Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Um estudo de simetrias de sólidos regulares

Wellington Ribeiro dos Santos

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática Universitária do Departamento de Matemática como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Alice Kimie Miwa Libardi

2012

512.2 Santos, Wellington Ribeiro dos
S237e Um estudo de simetrias de sólidos regulares/ Wellington Ribeiro dos Santos- Rio Claro: [s.n.], 2012.
75 f. : il., figs.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.
Orientadora: Alice Kimie Miwa Libardi

1. Teoria de Grupos. 2. Simetrias. 3. Sólidos de Platão. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Wellington Ribeiro dos Santos

Um estudo de simetrias de sólidos regulares

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Alice Kimie Miwa Libardi
Orientadora

Prof. Dr. Thiago de Melo
Departamento de Matemática - UNESP/Rio Claro

Profa. Dra. Denise de Mattos
Departamento de Matemática- USP/São Carlos

Rio Claro, 08 de Outubro de 2012

Dedicado a meus pais,
Ana Maria Ribeiro dos Santos e Cicero Alves dos Santos
e padrasto
Geraldo Fernandes Ribeiro (in memorian).

Agradecimentos

Fazer os agradecimentos não é uma tarefa fácil, lembrar de todos que foram importantes, que de alguma forma, direta ou indiretamente fizeram parte deste trabalho. Pois bem, quero agradecer a todas as pessoas que se fizeram presentes, que se preocuparam, que foram solidárias, que torceram por mim. Demonstro neste humilde gesto, minha profunda gratidão a meus amigos, que contribuíram com sua amizade, com palavras de incentivo, e que me proporcionaram fortes momentos de alegria. Em especial agradeço a eles: Camila Pedroso, Carine Pedroso, Gisele Matos, Renan Gutierrez, meus irmãos Eduardo Ribeiro e Tacyane Santos.

No meio acadêmico fiz grandes amigos, durante a graduação e também nas aulas do primeiro ano do mestrado, conhecendo pessoas de diferentes locais, que passaram comigo pelas mesmas dificuldades. Lembro em especial da turma de São José do Rio Preto, que estive junto nas viagens para Rio Claro, nas aulas e nos trabalhos em grupo.

Claro que meus amigos foram importantíssimos para mim, porém meu maior agradecimento é dirigido a meus familiares. Minha mãe Ana Maria R. Santos, meu pai Cícero A. Santos, minhas avós Rosa R. Santos e Marinete , meu padrasto falecido Geraldo F. Ribeiro que foi um pai para mim em todos os momentos, minha madrasta Maria Nishioka que sempre se preocupou em me dar o melhor a partir do momento que me conheceu. Foram eles que estiveram presentes desde meu nascimento até este momento, se preocupando e me ensinando tudo que hoje tenho de melhor, a dignidade, educação e bons valores. Agradeço em especial a minha mãe, pessoa que mostrou o verdadeiro significado da palavra mãe na vida de uma criança, jovem e hoje adulto.

Não poderia deixar de citar aqueles que têm como objetivo indicar melhores caminhos, que são responsáveis pela boa formação de todos, que passaram pela vida dos grandes sábios, e de todos nós, são eles os professores. Agradeço em especial a minha orientadora Alice e todos aqueles que foram meus orientadores durante a graduação, ao Prof. Dr. Thiago de Melo pelo apoio e ajuda com os softwares usados no trabalho e aqueles professores em que me inspirei no Ensino Fundamental e Médio.

Agradeço a todos os pesquisadores, autores, cientistas que colaboraram para o crescimento da ciência e desenvolvimento da humanidade. Não posso deixar de citar uma frase de Isaac Newton: "*Se cheguei até aqui foi porque me apoiei no ombro dos gigantes*".

Resumo

O objetivo deste trabalho é apresentar a teoria elementar de grupos, segundo uma abordagem geométrica. Apresentamos uma introdução aos grupos de simetrias de sólidos regulares e como aplicação apresentamos os sete grupos de frisos.

Palavras-chave: Teoria de Grupos, Simetrias, Sólidos de Platão.

Abstract

In this work we present a geometric approach to the study of elementary group theory. We give an introduction to symmetry groups of regular solids and as an application we present the seven Frieze groups.

Keywords: Theory of Groups, Symmetry, Plato's Solids.

Lista de Figuras

Sumário

1 Introdução

O ensino de Estruturas Algébricas nos cursos de graduação em Matemática em geral encontra dificuldades devido seu caráter abstrato e formal ao qual o aluno iniciante não está ainda acostumado.

Tem-se mostrado motivador e despertado interesse nos alunos, quando o estudo além da parte teórica é feito através de exemplos geométricos.

Esta dissertação tem por objetivo apresentar uma abordagem da teoria elementar de grupos, com exemplos baseados em simetrias dos sólidos de Platão. Pretende-se posteriormente transformar esta dissertação em notas de aulas.

A dissertação foi baseada no livro: Groups and Symmetry de M. A. Armstrong, incluindo algumas figuras do referido texto.

Esta dissertação está desenvolvida da seguinte maneira: no capítulo 2 apresentaremos algumas noções básicas ao desenvolvimento do trabalho. No capítulo 3 alguns resultados sobre simetrias e isometrias. No capítulo 4, apresentaremos a teoria de grupos com vários exemplos geométricos. Finalmente, no capítulo 5 apresentaremos os sete grupos de frisos como aplicações.

2 Preliminares

Neste capítulo introduziremos algumas noções básicas concernentes às estruturas algébricas que serão utilizadas no desenvolvimento da dissertação. Para os resultados aos quais não apresentarmos demonstrações, serão indicadas referências onde poderão ser encontradas.

2.0.1 Relações de Equivalência

Definição 2.1. *Seja X um conjunto e seja R um subconjunto do produto cartesiano $X \times X$. Em outras palavras, R é uma coleção de pares ordenados (x, y) cujas coordenadas são elementos de X. Dados dois pontos x e y de X, dizemos que x se relaciona com y, denotando por $x \sim y$ se o par ordenado (x, y) pertence a R.*

Se as propriedades

1. $\forall\ x \in X,\ x \sim x$;
2. $\forall\ x, y \in X, x \sim y \Longrightarrow y \sim x$;
3. $\forall\ x, y, z \in X,\ x \sim y\ \ e\ \ y \sim z \Longrightarrow x \sim z$.

são válidas, então chamaremos R ou $\sim$ uma ***relação de equivalência*** *em X. Para cada x pertencente a X, a coleção de todos os pontos que são relacionados com x é escrita $\bar{x}$ e é chamada de* ***classe de equivalência*** *de x. O conjunto de todas as classes de equivalência é chamado* ***conjunto quociente*** *e denotado por X/R.*

Definição 2.2. *Uma* ***partição*** *de um conjunto X é uma família $\{U_\alpha\}_{\alpha \in L}$ de subconjuntos não vazios de X, disjuntos e cuja reunião é o conjunto X.*

Proposição 2.1. *Seja $\{U_\alpha\}_{\alpha \in L}$ uma partição de X, e sejam x, y pontos de X. Temos que x está relacionado com y e denotaremos por $x \sim y$, se existe $\alpha \in L$ tal que x e y pertencem a U_α. Esta relação é de equivalência e, reciprocamente, as classes de equivalência distintas de uma relação de equivalência em X formam uma partição de X.*

Prova: Mostremos primeiramente que a relação acima é de equivalência.

a) Para todo $x \in X$, tem-se que $x \in U_\alpha$, para algum α, logo $x \sim x$.

b) Se $x \sim y$ então existe $\alpha \in L$ tal que x e y pertencem a U_α e portanto $y \sim x$.

c) Se $x \sim y$ e $y \sim z$ então existe U_α que contém x e y e existe U_β que contém y e z. Como $y \in U_\alpha \cap U_\beta$, segue da definição de partição que $U_\alpha = U_\beta$, donde se conclui que $x \sim z$.

Reciprocamente, temos que: cada classe de equivalência é não vazia, pois $\bar{x}$ sempre contém x pela propriedade a). Se $\bar{x} \cap \bar{y} \neq \emptyset$, então existe pelo menos um ponto z pertencente a esta intersecção. Logo z está relacionado com x e y. Pela propriedade b), x está relacionado com z, e portanto também está relacionado com y, pela propriedade c). Concluímos que $\bar{x} = \bar{y}$. Assim duas classes de equivalência tem intersecção vazia ou são coincidentes. Finalmente, como cada ponto x de X está em sua própria classe de equivalência $\bar{x}$, então $\{x\} \subset \bar{x} \subset X$. Logo

$$\bigcup_{x \in X} \{x\} \subset \bigcup_{x \in X} \bar{x} = X$$

o que implica que $X = \bigcup_{x \in X} \bar{x}$. $\square$

Apresentaremos a seguir alguns exemplos que ilustram a definição acima.

Exemplo 2.1. O conjunto dos inteiros módulo n, $n > 0$. Considere em $\mathbb{Z}$ a seguinte relação: a e b em $\mathbb{Z}$ são congruentes módulo n, denotada por $a \equiv b(mod\ n)$, se, e somente se, existe um inteiro k tal que $a - b = kn$. Esta relação é de equivalência e a classe de equivalência de $a \in \mathbb{Z}$ será denotada por $\bar{a} := \{x \in \mathbb{Z}, x \equiv a(mod\ n)\} = \{x \in \mathbb{Z}, x = a + kn\}$, para algum inteiro k. O conjunto quociente é denotado por $\mathbb{Z}_n$.

Exemplo 2.2. Seja $X = \{(x, y) \in \mathbb{R}^2, 0 \leq x, y \leq 1\} \subset \mathbb{R}^2$.

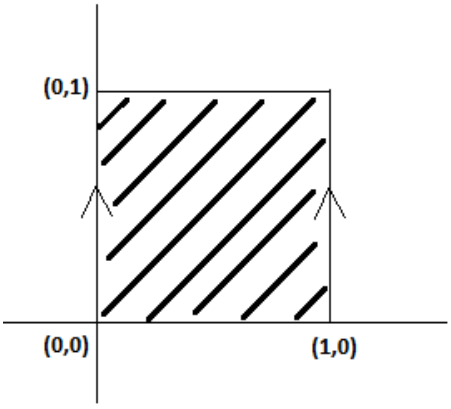


Figura 2.1: Conjunto $X = \{(x, y), 0 \leq x, y \leq 1\}$

Definimos as seguintes relações:

1 $(x, y) \sim (x', y') \iff (x, y) = (x', y')$ ou $\{x, x'\} = \{0, 1\}$ e $y = y'$.

2 $(x,y) \sim (x',y') \Longleftrightarrow (x,y) = (x',y')$ ou $\{x,x'\} = \{0,1\}$ e $y = 1 - y'$.

3 $(x,y) \sim (x',y') \Longleftrightarrow (x,y) = (x',y')$ ou $\{x,x'\} = \{0,1\}$ e $y = y'$ ou $\{y,y'\} = \{0,1\}$ e $x = x'$.

4 $(x,y) \sim (x',y') \Longleftrightarrow (x,y) = (x',y')$ ou $\{x,x'\} = \{0,1\}$ e $y = y'$ ou $\{y,y'\} = \{0,1\}$ e $x' = 1 - x$.

Vamos fazer a prova de que a primeira relação definida (item 1) é de equivalência.
Recordando a relação: $(x,y) \sim (x',y') \Longleftrightarrow (x,y) = (x',y')$ ou $\{x,x'\} = \{0,1\}$ e $y = y'$

Temos que:
i) $\forall\ (x,y) \in X, (x,y) = (x,y) \Rightarrow (x,y) \sim (x,y)$;

ii) *Se* $(x,y) \sim (x',y') \Rightarrow (x,y) = (x',y')$ ou $x = 0$ *e* $x' = 1$ e $y = y'$ ou $x = 1$ e $x' = 0$ e $y = y' \Rightarrow (x',y') \sim (x,y)$.

iii) Se tivermos $(x,y) \sim (x',y')$ e $(x',y') \sim (x'',y'')$, então:

$(x,y) = (x',y')$ ou $\{x,x'\} = \{0,1\}$ *e* $y = y'$.

também

$(x',y') = (x'',y'')$ ou $\{x',x''\} = \{0,1\}$ e $y' = y''$

Isto implica que $(x,y) = (x'',y'')$ ou $(x,y) = (x',y')$ e $\{x',x''\} = \{0,1\}$ e $y' = y''$

Logo $\{x,x''\} = \{0,1\}$ e $y = y''$

ou ainda, $\{x,x'\} = \{0,1\}$ e $y = y'$ com $\{x',x''\} = \{0,1\}$ e $y' = y''$

Assim $\{x,x''\} = \{0,1\}$ e $y = y''$.

No caso $\{x,x'\} = \{0,1\}$ e $(x',y') = (x'',y'')$, tem-se $\{x,x''\} = \{0,1\}$ e $y = y''$.
Portanto $(x,y) \sim (x'',y'')$.

Geometricamente o conjunto quociente é o cilindro, figura 2.2.
Os demais itens também constituem relações de equivalências e os respectivos conjuntos quocientes são geometricamente: a Faixa de Moëbius, o Toro e a Garrafa de Klein.

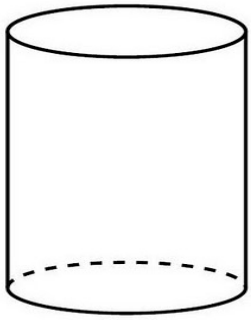


Figura 2.2: Cilindro

Definição 2.3. *Dado um conjunto não vazio G, uma operação em G é uma aplicação $\varphi : G \times G \longrightarrow G$, que associa a cada par de elementos de G um único elemento de G.*

Definição 2.4. *Um grupo é um conjunto G munido de uma operação $*$ satisfazendo os seguintes axiomas:*

1. *Para todos $x, y, z \in G$, tem-se $(x * y) * z = x * (y * z)$; i.e. vale a propriedade associativa;*

2. *existe um elemento e em G, chamado elemento neutro tal que, para todo $x \in G$, $x * e = x = e * x$.*

3. *para cada elemento x em G, existe o elemento $-x$ em G, chamado elemento oposto satisfazendo: $x * -x = e = -x * x$.*

   Se além disso tivermos:

4. *para todos $x, y \in G, x * y = y * x$, então dizemos que o grupo é comutativo ou abeliano.*

Observe que na notação multiplicativa o elemento que satisfaz o axioma 2. é chamado elemento identidade ou unidade e o que satisfaz o axioma 3. é chamado elemento inverso.

Definição 2.5. *Um anel é um conjunto A munido de duas operações: adição $(+)$ e multiplicação $(\cdot)$ tal que com a operação adição é um grupo abeliano e com a operação multiplicação satisfaz os seguintes axiomas:*

- *Para todos $x, y, z \in A$, tem-se $(x \cdot y) \cdot z = x \cdot (y \cdot z)$; i.e. vale a propriedade associativa.*

- *Para todos $x, y, z \in A$, tem-se $x \cdot (y + z) = x \cdot y + x \cdot z$ e $(x + y) \cdot z = x \cdot z + y \cdot z$, i.e. vale a propriedade distributiva.*

  Se além disso tivermos:

- *Para todos* $x, y \in A, x \cdot y = y \cdot x$ *, então dizemos que o anel é comutativo.*
- *Se existe um elemento* 1 *em* A*, chamado elemento identidade tal que, para todo* $x \in A$*,* $x \cdot 1 = x = 1 \cdot x$*, dizemos que o anel possui identidade.*

Definição 2.6. *Um corpo é um conjunto* $(K, +, \cdot)$ *que é um anel comutativo com identidade tal que todo elemento* $x \in K$*, não nulo, possui inverso, i.e. para cada elemento* x *em* K*,* $x \neq 0$*, existe o elemento* x^{-1} *em* K*, satisfazendo:* $x \cdot x^{-1} = 1 = x^{-1} \cdot x$*.*

Definição 2.7. *Um conjunto* V *é um espaço vetorial real se* V *é munido de duas operações, onde a primeira* $+ : V \times V \longrightarrow V$ *definida por* $(u, v) \longrightarrow u + v$ *é tal que* $(V, +)$ *é um grupo abeliano e a segunda operação* $\cdot : \mathbf{R} \times V \longrightarrow V$*, definida por* $(\lambda, v) \longrightarrow \lambda \cdot v$ *satisfaz os seguintes axiomas:*

1. $\forall\ \lambda \in \mathbb{R}\ e\ \forall\ u, v \in V,\ \lambda(u + v) = \lambda \cdot u + \lambda \cdot v$;
2. $\forall\ \lambda, \xi \in \mathbb{R}\ e\ \forall\ u \in V,\ (\lambda + \xi) \cdot u = \lambda \cdot u + \xi \cdot u$;
3. $\forall\ \lambda, \xi \in \mathbb{R}, \lambda(\xi \cdot u) = (\lambda\xi) \cdot u$;
4. $1 \cdot u = u, \forall\ u \in V$.

Observe que $\mathbb{R}^n = \{(x_1, x_1, \cdots, x_n); x_i \in \mathbb{R},\ i = 1, 2, \cdots, n\}$ é um espaço vetorial real, onde a adição é definida somando-se coordenada a coordenada e a multiplicação por um escalar é definida multiplicando-se cada coordenada pelo escalar.

Definição 2.8. *Uma aplicação sobrejetora* $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ *é uma isometria se preserva distância, i.e.* $\forall\ x, y \in \mathbb{R}^n, \|f(x) - f(y)\| = \|x - y\|$*.*

Observemos que toda isometria é uma aplicação injetora, pois $\forall x, y, \in \mathbb{R}^n, f(x) = f(y)$, tem-se que $\parallel f(x) - f(y) \parallel = 0$. Como $\parallel f(x) - f(y) \parallel = \parallel x - y \parallel$, então $\parallel x - y \parallel = 0$, que implica que $x = y$.

3 Simetrias e Isometrias

3.1 Simetrias

O objetivo deste capítulo é estudar as simetrias dos poliedros, como motivação para o estudo da teoria de grupos.

A ideia de simetria é bastante intuitiva. No plano, a ideia básica é bastante clara: uma figura no plano é simétrica se podemos dividi-la em partes de tal modo que estas partes coincidem perfeitamente, quando sobrepostas.

Há diversos tipos de simetrias, por exemplo, as simetrias axiais ou em relação a retas são aquelas onde pontos, objetos ou partes de objetos são a imagem espelhada um do outro em relação à reta dada, chamada eixo de simetria. O eixo de simetria ou reta de simetria é a mediatriz do segmento que une os pontos correspondentes. As simetrias rotacionais são aquelas obtidas por rotações em torno de um eixo de um dado ângulo.

Definição 3.1. *Um poliedro convexo é regular quando suas faces são polígonos regulares e congruentes entre si e o número de faces concorrentes em cada vértices é sempre o mesmo.*

Euclides no livro XIII de "Os Elementos", mostrou que existem pelo menos cinco deles: o **tetraedro** (quatro faces triangulares), o **cubo** (seis faces quadradas), **octaedro** (oito faces triangulares), **dodecaedro** (doze faces pentagonais) e **icosaedro** (vinte faces triangulares). O sufixo edro vem da palavra grega hédra que significa face. Os prefixos, também oriundos do grego, indicam a quantidade de faces de cada poliedro: tetra (4), hexa (6), octa (8), dodeca (12) e icosa (20).

Os nomes dos sólidos platônicos são devidos à Platão que associou a cada um dos elementos clássicos (terra, ar, água e fogo) um poliedro regular. Terra é associada com o cubo, ar com o octaedro, água com o icosaedro e fogo com o tetraedro. O quinto elemento, éter, foi introduzido por Aristóteles que postulou que os céus eram feitos deste elemento, mas não foi associado ao quinto sólido de Platão.

Euclides deu uma descrição matemática completa dos sólidos de Platão no último livro (Livro XIII) de "Os Elementos". As proposições 13 a 17 do Livro XIII descrevem as construções do tetraedro, octaedro, cubo, icosaedro e dodecaedro, nesta ordem.

