$.

2. as rotações de G_T que fixam o vértice 1 são três: a identidade (tetraedro regular em sua posição original) e as rotações no sentido horário e anti-horário do tetraedro regular em torno do eixo de simetria que passa por 1. Logo $|Stab_{G_T}(1)| = 3$.

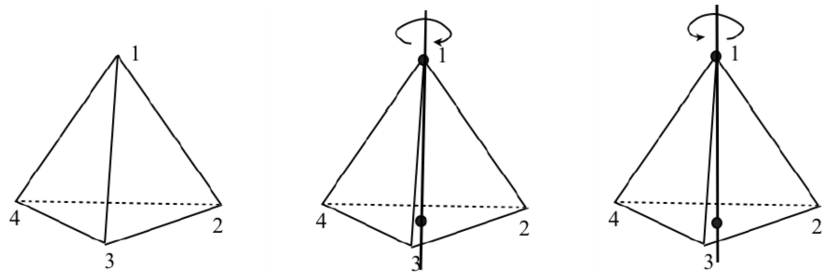

Figura 18: Rotações do tetraedro regular que preservam o vértice 1

Fonte: (MULHOLLAND, 2011)

Portanto, pelo teorema da órbita-estabilizador, temos

$$|G_T| = \sharp O_{G_T}(1) \cdot |Stab_{G_T}(1)| = 4 \cdot 3 = 12.$$

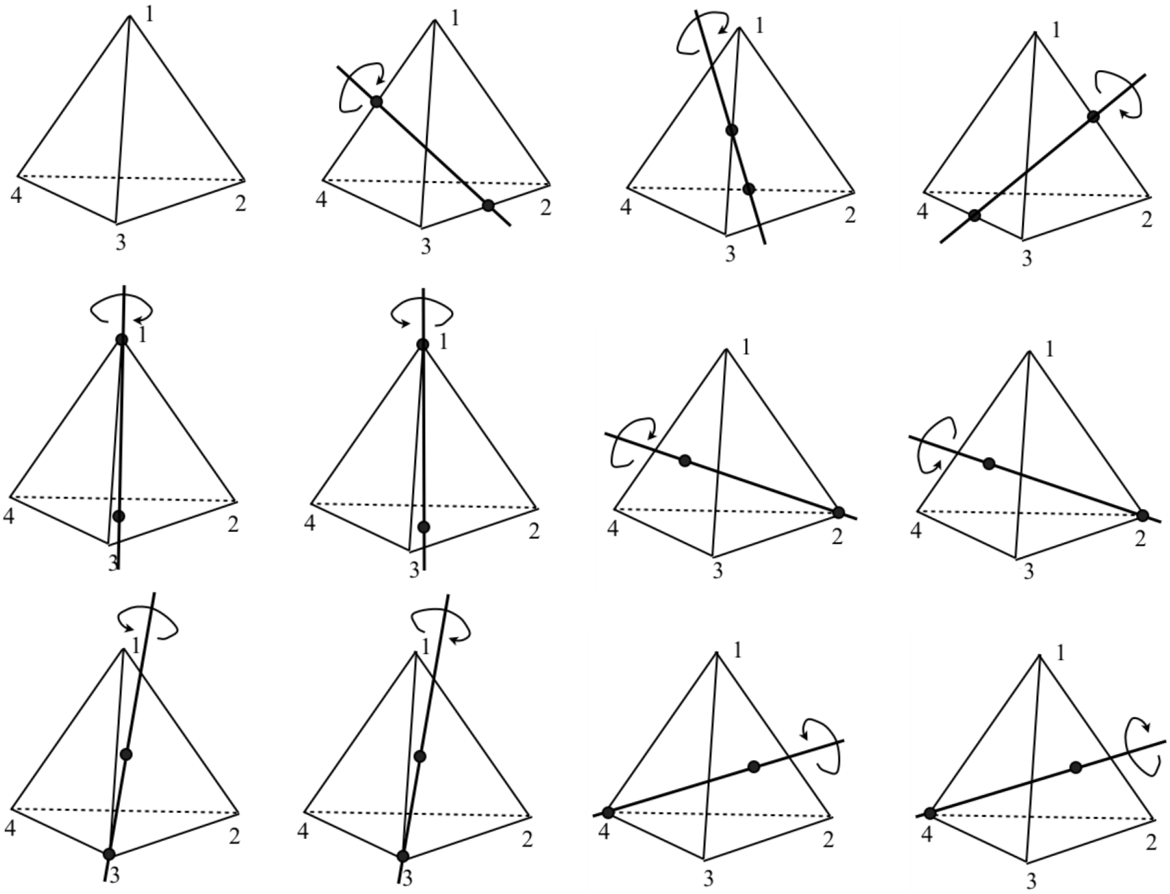

Figura 19: As 12 simetrias rotacionais do tetraedro regular

Fonte: (MULHOLLAND, 2011)

6.3.2 HEXAEDRO REGULAR

Seja G_H o grupo das simetrias rotacionais do hexaedro regular e $X = \{1,2,3,4,5,6,7,8\}$ o conjunto dos vértices deste hexaedro. Da mesma maneira que o tetraedro regular, cada rotação do hexaedro regular induz uma permutação sobre X. Deste modo, G_H pode ser visto como um subgrupo de S_8.

Note que:

1. os lugares para onde o vértice 1 pode ser movido são os vértices $1,2,3,4,5,6,7$ e 8. Logo $\sharp O_{G_H}(1) = 8$.

2. as rotações de G_H que fixam o vértice 1 são três: a identidade (hexaedro regular em sua posição original) e as rotações no sentido horário e anti-horário do hexaedro regular em torno do eixo de simetria (diagonal) que passa por 1 e 7. Logo $|Stab_{G_H}(1)| = 3$.

