Maria Manuela Pereira Pinto

Grupos e Simetrias

Universidade Portucalense

Infante D. Henrique

Departamento de Inovação, Ciência e Tecnologia

Porto 2009

Maria Manuela Pereira Pinto

Grupos e Simetrias

Tese submetida à Universidade Portucalense
para obtenção do grau de Mestre
em Matemática/ Educação

Trabalho realizado sob a orientação da
Professora Stella Abreu

Departamento de Inovação, Ciência e Tecnologia

Porto 2009

Declaração

Nome: **Maria Manuela Pereira Pinto**

N^o*B.I.*: 10388360 *Tel/Telem.*: **918171631** *e.mail*:**manuela – pinto@clix.pt**

Curso de Pós - Graduação:

Doutoramento ☐

Designação do Doutoramento: _____ **Ano de conclusão / /**

Mestrado ×

Designação do mestrado: Matemática/ Educação **Ano de conclusão / /**

Título da tese/ dissertação:

Grupos e Simetrias

Orientadora:

Professora Stella Abreu

Declaro, para os devidos efeitos, que concedo, gratuitamente, à Universidade Portucalense Infante D. Henrique, para além da livre utilização do título e do resumo por mim disponibilizados, autorização, para esta arquivar nos respectivos ficheiros e tornar acessível aos interessados, nomeadamente através do seu repositório institucional, o trabalho supra - identificado, nas condições abaixo indicadas:
Assinalar as opções aplicáveis em 1 e 2

1. Tipo de Divulgação:

☐ **Total.**

× **Parcial.**

2. Âmbito de Divulgação:

☐ **Mundial (Internet aberta)**

× **Intranet da Universidade Portucalense.**

☐ **Internet, apenas a partir de ☐ 1 ano ☐ 2 anos ☐ 3 anos - até lá apenas Intranet da UPT**

Advertência: O direito de autor da obra pertence ao criador intelectual, pelo que a subscrição desta declaração não implica a renúncia de propriedade dos respectivos direitos de autor ou o direito de a usar em trabalhos futuros, os quais são pertença do subscritor desta declaração.

Assinatura: _____

Porto, / /

Para a minha Família com amor.

Agradecimentos

Gostaria de agradecer em primeiro lugar à Professora Doutora Stella Abreu, minha orientadora científica, pela sua permanente disponibilidade e incentivo, pelo constante apoio científico e moral, pela cedência de bibliografia e, ainda, por todas as sugestões, conselhos e críticas que me foram bastante úteis na elaboração deste trabalho.

Quero expressar um agradecimento muito especial à minha família pela força e coragem que sempre me transmitiram e pela ajuda em tudo aquilo que estava ao seu alcance.

Resumo

Nesta dissertação, começamos por dar noções básicas necessárias sobre grupos e sobre o software "GAP". Ao longo do trabalho será introduzido, sempre que possível, no final de uma ou mais secções, um exemplo com o intuito de utilizar o software "GAP"na demonstração das noções dadas. Estudamos os grupos simétricos e a sua relação com as simetrias rotacionais dos sólidos platónicos. Apesar de existirem cinco sólidos platónicos, apenas faremos três análises, pois existem dois pares de sólidos que são duais. Terminamos este trabalho com o estudo da construção de tabelas de caracteres de grupos. Aplicamos este estudo aos grupos de rotações dos sólidos platónicos.

Abstract

In this dissertation, we begin by giving basic necessary notions on groups and on the software "GAP ". Along the work it will be introduced, whenever possible, in the end of one or more sections, an example with the intention of using the software "GAP "in the demonstration of the given notions.

We study the symmetric groups and their relationship with the group of rotational symmetries of platonic solids. In spite of studying the five Platonic solids, we will do three analyses, since there are two couples of solids that are dual. We finish this work with the study of the construction of the characters tables of groups. We apply this study to groups of rotations of the platonic solids.