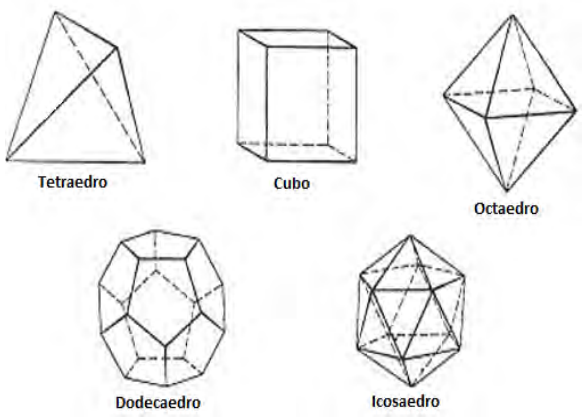


Figura 3.1: Os cinco sólidos de Platão

Para cada sólido, Euclides calculou a razão entre o diâmetro da esfera circunscrita e o comprimento da aresta do sólido. Na proposição 18, ele demonstrou que não existem outros poliedros regulares.

3.1.1 Simetrias Rotacionais

Consideremos agora as simetrias rotacionais de um tetraedro regular T. Sejam L e M dois eixos no tetraedro, um que passa por um vértice e o centro da face oposta e o outro que passa pelos pontos médios de duas arestas opostas, respectivamente. Observemos que é possível traçar quatro eixos do tipo L e cada um dá origem a duas rotações, uma de $2\pi/3$ e a outra de $4\pi/3$, cujo sentido é mostrado na figura 3.2. É claro que rotações de $2\pi/3$ (ou $4\pi/3$) no sentido oposto possuem o mesmo efeito em T que as rotações $4\pi/3$ (ou $2\pi/3$) respectivamente. No eixo M podemos fazer uma rotação por π, e existem 3 eixos deste mesmo tipo. Com isso, podemos ver que temos juntamente com a identidade (que fixa T e é equivalente a uma rotação completa por 2π) um total de 12 rotações.

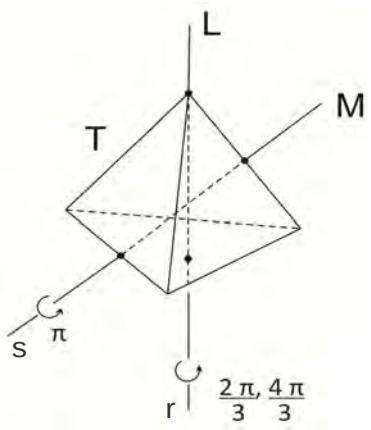


Figura 3.2: Tetraedro

Uma placa plana hexagonal com lados iguais também possui 12 rotações simétricas (figura 3.3), assim como uma pirâmide regular tendo o dodecaedro como base (figura 3.4).

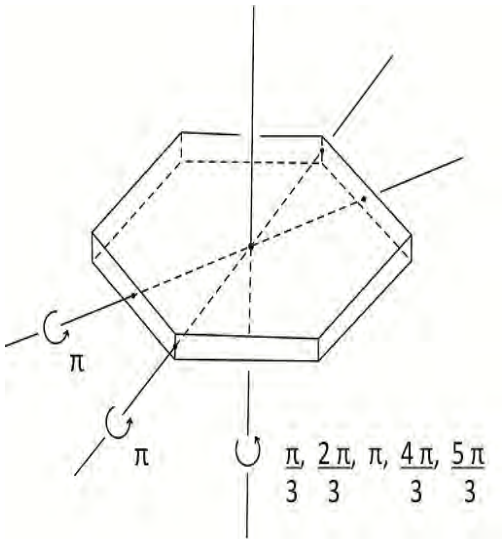


Figura 3.3: Placa plana hexagonal

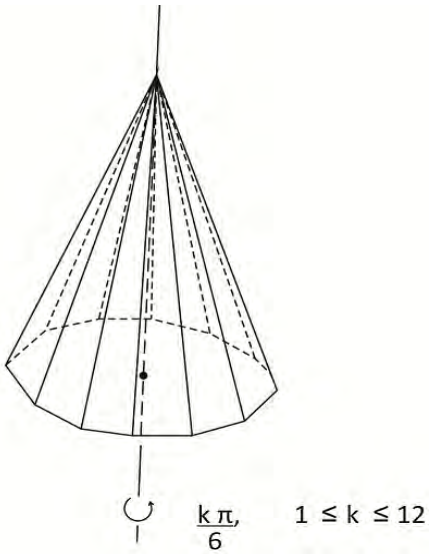


Figura 3.4: Pirâmide

Na placa, temos cinco rotações (de $\pi/3$, $2\pi/3$, π, $4\pi/3$ e $5\pi/3$) através do eixo perpendicular que passa pelo seu centro de gravidade. Temos três eixos de simetrias determinados por um par de vértices opostos, três que são determinados pelos pares de pontos médios de dois lados opostos, e podemos fazer uma rotação de π sobre cada um desses eixos. Não esquecendo a identidade, o total é doze novamente.

A pirâmide de base dodecágono regular possui apenas um eixo de simetria, que liga o vértice da pirâmide com o centro da base, e existem doze rotações distintas (de

$k\pi/6$, $1 \leq k \leq 12$). Apesar do fato de termos contado doze rotações em cada caso, o tetraedro, a placa e a pirâmide não possuem as mesmas simetrias. A principal diferença é que a pirâmide possui apenas um eixo de simetria. Uma rotação de $\pi/6$ sobre este eixo, deve ser repetida doze vezes antes da pirâmide voltar a posição inicial. Contudo, nenhuma rotação da placa se repetida nos dará todas as outras rotações. Podemos encontrar outras diferenças, todas com relação a forma de combinar as simetrias. Por exemplo, as simetrias da pirâmide comutam-se uma com as outras. Isto é, se escolhermos quaisquer duas rotações da pirâmide e as realizarmos seguidamente, o efeito na pirâmide será o mesmo independente de qual seja escolhida para ser a primeira. No tetraedro ou na placa isto não acontece. Vejamos para o tetraedro. Nomeie os vértices do tetraedro T como na (figura 3.5), que nos permite ver o efeito de cada simetria. Escolha a rotação r ($2\pi/3$ sobre o eixo L no sentido indicado) e s (π sobre o eixo M). Primeiramente faça r e depois s, deixando o vértice 2 na posição inicial e que seria da mesma forma se fosse feita a rotação sobre o eixo N. Mas, se começarmos com s e depois r, movemos o vértice 2 para o lugar ocupado pelo vértice 4 originalmente, e assim fica claro que não se trata da mesma rotação. Uma observação importante é a de que não devemos aplicar uma rotação enquanto a outra estiver sendo aplicada. Ambas r e s devem ser pensadas como movimentos rígidos do espaço, cada qual tem um eixo que é fixo no espaço, e cada um gira sobre si mesmo em T.

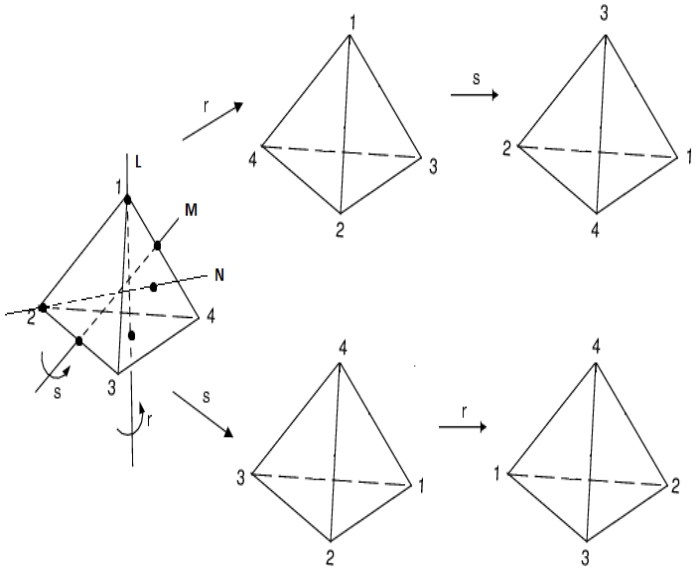


Figura 3.5: Algumas simetrias no Tetraedro

Existe somente uma rotação na pirâmide que, quando combinada com si própria, nos dá a identidade, a única rotação através de π. A placa possui sete tais simetrias e o tetraedro três. Estas três rotações através de π do tetraedro comutam uma com as outras, mas apenas uma das sete rotações da placa (a rotação por π no eixo perpendicular à placa) comuta com as restantes. Para obter uma contagem correta das simetrias, simplesmente contar as simetrias não é suficiente. Devemos levar em

consideração o modo como elas se combinam com as demais. É o chamado **grupo de simetrias** que nos dá essas informações.

Consideremos o conjunto das simetrias rotacionais do tetraedro T. Dadas duas rotações u e v, podemos combiná-las fazendo primeiramente v e depois u, produzindo uma nova rotação que também leva T em si mesmo, e que vamos escrever uv, da mesma forma que na composição de funções. A rotação identidade, que denotaremos por e, se comporta de uma maneira especial. Aplicando primeiramente e e depois a rotação u, ou primeiramente u e depois e, o resultado será sempre o mesmo, nada mais que a rotação u apenas. Em outras palavras $ue = u = eu$ para toda simetria u de T. Cada rotação u possui uma rotação inversa u^{-1}, que também é uma simetria em T e satisfaz $u^{-1}u = e = uu^{-1}$. Para obter u^{-1}, basta girar o mesmo eixo , com o mesmo ângulo de u, porém em sentido contrário. No caso da rotação r descrita acima, a inversa da rotação r é rr, pois aplicando r três vezes temos a identidade. Finalmente, se tomarmos três de nossas rotações u, v e w teremos que $(uv)w = u(vw)$.

As doze simetrias do tetraedro juntamente com esta estrutura algébrica formam o seu **grupo de simetria rotacional.**

Um cubo tem vinte e quatro simetrias rotacionais. Elas podem ser contadas da mesma forma que no tetraedro, encontrando todos os eixos de simetrias juntamente com o número de rotações distintas sobre cada eixo. Os diferentes tipos de eixos são representados por L, M e N na figura 3.6. Existem três eixos do tipo L que juntos fornecem um total de nove rotações, seis eixos do tipo M com apenas uma rotação cada, e quatro diagonais principais como N na qual o cubo pode ser rotacionado por $2\pi/3$ e $4\pi/3$. Estas são responsáveis por 24 simetrias.

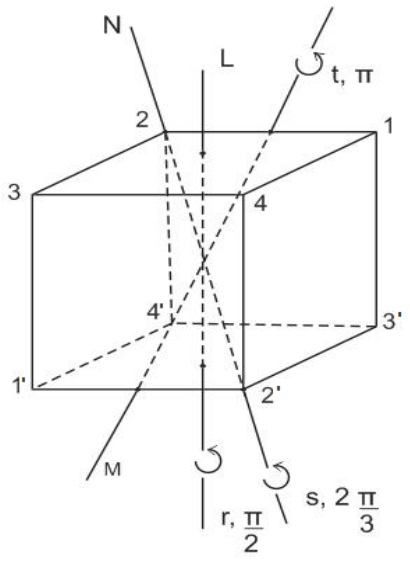


Figura 3.6: Rotações do Cubo

Ligando o centro de cada par de faces adjacentes de um cubo podemos construir um **octaedro** inscrito no cubo (figura 3.7).

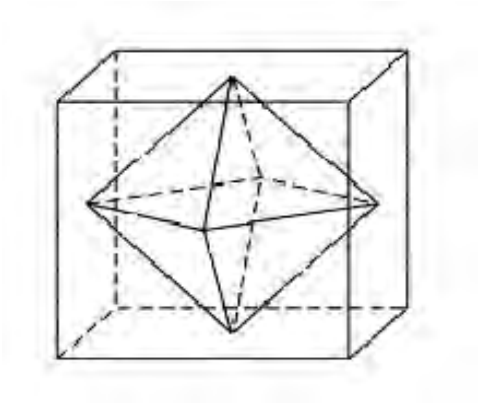


Figura 3.7: Octaedro Inscrito no Cubo

Usando o mesmo procedimento podemos obter um cubo inscrito no octaedro. Quando este fato ocorre, dizemos que os sólidos são duais, ou seja, o cubo e o octaedro são sólidos duais. Eles claramente possuem a mesma quantidade de simetrias. Qualquer simetria do cubo é uma simetria do octaedro dual inscrito, e vice-versa. Em linguagem algébrica, dizemos que o grupo das rotações do cubo e do octaedro são isomorfos. Existem mais dois sólidos regulares, o dodecaedro e o icosaedro e, eles são duais um ao outro.

3.2 Isometrias

Nesta seção faremos uma breve apresentação dos grupos de isometrias.

Primeiramente, vamos considerar as isometrias no plano e no espaço. No caso do plano consideramos ou $\mathbb{R}^2$ ou $\mathbb{C}$, dependendo da conveniência. Há 4 tipos de isometrias : reflexão em torno de uma reta, translação, rotação e reflexão deslizante.

Definição 3.2. *Uma translação no espaço é uma transformação $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ definida por $T(x, y, z) = (x + a, y + b, z + c)$, onde $(a, b, c) \in \mathbb{R}^3$ é fixado. Uma translação no plano é definida da mesma forma, com apenas duas coordenadas. Dada uma reta r, definimos uma reflexão em torno de r como sendo a transformação σ_r definida por $\sigma_r(P) = P$, $P \in r$ e $\sigma_r(P) = Q$, se $P \notin r$ e r é a perpendicular no ponto médio de $\overline{PQ}$. Dado um plano $\pi :< x, \eta >= d$, onde η é o vetor normal ao plano π, com $\mid \eta \mid = 1$, definimos uma reflexão em relação a π, como sendo a aplicação $R : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ tal que $\forall x \in \mathbb{R}^3$, $R(x) = x + 2t\eta$, onde t é escolhido de tal forma que $x + t\eta \in \pi$. Uma rotação no $\mathbb{R}^3$ é a composta de reflexões em relação a dois planos não paralelos. A reta interseção dos dois planos é o eixo da rotação. E finalmente, uma reflexão deslizante que é uma reflexão em torno de uma reta r, seguida de uma translação por um número não nulo ao longo de r.*

Considerando as isometrias em $\mathbb{C}$ temos a seguinte classificação: isometrias diretas $z \to az + b$ ou isometrias indiretas $z \to a\bar{z} + b$, onde em cada caso $\mid a \mid = 1$.

O próximo resultado mostra que toda isometria é uma destes tipos.

Teorema 3.1. *Seja $f : \mathbb{C} \to \mathbb{C}$ que leva z em $f(z) = az + b$ com $a, b \in \mathbb{C}$.*

i) Suponha que $f(z) = az + b$, onde $\mid a \mid = 1$. Se $a = 1$, então f é uma translação; se $a \neq 1$, então f é uma rotação.

ii) Suponha que $f(z) = a\overline{z} + b$, onde $\mid a \mid = 1$. Se $a\overline{b} + b = 0$, então f é uma reflexão em torno de uma reta; se $a\overline{b} + b \neq 0$, então f é uma reflexão deslizante. Em particular, qualquer isometria é de uma das quatro listadas acima.

Prova: (i) Assuma que $f(z) = az + b$. Se $a = 1$, então f é uma translação. Se $a \neq 1$, então $f(w) = w$, onde $w = b/(1 - a)$ e $f(z) - w = az + b - aw - b = a(z - w)$. Então f é uma rotação sobre w de ângulo θ, onde $a = e^{i\theta}$. Assuma que $f(z) = a\overline{z} + b$, onde $a = e^{i\theta}$.

(ii) Assuma que $f(z) = a\overline{z}+b$ onde $\mid a \mid = 1$, e que $f = t \circ r$, onde r é uma reflexão em relação a uma reta s, t é uma translação ao longo de s e onde r e t comutam. Assumindo que isto é verdadeiro, temos então que $f^2 = f \circ f = (t \circ r) \circ (t \circ r) = t \circ t \circ r \circ r = t^2$ o que nos indica como podemos encontrar t e r, pois $r = t^{-1} \circ f$. Como $f^2(z) = z + a\overline{b} + b$, definimos as aplicações t e r por $t(z) = z+1/2(a\overline{b}+b)$, $r(z) = t^{-1}f(z) = a\overline{z}+1/2(a\overline{b}+b)$. É claro que t é uma translação e como

$$1/2(a\overline{b} + b) = 1/2e^{i\theta}/2(e^{i\theta}/2\overline{b} + e^{-i\theta}/2b),$$

vemos que a translação está na direção $e^{i\theta}/2$. Agora, um cálculo mostra que $r^2(z) = z$ e que $r(z) = z$, sempre que $z = 1/2b + \rho e^{i\theta}/2$, onde ρ é qualquer número real. Como r não é a identidade, vemos que r é a reflexão em relação à reta $s = \{1/2b+\rho e^{i\theta}/2; \rho \in \mathbb{R}\}$ e t é uma translação de $1/2(a\overline{b} + b)$ na direção de s. Segue que f é uma reflexão se $a\overline{b}+b = 0$ e uma reflexão deslizante se $a\overline{b}+b \neq 0$. Finalmente, como qualquer isometria é da forma $f(z) = az + b$ ou $f(z) = a\overline{z} + b$, com $\mid a \mid = 1$, então segue que qualquer isometria é uma das quatro listadas.□

Corolário 3.1. *Cada isometria f é uma aplicação invertível de $\mathbb{C}$ em $\mathbb{C}$, cuja inversa é também uma isometria.*

Prova Se $f(z) = az + b$, então $f^{-1}(z) = \overline{a}z + \overline{b}$, enquanto que se $f(z) = a\overline{z} + b$, então $f^{-1}(z) = a\overline{z} + a\overline{b}$. Em cada caso, f^{-1} é de uma das formas indicadas e assim é uma isometria. □

Vamos agora considerar as isometrias no espaço euclidiano. Cada reflexão em relação a um plano é uma isometria e veremos depois que toda isometria é uma composição de reflexões. Dado um plano $\pi :< x, \eta >= d$, onde η é o vetor normal ao plano π, com $\mid \eta \mid = 1$, consideremos a aplicação $R : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ tal que $\forall x \in \mathbb{R}^3$, $R(x) = x + 2t\eta$, onde t é escolhido de tal forma que $x + t\eta \in \pi$, que é uma reflexão em relação a π.

Observe que se $x+t\eta \in \pi$, então $< x+t\eta, \eta >=< x, \eta > +t < \eta, \eta >= d$, o que implica $t = d- < x, \eta >$, portanto

$$R(x) = x + 2t\eta = x + (d- < x, \eta >)\eta = x + 2d\eta - 2 < x, \eta > \eta$$

Tem-se então que R é uma isometria, $R(R(x)) = x$ e $R(x) = x$, se $x \in \pi$.

Considerando-se dois planos paralelos $\pi_1 =< x, \eta >= d_1$ e $\pi_2 =< x, \eta >= d_2$, sejam R_1 e R_2 reflexões em relação a estes planos, respectivamente. Então $R_1(R_2(x)) = R_1(x + 2d_1- < x, \eta >)\eta) = x + 2(d_1 - d_2)\eta$ o que implica que é uma translação.

Se considerarmos dois planos π_1 e π_2 que se interceptam em uma reta r e as reflexões R_1 e R_2 respectivas em relação aos planos, então cada reflexão fixa todos os elementos de r e para qualquer plano π ortogonal a r, tem-se que R_2R_1 é a reflexão em torno da reta $\pi \cap \pi_1$ seguida da reflexão em torno da reta $\pi \cap \pi_2$, então R_2R_1 é uma rotação de $\mathbb{R}^3$ em torno da reta r de uma ângulo igual a duas vezes o ângulo entre os planos π_1 e π_2.

Proposição 3.1. *A isometria $f : \mathbb{R}^3 \to \mathbb{R}^3$ mais geral é da forma $f(x) = A(x) + f(0)$, onde $A : \mathbb{R}^3 \to \mathbb{R}^3$ é uma aplicação linear.*

Prova: Suponha que f é uma isometria. Então $A(x) = f(x)-f(0)$ é uma isometria, pois $\forall x, y, \|A(x) - A(y)\| = \|f(x) - f(0) - f(y) + f(0)\| = \|f(x) - f(y)\| = \|x - y\|$ e além disso, $A(0) = f(0) - f(0) = 0$, ou seja, fixa 0. Então A é a composta de reflexões no espaço passando por 0. Como cada tal reflexão é uma aplicação linear, então A também o é. □

4 Um estudo de Grupos através de exemplos geométricos

Vamos recordar a definição de grupos que foi apresentada nas preliminares, devido ao fato de que no capítulo 3, muitas vezes nos referimos a eles na apresentação de exemplos.