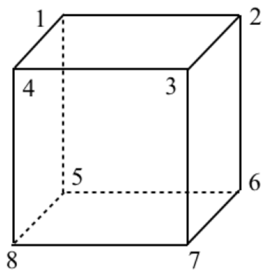

Figura 20: Hexaedro regular de vértices 1,2,3,4,5,6,7,8

Fonte: (MULHOLLAND, 2011)

Portanto, pelo teorema da órbita-estabilizador, temos

$$|G_H| = \sharp O_{G_H}(1) \cdot |Stab_{G_H}(1)| = 8 \cdot 3 = 24.$$

6.3.3 DODECAEDRO REGULAR

Seja G_D o grupo das simetrias rotacionais do dodecaedro regular e

$$X = \{x \in \mathbb{N} | 1 \leq x \leq 20\}$$

o conjunto dos vértices deste dodecaedro. Como foi feito com o tetraedro regular e o hexaedro regular, cada rotação do dodecaedro regular induz uma permutação sobre X. Deste modo, G_D pode ser visto como um subgrupo de S_{20}.

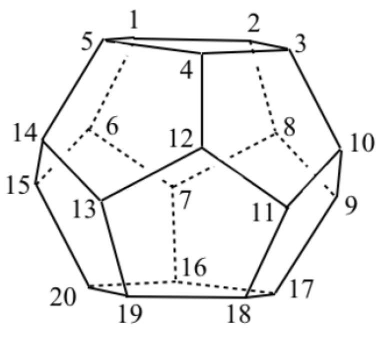

Figura 21: Dodecaedro regular de vértices 1 ao 20

Fonte: (MULHOLLAND, 2011)

Note que:

1. o conjunto de lugares para onde o vértice 1 pode ser movido são os vértices

$$\{x \in \mathbb{N} | 1 \leq x \leq 20\}.$$

Logo $\sharp O_{G_D}(1) = 20$.

2. as rotações de G_D que fixam o vértice 1 são três: a identidade (dodecaedro regular em sua posição original) e as rotações no sentido horário e anti-horário do dodecaedro regular em torno do eixo de simetria (diagonal) que passa por 1 e 18. Logo $|Stab_{G_D}(1)| = 3$.