Definição 4.1. *Um grupo é um conjunto G munido de uma operação $*$ satisfazendo os seguintes axiomas:*

1. *Para todos $x, y, z \in G$, tem-se $(x * y) * z = x * (y * z)$; i.é. vale a propriedade associativa;*

2. *existe um elemento e em G, chamado elemento neutro tal que, para todo $x \in G$, $x * e = x = e * x$;*

3. *para cada elemento x em G, existe o elemento $-x$ em G, chamado elemento oposto , satisfazendo: $x * -x = e = -x * x$;*

   Se além disso tivermos:

4. *para todos $x, y \in G, x * y = y * x$, então dizemos que o grupo é comutativo ou abeliano.*

A ordem de um grupo finito é o número de elementos do grupo. Um grupo que possui infinitos elementos é dito ter ordem infinita.

Escreveremos $|G|$ para denotar a ordem do grupo G.

Um grupo que será bastante utilizado no texto é o grupo $\mathbb{Z}_n$ dos inteiros módulo n. Ele é definido como segue:

Considere em $\mathbb{Z}$ a seguinte relação: a e b em $\mathbb{Z}$ são congruentes módulo n, denotada por $a \equiv b(mod\ n)$, se, e somente se, existe um inteiro k tal que $a - b = kn$. Esta relação é de equivalência e a classe de equivalência de $a \in \mathbb{Z}$ será denotada por $\bar{a} := \{x \in \mathbb{Z}, x \equiv a(mod\ n)\} = \{x \in \mathbb{Z}, x = a + kn, \text{para algum inteiro k}\}$. O conjunto quociente é denotado por $\mathbb{Z}_n$

Definamos em $\mathbb{Z}_n$, uma operação denotada $+_n$ por:

$\forall \bar{a}, \bar{b} \in \mathbb{Z}_n, \bar{a} +_n \bar{b} = \overline{a+b}$. Esta operação está bem definida, pois se $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$, então existem k_1 e k_2 inteiros tais que:

$a - a' = k_1 \cdot n$ e $b - b' = k_2 \cdot n$. Logo $(a+b) - (a'+b') = (k_1 + k_2) \cdot n$, o que implica que $\overline{a+b} = \overline{a'+b'}$.

Então $\mathbb{Z}_n$, com esta operação $+_n$ é um grupo abeliano, sendo $\bar{0}$ o elemento neutro.

Definição 4.2. *Um subgrupo de um grupo G é um subconjunto H de G, que juntamente com a operação $*$ de G é um grupo, ou seja:*

1. *o elemento neutro e de G pertence a H;*
2. *para todos x, y pertencentes a H, $x * y$ também pertence a H;*
3. *para todo x pertencente a H, x^{-1} pertence a H.*

Notação: $H < G$.

Teorema 4.1. *A interseção de dois subgrupos H e K de um grupo G também será um subgrupo.*

Prova: O elemento identidade está em ambos H e K, pois $e \in H < G$ e $e \in K < G$, então $H \cap K \neq \emptyset$.

Se x e $y \in H \cap K$, pelo fato de $H < G$ e $K < G$ segue que xy^{-1} está em $H \cap K$. Pela definição anterior segue que $H \cap K < G$. □

Por exemplo, o conjunto dos números inteiros pares $(2\mathbb{Z})$é um subgrupo do grupo $(\mathbb{Z}, +)$, mas o conjunto dos números inteiros ímpares $(2\mathbb{Z}+1)$ não é subgrupo de $\mathbb{Z}$, pois a soma de dois números ímpares é um número par.

Definição 4.3. *Seja X um conjunto não vazio de um grupo G. Um elemento da forma*

$$X_1^{m_1} \cdot X_2^{m_2} \cdots X_k^{m_k}$$

onde $X_1, X_2, ..., X_k \in X$ e $m_1, m_2, ..., m_k$ são inteiros, é chamado uma palavra *nos elementos de X. A coleção de todas as palavras é um subgrupo de G, chamado subgrupo gerado por X.*

Exemplo 4.1. O grupo dos inteiros Gaussianos $G = \{a + bi, \text{ com } a, b \in \mathbb{Z}\}$ é o subgrupo de $(\mathbb{C}, +)$ gerado por $\{1, i\}$.

Definição 4.4. *O subgrupo gerado por x e denotado por $< x >$ é constituído por todas as potências inteiras de x. Se $G =< x >$ então G é chamado cíclico, ou seja, G é cíclico se existe um elemento x de G que gera todos os elementos de G.*

Exemplo 4.2. 1. $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ é um grupo cíclico gerado por $\overline{1}$.

2. $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots \overline{n-1}\}$ é também cíclico. Observemos que $< \overline{1} >$ é um gerador de $\mathbb{Z}_n$, porém qualquer m tal que $(m, n) = 1$ também é um gerador, onde (m, n) denota o maior divisor entre m e n.

Definição 4.5. *Se para qualquer elemento x de um grupo, existe um inteiro positivo n tal que $x^n = e$, então dizemos que x tem ordem finita e o menor inteiro positivo m tal que $x^m = e$ é chamado a ordem de x e será denotado por $o(x)$. Caso contrário, x tem ordem infinita. Ou, equivalentemente, a ordem de um elemento x de um grupo G é a ordem do subgrupo cíclico $< x >$, gerado por x.*

Exemplo 4.3. $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. $\mathbb{Z}_4$ é cíclico e pode ser gerado por $\overline{1}$ ou por $\overline{3}$.

Observemos que a ordem de $\overline{1}$ é $o(\overline{1}) = 4$, $o(\overline{3}) = 4$, $o(\overline{2}) = 2$, pois, $< \overline{2} >= \{\overline{0}, \overline{2}\}$ e $o(\overline{0}) = 1$.

4.1 Exemplos de Grupos

4.1.1 Grupo das Isometrias no Plano

Seja G o conjunto das transformações do plano, com a operação composição de funções, onde uma transformação é simplesmente uma bijeção do plano no plano.

Sabemos que a composição de funções é associativa, a transformação identidade é o elemento neutro e dada uma transformação f, sua inversa é o elemento inverso, concluindo que G é um grupo, em geral, não abeliano.

A seguir daremos alguns exemplos de subgrupos do grupo G das transformações do plano.

a) Uma colineação é uma transformação f que tem a propriedade: "l é uma reta se, e somente se, $f(l)$ é uma reta." O conjunto de todas as colineações do plano é um subgrupo de G.

b) Uma involução é uma transformação $\gamma \neq id$ do plano tal que $\gamma^2 = \gamma \circ \gamma = id$. O conjunto das involuções no plano é também um subgrupo do grupo G.

c) Uma isometria no plano é uma função $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ tal que $\forall x, y \in \mathbb{R}^2$, $\|f(x) - f(y)\| = \|x - y\|$.

A transformação $id : \mathbb{R}^2 \to \mathbb{R}^2$ é uma isometria e dadas duas isometrias $f, g : \mathbb{R}^2 \to \mathbb{R}^2$, temos que $\forall x, y \in \mathbb{R}^2$, $\| (f \circ g)(x) - (f \circ g)(y) \| = \| f(g(x)) - f(g(y)) \| = \| g(x) - g(y) \| = \| x - y \|$.

Também dada uma isometria $f : \mathbb{R}^2 \to \mathbb{R}^2$, para todos $x, y \in \mathbb{R}^2$, existem $a, b \in \mathbb{R}^2$, tais que $x = f(a)$ e $y = f(b)$, pois f é sobrejetora. A inversa f^{-1} satisfaz: $\forall x, y \in \mathbb{R}^2$, $\| f^{-1}(x) - f^{-1}(y) \| = \| f^{-1}(f(a)) - f^{-1}(f(b)) \| = \| a - b \| = \| f(a) - f(b) \| = \| x - y \|$.

Portanto, f^{-1} é também uma isometria, mostrando assim que o conjunto das isometrias no plano é um subgrupo de G.

4.1.2 Grupo G de Simetrias de um Quadrado.

Imagine um cartão quadrado tendo os lados paralelos aos eixos do sistema de coordenadas e centro na origem. Os elementos de G são obtidos por rotações no sentido horário R_{90}, R_{180}, R_{270} e R_{360} em torno do centro através de ângulos de 90, 180, 270 e 360, respectivamente e reflexões H, V, em torno de retas horizontal e vertical passando pela origem e reflexões D_1 e D_2 nas diagonais indicadas.

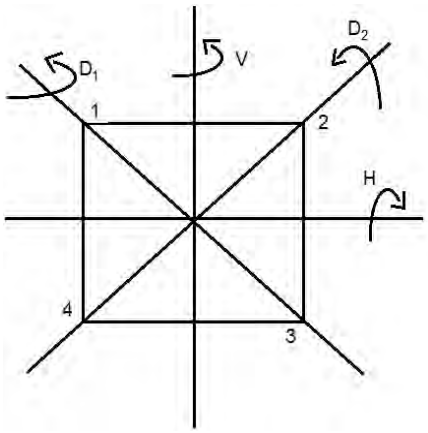


Figura 4.1: Simetrias de um quadrado

Considerando G com a operação composição temos a tabela do grupo G das simetrias de um quadrado

o	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
R_{90}	R_{180}	R_{270}	R_{360}	R_{90}	D_1	D_2	V	H
R_{180}	R_{270}	R_{360}	R_{90}	R_{180}	V	H	D_2	D_1
R_{270}	R_{360}	R_{90}	R_{180}	R_{270}	D_2	D_1	H	V
R_{360}	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
H	D_2	V	D_1	H	R_{360}	R_{180}	R_{270}	R_{90}
V	D_1	H	D_2	V	R_{180}	R_{360}	R_{90}	R_{270}
D_1	H	D_2	V	D_1	R_{90}	R_{270}	R_{360}	R_{180}
D_2	V	D_1	H	D_2	R_{270}	R_{90}	R_{180}	R_{360}

Figura 4.2: Tabela do grupo das simetrias de um quadrado

4.1.3 Grupos Diedrais e Cíclicos.

O grupo diedral D_n, $n \geq 2$ é o grupo de ordem $2n$ gerado por r e s, tal que $r^n = 1$, $s^2 = 1$, $srs = r^{-1}$.

No caso $n = 2$, temos o grupo diedral D_2 de ordem 4, gerado por r e s, tal que $r^2 = 1,\ s^2 = 1,\ srs = r^{-1}$.

$D_2 = \{1, r, s, rs\}$

•	1	r	s	rs
1	1	r	s	rs
r	r	1	rs	s
s	s	rs	1	r
rs	rs	s	r	1

Figura 4.3: D_2 é o grupo diedral de ordem 4

Exemplo 4.4. $D_3 = \{e, r, r^2, s, rs, r^2s\}$

	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

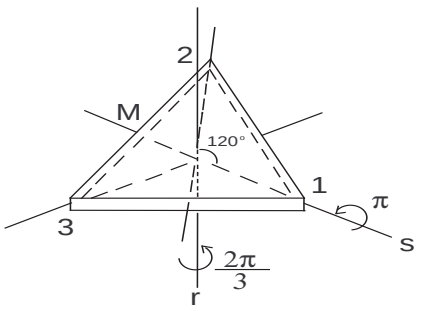


Figura 4.4: D_3

Observamos na figura acima que os geradores do grupo diedral estão representados por uma reflexão s em torno do eixo M e por uma rotação r de ângulo $2\pi/3$ em torno de um eixo perpendicular ao triângulo passando pelo baricentro da figura.

Exemplo 4.5. Vejamos que $r^2s = sr$ de acordo com a figura 4.5.

Exemplo 4.6. D_6, o grupo diedral dado pelas rotações $r^6 = e$, $s^2 = e$ e $srs = r^{-1}$.

$$< r >= \{e, r, r^2, r^3, r^4, r^5\} < D_6.$$

O grupo cíclico nos fornece informações úteis dos grupos, em geral. Vamos nos aprofundar um pouco sobre este tipo de grupos.

Teorema 4.2. *Se o grupo cíclico* $G =< x >$ *tem ordem n, então* $G = \{e, x, ..., x^{n-1}\}$.

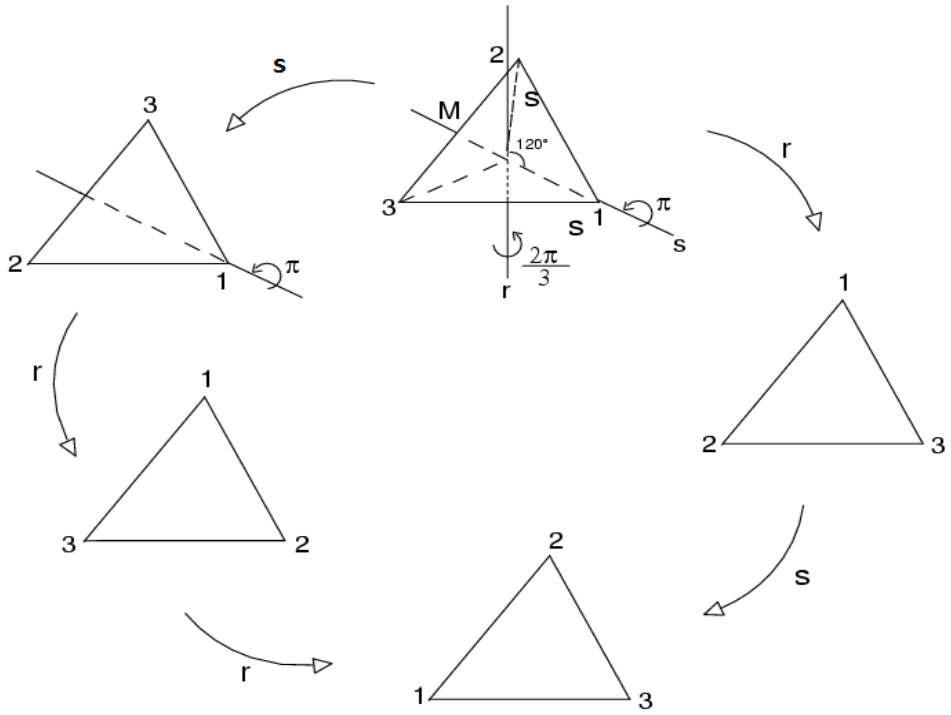


Figura 4.5: $r^2s = sr$

Prova: Como $< x >$ tem n elementos, então existem $i, j, \in \mathbb{Z}$ tais que $x^i = x^j$. Suponhamos $i < j$. Então $x^{j-i} = e$. Assim, o conjunto dos números inteiros l tal que $x^l = e$ é não vazio. Pelo princípio do menor inteiro positivo, existe um m tal que $x^m = e\,(x^l \neq e,\ 0 < l < m)$.

Seja $S = \{e, x, x^2, \cdots, x^{m-1}\}$ de elementos distintos. Provemos que $S =< x >$. Se $y \in S$, então $y \in< x >$. Seja $x^k \in< x >$. Pelo algoritmo da divisão, existem q e r tais que $k = qm + r$, para $0 \leq r < m$. Então, $x^k = (x^m)^q.x^r = x^r \in S$, porque $r < m$.

Logo $< x > \subset S$ e $m = n$.

Teorema 4.3. *a) Todo subgrupo de $\mathbb{Z}$ é cíclico.*

Prova: Seja $H < \mathbb{Z}$. Se $H = \{0\}$ então H é cíclico.

Se $H \neq \{0\}$, então H contém um inteiro $x \neq 0$, e pelo fato de $H < \mathbb{Z}$, então $-x \in H$.

Assim H contém um número inteiro positivo.

Pelo princípio do menor inteiro positivo, existe d que é o menor inteiro positivo pertencente a H.

Afirmamos que $H =< d >$.

Se $n \in H$, aplicando o algoritmo da divisão, existem q e $m \in \mathbb{Z}$ tais que, $n = qd+m$, onde $0 \leq m < d$. Sabemos que $n \in H$ e $d \in H$, $q \in \mathbb{Z}$ e como $H < \mathbb{Z}$, $qd \in H$ ($d+...+d$, q vezes).

Logo $-qd \in H$, e então
$m = n - qd \in H$ que é uma contradição, pois d é o menor inteiro positivo pertencente a H. Concluímos que $m = 0$, portanto $n = qd$. □

b) Todo subgrupo de um grupo cíclico é cíclico.

Prova: Seja G um grupo cíclico e $K < G$, $K \neq \{e\}$.

Seja x um gerador de G, então todo elemento de G, em particular todo elemento de K, é uma potência de x. (1)

Seja $H = \{n \in \mathbb{Z}/x^n \in K\}$. Provemos que $H < \mathbb{Z}$.

De fato, de (1) segue que $x^0 \in K$, logo $0 \in H$.

Sejam n_1 e $n_2 \in H$. Provemos que $n_1 - n_2 \in H$.

$$x^{n_1 - n_2} = x^{n_1} \cdot x^{-n_2} \in K, \text{ logo } n_1 - n_2 \in H.$$

Portanto H é cíclico por a), isto é, existe $d \in \mathbb{Z}$, tal que $H =< d >$.

Então $K =< x^d >$.

De fato, se $y \in K$, por (1), $y = x^l$, $l \in \mathbb{Z}$.

Como $H = \{n \in \mathbb{Z}, x^n \in K\} =< d >$, segue que $l = \alpha d$, $\alpha \in \mathbb{Z}$ e portanto $y = x^{\alpha d} = (x^d)^\alpha$. □

Prova II: Apresentaremos abaixo outra demonstração do teorema acima.

Seja $G =< a >$ um grupo cíclico e consideremos H um subgrupo de $< a >$. Se $H = \{e\}$, então H é cíclico.
Se $H \neq \{e\}$, existe $a^k \in H$, se $k < 0$ então $-k > 0$ e $a^{-k} \in H$. Então existem inteiros positivos k tais que $a^k \in H$.
Afirmamos que $H =< a^n >$.
Temos $< a^n > \subset H$, pois $\forall x \in < a^n >$, tem-se que $x = (a^n)^l \in H$, pois $H < G$.

Por outro lado, se $x \in H$ então $x = a^k$ para algum k.
Pelo algoritmo da divisão, $\exists q, r$ tal que

$$k = qn + r \text{ com } 0 \leq r < n. \text{ Segue que}$$

$$r = k - qn \text{ e } a^r = a^{k-qn} = a^k \cdot (a^n)^{-q}$$

ou seja, $a^r \in H$. Logo $r = o$, assim $k = qn$ e então $a^k = (a^n)^q \in < a^n >$. □

Exemplo 4.7. Em D_3 temos:

$< e >= e$	$o(e) = 1$
$< r >= \{e, r, r^2\}$	$o(r) = 3$
$< s >= \{e, s\}$	$o(s) = 2$
$< rs >= \{e, rs\}$	$o(rs) = 2$
$< r^2 s >= \{e, r^2 s\}$	$o(r^2 s) = 2$

Observe que D_3 não é cíclico. Ele é gerado por r, s com as relações $srs = r^{-1}$, $r^3 = e$, $s^2 = e$.

Exemplo 4.8. O grupo diedral infinito D_∞.

Considere a reta real com o conjunto dos inteiros em destaque, como na figura a seguir:

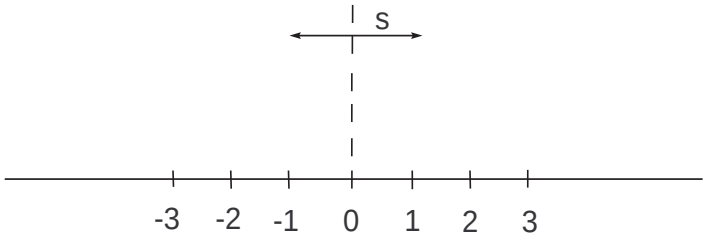


Figura 4.6: Reta real

Seja $G = \{f : \mathbb{R} \to \mathbb{R} / f(\mathbb{Z}) = \mathbb{Z} \text{ e } |x - y| = |f(x) - f(y)|, \forall\, x, y \in \mathbb{R}\}$.

G é um grupo com a composição de funções, $(G, \circ)$.

Seja f uma função da reta na reta que preserva distância entre quaisquer dois pontos e que leva números inteiros em números inteiros.

a) Assumindo que f não possui ponto fixo, i.e. $f(x) \neq x$, $\forall x \in \mathbb{R}$ mostremos que f é uma translação.