Portanto, pelo teorema da órbita-estabilizador, temos

$$|G_D| = \sharp O_{G_D}(1) \cdot |Stab_{G_D}(1)| = 20 \cdot 3 = 60.$$

6.3.4 OCTAEDRO REGULAR E ICOSAEDRO REGULAR

Seja G_O e G_I os grupos das simetrias rotacionais do octaedro regular e do icosaedro regular, respectivamente. Para calcular a quantidade de elementos destes grupos, podemos usar a mesma estratégia que usamos anteriormente, porém não o faremos. O motivo é simples: nós já contamos as simetrias rotacionais de seus duais. É fácil observar (fig 10 e fig 11) que os eixos de simetria responsáveis pelas rotações do octaedro regular e do icosaedro regular são os mesmos eixos de simetria de seus duais: os eixos que passam pelos vértices de um sólido são os eixos que passam pelos centros geométricos das faces de seu sólido dual, e vice-versa.

Deste modo, é elementar concluir que

$$|G_O| = |G_H| = 24,$$

e que

$$|G_I| = |G_D| = 60.$$

7 APLICAÇÃO PRÁTICA

7.1 DESCRIÇÃO DA ATIVIDADE

Com o intuito de saber se os adolescentes, estudantes do ensino fundamental e médio, conseguem enxergar as simetrias do quadrado e enxergar e operar as simetrias do triângulo equilátero, foi aplicada uma atividade sobre o assunto em dois colégios particulares de Curitiba, capital do estado do Paraná. Durante o período de uma aula de cinquenta minutos, os alunos de três turmas diferentes do 9º ano do ensino fundamental e uma turma de 1º ano do ensino médio realizaram uma aplicação prática de composição de funções dos elementos do grupo das simetrias do quadrado e do triângulo equilátero. Primeiramente foi dado aos alunos dois quadrados de papel, um branco e um hachurado e dois triângulos equiláteros de papel, também um branco e outro hachurado. Também foi entregue um roteiro da atividade composto por tópicos, citados e comentados a seguir:

1. Você está recebendo dois triângulos equiláteros, um branco e outro hachurado, e dois quadrados, um branco e outro hachurado.

   Comentário: Foi entregue aos alunos os triângulos equiláteros de papel e os quadrados de papel.

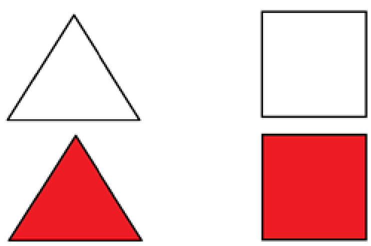

Figura 22: Triângulos equiláteros e quadrados hachurados

2. Nomeie os vértices do triângulo hachurado de A a C e os vértices quadrado hachurado de A a D, seguindo o sentido horário. Proceda da mesma maneira com o triângulo branco e o quadrado branco. Separe os quadrados, pois começaremos a atividade pelos triângulos.

Comentário: Alguns começaram colocando a letra A em vértices diferentes dos polígonos da figura 23, porém não houve problema, pois a posição dos vértices foi padronizada em seguida.

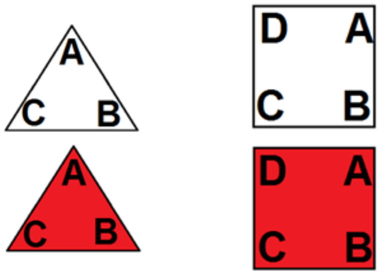

Figura 23: Triângulo de vértices A, B e C e quadrado de vértices A, B, C e D

3. Deixe o triângulo hachurado em cima da mesa, de modo que o vértice A esteja ao norte. Esta posição do triângulo hachurado será fixa, até o fim da atividade. Segure o triângulo branco na mesma posição, sobre o triângulo hachurado. Para relacionar as posições dos triângulos, vamos usar a notação (H,B) para indicar a correspondência entre os vértices do triângulo hachurado e do triângulo branco. Nesta posição inicial, temos $R0 = \{(A,A);(B,B);(C,C)\}$.

   Comentário: A notação em forma de par ordenado não foi um desafio para os alunos, pois já tinham familiaridade com esta representação. Terminado este item, muitos alunos questionaram o porquê do símbolo $R0$.

4. Tente responder as perguntas abaixo:

   (a) Você consegue rotacionar o triângulo branco, no sentido horário, para achar outras correspondências? Note que, para isto ser possível, os triângulos devem estar na mesma posição. Anote abaixo quais correspondências você achou?

   $$R120 = \{(,);(,);(,)\}$$

   $$R240 = \{(,);(,);(,)\}$$

   $$R360 = \{(,);(,);(,)\}$$

   (b) Qual é a relação entre $R0$ e $R360$?