Prova: De fato se $|z - 0| = |f(z) - f(0)|$, obtemos $z = \pm[f(z) - f(0)]$, então $z = f(z) - f(0)$ ou $z = -f(z) + f(0)$, logo, $f(z) = z + f(0)$ ou $f(z) = -z + f(0)$ e como $f(0) \neq 0$, temos que f é uma translação. □

b) Se f possui exatamente um ponto fixo, mostraremos que este ponto ou é um inteiro ou está entre dois inteiros, e que f é a reflexão em torno deste ponto.

Prova: Suponhamos que z_0 seja o único ponto fixo de f i.e. $f(z_0) = z_0$ e $f(z) \neq z$, $\forall z \neq z_0$. Assim para $z \neq z_0$ e de

$|z - z_0| = |f(z) - f(z_0)|$, segue que $z^2 - 2z_0 z + z_0^2 = f(z)^2 - 2f(z)z_0 + z_0^2$

ou ainda, $f(z)^2 - z^2 = (f(z) - z)2z_0$, ou seja, $(f(z) - z)(f(z) + z) = (f(z) - z)2z_0$.

Como $f(z) \neq z$ então $f(z) = 2z_0 - z$, que é uma reflexão em torno de z_0.

Em particular $f(0) = 2z_0 \in \mathbb{Z}$.

c) Finalmente, veremos que f será a identidade se existir mais que um ponto fixo.

Prova: Sejam $x_0 \neq x_1$ pontos fixos, ou seja, $f(x_0) = x_0$ e $f(x_1) = x_1$. Dessa forma das relações abaixo

$|f(x) - x_0| = |x - x_0|$ e $|f(x) - x_1| = |x - x_1|, \forall x \in \mathbb{R}$, obtemos

$$f(x)^2 - 2f(x)x_0 + x_0^2 = x^2 - 2xx_0 + x_0^2$$
$$f(x)^2 - 2f(x)x_1 + x_1^2 = x^2 - 2xx_1 + x_1^2$$

Subtraindo essas duas equações teremos:

$2f(x)(x_1 - x_0) = 2x(x_1 - x_0)$, mas $x_1 \neq x_0$, logo

$f(x) = x$. □

Dessa forma concluímos que G é constituído por translações e reflexões.

Tomemos $t, s \in G$, onde, $t(x) = x + 1$ e $s(x) = -x$.

$t \circ t(x) = t(x + 1) = x + 1 + 1 = x + 2$
$t^k(x) = x + k$
$t^{-1}(x) = x - 1$
$t^{-2}(x) = x - 2$ $\qquad ..., t^{-k}, ..., t^{-1}, e, t, t^2, ...$

$s(x) = -x$
$s^2(x) = s(s(x)) = s(-x) = x$
$s^3(x) = -x$

Notemos que,

$s^2 = e$
$-sts(x) = st(-x) = s(-x + 1) = x - 1 = t^{-1}(x)$.

Cada elemento de G é uma translação da esquerda para a direita através de um número inteiro, uma reflexão de um inteiro, ou uma reflexão em um ponto que fica entre dois inteiros.

Seja t uma translação para a direita através de uma unidade, então $t(x) = x+1$, e seja s a reflexão na origem, então $s(x) = -x$. Logo os elementos de G são

$$..., t^{-2}, t^{-1}, e, t, t^2, ...$$
$$..., t^{-2}s, t^{-1}s, s, ts, t^2s, ... \qquad (**)$$

onde e é a função identidade. Por exemplo $t^{-2}(x) = x - 2$, mostrando que t^{-2} é translação para a esquerda duas unidades, e $ts(x) = t(-x) = -x + 1$, mostrando que ts é reflexão no ponto $1/2$. A translação t e a reflexão s juntas geram G. Da mesma forma as duas reflexões ts e s geram G. Note que

$$st(x) = s(x + 1) = -x - 1$$
$$t^{-1}s(x) = t^{-1}(-x) = -x - 1$$

o que significa $st = t^{-1}s$. Sabendo que $s^2 = e$ e $st = t^{-1}s$, e multiplicando quaisquer dois elementos da lista $(**)$ obtemos também um elemento da lista. Isto nos faz lembrar muito do D_n. Na verdade, a única diferença é que a rotação r de ordem n foi substituída pela translação t de ordem infinita.

Por esta razão chamamos G de **grupo diedral infinito** e denotamos por D_∞.

4.1.4 Grupos de Permutação

Por uma permutação de um conjunto arbitrário X entendemos uma bijeção de X em si mesmo. A coleção de todas as permutações de X forma um grupo S_X com a composição de funções.

1. Se $\alpha : X \to X$ e $\beta : X \to X$ são permutações com a composição de funções $\alpha\beta : X \to X$ definida por $\alpha\beta(x) = \alpha(\beta(x))$ é também uma permutação, pois a composta de bijeções é também uma bijeção;

2. Composição de funções é associativa e a função identidade Id_X é o elemento identidade de S_X.

3. Finalmente, cada permutação α é uma bijeção e portanto possui uma inversa $\alpha^{-1} : X \to X$ que é também uma permutação e que satisfaz $\alpha^{-1}\alpha = Id_X = \alpha\alpha^{-1}$.

Se X é um conjunto infinito, S_X é um grupo infinito. Quando X é formado por n inteiros positivos, então S_X é escrito S_n e chamado o **grupo simétrico** de grau n. A ordem de S_n é $n!$ (n fatorial.)

Aqui temos os elementos de S_3:

$$Id_3 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}.$$

Observamos que $\alpha\beta$ significa aplicar primeiro β e depois α, vamos calcular

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad e \quad \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} (*)$$

temos que $\alpha\beta \neq \beta\alpha$.

Portanto S_3 não é abeliano. Podemos dizer que S_n não é abeliano quando $n \geq 3$. Para facilitar a notação, nos casos em que $n \geq 3$, denotaremos por exemplo para

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

como

$$\alpha = (15)(246).$$

Observe que aqueles inteiros que são fixados não aparecem na nova notação. Podemos escrever qualquer permutação dessa forma: abra um par de parênteses, em seguida anote o menor inteiro que não é fixado pela permutação dada. Agora, liste a imagem deste inteiro sob a permutação, seguido por sua imagem e assim por diante, feche os parênteses quando completar o ciclo. Abra um novo par de parênteses, liste o menor inteiro que até agora não foi mencionado e que é movido pela permutação, e assim sucessivamente.

Exemplo 4.9.

$i)$ $$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 8 & 9 & 3 & 6 & 2 & 7 & 5 & 4 \end{bmatrix} = (2856)(394)$$

$ii)$ $$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 6 & 7 & 3 & 5 & 4 & 2 \end{bmatrix} = (182)(365)(47)$$

$iii)$ Os elementos de S_3 são: $\varepsilon, (12), (13), (23), (123), (132)$.

$iv)$ O cálculo $(*)$ torna-se: $(12)(23) = (123)$ e $(23)(12) = (132)$.

Com esta nova notação uma permutação $(a_1a_2...a_k)$ dentro de um par de parênteses é chamada uma **permutação cíclica**. Que envia a_1 em a_2, a_2 em a_3, ..., a_{k-1} em a_k e a_k em a_1, deixando todos os outros fixados. O número k é seu comprimento e a permutação cíclica de comprimento k é chamada um k-ciclo. Um 2-ciclo é chamado uma transposição. O argumento acima mostra que todo elemento de S_n pode ser escrito como um produto de permutações cíclicas disjuntas, no sentido de que nenhum inteiro é movido mais de uma vez.

Veja novamente o exemplo (i) onde temos (2856) e (394). O primeiro deles afeta apenas os inteiros $2, 5, 6$ e 8 e o segundo move apenas $3, 4$ e 9. Como estas permutações são disjuntas, elas comutam entre si, ou seja, $(2856)(394) = (394)(2856)$. Claro que isto é um resultado geral, se α e β são elementos de S_n e se nenhum inteiro é movido por ambas α e β então $\alpha\beta = \beta\alpha$. A decomposição de um elemento de S_n como um produto de permutações cíclicas disjuntas é única a menos da ordem na qual elas são escritas.

Teorema 4.4. *As transposições em S_n juntas, geram S_n.*

(Ver [3])

Tomemos o exemplo do S_4,

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_2 & a_3 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_2 & a_1 & a_4 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_3 & a_4 \end{pmatrix}$$

Na nossa notação temos:

$$(a_1a_2a_3a_4) = (a_1a_4)(a_1a_3)(a_1a_2)$$

Um elemento de S_n que pode ser expresso como produto de um número par de transposições é chamado uma **permutação par**; os que podem ser escritos como produto de um número ímpar de transposições são **permutações ímpares.**

$$(a_1a_2...a_k) = (a_1a_k)...(a_1a_3)(a_1a_2),$$

uma permutação cíclica é precisamente par quando seu comprimento é ímpar.

Definição 4.6. *O grupo alternado de grau n, denotado por A_n, é o conjunto de todas as permutações pares em S_n.*

Teorema 4.5. *$A_n \triangle S_n$ de ordem $\frac{1}{2}n!$*

(Ver [3])

Teorema 4.6. *Para $n \geq 3$, A_n é gerado pelos 3-ciclos.*

(Ver [3])

Exemplo 4.10. Os doze elementos do A_4 são

$$\begin{array}{cccc} \varepsilon, & (12)(34), & (13)(24), & (14)(23), \\ (123), & (124), & (134), & (234), \\ (132), & (142), & (143), & (243). \end{array}$$

Os elementos restantes de S_4, as permutações ímpares, são

$$\begin{array}{ccc} \varepsilon, & (12), (13), (14), (23), & (24), (34), \\ (1234), & (1243), & (1324), \\ (1432), & (1342), & (1423). \end{array}$$

Propriedade 4.1. O grupo de simetria rotacional do tetraedro é isomorfo ao A_4. O cubo e o octaedro possuem grupos de simetrias rotacionais que são isomorfos ao S_4. O dodecaedro e o icosaedro possuem grupos de simetrias que são isomorfos ao A_5.

O cubo e o dodecaedro são sólidos duais ao octaedro e icosaedro, respectivamente e, portanto possuem grupos das rotações isomorfos. Como exemplo vamos examinar um deles, o dodecaedro.

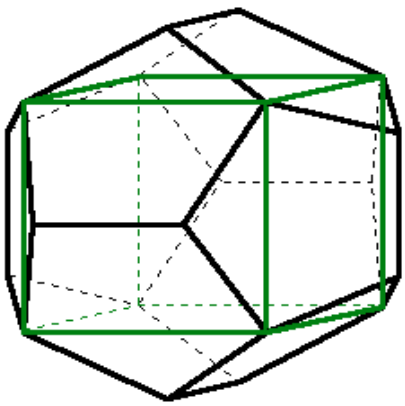


Figura 4.7: Cubo Inscrito no Dodecaedro

A figura 4.7 mostra um cubo dentro de um dodecaedro. Cada vértice do cubo é um vértice do dodecaedro, e cada aresta é uma diagonal de uma das faces pentagonais. Se você olhar para um pentágono em particular, exatamente uma das suas cinco diagonais

será um lado do cubo. Não existe nada de especial sobre esta diagonal e claro existem quatro outros cubos inscritos correspondendo as outras quatro diagonais do pentágono. Estes cinco cubos são permutados através de cada rotação do dodecaedro.

Vamos checar que o grupo das rotações de um dodecaedro regular é isomorfo ao A_5, daremos uma ideia de como deve ser feito, usando os seguintes passos:

i) Existem 20 vértices, 30 arestas e 12 faces. Em cada par de faces opostas (6 pares) temos 4 rotações diferentes, ou seja, um total de 24 rotações. Temos uma única rotação por pares de arestas opostas (15 pares), totalizando 15 rotações. Pelos pares de vértices opostos, que são 10 pares, temos 2 rotações em cada par, gerando 20 rotações ao todo. Logo, $24 + 15 + 20$ juntamente com a rotação identidade nos fornece um total de 60 rotações distintas no dodecaedro.

ii) De acordo com o Teorema 4.5 a ordem de A_5 é $5!/2 = 60$.

iii) Temos cinco cubos inscritos no dodecaedro, veremos que cada rotação do dodecaedro produz um elemento de S_5, basta enumerar os cubos inscritos de 1 até 5.

Vamos analisar primeiramente uma rotação sobre o eixo que passa pelo centro de faces opostas, girando $2\pi/5$. Neste caso, antes de aplicarmos a rotação temos

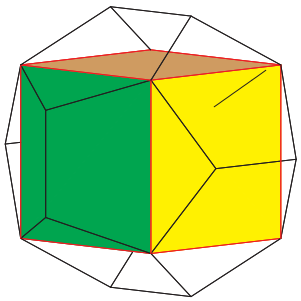


Figura 4.8: Rotação pelo centro de faces opostas (antes)

e após aplicarmos a rotação sobre o eixo

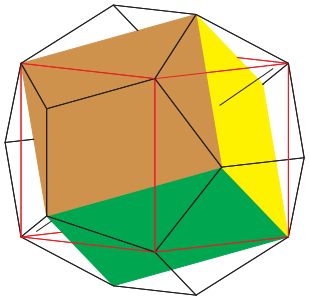


Figura 4.9: Rotação pelo centro de faces opostas (depois)

vemos claramente que obtemos outro elemento de S_5 (um cubo diferente).

Agora vamos analisar uma rotação sobre um eixo que passa pelos pontos médios de arestas opostas, girando π. Antes da rotação temos

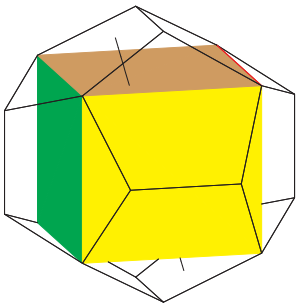


Figura 4.10: Rotações por pontos médios de arestas opostas (antes)

e após a rotação teremos

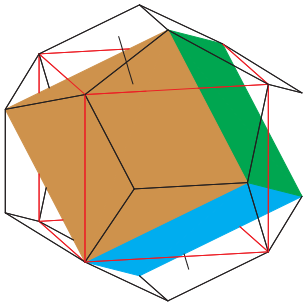


Figura 4.11: Rotações por pontos médios de arestas opostas (depois)

Observamos que o cubo é diferente do anterior (outro elemento de S_5)

Da mesma forma que nos casos anteriores, veremos que uma rotação sobre um eixo que passa por pares de vértices opostos, girando π, nos fornece outro elemento de S_5.
Antes da rotação

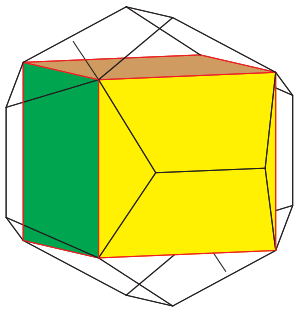


Figura 4.12: Rotações por pares de vértices opostos (antes)

depois da rotação

.

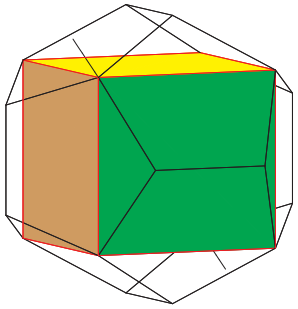


Figura 4.13: Rotações por pares de vértices opostos (depois)

iv) Considerando as rotações em torno dos eixos que ligam pares de vértices opostos, mostramos que todo 3-ciclo em S_5 é dado dessa forma.

v) Lembrando do teorema 4.6 que diz que para $n \geq 3$ os 3- ciclos geram A_n, temos que os 3-ciclos em S_5 geram o A_5. □

4.1.5 O Grupo dos Quatérnios

Em 1843, Hamilton introduziu os quatérnios como um modo de generalizar a álgebra dos números complexos para dimensões mais altas. Nós os usaremos também para representar reflexões e rotações no $\mathbb{R}^3$, algebricamente. Há varias maneiras de descrever os quatérnios, mas fundamentalmente eles são pontos do espaço euclidiano 4-dimensional $\mathbb{R}^4$.

Um quatérnio é uma expressão $a + bi + cj + dk,\ a, b, c, d \in \mathbb{R}$. O conjunto dos quatérnios é denotado por $\mathbb{H}$.

Vamos definir uma adição ao conjunto dos quatérnios, de modo que $(\mathbb{H}, +)$ seja um grupo abeliano.

Sejam $x = a_1 + a_2i + a_3j + a_4k$ e $y = b_1 + b_2i + b_3j + b_4k$ dois quatérnios. A soma é um quatérnio definido por $z = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$.

O elemento neutro é $0+0i+0j+0k$ e o oposto do elemento $x = a_1+a_2i+a_3j+a_4k$ é o elemento $-x = -a_1 + (-a_2)i + (-a_3)j + (-a_4)k$.

Este exemplo é interessante, pois definindo-se a multiplicação de seus elementos de maneira a respeitar a multiplicação dos complexos, obtemos um anel de divisão, ou seja, um anel que só não tem a propriedade comutativa para ser um corpo.

4.2 Homomorfismos de Grupos

Definição 4.7. *Sejam $(G, *)$ e $(H, \triangle)$ dois grupos. Um homomorfismo é uma função $h : G \longrightarrow H$ tal que para todos x, y em G, tem-se $h(x * y) = h(x) \triangle h(y)$. Se o homomorfismo for injetor, então é chamado de monomorfismo, se for sobrejetor, é chamado de epimorfismo e se for bijetor, então é um isomorfismo.*

O kernel ou o núcleo de um homomorfismo h, denotado por $\ker h$ é o conjunto dos pontos de G que são levados por h no elemento neutro de H, i.e.

$$ker h = \{x \in G,\, h(x) = e_H\}.$$

Observemos que um homomorfismo h é injetor se, e somente se, $ker h = \{e_G\}$.

Definição 4.8. *Dois grupos $(G, *)$ e $(G', \cdot)$ são isomorfos se existir uma bijeção φ entre G e G' que satisfaz $\varphi(x * y) = \varphi(x) \cdot \varphi(y)$ para todo $x, y \in G$. A função φ é chamada de isomorfismo entre G e G', e denotaremos $G \cong G'$.*

Observemos que a composta de dois isomorfismos é um isomorfismo. De fato, dados $f : G \longrightarrow H$ e $g : H \longrightarrow G'$ dois isomorfismos, então a composta $g \circ f$ é uma bijeção de G em G' e além disso, dados $x, y, \in G$, tem-se:

$$(g \circ f)(x * y) = g(f(x) \triangle f(y)) = g(f(x)) \cdot g(f(y)) = (g \circ f)(x) \cdot (g \circ f)(y).$$

Segue deste resultado que se $G \cong H$ e $H \cong G'$, então $G \cong G'$.

Exemplo 4.11. Defina $\varphi : \mathbb{R} \to \mathbb{R}_+^*$ por $\varphi(x) = e^x$. Então φ é uma bijeção e $\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$ para todos $x, y \in \mathbb{R}$. Então $\mathbb{R}$ e $\mathbb{R}_+$ são grupos isomorfos. Lembrando que a operação do grupo é a adição em $\mathbb{R}$, considerando que em $\mathbb{R}_+^*$ é a multiplicação.

Exemplo 4.12. Conhecemos uma boa parte do tetraedro. Este possui doze rotações que formam um grupo não abeliano G. Podemos aprender mais da seguinte forma.

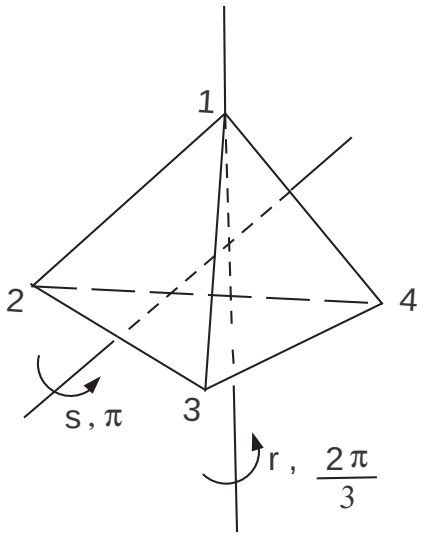


Figura 4.14: Rotações no Tetraedro

Numerando os vértices por $1, 2, 3$ e 4 como na figura 4.14, cada rotação simétrica induzem uma permutação dos vértices e portanto uma permutação dos primeiros 4 inteiros. Por exemplo, a rotação r ilustrada induz uma permutação cíclica (234) e s induz $(14)(23)$.