   Comentário: Enquanto os alunos foram rotacionavam o triângulo equilátero e comparavam os vértices, foi sendo esclarecida a dúvida sobre a notação do nome do conjunto. Perceberam que se tratava da medida do ângulo de rotação, em graus. Alguns alunos, ainda sem entender este significado, foram ajudados com a resposta da seguinte pergunta:

quanto resulta 180° dividido em 3 partes? Quanto a resposta da pergunta sobre a relação entre $R0$ e $R360$, não apresentaram qualquer dificuldade.

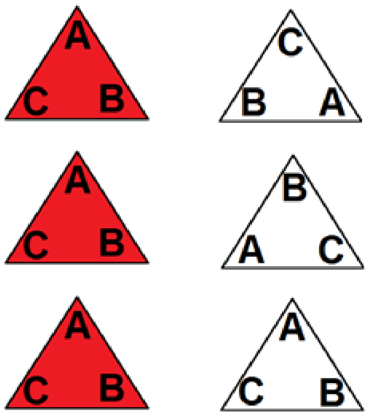

Figura 24: Rotação do triângulo em $120°$**,** $240°$ **e** $360°$

5. Agora separe os triângulos e vamos fazer o mesmo procedimento anterior com os quadrados. Deixe o quadrado hachurado em cima da mesa, de modo que o vértice A esteja a nordeste e segure o quadrado branco na mesma posição sobre o quadrado hachurado. Nesta posição, a correspondência é $R0 = \{(A,A);(B,B);(C,C);(D,D)\}$.

   (a) Rotacione o quadrado no sentido horário e escreva quais as novas correspondências que você encontrou. Dê nome aos conjuntos.

$$= \{(,);(,);(,);(,)\}$$

$$= \{(,);(,);(,);(,)\}$$

$$= \{(,);(,);(,);(,)\}$$

$$= \{(,);(,);(,);(,)\}$$

Comentário: Depois de efetuar as rotações com o triângulo equilátero, os alunos não tiveram qualquer dificuldade para encontrar as correspondências dos vértices da rotação do quadrado. Deram os nomes corretos aos conjuntos, superando a dúvida do símbolo que se refere ao ângulo de rotação, em graus, que dá nome aos conjuntos.

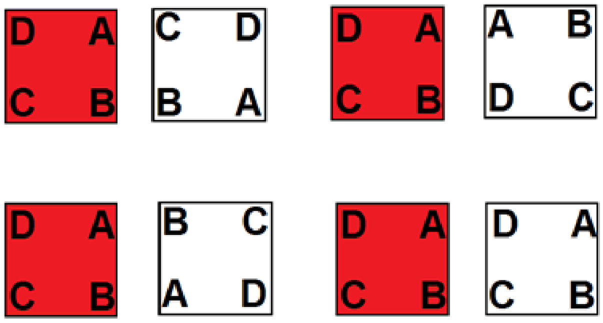

Figura 25: Rotação do quadrado em 90°, 180°, 270° **e** 360°

6. Agora, analise as figuras a seguir:

Disponível em http://www.dw.de/1928-mickey-mouse-aprende-a-falar/a-329435

Disponível em http://www.todofondosde lugaresdelmundo.com /category/ india/page/2

Figura 26: Imagem do Mickey e do castelo Taj Mahal

A primeira figura é do personagem Mickey Mouse, dos estúdios Walt Disney e a segunda figura é o castelo Taj Mahal, uma das sete novas maravilhas do mundo moderno.

(a) Você consegue enxergar um eixo de simetria na primeira figura? Se sim, desenhe este eixo com o auxílio de uma régua.

(b) E na segunda figura, quantos eixos de simetria você enxerga?

Comentário: Localizaram sem dificuldade os eixos de simetria: um eixo vertical na imagem do Mickey e dois eixos na imagem do Taj Mahal: um vertical e outro horizontal. Grande parte do alunos comentou que estas imagens não eram simétricas em relação ao eixos encontrados, pois, na primeira imagem, há uma mancha na ponta da língua do Mickey que não existe do outro lado do eixo de simetria e, na segunda imagem, as árvores do lado esquerdo do eixo vertical são maiores que no lado direito.