Trabalhando da mesma forma com todas as outras possibilidades produzimos os doze elementos de A_4. Se duas rotações u, v induz permutações α, β respectivamente então uv claramente induz $\alpha\beta$.

Portanto, a correspondência

$$\text{rotação simétrica} \rightarrow \text{permutação induzida}$$

mostra que G é isomorfo ao A_4 .

Exemplo 4.13. Qualquer grupo cíclico infinito é isomorfo a $\mathbb{Z}$.
Se $(G, \cdot)$ é um grupo cíclico infinito, e se x gera G, isto é $G = \{e, x, x^2, ...\}$ e seja $\varphi : G \rightarrow \mathbb{Z}$ dada por $\varphi(x^m) = m$, então φ é uma bijeção e

$$\varphi(x^m \cdot x^n) = \varphi(x^{m+n}) = m + n = \varphi(x^m) + \varphi(x^n).$$

Isto mostra que φ é um isomorfismo.

Exemplo 4.14. Qualquer grupo cíclico finito de ordem n é isomorfo a $\mathbb{Z}_n$. Se G é um grupo cíclico de ordem n, e se x gera G, isto é $G = \{e, x, x^2, ..., x^{n-1}\}$ define-se $\varphi : G \rightarrow \mathbb{Z}_n$ por $\varphi(x^m) = \alpha$, onde $\alpha \equiv m(mod\ n)$. Então φ é um isomorfismo.

Exemplo 4.15. Não existe um isomorfismo entre $(\mathbb{Q}, +)$ e $(\mathbb{Q}_+^*, \cdot)$.
Suponhamos $\varphi : \mathbb{Q} \rightarrow \mathbb{Q}_+^*$ seja um candidato. Escolhemos $x \in \mathbb{Q}$ tal que $\varphi(x) = 2$, então

$$\varphi\left(\frac{x}{2} + \frac{x}{2}\right) = \varphi\left(\frac{x}{2}\right)\varphi\left(\frac{x}{2}\right) = 2$$

e $\varphi\left(\frac{x}{2}\right)$ tem que ser $\sqrt{2}$. Devido $\sqrt{2}$ ser irracional, temos uma contradição.

Exemplo 4.16. D_3 e S_3 são isomorfos.

$D_3 = \{e, r, s, r^2, rs, r^2s\}$
$S_3 = \{\varepsilon, (12), (13), (23), (123) \text{ e } (132)\}$

Faremos a seguinte correspondência:

$$e \rightarrow \varepsilon, \quad s \rightarrow (12), \quad r \rightarrow (123), \quad r^2 \rightarrow (132), \quad rs \rightarrow (13), \quad r^2s \rightarrow (23).$$

Observamos que o Núcleo é igual a e, e portanto é injetora. Esta correspondência também é sobrejetora e é um homomorfismo. Basta verificar nos geradores r e s,

$$rs \rightarrow (13) = (123)(12);$$
$$r^2 \rightarrow (132) = (123)(123);$$
$$sr = r^2s \rightarrow (23) = (132)(12).$$

Exemplo 4.17. Consideremos $G = \{1, -1, i, -i\}$ com a multiplicação de números complexos. Temos que $G =< i >$ ou $G =< -i >$. Por exemplo, para $G =< i >$ temos $1 = i^4$, $-1 = i^2$, $i = i$ e $-i = i^3$.
A correspondência dá um isomorfismo entre G e $\mathbb{Z}_4$

$$\begin{array}{cc} G \to & \mathbb{Z}_4 \\ 1 \to & \overline{0} \\ i \to & \overline{1} \\ -1 \to & \overline{2} \\ -i \to & \overline{3} \end{array}$$

Propriedade 4.2. Seja $\varphi = G \to G'$ um homomorfismo.

1. $\varphi(e) = e'$.

   Para todo x pertencente a G, temos:

   $$e'\varphi(x) = e'\varphi(e * x) = \varphi(e) \cdot \varphi(x), \ \ \forall x \in G.$$

   Pela lei do cancelamento, segue que $\varphi(e) = e'$, o elemento neutro de G'

2. $\varphi(x^{-1}) = [\varphi(x)]^{-1}$.

   Observemos que,

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

   portanto $\varphi(x^{-1})$ é o inverso de $\varphi(x)$.

3. Se $H < G$ então $\varphi(H) < G'$.

   Sejam x', $y' \in \varphi(H)$. Assim, existem $x, y \in H$ tal que $\varphi(x) = x'$ e $\varphi(y) = y'$.
   H é subgrupo de G, o que implica que $xy^{-1} \in H$.
   Temos que,

   $$\varphi(x * y^{-1}) = \varphi(x) \cdot \varphi(y^{-1}) = \varphi(x) \cdot \varphi(y)^{-1} = x'(y')^{-1},$$

   portanto $x'(y')^{-1} \in \varphi(H)$.

   Como $H < G$, o elemento neutro pertence a H, logo $\varphi(e)$ pertence a $\varphi(H)$, mas $\varphi(e) = e$.

4. A composta de dois homomorfismos é um homomorfismo.

   De fato, sejam $f : G \to G'$ e $g : G' \to G''$ dois homomorfismos entre grupos $(G, *), (G', \cdot)$ e $(G'', \triangle)$. Então $\forall x, y \in G$,

   $$(g \circ f)(x * y) = g(f(x * y)) = g(f(x) \cdot f(y)) = g(f(x)) \triangle g(f(y)) = (g \circ f)(x) \triangle (g \circ f)(y).$$

   Observemos que se f e g forem isomorfismos, então $g \circ f$ também o será.

5. Se φ é um isomorfismo e $o(x) = m$ então $o(\varphi(x)) = m$.

   De fato, se $x \in G$ tem ordem m, então m é o menor inteiro positivo tal que $x^m = e$. Segue do fato de que φ é um isomorfismo e pela propriedade 1, que $\varphi(x^m) = (\varphi(x))^m = e'$. Mostremos que m é o menor inteiro positivo com esta propriedade. Suponhamos que exista um inteiro positivo $k < m$ tal que $(\varphi(x))^k = e'$. Então $\varphi(x^k) = e'$, o que implica que $x^k \in \ker\varphi$ que por ser um isomorfismo só tem o elemento neutro e. Isto nos dá uma contradição, pois m é a ordem de x.

Exemplo 4.18. Os grupos $(\mathbb{Z}, +)$ e $(\mathbb{Q}^*, \cdot)$ não são isomorfos. De fato, suponhamos que existe um isomorfismo $f : \mathbb{Z} \to \mathbb{Q}^*$. Então $f(0) = 1$. Além disso, $-1 \in \mathbb{Q}^*$ e f é sobrejetora, então existe $x \in \mathbb{Z}$ tal que $f(x) = -1$.

Logo
$f(x + x) = f(x) \cdot f(x) = 1$, e portanto $2x \in Ker\ f = \{0\}$, pois f é injetora.
Logo $2x = 0 \Rightarrow x = 0$ (contradição), pois teríamos
$f(0) = 1$ e $f(0) = -1$.

4.3 Grupos Quocientes

Exemplo 4.19. Seja H um subgrupo de G e seja $\Re$ a coleção de pares ordenados (x, y) com elementos de G que satisfazem $y^{-1}x \in H$. É fácil verificar que $\Re$ é uma relação de equivalência em G (Para qualquer $x \in G$ temos $x^{-1}x = e \in H$, se $y^{-1}x \in H$, então $x^{-1}y = (y^{-1}x)^{-1} \in H$, e se $y^{-1}x,\ z^{-1}y \in H$, então $z^{-1}x = (z^{-1}y)(y^{-1}x) \in H$). A classe de equivalência de um elemento g *de* G é formada por todos os $x \in G$ que satisfazem $g^{-1}x \in H$. Sempre que $x = gh$ para qualquer elemento h de H, podemos garantir que $g^{-1}x$ pertence a H. Portanto, $\Re(g)$ é o conjunto gH obtido pela multiplicação de todo elemento de H pela esquerda por g. Este conjunto gH é chamado classe lateral à esquerda de H determinado por g. Pela proprosição a seguir sabemos que classe lateral à esquerda distintas de H em G formam uma partição de G. Se $\Re$ for mudada para a coleção de pares ordenados $(x, y) \in G \times G$, tal que $xy^{-1} \in H$, novamente teremos uma relação de equivalência em G. Dessa forma a classe de equivalência de g é classe lateral à direita Hg, obtida se multiplicarmos todo elemento de H à direita por g.

Proposição 4.1. *Seja $H < (G, *)$. O conjunto $\{aH, a \in G\}$ constitui uma partição de G.*

Prova: para cada $a \in G$, temos:

$$a = a * e \in aH \subset G \text{ ou } \{a\} \subset aH \subset G.$$

Também

$$\bigcup_{a \in G} \{a\} \subset \bigcup_{a \in G} (aH) \subset G.$$

Pelo fato de $G = \bigcup_{a \in G} \{a\}$ temos:

$$G = \bigcup_{a \in G} (aH).$$

Dados duas classes aH e bH, então

1. $aH = bH$

   ou

2. $aH \neq bH$

Suponhamos que $aH \cap bH \neq \varnothing$ então existe $x \in aH$ e $x \in bH \Rightarrow x = a * h, h \in H$ e $x = b * k, k \in H \Rightarrow a * h = b * k \Rightarrow a = b * k * h^{-1} \Rightarrow b^{-1} * a * h = k \Rightarrow b^{-1} * a = k * h^{-1} \Leftrightarrow aH = bH$.

Provaremos que $aH = bH \Leftrightarrow b^{-1} * a \in H, H < G$.

($\Rightarrow$) Se $aH = bH$, então existe $x = a * h, h \in H$ e $x = b * k, k \in H \Rightarrow a * h = b * k \Rightarrow b^{-1} * a * h = k \Rightarrow b^{-1} * a = k * h^{-1}$, como $k \in H$ e $h \in H$ então $k * h^{-1} \in H$ pois H é grupo, então $b^{-1}a \in H$.

($\Leftarrow$) provaremos que $aH \subset bH$ (i) e $bH \subset aH$ (ii).

(i) Seja $x \in aH$. Então $x = a * h$, com $h \in H$. Temos que $b^{-1} * x = (b^{-1} * a) * h = \alpha \in H$. Logo

$$b^{-1} * x = \alpha \Rightarrow x = b * \alpha \in bH,$$

(ii) Seja $x \in bH$. Então $x = b * h$, com $h \in H$. Temos que $x * h^{-1} = b \Rightarrow b^{-1} = h * x^{-1} \Rightarrow b^{-1} * a = h * x^{-1} * a$. Logo

$x^{-1} * a = h^{-1} * (b^{-1} * a) \in H$. Então,

$x^{-1} * a = k$, com $k \in H$, ou seja $x = a * k^{-1}$, com $k^{-1} \in H$. Portanto $x \in aH$. □

Teorema 4.7. ***Teorema de Lagrange:*** *Seja G um grupo finito. A ordem de qualquer subgrupo de G divide a ordem de G.*

Prova: Suponhamos que $|G| = n$ e seja $H < G$, com $|H| = m$. Já vimos que $\{aH, a \in G\}$ constitui uma partição de G. Disto segue que $n = |G|$ é igual a k vezes o número de elementos de cada classe lateral onde k é o número de classes laterais distintas, i.e., $G = a_1H \cup ... \cup a_kH$ e $a_iH \cap a_jH = \varnothing$ para $i \neq j$.

Lembrando que aH tem o mesmo número de elementos de H, dada pela bijeção $a * h \to h$, com $h \in H$, segue que $n = km$, ou seja $m \mid n$. □

Corolário 4.1. *A ordem de todo elemento de G é um divisor da ordem de G.*

Prova: Basta lembramos que a ordem de um elemento é igual a ordem do subgrupo gerado por aquele elemento.

Corolário 4.2. *Se a ordem de G é um número primo, então G é cíclico.*

Definição 4.9. *Dizemos que H é um subgrupo normal de G, denotado por $H \lhd G$, se:*
i) $H < G$;
ii) $\forall a \in G, aH = Ha$.

Proposição 4.2. *Seja $H < G$. Então $H \lhd G$ se, e somente se, $\forall a \in G, aHa^{-1} \subset H$.*

Prova:
($\Rightarrow$) Suponhamos $H \lhd G$. Para todo $a \in G$, seja $y \in aHa^{-1}$. Então $y = a * h * a^{-1}$, com $h \in H$. Observe que $a * h \in aH = Ha$ pois, $H \lhd G$. Portanto $a * h = l * a, l \in H$. Temos

$$y = (a * h) * a^{-1} = (l * a) * a^{-1} = l \in H.$$

($\Leftarrow$) Provemos primeiramente que $\forall a \in G, aH \subset Ha$. Seja $y \in aH$. Então $y = a * h, h \in H$.

$$y = a * h * a^{-1} * a \in Ha$$

pois $(a * h * a^{-1}) \in aHa^{-1} \subset H$.

Mostremos agora que $\forall a \in G, aH \supset Ha$. Seja $z \in Ha$. Então $z = h * a$. Tomando $a = a^{-1}$,

$$a * a^{-1} * h * a \in aH.$$

pois, $a = (a^{-1})^{-1}$ e $a^{-1}Ha \subset H$ por hipótese. □

Exemplo 4.20. Se $f : G \to G'$ é um homomorfismo, então $ker\, f \lhd G$. As operações de G e G' são, respectivamente, $*$ e $\triangle$.

Prova: Já vimos que $ker\, f < G$. Provemos que $\forall a \in G, a \cdot ker\, f \cdot a^{-1} \subset ker\, f$.
Seja $y \in a \cdot ker\, f \cdot a^{-1}$, logo $y = a * \alpha * a^{-1}$, com $\alpha \in ker\, f$. Portanto

$$f(y) = f(a * \alpha * a^{-1}) = f(a) \triangle f(\alpha) \triangle f(a^{-1}) = f(a) \triangle [f(a)]^{-1} = e_{G'} \Rightarrow y \in ker\, f. \square$$

Definição 4.10. *Seja $H \triangleleft G$. Definimos o conjunto quociente $G/H := \{gH, g \in G\}$.*

Vamos definir uma operação em G/H.
$G/H \times G/H \xrightarrow{\oplus} G/H$
$(g_1H, g_2H) \xrightarrow{\oplus} (g_1H) \oplus (g_2H) = (g_1 * g_2)H$.
Provemos que $\oplus$ está bem definida:
Seja $(g_1H, g_2H) = (k_1H, k_2H)$.
Isto implica que:

$$g_1H = k_1H \Rightarrow k_1^{-1} * g_1 \in H$$

$$g_2H = k_2H \Rightarrow k_2^{-1} * g_2 \in H$$

temos que $(k_1 * k_2)^{-1} * (g_1 * g_2) = k_2^{-1} * (k_1^{-1} * g_1) * g_2 = k_2^{-1} * (h * g_2) = k_2^{-1} * (g_2 * h') \in H$ pois, $h = k_1^{-1} * g_1 \in H$ e $Hg_2 = g_2H$.
Logo $(k_1 * k_2)^{-1} * (g_1 * g_2) \in H \Rightarrow g_1 * g_2H = k_1 * k_2H$.

Teorema 4.8. *Seja $H \triangleleft G$, onde $(G, *)$ grupo. Então $(G/H, \oplus)$ é um grupo.*

Prova:

a) Associativa: Sejam aH, bH, cH em G/H.
$[(a * h) \oplus (b * h)] \oplus cH = [(a * b)H] \oplus cH = ((a * b) * c)H = [a * (b * c)]H = (aH)[(b * c)H] = (aH) \oplus [(aH) \oplus (cH)]$

b) Elemento Neutro: Existe um elemento da forma $e_GH \in G/H$, tal que

$$(aH) \oplus (e_GH) = (a * e_G)H = aH$$

$$(e_GH) \oplus (aH) = (e_G * a)H = aH \ \forall aH \in G/H.$$

Observe que $e_GH = H$ pois $e_G \in H$.

c) Elemento oposto: $\forall aH \in G/H$, existe $a^{-1}H \in G/H$, pois $a \in G \Rightarrow a^{-1} \in G$.

$$(aH) \oplus (a^{-1}H) = (a * a^{-1})H = e_GH = H$$

$$(a^{-1}H) \oplus (aH) = (a^{-1} * a)H = e_GH = H$$

Portanto $(G/H, \oplus)$ é grupo. □

4.4 Teoremas de Isomorfismo

Teorema 4.9. ***Primeiro Teorema de Isomorfismo.*** *O núcleo K de um isomorfismo $\varphi : G \to G'$ é um subgrupo normal de G e a correspondência $xK \to \varphi(x)$ é um isomorfismo do grupo quociente G/K na imagem de φ.*

Prova: Suponhamos que $x, y \in K$, então $\varphi(x*y^{-1}) = \varphi(x)\cdot\varphi(y)^{-1} = e$, mostrando que $xy^{-1} \in K$. Certamente K é não vazio pois, $e \in K$, por isso K é um subgrupo de G pela definição 4.2. Se $x \in K$ e $g \in G$, então

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

Portanto, gxg^{-1} pertence a K e o subgrupo K é normal em G.

Se duas classes laterais xK, yK são iguais, então $y^{-1}x \in K$. Aplicando φ temos $\varphi(y^{-1} * x) = \varphi(y)^{-1} \cdot \varphi(x) = e$, e portanto $\varphi(x) = \varphi(y)$. Isto significa que temos uma função $\psi(xK) = \varphi(x)$. Invertendo o cálculo acima, mostra-se que se $\varphi(x) = \varphi(y)$, então $xK = yK$, logo ψ é injetora. Esta é um isomorfismo pois,

$$\psi(xKyK) = \psi(xyK) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(xK)\psi(yK)$$

para quaisquer duas classes laterais $xK,\ yK \in G/K$. Finalmente, a imagem de ψ é a mesma imagem de φ. Provamos que ψ é um isomorfismo de G/H na imagem de φ. □

Corolário 4.3. *Se a imagem de φ é todo G', então G/K é isomorfo a G'.*

Exemplos: Podemos verificar facilmente que cada uma das seguintes funções é um homomorfismo sobrejetor.

(i) $\mathbb{Z} \to \mathbb{Z}_n, \quad x \to x(mod\ n)$.
$K = n\mathbb{Z}$, *o conjunto de todos os múltiplos de* n, e $\mathbb{Z}/n\mathbb{Z}$ *é isomorfo a* $\mathbb{Z}_n$.

(ii) $\mathbb{R} \to S^1, \quad x \to e^{2\pi ix}$
$K = \mathbb{Z}$ e $\mathbb{R}/\mathbb{Z}$ *é isomorfo a* S^1.

(iii) $\mathbb{C} - \{0\} \to S^1, \quad z \to z/|z|$.
$K = \mathbb{R}^+$ e $\mathbb{C} - \{0\}/\mathbb{R}^+$ *é isomorfo a* S^1.

Seja O_n o grupo das matrizes reais de ordem n cujo determinante é ± 1, SO_n o grupo das matrizes reais de ordem n cujo determinando seja 1 e U_n o grupo das matrizes complexas.

(iv) $O_n \to \{\pm 1\}, \quad A \to det\, A$.
$K = SO_n$ e O_n/SO_n *é isomorfo a* $\mathbb{Z}_2$.

(v) $U_n \to \mathbb{C}, \quad A \to det\, A$.
$K = SU_n$ e U_n/SU_n *é isomorfo a* $\mathbb{C}$.

(vi) $\mathbb{C} \to \mathbb{C}, \quad z \to z^2$.
$K = \{\pm 1\}$ e $\mathbb{C}/\{\pm 1\}$ *é isomorfo a* $\mathbb{C}$.

(vii) O grupo S_4 contém três elementos de ordem 2, a saber $(12)(34), (13)(24), (14)(23)$. Juntamente com a identidade, estes elementos formam um subgrupo do S_4 que é isomorfo ao grupo de Klein (vide página 64)e que denotaremos por V. Uma conjugação de uma permutação $\theta \in S_4$ deve permutar nossos três elementos de ordem 2 entre si, pois elementos conjugados sempre têm a mesma ordem. Pelo envio de cada θ para a permutação correspondente (desses elementos de ordem 2) podemos produzir uma função de S_4 em S_3 que é um homomorfismo e sobrejetora. Seu núcleo é precisamente V e o corolário 4.3 mostra que S_4/V é isomorfo a S_3.