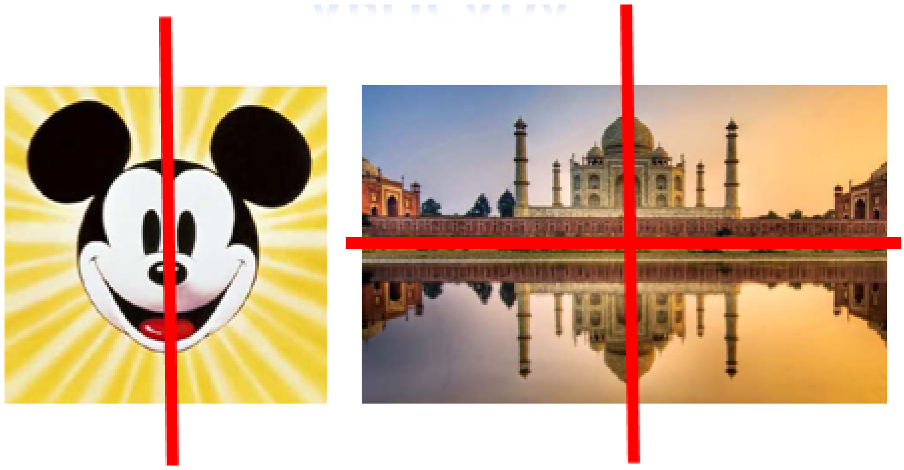

Figura 27: Eixos de simetria

7. Tenha em mãos o triângulo e o quadrado hachurados e responda: quantos eixos de simetria tem cada um? Desenhe cada um dos eixos nestes polígonos hachurados, com o auxílio de uma régua. Nomeie-os, propositalmente, de EA, EB e EC para o triângulo e de EAC, EBD, MAB e MBC. Repare que a letra E significa Eixo e a letra M, Mediatriz.

   Comentário: Enxergar os eixos inclinados não foi tarefa fácil para os alunos. O eixo de simetria vertical do triângulo equilátero e os eixos horizontal e vertical de simetria do quadrado foram encontrados com facilidade. No momento de nomear os eixos do quadrado, a imensa maioria dos alunos teve dificuldade para entender os símbolos MAB e MBC. Mesmo sendo explicado que o significado de M é de mediatriz, eles não entendiam se a mediatriz MAB é perpendicular ou paralela ao lado AB. Para resolver este problema, as notações foram mudadas para EV e EH.

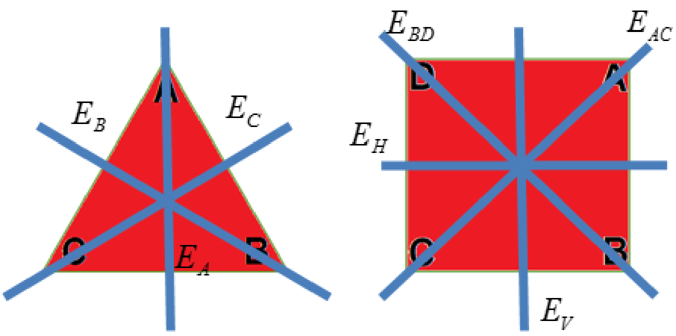

Figura 28: Eixos de simetria do triângulo equilátero e do quadrado

8. Separe os quadrados e deixe, novamente, o triângulo hachurado sobre a mesa e segure o triângulo branco sobre o triangulo hachurado na mesma posição, fazendo a correspondência $R0$. Responda a pergunta:

(a) Você consegue encontrar novas correspondências rotacionando em 180° o triângulo branco em torno de cada eixo? Anote as correspondências que você encontrou:

$$RA = \{(,);(,);(,)\}$$

$$RB = \{(,);(,);(,)\}$$

$$RC = \{(,);(,);(,)\}$$

Comentário: Os alunos apresentaram grande dificuldade neste item. Foram orientados com a resolução de RA. Deste modo, entenderam que o item se tratava de uma reflexão, porém dificilmente enxergavam as reflexões em torno dos eixos inclinados EB e EC.

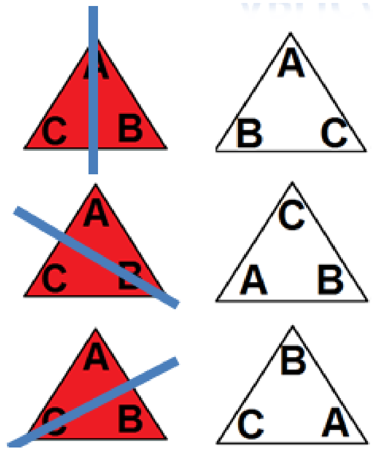

Figura 29: Reflexão dos vértices em torno dos eixos de simetria do triângulo

9. Agora que você viu que existem 3 operações de rotação do triângulo equilátero, no sentido horário, e três operações de reflexão em torno de seus 3 eixos de simetria, tente responder o que se pede:

   (a) Partindo de $R0$, encontre os seguintes conjuntos:

   - RB , fazendo uma rotação e uma reflexão, respectivamente.
   - RB, fazendo uma reflexão e uma rotação, respectivamente.
   - $R240$, fazendo duas reflexões.

Comentário: A esperança era que os alunos conseguissem operar os elementos deste grupo de simetrias. Porém, não conseguiram abstrair o que estava sendo pedido. Deste modo, foram orientados quanto ao primeiro item. Em seguida, com algumas dificuldades, efetuaram os outros itens.