(viii) Um elemento de H da forma $bi+cj+dk$ é chamado "um quatérnio puro". Identifique o conjunto de todos os quatérnios puros com $\mathbb{R}^3$ através da correspondência $bi + cj + dk \to (b, c, d)$. Se q é um quatérnio diferente de zero, a conjugação de q envia os quatérnios puros em si mesmos e induz uma rotação de $\mathbb{R}^3$. Esta construção fornece um homomorfismo de $\mathbb{H} - \{0\}$ em SO_3. Sua imagem é todo o SO_3, seu núcleo é $\mathbb{R} - \{0\}$, e o corolário 4.3 mostra que $H - \{0\}/\mathbb{R} - \{0\}$ é isomorfo a SO_3.

Teorema 4.10. ***Segundo Teorema de Isomorfismo.*** *Suponha que H, J são subgrupos de G, com J normal em G. Então HJ é um subgrupo de G, $H \cap J$ é um subgrupo de H, e os grupos quocientes HJ/J e $H/H \cap J$ são isomorfos.*

Prova: Sejam g, g' elementos de HJ e escreva $g = xy$ e $g' = x'y'$, onde $x, x' \in H$ e $y, y' \in J$. Então

$$gg'^{-1} = xyy'^{-1}x'^{-1} = (xx'^{-1})(x'yy'^{-1}x'^{-1}) \in HJ,$$

pois $J \triangle G$.

Logo HJ é um subgrupo de G pela definição 4.2.

A função $\varphi : H \to HJ/J$ definida por $\varphi(x) = xJ$ é um homomorfismo. É sobrejetora pois, se $g = xy \in HJ$, com $x \in H$ e $y \in J$ e, observando que $J = yJ$ temos

$$\varphi(x) = xJ = xyJ = gJ.$$

O elemento x de H pertence ao núcleo de φ precisamente quando $xJ = J$, em outras palavras, quando $x \in J$. Portanto, o núcleo de φ é $H \cap J$ e o resultado segue do teorema 4.9. □

Teorema 4.11. ***Terceiro Teorema de Isomorfismo.*** *Sejam H, J subgrupos normais de G e suponha que H está contido em J. Então J/H é um subgrupo normal de G/H e o grupo quociente $(G/H)/(J/H)$ é isomorfo a G/J.*

Prova: A função $\varphi : G/H \to G/J$ definida por $\varphi(xH) = xJ$ é um homomorfismo e é sobrejetora. Uma classe lateral xH pertence ao núcleo de φ precisamente quando

$xJ = J$, em outras palavras, quando $x \in J$. Portanto, o núcleo de φ é J/H e o resultado segue do teorema 4.9. □

4.4.1 Aplicações dos Teoremas de Isomorfismo

Lema 4.1. *$\mathbb{Z}/p\mathbb{Z}$ é isomorfo a $\mathbb{Z}_p$.*

Prova: $p\mathbb{Z} = \{pz, \text{ com } z \text{ em } \mathbb{Z}\}$, $(\mathbb{Z}, +)$, $(\mathbb{Z}_p, +_p)$ e $\mathbb{Z}_p = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$.

Seja $\varphi : \mathbb{Z} \to \mathbb{Z}_p$
$m \to \overline{m}$
$\forall m, n \in \mathbb{Z}, \varphi(m+n) = \overline{m+n} = \overline{m} +_p \overline{n} = \varphi(m) +_p \varphi(n) \Rightarrow \varphi$ é homomorfismo.
Dado $\overline{z} \in \mathbb{Z}_p$, então $0 \leq z \leq p-1$ e $\varphi(z) = \overline{z}$. Portanto φ é sobrejetora e então é isomorfismo.
$ker\,\varphi = \{m \in \mathbb{Z}; \varphi(m) = \overline{m} = \overline{0}\} = p\mathbb{Z}$.
$\overline{m} = \overline{0} \Leftrightarrow m \equiv 0 (mod\, p) \Leftrightarrow m = kp, k \in \mathbb{Z}$.
Aplicando o primeiro Teorema do Isomorfismo, $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p$. □

Exemplo 4.21. Seja $G =< a >$ um grupo cíclico. Então
1)$G \simeq \mathbb{Z}$, se G for infinito, ou seja $G = \{e, a, a^2, ...\}$.
2)$G \simeq \mathbb{Z}_n$, se $o(G) = n$, ou seja $G = \{e, a, a^2, ..., a^{n-1}\}$.

Prova: Definamos: $\varphi : \mathbb{Z} \to G$, onde, $l \in \mathbb{Z} \to a^l \in G$.

1)φ é um homomorfismo.
Sejam $l_1, l_2 \in \mathbb{Z}, \varphi(l_1 + l_2) = a^{l_1+l_2} = a^{l_1} * a^{l_2} = \varphi(l_1) * \varphi(l_2)$.

2)φ é sobrejetora.
Seja $z \in G$, existe $k \in \mathbb{Z}$ tal que $z = a^k$. Logo $\varphi(k) = a^k = z$.

3) *i*) Suponhamos G infinito.

$$ker\ \varphi = \{l \in \mathbb{Z}/\varphi(l) = a^l = e\} = \{0\}.$$

Pelo primeiro teorema do isomorfismo, $\mathbb{Z}/\{0\} = \mathbb{Z} \simeq G$.
ii) Suponhamos agora que G tem a ordem n, $G = \{e, a, a^2, ..., a^{n-1}\}$.

$$Ker\ \varphi = \{l \in \mathbb{Z}/\varphi(l) = e\} = n\mathbb{Z}$$

Assim, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}n$ e $\mathbb{Z}/n\mathbb{Z} \simeq G \Rightarrow \mathbb{Z}n \simeq G$.

Exemplo 4.22. Provaremos que $\mathbb{R}/\mathbb{Z} \simeq S^1$.

$\mathbb{Z} \lhd \mathbb{R}$, com $(\mathbb{R}, +)$

$$S^1 = \{z \in \mathbb{C}^* || z|| = 1\} \to (S^1, \cdot)$$

$$f : \mathbb{R} \to S^1$$
$$t \to e^{2\pi it} = cos(2\pi t) + isen(2\pi t).$$

i) f é sobrejetora, pois $\forall z \in S^1, \exists\ \theta$ tal que $z = cos\theta + isen\theta$.
Para $t = \theta/2\pi$
$f(t) = f(\theta/2\pi) = cos\theta + isen\theta$.

ii) f é homomorfismo, pois $\forall t_1, t_2 \in \mathbb{R}$
$f(t_1 + t_2) = e^{2\pi i(t_1+t_2)} = e^{2\pi it_1} \cdot e^{2\pi it_2} = f(t_1) \cdot f(t_2)$.

iii) $ker\, f = \{t \in \mathbb{R}/f(t) = 1\}$. Mas, $f(t) = e^{2\pi it} = e^0 = 1$, como $e^{2\pi it} = cos2\pi t + isen2\pi t = 1 + 0i$, temos

$$cos(2\pi t) = 1 \Leftrightarrow t \in \mathbb{Z} \text{ e } sen(2\pi t) = 0$$

Portanto $ker\, f = \mathbb{Z}$.
Pelo primeiro teorema do isomorfismo, $\mathbb{R}/\mathbb{Z} \simeq S^1$.

Exemplo 4.23. Seja $G = \left(\left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z} \right\}, \cdot \right)$ um grupo. Provaremos que G é isomorfo a $\mathbb{Z}$.

Prova: $(\mathbb{Z}, +)$, definimos $\varphi : \mathbb{Z} \to G$ como $\varphi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

i) φ é homomorfismo.
Sejam $x, y \in \mathbb{Z}$, então
$\varphi(y + x) = \varphi(x + y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \varphi(y)\varphi(x)$.

ii) φ é injetora.
$Ker\, \varphi = \left\{ z \in \mathbb{Z} \mid \varphi(z) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = \{0\}$. Logo, φ é injetora.

iii) φ é sobrejetora.
Seja $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G$, tomando $a \in \mathbb{Z}$. Então $\varphi(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Portanto φ é sobrejetora.

Por $i), ii), iii)$ e concluímos que φ é um isomorfismo e portanto $\mathbb{Z} \simeq G$.

Exemplo 4.24. Seja $(S^1, \cdot), S^1 \subset \mathbb{C}^*$. Veremos que $S^1 < \mathbb{C}^*$ e que $\theta : \mathbb{C} \to S^1$ definida por $\theta(z) = z/||z||$ é homomorfismo.

Prova: Primeiramente vamos mostrar que $S^1 < \mathbb{C}^*$.

i) Fechamento.

Sejam $z_1, z_2 \in S^1$ então $||z_1|| = ||z_2|| = 1$, logo $||z_1 z_2|| = ||z_1|| \cdot ||z_2|| = 1$, portanto $z_1 z_2 \in S^1$.

ii) Elemento Neutro.

1 é o elemento neutro de $(\mathbb{C}^*, \cdot)$ e $||1|| = 1$, portanto $1 \in S^1$.

iii) Elemento Oposto.

Seja $z \in S^1$, como $\mathbb{C}^*$ é grupo, existe $z^{-1} \in \mathbb{C}^*$, veremos que $||z^{-1}|| = 1$, de fato $zz^{-1} = 1 \Rightarrow ||zz^{-1}|| = ||1|| \Leftrightarrow ||z|| \cdot ||z^{-1}|| = 1 \Rightarrow ||z^{-1}|| = 1 \Rightarrow z^{-1} \in S^1$.

Por $i), ii)$ e $iii)$ concluímos que $S^1 < \mathbb{C}^*$.

Vejamos agora que θ é homomorfismo.

Sejam $z_1, z_2 \in \mathbb{C}^*$. Então,

$\theta(z_1 z_2) = z_1 z_2/||z_1 z_2|| = z_1/||z_1|| \cdot z_2/||z_2|| = \theta(z_1) \cdot \theta(z_2)$. Portanto θ é homomorfismo.

Sendo $H = Ker\ \theta$ veremos aH geometricamente.

$Ker\ \theta = \{z \in \mathbb{C} | \theta(z) = 1\} = \mathbb{R}_+^*$.

Geometricamente, $aH = \{a + r; r \in \mathbb{R}_+^*\}$ é a semirreta abaixo (figura 4.15).

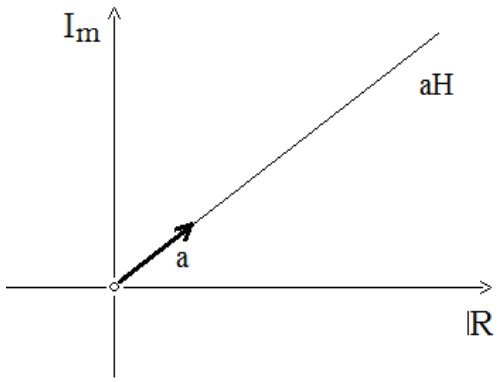
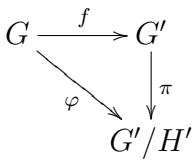


Figura 4.15: Semirreta aH

Exemplo 4.25. Consideremos $(G, *)$, $(G', \triangle)$ e $f : G \to G'$ epimorfismo.

Se $H' < G'$, provaremos que $G/f^{-1}(H') \simeq G'/H'$.

$f^{-1}(H') < G$.



Definamos $\varphi : G \to G'/H'$ por $\varphi(x) = f(x) \triangle H'$.

i) φ é homomorfismo, $\forall x, y \in G$, $\varphi(x+y) = f(x*y) \triangle H' = f(x) \triangle f(y) \triangle H' = f(x) \triangle H' + f(y) \triangle H' = \varphi(x) + \varphi(y)$.

ii) φ é sobrejetora. Seja $\alpha \in G'/H'$, então $\alpha = g' \triangle H'$, $g' \in G'$, como f é sobrejetora, $\exists a \in G$, tal que $f(a) = g'$. Logo

$$\varphi(a) = f(a) \triangle H' = g' * H' = \alpha.$$

Portanto φ é epimorfismo.

iii) $Ker\,\varphi = \{x \in G | \varphi(x) = H'\} = \{x \in G | f(x) \triangle H' = H'\} = f^{-1}(H')$.
$f(x) \triangle H' = H' \Leftrightarrow f(x) \in H' \Leftrightarrow x \in f^{-1}(H')$.
Assim, pelo primeiro Teorema do Isomorfismo segue que

$$G/Ker\,\varphi \simeq G'/H' \Rightarrow G/f^{-1}(H') \simeq G'/H'.$$

Exemplo 4.26. Seja $(G, *)$ um grupo. Fixando $a \in G$, definimos:
$\sigma_a : G \to G$ por $\sigma_a(x) = a * x * a^{-1}, \forall x \in G$.

1) σ_a é um isomorfismo.

Prova: *i)* σ_a é homomorfismo. De fato, sejam $x, y \in G$, $\sigma_a(x*y) = a*x*y*a^{-1} = a*x*a^{-1}*a*y*a^{-1} = \sigma_a(x) * \sigma_a(y)$.

ii) σ_a é injetora. De fato, $Ker\,\sigma_a = \{x \in G | \sigma_a(x) = e_G\} = \{e_G\}$.
Mas, $\sigma_a(x) = a * x * a^{-1}$, portanto $x = e_G$

iii) σ_a é sobrejetora. De fato, $\forall x \in G$, tomemos $y = a^{-1} * x * a$. Então

$$\sigma_a(y) = a * y * a^{-1} = a * a^{-1} * x * a * a^{-1} = x.$$

2) Denotando $I(G) = \{\sigma_a; a \in G\}$, veremos que $(I(G), \circ)$ é um grupo.

i) (Associativa). Sejam $\sigma_a, \sigma_b, \sigma_c \in I(G)$, então
$((\sigma_a \circ \sigma_b) \circ \sigma_c)(x) = (\sigma_a \circ \sigma_b)(c*x*c^{-1}) = \sigma_a(b*c*x*c^{-1}*b^{-1}) = a*(b*c)*x*(c^{-1}*b^{-1})*a^{-1} = a*(b*\sigma_c(x)*b^{-1})*a^{-1} = a*((\sigma_b \circ \sigma_c)(x))*a^{-1} = (\sigma_a \circ (\sigma_b \circ \sigma_c))(x) \Rightarrow$

$(\sigma_a \circ \sigma_b) \circ \sigma_c = \sigma_a \circ (\sigma_b \circ \sigma_c)$.

ii) (Elemento neutro). σ_e é o elemento neutro, pois $\sigma_e \circ \sigma_a = \sigma_a$, de fato
$\forall x \in G, (\sigma_e \circ \sigma_a)(x) = \sigma_e(\sigma_a(x)) = \sigma_e(a*x*a^{-1}) = e*a*x*a^{-1}*e^{-1} = a*x*a^{-1} = \sigma_a(x)$. e
$\sigma_a \circ \sigma_e = \sigma_a$, pois $\forall x \in G, (\sigma_a \circ \sigma_e)(x) = \sigma_a(e*x*e^{-1}) = \sigma_a(x)$.

iii) (Elemento inverso). Seja $\sigma_a \in I(G)$ então o elemento inverso de σ_a é $\sigma_{a^{-1}}$, de fato
$(\sigma_a \circ \sigma_{a^{-1}})(x) = \sigma_a(a^{-1} * x * (a^{-1})^{-1}) = a * a^{-1} * x * a * a^{-1} = (\sigma_{a^{-1}} \circ \sigma_a)(x) = \sigma_{a^{-1}}(a*x*a^{-1}) = a^{-1}*a*x*a^{-1}*a = x = \sigma_e(x)$. Ou seja, $\sigma_a \circ \sigma_{a^{-1}} = \sigma_e = \sigma_{a^{-1}} \circ \sigma_a$.

Portanto $I(G)$ é um grupo.

3) Seja $A(G) = \{f : G \to G; \text{isomorfismo}\}$, com a operação composição. Mostraremos que $I(G) \triangle A(G)$.
Prova: $I(G) \triangle A(G) \Leftrightarrow f \circ I(G) \circ f^{-1} \subset I(G), \forall f \in A(G)$.
Seja $h \in f \circ I(G) \circ f^{-1}$ então $h = f \circ \sigma_a \circ f^{-1}$ mas, $h(x) = (f \circ \sigma_a \circ f^{-1})(x) = (f \circ \sigma_a)(f^{-1}(x)) = f(a * f^{-1}(x) * a^{-1}) = f(a) * ff^{-1}(x) * f(a^{-1}) = f(a) * x * [f(a)]^{-1} = \sigma_{f(a)}(x)$.
Logo
$h = \sigma_{f(a)} \in I(G)$. Portanto $I(G) \triangle A(G)$.

4) Provaremos que $G/cent\,(G) \simeq I(G)$, com $cent\,(G) = \{c \in G; c*x = x*c, \forall x \in G\}$.
Prova: Defina $\varphi : G \to I(G)$, tal que $\varphi(a) = \sigma_a$

i) φ é homomorfismo. De fato, $\forall a, b \in G, \varphi(a*b) = \sigma_{a*b} = \sigma_a \circ \sigma_b = \varphi(a) \circ \varphi(b)$.

ii) φ é sobrejetora. De fato, seja $\sigma_a \in I(G)$, então $a \in G$ e $\varphi(a) = \sigma_a$

iii) $Ker\,\varphi = \{a \in G | \varphi(a) = \sigma_e\} = cent\,(G)$.
$\varphi(a) = \sigma_e \Leftrightarrow \sigma_a = \sigma_e \Leftrightarrow \sigma_a(x) = \sigma_e(x) = x, \forall x \in G$
$\sigma_a(x) = a*x*a^{-1} = x \Rightarrow ax = xa \forall x \in G \Rightarrow a \in cent\,(G)$.
Logo pelo primeiro Teorema do Isomorfismo
$G/cent\,(G) \simeq I(G)$.

Exemplo 4.27. $\mathbb{Q}/\mathbb{Z}$ é um grupo infinito no qual todo elemento tem ordem finita.
Prova: $\mathbb{Q}/\mathbb{Z} = \{p/q + \mathbb{Z}; p/q \in \mathbb{Q}\} = \{\mathbb{Z}, p/q + \mathbb{Z}; (p,q) = 1\}$ é infinito pois existem infinitos racionais (tem a mesma cardinalidade).

Seja $p/q+\mathbb{Z}$ em $\mathbb{Q}/\mathbb{Z}$. Note que $(p/q+\mathbb{Z})^{|q|}=\mathbb{Z}$ e portanto $p/q+\mathbb{Z}$ tem ordem $|q|$, ou seja, finita.

4.5 Teorema de Cayley

Definamos $f_a : G \to G$ por $f_a(x) = a * x$, para todo x pertencente a G, que é bijetora, pois $f_a(x) = f_a(y) \Rightarrow a*x = a*y$, pela lei do cancelamento, $x = y$, para todo $y \in G$, $x = a^{-1}*y \in G$ e $f_a(x) = f_a(a^{-1}*y) = a*a^{-1}*y = y$. Além disso, $f_a \circ f_b = f_{a*b}$. De fato, para todo $x \in G$, $(f_a \circ f_b)(x) = f_a(b*x) = a*(b*x) = (a*b)*x = f_{a*b}(x)$.

Seja $F_G = \{f_a, a \in G\}$ com a composição de funções. F_G é um grupo.

Na realidade $F_G < S_G$, onde S_G é o grupo das permutações de G, definido na página 40.

De fato, a função $f_e, e \in G$ é a permutação identidade, que pertence a F_G.

Também se f_a, f_b são dois elementos quaisquer de F_G então $f_a \circ (f_b)^{-1} = f_a \circ f_{b^{-1}} = f_{a*b^{-1}}$ que pertence a F_G.

Teorema 4.12. ***Teorema de Cayley****: Se G é um grupo, então G é isomorfo a um subgrupo do S_G.*

Prova:

Definimos $\varphi : G \to F_G$ por $\varphi(a) = f_a$.

Temos: $\varphi(a*b) = f_{a*b} = f_a \circ f_b = \varphi(a) \circ \varphi(b)$, logo é um homomorfismo.

O $Ker\,\varphi = \{a \in G/\varphi(a) = f_e\}$, o que implica $f_a = f_e \Leftrightarrow \forall x \in G, f_a(x) = f_e(x) \Rightarrow a*x = x \Rightarrow a = e$, logo é injetora.

$\forall f_a \in F_G$, temos $a \in G$ e $\varphi(a) = f_a$, logo é sobrejetora.