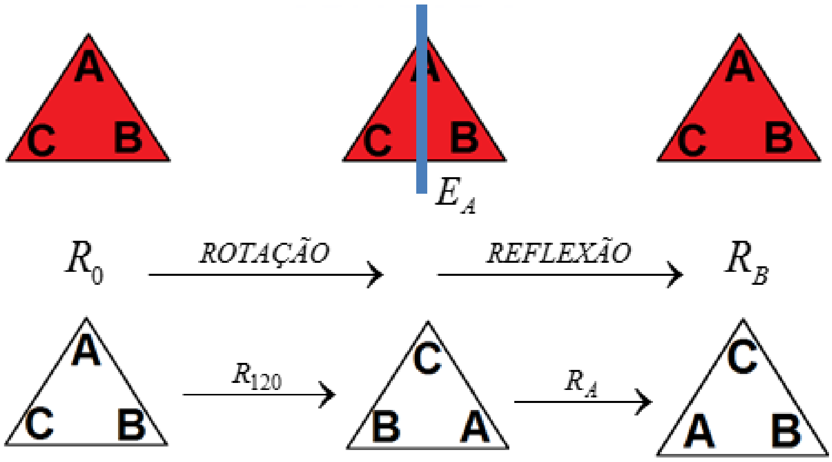

Figura 30: Uma rotação e uma reflexão para encontrar *RB*

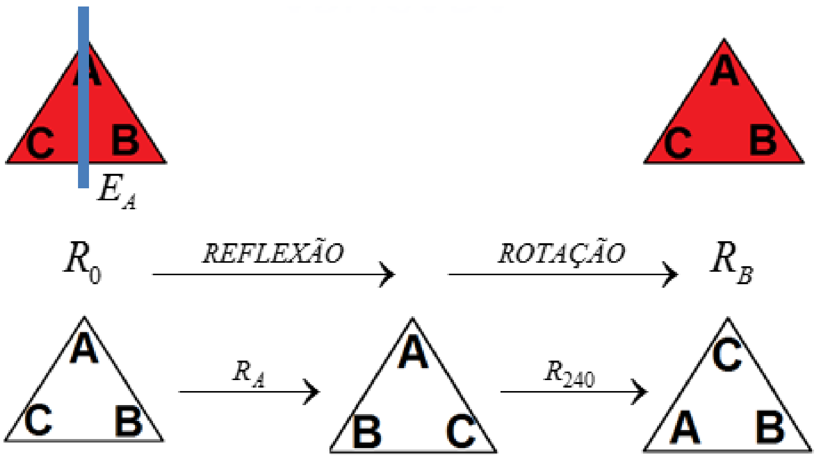

Figura 31: Uma reflexão e uma rotação para encontrar *RB*

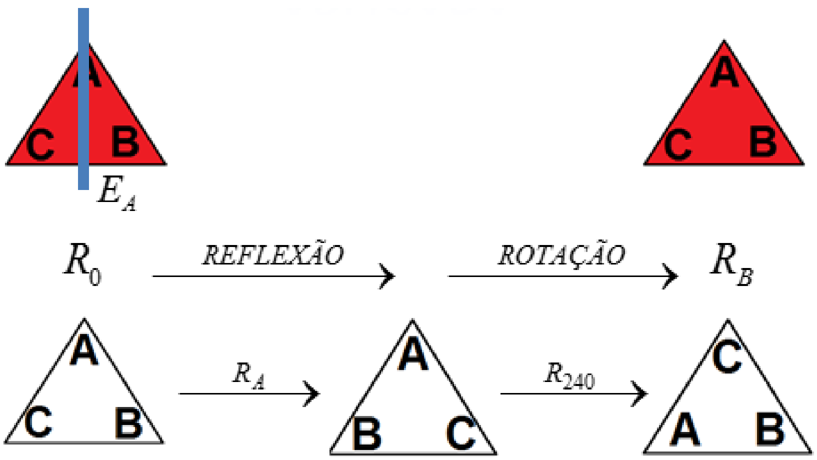

Figura 32: Duas reflexões para encontrar *R*240

8 CONCLUSÃO

Vimos que o teorema da órbita-estabilizador é uma proposição de contagem, que permite determinar o número de elementos de um conjunto, em especial, das simetrias rotacionais dos poliedros regulares e que, apesar de sua simples demonstração, exige conhecimentos intermediários de teoria de grupos, por exemplo, os conceitos de ação, órbitas e estabilizadores. A tabela a seguir apresenta a quantidade de simetrias rotacionais dos poliedros regulares, determinadas por meio da aplicação do teorema da órbita-estabilizador, feita no capítulo 6:

Poliedro Regular	Simetrias Rotacionais
Tetraedro	12
Hexaedro	24
Octaedro	24
Dodecaedro	60
Icosaedro	60

Tabela 2: Simetrias Rotacionais dos Poliedros Regulares

Com relação a atividade prática, esta permitiu concluir que os alunos da última série do ensino fundamental e primeira série do ensino médio são capazes de enxergar e operar as simetrias que, na realidade, se trata da composição das permutações de subconjuntos de S_n. Algumas noções básicas de eixo de simetria são suficientes para o desenvolvimento da criatividade dos alunos, que sugerem uma matemática sem números. A ideia da simetria, de mesclar a álgebra e a geometria, é necessária, em atividades da educação básica, de modo a ser uma das maneiras de incentivar os alunos a enxergar a simetria em todos os lugares a sua volta. Outras estratégias podem ser utilizadas para esse incentivo, como atividades de simetrias de sólidos, desenhos, visita a exposições de arte (como Escher que trabalha com imagens simétricas e imagens propositalmente não simétricas) e o consequente uso do que foi visto para experiências práticas com simetria e para a busca constante de simetrias na natureza.

REFERÊNCIAS

CONRAD, K. Group action. University of Connecticut, p. 7, 2011. Disponível em: <http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/gpaction.pdf>.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. 4. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2003. (Coleção Projeto Euclides).

HUNGERFORD, T. W. **Algebra**. Nova York: Springer-Verlag, 1974.

LIMA, E. L. et al. **A Matemática do Ensino Médio**. 6. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006. (Coleção do Professor de Matemática, v. 2).

MULHOLLAND, J. Symmetry and counting 1 - the orbit-stabilizer theorem. Simon Fraser University, p. 22–1–22–12, 2011. Disponível em: <http://people.math.sfu.ca/ jtmulhol/math302/notes/22-Orbit-Stabilizer.pdf>.

PAIVA, M. R. **Matemática**. 1. ed. [S.l.]: Editora Moderna, 1995.

ROSEN, K. H. **Matemática Discreta e suas Aplicações**. 6. ed. [S.l.]: McGraw - Hill, 2009.