Portanto φ é um isomorfismo. □

Exemplo: Todo grupo de simetria de um sólido regular é um grupo de permutação. Além disso, pelo Teorema de Cayley, todo grupo é isomorfo a algum subgrupo do grupo de permutações.

Teorema 4.13. *Se G é um grupo finito de ordem n, então G é isomorfo a um subgrupo de S_n.*

Prova: Se os elementos de G são enumerados $1, 2, ..., n$ de alguma forma, então cada permutação de G induz uma permutação de $1, 2, ..., n$. Isto nos dá um isomorfismo de S_G para S_n e o subgrupo G' de S_G é portanto isomorfo a um subgrupo G'' de S_n. Como G é isomorfo a G', e como a composição de dois isomorfismos é um isomorfismo, G é isomorfo a G''. □

Teorema 4.14. ***Teorema de Cauchy:*** *Se p é um divisor primo da ordem de um grupo finito G, então G contém um elemento de ordem p.*

Prova: Precisamos de um elemento $x \in G - \{e\}$ tal que $x^p = e$. Considere o conjunto X formado por todas as sequências ordenadas $x = (x_1, x_2, ..., x_p)$ de elementos de G para o qual $x_1 x_2 \cdots x_p = e$. Nosso problema é encontrar uma sequência que possua todas as coordenadas iguais, mas que não seja $(e, e, ..., e)$. Para isto, vamos analisar o tamanho de X. Se a sequência $(x_1, x_2, ..., x_p)$ é para estar em X podemos escolher $x_1, x_2, ..., x_{p-1}$ arbitrariamente de G e então x_p é completamente determinado por $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$. Logo, o número de sequências em X é $|G|^{p-1}$, que é um múltiplo de p.

Seja $\Re$ um subconjunto de $X \times X$ definido da seguinte forma. Um par ordenado (x, y) pertence a $\Re$ se y pode ser obtido por uma permutação cíclica das coordenadas de x (x e y são p-úplas de elementos de G).

Em outras palavras y é uma das

$$\begin{array}{c} (x_1, x_2, ..., x_p) \\ (x_p, x_1, ..., x_{p-1}) \\ \vdots \\ (x_2, ..., x_p, x_1) \end{array} \qquad (*)$$

Note que todas estas permutações cíclicas pertencem a X. Por exemplo,

$$x_p x_1 \cdots x_{p-1} = x_p (x_1 \cdots x_{p-1} x_p) x_p^{-1} = x_p e x_p^{-1} = e$$

mostra que $(x_p x_1 \cdots x_{p-1}) \in X$, e repetimos este processo da mesma forma com as outras sequências.

É fácil ver que $\Re$ é uma relação de equivalência em X e que a classe de equivalência $\Re(x)$ das sequências x $= (x_1, x_2 \cdots x_p)$ é precisamente a coleção $(*)$.

Se fizermos permutações cíclicas das coordenadas de uma sequência, sempre vamos gerar p sequência diferentes? Certamente não, no caso de $e = (e, e, ..., e)$ onde permutando ciclicamente as entradas não temos nada de novo, e $\Re(e)$ contém apenas um elemento. As distintas classes de equivalência de $\Re$ constituem uma partição de X.

Somando os tamanhos dessas classes temos o total de elementos em X. Se cada classe de equivalência de $\Re(e)$ contém p elementos, então o tamanho de X será congruente a 1 módulo p, contradizendo nosso cálculo anterior. Portanto, deve haver uma sequência $x = (x_1, x_2, ..., x_p)$, que não seja e, cuja classe de equivalência contém menos que p elementos. Então duas das permutações cíclicas em $(*)$ são iguais, dizemos

$$(x_{r+1}, ..., x_p, x_1, ..., x_r) = (x_{s+1}, ..., x_p, x_1, .., x_s)$$

Assumindo $r > s$ e repetindo o ciclo $p - r$ vezes para dar

$$(x_1, x_2, ..., x_p) = (x_{k+1}, ..., x_p, x_1, ..., x_k)$$

onde $k = p - r + s$. Igualando as coordenadas correspondentes observamos que $x_i = x_{k+i(mod\ p)}$ para $1 \leq i \leq p$, e consequentemente

$$(x_1, x_2, ..., x_p) = (x_{k+1}, ..., x_p, x_1, ..., x_s)$$

onde os índices são lidos "módulo p". Suponhamos $ak + 1$ e $bk + 1$ congruentes módulo p com $0 \leq a \leq b \leq p - 1$. Então p divide $(b - a)k$, o que é impossível, pois p é primo e ambos $b - a$ e k são menores que p. Portanto os números

$$1, k + 1, 2k + 1, ..., (p - 1)k + 1$$

são todos diferentes quando lidos módulo p. Como existem p deles, lê-los módulo p dá apenas $1, 2, ..., p$ possibilidades.

Concluímos que $x_1 = x_2 = ... = x_p$, isto nos dá $x_1^p = e$ como queríamos. □

4.5.1 Conjugação

Vamos começar com o seguinte problema. Suponha que R_L é a reflexão em torno da reta L no plano complexo $\mathbb{C}$ e que f é uma isometria de $\mathbb{C}$. Qual é a fórmula para a reflexão $R_{f(L)}$ em torno da reta $f(L)$? Considere a aplicação fR_Lf^{-1}. Ela é uma isometria que fixa todo ponto da forma $f(z)$, onde $z \in L$. Assim, fR_Lf^{-1} é uma isometria que fixa todo ponto de $f(L)$ e assim ou é a identidade I ou $R_{f(L)}$. Mas $fR_Lf^{-1} \neq I$, pois do contrário $R_L = I$, assim $fR_Lf^{-1} = R_{f(L)}$. Um argumento similar mostra que se $f(z) = e^{i\theta}z$, uma rotação em torno da origem, e se $g(z) = z - a$, então gfg^{-1} é uma rotação em torno do ponto $a \in \mathbb{C}$. Estes são exemplos de conjugação em um grupo, que é muito importante em grupos abstratos.

Definição 4.11. *Seja G um grupo e suponha que f e g estão em G. Dizemos que f e g são conjugados em G se existe algum h em G tal que $f = hgh^{-1}$. A classe de conjugação de g, denotada por $[g]$, é o conjunto $\{hgh^{-1} : h \in G\}$ de todos os conjugados de g. Finalmente, subgrupos H_1 e H_2 são subgrupos conjugados de G se, para algum $h \in G$, tem-se $H_1 = hH_2h^{-1}$.*

Observemos que se f e g são conjugados, então $f^n = (hgh^{-1})^n = hg^nh^{-1}$, assim $f^n = e$ se, e somente se, $g^n = e$. Assim, elementos conjugados tem a mesma ordem.

Teorema 4.15. *A relação de conjugação em um grupo G é uma relação de equivalência, assim G é a união disjunta de classes de conjugação mutuamente disjuntas.*

Prova: Seja $\Re$ o subconjunto de $G \times G$ formado pelos pares (x, y) tal que x é conjugado de y. Cada $x \in G$ é conjugado de si mesmo, pois $exe^{-1} = x$. Se x é conjugado de y, $gxg^{-1} = y$, então y é conjugado de x, pois $g^{-1}yg = x$. Finalmente, se x é conjugado de y e y é conjugado de z, $g_1xg_1^{-1} = y$, $g_2yg_2^{-1} = z$, então x é conjugado de z, pois

$$(g_2g_1)x(g_2g_1)^{-1} = g_2(g_1xg_1^{-1})g_2^{-1} = g_2yg_2^{-1} = z.$$

Portanto, $\Re$ é uma relação de equivalência em G.

Desta forma, um subgrupo H de G é normal se, e somente se, H é uma reunião de classes de conjugação. □

Exemplo 4.28. Seja G o grupo diedral D_6. Os elementos de D_6 são

$$e, r, r^2, r^3, r^4, r^5$$

$$s, rs, r^2s, r^3s, r^4s, r^5s$$

e a multiplicação é completamente determinada, uma vez que sabemos $r^6 = e, s^2 = e, sr = r^5s$. Para encontrar a classe de conjugação de uma potência de r, dizemos r^a onde $1 \leq a \leq 5$, devemos calcular gr^ag^{-1}, para algum g em D_6. Se g é a identidade ou uma potência de r, obtemos r^a novamente. Tomando $g = s$ (e relembrando que $s^{-1} = s$) temos

$$sr^as = r^{6-a}s^2 = r^{6-a}.$$

Finalmente, se $g = r^bs$, onde $1 \leq b \leq 5$, então

$$(r^bs)r^a(r^bs)^{-1} = r^b(sr^as)r^{6-b} = r^b(r^{6-a})r^{6-b} = r^{6-a}.$$

Portanto, a classe de conjugação de r^a é $\{r^a, r^{6-a}\}$. Para os elementos restantes note que,

$$r^bsr^{-b} = r^br^bs = r^{2b}s$$

e

$$r^b(rs)r^{-b} = r^{b+1}r^bs = r^{2b+1}s.$$

Conjugações por r^bs enviam s em $r^{2b}s$, $(r^bs)s(r^bs)^{-1} = r^{2b}s$, e enviam rs em $r^{2b-1}s$, $(r^bs)rs(r^bs)^{-1} = r^{2b-1}s$. Portanto , os elementos s, r^2s, r^4s formam uma classe de conjugação, como fazem rs, r^3s, r^5s. Em resumo, as classes de conjugação do D_6 são

$$\{e\}, \{r, r^5\}, \{r^2, r^4\}, \{r^3\}, \{s, r^2s, r^4s\}, \{rs, r^3s, r^5s\}.$$

Teorema 4.16. *O grupo diedral D_{2n} tem uma classe de conjugação de reflexões se n é ímpar e duas classes de conjugação, se n é par.*

Prova: O grupo D_{2n} é gerado pela rotação $r(z) = e^{2\pi i/n}z$ e pela reflexão $\sigma(z) = \overline{z}$ no eixo real e elas satisfazem $r^m\sigma = \sigma r^{-m}$ para todo inteiro m. Agora D_{2n} contém exatamente n reflexões, $\sigma, r\sigma, \cdots, r^{n-1}\sigma$ e então:

a) se k é par, então $r^k\sigma$ é conjugado a σ;

b) se k é ímpar, então $r^k\sigma$ é conjugado a $r\sigma$;

c) $r\sigma$ é conjugado a σ se, e somente se, n é ímpar.

Primeiro, se $k = 2q$, então $r^k\sigma = r^q(r^q\sigma) = r^q(\sigma r^{-q}) = r^q\sigma r^{-q}$. Segundo, se $k = 2q+1$, então $r^k\sigma = (r^{q+1})(r^q\sigma) = r^q(r\sigma)r^{-q}$, que prova b). E se $n = 2m-1$, então $r^m\sigma r^{-m} = r^{2m}\sigma = r^{n+1}\sigma = r\sigma$. Reciprocamente, se $r\sigma = r^p\sigma r^{-p}$, para algum p, então $r\sigma = r^{2p}\sigma$, assim $r^{2p-1} = e$. Assim, n divide $2p-1$ e n deve ser ímpar. □

Exemplo 4.29. Dois elementos de S_n são ditos ter a mesma estrutura cíclica se, quando são decompostos como produtos de permutações cíclicas disjuntas, ambos possuem o mesmo número de $2-ciclos$, o mesmo número de $3-ciclos$, e assim por diante. Se $\theta, \varphi \in S_n$ possuem a mesma decomposição cíclica, escreva as decomposições cíclicas de φ e θ tomando os ciclos em ordem decrescente. Em ambos os casos incluem os inteiros fixados a esquerda pela permutação como ciclos de comprimento 1. Seja g o elemento de S_n que envia cada inteiro mencionado em θ no inteiro verticalmente abaixo em φ. Então $g\theta g^{-1} = \varphi$ pois ao movimentar um inteiro de φ para θ, empurrando ao longo de uma posição em θ, então voltando para φ é o mesmo que mover ao longo de uma posição em φ. Portanto, permutações que possuem a mesma estrutura cíclica são conjugadas em S_n.

Aqui está um cálculo específico. As permutações $\theta = (67)(2539)(14)$, $\varphi = (12)(38)(5467)$ são ambas elementos de S_9 e possuem a mesma estrutura cíclica consistindo de duas transposições mais um $4-ciclo$. Nosso procedimento dá

$$\begin{array}{ll} (2539)(67)(14)(8) & \downarrow g \\ (5467)(12)(38)(9) & \end{array}$$

e lemos $g = (136)(254897)$. Assim, $g\theta g^{-1}(1) = g\theta(6) = g(7) = 2 = \varphi(1), etc.$

O elemento g não é único. Escrevendo θ como $(2539)(14)(67)(8)$ e mantendo φ a mesma temos $g = (254)(36)(789)$.

Reciprocamente, permutações conjugadas têm a mesma estrutura cíclica. De fato, seja $\theta = \theta_1\theta_2\cdots\theta_t$ um elemento de S_n escrito como um produto de permutação cíclicas disjuntas. Para qualquer $g \in S_n$ temos

$$g\theta g^{-1} = g(\theta_1\theta_2\cdots\theta_t)g^{-1} = (g\theta_1 g^{-1})(g\theta_2 g^{-1})\cdots(g\theta_t g^{-1}).$$

Assumindo que θ_i possui comprimento k, $\theta_i = (a_1a_2\cdots a_k)$, então

$$\begin{array}{c} g\theta_i g^{-1}(g(a_1)) = g\theta_i(a_1) = g(a_2), \\ g\theta_i g^{-1}(g(a_2)) = g\theta_i(a_2) = g(a_3), \\ \vdots \\ g\theta_i g^{-1}(g(a_k)) = g\theta_i(a_k) = g(a_1). \end{array}$$

também, se m não é um dos $g(a_1), ..., g(a_k)$ então θ_i fixa $g^{-1}(m)$ e

$$g\theta_i g^{-1}(m) = gg^{-1}(m) = m.$$

Portanto, $g\theta_i g^{-1} = (g(a_1)g(a_2)\cdots g(a_k))$, uma permutação cíclica de mesmo comprimento que θ_i. Desde que $g\theta_1 g^{-1}, g\theta_2 g^{-1}, ..., g\theta_t g^{-1}$ são claramente disjuntas, concluímos que $g\theta g^{-1}$ tem a mesma estrutura cíclica que θ.

Exemplo 4.30. Do exemplo anterior sabemos que as classes de conjugação do S_4 são
$\{\varepsilon\}$
$\{(12),(13),(14),(23),(24),(34)\}$
$\{(123),(132),(142),(124),(134),(143),(243),(234)\}$
$\{(1234),(1432),(1243),(1342),(1324),(1423)\}$
$\{(12)(34),(13)(24),(14)(23)\}$.

E sobre as classes de conjugação do A_4? Devemos ter cuidado, se $\theta, \varphi \in A_4$ tem a mesma estrutura cíclica, existe certamente um elemento $g \in S_4$ tal que $g\theta g^{-1} = \varphi$, mas pode não ser possível produzir uma mesma permutação g com estas propriedades. Por exemplo se $g(123)g^{-1} = (132)$, então $(g(1)g(2)g(3)) = (132)$ e g deve ser uma das transposições $(23),(13),(12)$. Então g não pode estar em A_4. As classes de conjugação do A_4 são

$\{\varepsilon\}$
$\{(123),(142),(134),(243)\}$
$\{(132),(124),(143),(234)\}$
$\{(12)(34),(13)(24),(14)(23)\}$

Estas classes possuem uma interpretação geométrica simples. Identifique A_4 com o grupo de simetria rotacional de um tetraedro regular da forma usual. Dado um eixo de simetria através de um dos vértices, podemos girar por $2\pi/3$ para que , quando visto a partir do vértice em questão, a face oposta move-se no sentido horário. As quatro rotações desse tipo são conjugadas, como são as outras quatro, onde as faces se movem no sentido contrário. Essas classes correspondem às duas classes de conjugação distintas de quatro $3-ciclos$. A rotação identidade forma uma classe de conjugação por si só, e as classes restantes consistem de três rotações por π sobre os eixos determinados pelos pontos médios de pares de arestas opostas.

4.6 Produtos

O produto direto $G \times H$ de dois grupos G e H é constituído por pares ordenados (g,h), onde $g \in G$ e $h \in H$ e com a multiplicação definida por

$$(g,h)(g',h') = (gg',hh'), \forall g,g' \in G; \forall h,h' \in H.$$

A propriedade associativa segue diretamente da associatividade de G e H. O par (e,e) é a identidade, e (g^{-1},h^{-1}) é o inverso de (g,h). Então $G \times H$ com esta operação

é um grupo.

A correspondência $(g,h) \to (h,g)$ deixa claro que $G \times H$ é isomorfo a $H \times G$. Se G ou H for um grupo infinito, então $G \times H$ é infinito, por outro lado a ordem de $G \times H$ é o produto da ordem de G pela ordem de H. Se G e H são ambos abelianos, então $G \times H$ é abeliano. Também G é isomorfo ao subgrupo $\{(g,e)/g \in G\}$ de $G \times H$ pela correspondência $g \to (g,e)$, e H é isomorfo ao subgrupo $\{(e,h)/h \in H\}$ por $h \to (e,h)$. Uma vez que todo subgrupo de um grupo abeliano é abeliano, temos que se $G \times H$ é abeliano, então ambos G e H são abelianos. O produto direto $G_1 \times \cdots \times G_n$ de uma coleção finita de grupo tem elementos $(x_1, \cdots, x_n)$ onde $x_i \in G_i$, $1 \leq i \leq n$, que são operados segundo a lei:

$$(x_1, \cdots, x_n)(x_1', \cdots, x_n') = (x_1x_1', \cdots, x_nx_n').$$

Novamente, se alterarmos a ordem dos fatores sempre teremos um grupo isomorfo.

Exemplo 4.31. $\mathbb{Z}_2 \times \mathbb{Z}_3$ possui seis elementos, $(\overline{0},\overline{0}), (\overline{1},\overline{0}), (\overline{0},\overline{1}), (\overline{1},\overline{1}), (\overline{0},\overline{2}), (\overline{1},\overline{2})$ com a operação

$$(x,y) + (x',y') = (x +_2 x', y +_3 y').$$

Usaremos $+$ para a estrutura de grupo, uma vez que temos "adição" em cada fator. Adicionando o elemento $(1,1)$ várias vezes com ele mesmo podemos completar todo o grupo. Portanto, $\mathbb{Z}_2 \times \mathbb{Z}_3$ é cíclico e isomorfo ao $\mathbb{Z}_6$. Um específico isomorfismo entre $\mathbb{Z}_2 \times \mathbb{Z}_3$ e $\mathbb{Z}_6$ é dado por

$$\begin{array}{lll} (0,0) \to 0 & (1,1) \to 1 & (0,2) \to 2 \\ (1,0) \to 3 & (0,1) \to 4 & (1,2) \to 5 \end{array}$$

Exemplo 4.32. De forma semelhante podemos escrever os quatro elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ como $(0,0), (1,0), (0,1), (1,1)$, desta vez se tratando da adição módulo 2 em ambas as coordenadas. Cada elemento diferente da identidade possui ordem 2, logo o grupo não é cíclico.

$\mathbb{Z}_2 \times \mathbb{Z}_2$ as vezes é chamado de **grupo de Klein**.

Exemplo 4.33. Vamos agora escrever $\mathbb{R}^n$ como produto direto de n cópias de $\mathbb{R}$. Os elementos de $\mathbb{R}^n$ são vetores $x = (x_1, \cdots, x_n)$ e a operação do grupo é a adição de vetores

$$x + y = (x_1 + y_1, \cdots x_n + y_n).$$

Teorema 4.17. *$\mathbb{Z}_m \times \mathbb{Z}_n$ é cíclico se, e somente se, $(m,n) = 1$, onde $(,)$ denota o maior divisor comum entre m e n.*

Prova: Seja k a ordem do elemento $(1,1)$ em $\mathbb{Z}_m \times \mathbb{Z}_n$. Adicionando $(1,1)$ k vezes teremos $(0,0)$, em outras palavras

$$(k(mod\, m), k(mod\, n)) = (0,0).$$

Isto significa que m e n são ambos fatores de k. Se o maior divisor comum de m e n é 1, então mn pode ser um divisor de k, e portanto $k = mn$. Logo, neste caso $(1,1)$ gera $\mathbb{Z}_m \times \mathbb{Z}_n$ e teremos um grupo cíclico. Agora seja d o maior divisor comum de m e n, e suponhamos que d seja maior que 1. Mostraremos que $\mathbb{Z}_m \times \mathbb{Z}_n$ não é cíclico. Sejam $m' = m/d$ e $n' = n/d$. Para qualquer elemento (x,y) de $\mathbb{Z}_m \times \mathbb{Z}_n$, temos

$$m'dn'(x,y) = (m'dn'x(mod\, m), m'dn'y(mod\, n)) = (mn'x(mod\, m), m'ny(mod\, n)) = (0,0)$$

Então a ordem de (x,y) é $m'dn'$. Portanto, $\mathbb{Z}_m \times \mathbb{Z}_n$ não contém um elemento de ordem mn e consequentemente não é cíclico. □

Exemplo 4.34. Seja I a matriz identidade 3×3 e vamos denotar por J a matriz $-I$. Ambas I e J comutam com todas as matrizes em O_3, e juntas formam um subgrupo de O_3 de ordem 2. Vamos mostrar que O_3 é isomorfo ao produto direto de SO_3 e este é subgrupo. Definimos

$$\varphi : SO_3 \times \{I, J\} \to O_3 \text{ por } \varphi(A,U) = AU,$$

onde $A \in SO_3$ e $U \in \{I,J\}$. Então φ preserva a estrutura algébrica envolvida, pois,

$$\varphi(A,U)(B,V) = \varphi(AB,UV) = ABUV = AUBV = \varphi(A,U)\varphi(B,V)$$

para todo $A, B \in SO_3$ e $U, V \in \{I,J\}$. Se $\varphi(A,U) = \varphi(B,V)$, então $AU = BV$, logo $det\ (AU) = det\ (BV)$. Mas

$$det\ (A \cdot U) = det\ (A) \cdot det\ (U) = det\ (U)$$

pois, $A \in SO_3$, e da mesma forma $det\ (BV) = det\ (V)$. Por isso, $U = V, A = B$, e concluímos que φ é injetora. Só nos resta checar que φ é sobrejetora. Dado $A \in O_3$, ou $A \in SO_3$, neste caso $A = \varphi(A,I)$, ou $AJ \in SO_3$ e $A = \varphi(AI,J)$. Isto completa o argumento.

Notamos que $\{I,J\}$ é isomorfo a $\mathbb{Z}_2$, enviando I em 0 e J em 1. Portanto, O_3 é isomorfo a $SO_3 \times \mathbb{Z}_2$ quando n é ímpar. Para n par este resultado não é válido.

Teorema 4.18. *Se H e K são subgrupos de G para o qual $HK = G$, se eles possuem apenas o elemento identidade em comum, e se todos os elementos de H comutam com todos os elementos de K, então G é isomorfo a $H \times K$.*

Prova: Definamos $\varphi : H \times K \to G$ por $\varphi(x,y) = xy$ para todo $x \in H, y \in K$. Então

$$\varphi((x,y)(x^{'},y^{'})) = \varphi(xx^{'},yy^{'}) = xx^{'}yy^{'} = xyx^{'}y^{'} = \varphi(x,y)\varphi(x^{'},y^{'}).$$

Dessa forma φ leva a multiplicação de $H \times K$ na mesma operação de G. Se $\varphi(x,y) = \varphi(x^{'},y^{'})$, então $xy = x^{'}y^{'}$ e, portanto,

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

Como o lado esquerdo pertence a H e o lado direito pertence a K, ambos pertencem a $H \cap K$ e portanto deve ser a identidade. Assim, $x = x^{'}$, $y = y^{'}$ e φ é injetora. Sabemos também que $HK = G$, o que significa que todo elemento de G pode ser escrito como um produto de $x \cdot y$ para algum $x \in H, y \in K$. Portanto, φ é sobrejetora e nos dá um isomorfismo de $H \times K$ em G. □

Como uma aplicação do teorema de Cauchy, mostraremos que um grupo de ordem 6 deve ser cíclico ou diedral.

Teorema 4.19. *Um grupo de ordem 6 é isomorfo ao $\mathbb{Z}_6$ ou isomorfo ao D_3.*

Prova: Seja G um grupo que contém 6 elementos. Usaremos o teorema de Cauchy para selecionar um elemento x de ordem 3 e um elemento y de ordem 2. As classe laterais $< x >$, $< x > y$ nos dão seis elementos

$$e, x, x^2, y, xy, x^2y$$

que preenchem G. Agora yx é um desses seis elementos e certamente não está em $< x >$ nem é igual a y. Se $yx = xy$, então 4.18 mostra que G é isomorfo a $< x > \times < y >$, e por isso $\mathbb{Z}_3 \times \mathbb{Z}_2$ é cíclico por 4.17. Por outro lado $yx = x^2y$ e trocando x por r e y por s temos um isomorfismo de G e D_3. □

Não é muito difícil de mostrar que se p é um primo ímpar, então qualquer grupo de ordem $2p$ pode ser cíclico ou diedral (ver seção 4.3).

Temos uma boa quantidade de informações sobre grupos de pequena ordem. Qualquer grupo de ordem 2,3,5 ou 7 é cíclico pelo corolário 4.2, um grupo de ordem 4 é isomorfo ao $\mathbb{Z}_4$ ou grupo de Klein, e qualquer grupo de ordem 6 é cíclico ou diedral. A situação para ordem 8 é mais complicada. Temos a união de quatro grupos, cada um com 8 elementos, são eles, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e D_4.

Um quatérnio (ou número híper - complexo) é uma expressão da forma

$$a + bi + cj + dk,$$

onde a, b, c, d são números reais e i, j, k satisfazem

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k. \qquad (*)$$

O conjunto de todos os quartérnios é denotado por $\mathbb{H}$ (vide exemplo 4.15).

Os oito símbolos $\pm 1, \pm i, \pm j, \pm k$, quando multiplicados entre si de acordo com $(*)$ formam um grupo $\mathbf{Q}$.

O grupo $\mathbf{Q}$ não é abeliano (por isso não pode ser isomorfo a $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) e como ± 1 são os únicos elementos de ordem 2, este não é isomorfo ao D_4, que contém 5 elementos de ordem 2.

Teorema 4.20. *Um grupo de ordem 8 é isomorfo a algum dos seguintes grupos:* $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4 *e* $\mathbf{Q}$.

Prova: Seja G um grupo que possui oito elementos. Se existe um elemento de ordem 8, então G é isomorfo ao $\mathbb{Z}_8$. Suponhamos que a maior ordem de um elemento de G é 4. Escolhemos um elemento x cuja ordem é 4 e um elemento y de $G - < x >$. As classes $< x >$, $< x > y$ preenchem G e fornecem os elementos

$$e, x, x^2, x^3, y, xy, x^2y, x^3y.$$

Sabemos que yx não está em $< x >$, não pode ser igual a y (pois, se $yx = y$ nos dá $x = e$) e não pode ser igual a x^2y (pois, se $yx = x^2y$, leva em $x = y^{-1}x^2y$, que por sua vez nos dá $x^2 = y^{-1}x^2yy^{-1}x^2y = e$). Portanto, yx é xy ou x^3y. Além da ordem do elemento y ser 2 ou 4. Observe que y^2 não pode pertencer a $< x > y$ (y não pertende a $< x >$) e não pode ser igual a x ou x^3 (pois a ordem de y não é 8). Então se y possui ordem 4, então $y^2 = x^2$. Por isso temos quatro possibilidades:

i) Se $yx = xy$ e $y^2 = e$, o grupo é abeliano e $x \to (1,0),\ y \to (0,1)$ leva um isomorfismo entre G e $\mathbb{Z}_4 \times \mathbb{Z}_2$.

ii) Se $yx = x^3y$ e $y^2 = e$, então $x \to r,\ y \to s$ determinam um isomorfismo entre G e D_4.

iii) Se $yx = xy$ e $y^2 = x^2$, o grupo é abeliano, xy^{-1} tem ordem 2, e $x \to (1,0),\ xy^{-1} \to (0,1)$ fornecem um isomorfismo entre G e $\mathbb{Z}_4 \times \mathbb{Z}_2$.

iv) Finalmente, se $yx = x^3y$ e $y^2 = x^2$, então $x \to i,\ y \to j$ determinam um isomorfismo entre G e $\mathbf{Q}$.

E se cada elemento de $G - \{e\}$ tivesse ordem 2 ?

Neste caso G é um grupo abeliano. Escolhendo x, y, z de $G - \{e\}$ de tal forma que $z \neq xy$, o subgrupo $H = \{e, x, y, xy\}$ é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ e se $K =< z >$ checamos facilmente que $HK = G$ e $H \cap K = \{e\}$. Portanto, $G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ por 4.18.

5 Grupo de Frisos

Os grupos de isometrias mais conhecidos em $\mathbb{C}$ são os grupos de papel de parede e os grupos de frisos. Nosso objetivo é apresentar os grupos de frisos como uma aplicação dos estudos desenvolvidos.

Um friso é uma faixa decorativa com um padrão repetido e um grupo de frisos é um grupo de simetrias de algum friso. Grupos de frisos são frequentemente descritos através de desenhos repetidos, ao longo de uma reta, mas iremos dar uma abordagem mais analítica a fim de ilustrar o uso da teoria de grupos.

Dado qualquer grupo G de isometrias em $\mathbb{C}$, o conjunto $\mathcal{T}$ de translações em G é um subgrupo normal de G. Para vermos isto, tomemos qualquer translação em G, $f(z) = z+t$. Lembramos que qualquer isometria direta em G é da forma $g(z) = az+b$, e qualquer isometria indireta é da forma $h(z) = c\overline{z} + d$. Um cálculo simples mostra que gfg^{-1} e hfh^{-1} são translações, e isto mostra que $\mathcal{T}$ é um subgrupo normal de G. A consequência mais importante desde fato é que podemos agora considerar o grupo quociente $G/\mathcal{T}$.

Definição 5.1. *Um grupo de frisos é um grupo $\mathcal{F}$ de isometrias de $\mathbb{C}$ que deixa a reta real $\mathbb{R}$ invariante, e cujo subgrupo de translação $\mathcal{T}$ é um grupo cíclico infinito.*

Nosso objetivo é classificar os grupos de frisos e para isso veremos que o grupo quociente $\mathcal{F}/\mathcal{T}$ tem no máximo 4 elementos, e então consideramos todas as possibilidades. Contudo, antes de podermos listar as possibilidades, temos que analisar quando dois grupos de frisos são considerados como o mesmo grupo.

Se $\mathcal{T}_1$ e $\mathcal{T}_2$ são grupos cíclicos de translações, gerados por $z \mapsto z + t_1$ e $z \mapsto z + t_2$, respectivamente, então $\mathcal{T}_2 = g\mathcal{T}_1 g^{-1}$, onde $g(z) = (t_2/t_1)z$.

Portanto, qualquer grupo de frisos é conjugado a outro grupo de frisos cujo subgrupo de translação $\mathcal{T}$ é gerado por $z \mapsto z+1$. A partir de agora restringiremos nossa atenção para os grupos de frisos cujo subgrupo $\mathcal{T}$ de translação é o grupo de translações inteiras $z \mapsto z + n$, onde $n \in \mathbb{Z}$. É conveniente chamar tal grupo de frisos como um grupo de frisos padrão. Provaremos o seguinte resultado.

Teorema 5.1. *Qualquer grupo de frisos é conjugado a exatamente um dos sete grupos a seguir:*

1. $< z+1 >$;

2. $< z+1, -z >, < z+1, -\overline{z} >, < z+1, \overline{z} >, < z+1, \overline{z}+1/2 >$;

3. $< z+1, -z, \overline{z} >, < z+1, -z, \overline{z}+1/2 >$

onde $< a_1, ..., a_k >$ denota o grupo gerado por $a_1, ..., a_k$.

Observamos que o primeiro passo é mostrar que, além das translações, existem somente quatro tipos de elementos em um grupo de frisos. Depois veremos que 2 elementos do mesmo tipo produzem a mesma classe lateral em relação a $\mathcal{T}$, assim, o grupo quociente $\mathcal{F}/\mathcal{T}$ tem ordem no máximo cinco. O próximo passo é mostrar que todo elemento não trivial no grupo quociente possui ordem 2, e isso nos leva ao seguinte resultado:

Lema 5.1. *Seja $\mathcal{F}$ um grupo de frisos padrão. Então $\mathcal{F}/\mathcal{T}$ ou é o grupo trivial ou um grupo cíclico de ordem dois ou é isomorfo ao grupo de Klein de ordem 4.*

Prova:

Vamos procurar uma forma geral de um elemento g em um grupo de friso padrão $\mathcal{F}$. Observemos primeiramente que $g(z)$ ou é $az+b$ ou $a\overline{z}+b$, onde $b = g(0)$ e $a = g(0) - g(1)$. Como $g(\mathbb{R}) = \mathbb{R}$ vemos que a e b são reais. Como $|a| = 1$, temos $a = \pm 1$. Finalmente, se $g(z) = \overline{z} + b$ então $g^2(z) = g(\overline{z}+b) = z + 2b$ é uma translação de modo que $2b \in \mathbb{Z}$. Isto mostra que todo elemento de um grupo de friso padrão é um dos tipos a seguir:

1. $z \mapsto z + m, m \in \mathbb{Z}$;

2. $z \mapsto -z + b, b \in \mathbb{R}$;

3. $z \mapsto -\overline{z} + b, b \in \mathbb{R}$;

4. $z \mapsto \overline{z} + m, m \in \mathbb{Z}$;

5. $z \mapsto \overline{z} + 1/2 + m, m \in \mathbb{Z}$.

Há portanto 5 *tipos* diferentes de elementos.

Note que $\mathcal{F}$ não pode conter elementos do tipo (4) e elementos do tipo (5), caso contrário, $\mathcal{F}$ conteria $z \mapsto z + 1/2$ (que não está em $\mathcal{T}$).

A obervação principal é que se g e h são do mesmo tipo, então $g^{-1}h$ é uma translação; assim temos a igualdade $g\mathcal{T} = h\mathcal{T}$ de classes laterais. Isto implica que cada um dos 5 tipos fornece no máximo uma classe lateral para $\mathcal{F}/\mathcal{T}$. Assim $\mathcal{F}/\mathcal{T}$ tem ordem no máximo 5. Em seguida, se g é um elemento qualquer de $\mathcal{F}$ então $g^2 \in \mathcal{T}$ de modo que no grupo quociente, $(g\mathcal{T})(g\mathcal{T}) = g^2\mathcal{T} = \mathcal{T}$. Assim, cada elemento de $\mathcal{F}/\mathcal{T}$ tem ordem 2, e como $\mathcal{F}/\mathcal{T}$ tem ordem no máximo 5, isto implica que $\mathcal{F}/\mathcal{T}$ deve ter ordem 1,2 ou

4. Além disso, se tiver ordem 4, não poderá ser cíclico e por isso deve ser isomorfo ao grupo de Klein de ordem 4. □

Vamos agora analisar os casos onde $\mathcal{F}/\mathcal{T}$ tem ordem 1, 2 ou 4.

Caso1: $\mathcal{F}/\mathcal{T}$ tem ordem 1, logo é o grupo trivial.

Neste caso $\mathcal{F} = \mathcal{T}$, e $\mathcal{F}$ é o grupo dado no item 1 do teorema anterior.

Caso2: $\mathcal{F}/\mathcal{T}$ tem ordem 2.

Neste caso $\mathcal{F} = \mathcal{T} \cup g\mathcal{T}$, onde g é um dos 4 tipos , de 2 até 5, e $\mathcal{F}$ é gerado por g e t, onde $t(z) = z + 1$.

Se g é do tipo (2), $g(z) = -z + b$, seja $h(z) = z - b/2$. Então $hgh^{-1} = -z$ e $hth^{-1} = t$, assim,

$$h\mathcal{F}h^{-1} =< z + 1, -z > .$$

Se g é do tipo (3), $g(z) = -\overline{z} + b$, tomamos h como acima, e então

$$h\mathcal{F}h^{-1} =< z + 1, -\overline{z} > .$$

Se g é do tipo (4), $g(z) = \overline{z} + m$, onde $m \in \mathbb{Z}$, então

$$\mathcal{F} =< z + 1, \overline{z} > .$$

Finalmente, se g é do tipo (5), $g(z) = \overline{z} + 1/2 + m$, onde $m \in \mathbb{Z}$, então

$$\mathcal{F} =< z + 1, \overline{z} + 1/2 > .$$

Caso3: $\mathcal{F}/\mathcal{T}$ é o grupo quociente consistindo de exatamente 4 classes laterais, com cada classe contendo um elemento de cada tipo listado acima.

Como $\mathcal{T}$ é uma dessas classes laterais, e $\mathcal{F}$ não contém elementos do tipo (4) e (5), vemos que existem apenas duas possibilidades para $\mathcal{F}/\mathcal{T}$, são elas:

$$\mathcal{T} \cup g_2\mathcal{T} \cup g_3\mathcal{T} \cup g_4\mathcal{T}, \quad \mathcal{T} \cup g_2\mathcal{T} \cup g_3\mathcal{T} \cup g_5\mathcal{T},$$

onde g_j é do tipo j. Em ambos os casos, $\mathcal{F}$ contém $g_2(z) = -z + b$ e substituindo $\mathcal{F}$ por $h\mathcal{F}h^{-1}$, onde $h(z) = z - b/2$, podemos assumir que $g_2(z) = -z$. Note que, como h é uma translação, esta comuta com $t(z) = z + 1$. Além disso, hg_jh^{-1} tem o mesmo tipo de g_j de modo que a descrição das duas possibilidades para $\mathcal{F}/\mathcal{T}$ continua válida. Na primeira possibilidade, $\mathcal{F}$ contém $g_3(z) = -\overline{z} + b$, e $g_2(z) = -z$ de modo que também contém $\overline{z} - b$. Como este elemento é do tipo (4) (a primeira possibilidade não tem elementos do tipo (5)), vemos que $b \in \mathbb{Z}$, assim

$$\mathcal{F} =< z + 1, -z, \overline{z} > .$$

Finalmente, considerando a segunda possibilidade. Como antes, $\mathcal{F}$ contém $g_3(z) = -\overline{z} + b$ e por isso contém $\overline{z} - b$. Dessa vez, este elemento pode ser do tipo (5), então vemos que $b - 1/2 \in \mathbb{Z}$. E claramente $\mathcal{F}$ contém $\overline{z} + 1/2$, e

$$\mathcal{F} =< z + 1, -z, \overline{z} + 1/2 > .$$

Isto completa a prova do teorema. □

Há sete tipos de grupos de frisos que podem ser ornamentados da seguinte forma:

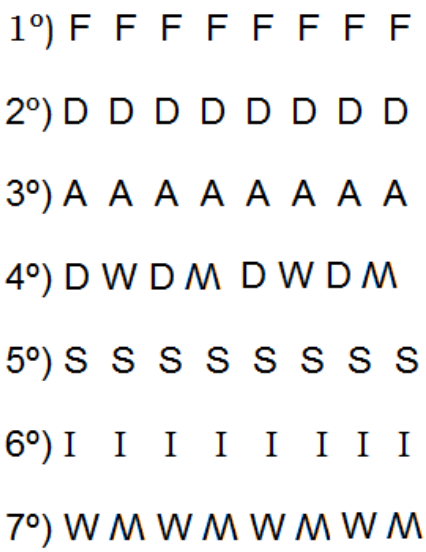


Figura 5.1: Grupos de Frisos

onde:
1) é gerado por uma translação;
2) é gerado por uma translação e uma reflexão horizontal;
3) é gerado por uma translação e uma reflexão vertical;
4) é gerado por uma reflexão deslizante;
5) é gerado por uma translação e uma rotação de 180;
6) é gerado por uma translação, rotação de 180 e uma reflexão horizontal;
7) é gerado por uma reflexão deslizante e rotação de 180.

Referências

1. ARMSTRONG, M. A. *Groups and symmetry*, New York: Springer-Verlag, 1988.
2. MARTIN, G. E. *Transformation Geometry*, New York: Springer-Verlag, 1983.
3. ROTMAN, J. J. *The Theory of Grupos*, Boston: Allyn and Bacon, Inc., 1978.
4. LIMA, E. L. *Isometrias*, Rio de Janeiro: SBM, 1996.