Sumário

Lista de Tabelas

Lista de Figuras

Notação

Símbolo	Uso	Significado
$\in$	$x \in \mathbb{S}$	x **é um elemento de** $\mathbb{S}$
$\notin$	$x \notin \mathbb{S}$	x **não é um elemento de** $\mathbb{S}$
$\subset$	$\mathbb{S} \subset \mathbb{X}$	$\mathbb{S}$ **é um subconjunto de** $\mathbb{X}$
$\subset$	$\mathbb{S} \subset \mathbb{G}$	$\mathbb{S}$ **é um subgrupo de** $\mathbb{G}$
$\leq$	$\mathbb{S} \leq \mathbb{G}$	$\mathbb{S}$ **é um subgrupo impróprio de** $\mathbb{G}$
$<$	$\mathbb{S} < \mathbb{G}$	$\mathbb{S}$ **é um subgrupo próprio de** $\mathbb{G}$
$\emptyset$	$\emptyset$	**Conjunto vazio**
{ }	$\{x\|—\}$	**Todo o elemento** x
$\cap$	$\mathbb{S} \cap \mathbb{G}$	**Intersecção de** $\mathbb{S}$ **com** $\mathbb{G}$
$\cup$	$\mathbb{S} \cup \mathbb{G}$	**Reunião de** $\mathbb{S}$ **com** $\mathbb{G}$
()	(x, y)	**Par ordenado**
$\times$	$\mathbb{X} \times \mathbb{Y}$	**Produto de** $\mathbb{X}$ **por** $\mathbb{Y}$
$\Rightarrow$	... $\Rightarrow$ —	... **implica** —
$\Leftrightarrow$	... $\Leftrightarrow$ —	... **se e só se** —
$\circ$	$f \circ g$	**Composição,** f **após** g

$\rightarrow$	$\mathbb{X} \rightarrow \mathbb{Y}$	**Função de $\mathbb{X}$ para $\mathbb{Y}$**
$\cong$	$\mathbb{X} \cong \mathbb{Y}$	**É um isomorfismo de $\mathbb{X}$ para $\mathbb{Y}$**
∞	∞	**Infinito**
$\perp$	$u \perp v$	**u é ortogonal a v**
<>	$< u, v >$	**Produto interno de u por v**
$\triangleleft$	$\mathbb{H} \triangleleft \mathbb{G}$	**$\mathbb{H}$ é um subgrupo normal de $\mathbb{G}$**
$\square$	$\square$	**Terminação da demonstração de um teorema**

Símbolos de Conjuntos	**Significado**
$\mathbb{Z}$	**Conjunto dos números inteiros**
$\mathbb{C}$	**Conjunto dos números complexos**
$\mathbb{N}$	**Conjunto dos números naturais**
$\mathbb{Q}$	**Conjunto dos números racionais**
$\mathbb{R}$	**Conjunto dos números reais**
$\mathbb{S}_n$	**Grupo Simétrico**
$\mathbb{A}_n$	**Grupo Alterno**
$\mathbb{B}_n$	**Subconjunto de $\mathbb{S}_n$**
$\mathbb{D}(n)$	**Grupo Diedral**
$\mathbb{C}_n$	**Grupo Cíclico Finito**
$\mathbb{Z}_n$	**Grupo Cíclico Infinito**

Introdução

Grupo é uma estrutura matemática simples que transformou toda a ciência Matemática. O seu estudo, a "Teoria dos Grupos", reflecte-se na teoria das equações, na teoria dos números, na geometria diferencial, na cristalografia, em estudos sobre o átomo e partículas subatómicas, etc.

O conceito de grupo surge, pela primeira vez, num trabalho de 1829 de autoria de um jovem irrequieto e genial matemático francês com apenas 18 anos, Evariste Galois.

Galois participou como republicano na revolução de 1830 e morreu em 1832, com apenas 21 anos, ferido num duelo.

Tendo-lhe sido recusada, por duas vezes, a adimissão à Escola Politécnica de Paris, acabou por ser admitido à Escola Normal, onde ficaria pouco tempo, face à sua intensa actividade política.

Interessou-se, entre outros assuntos, pelo problema da " resolubilidade algébrica das equações do 5^o grau ou de grau superior, que não eram resolúveis pelos métodos tradicionais"(isto é, usando um número finito de vezes a extracção de raizes quadradas ou cúbicas, e outras operações triviais). Foi a propósito deste problema que Galois criou o conceito de grupo, analisou as propriedades dos grupos de substituições e estabeleceu as condições em que a resolução daquelas equações era possível.

Destes factos e doutros tentou dar conta através de várias comunicações que foram ignoradas pelos matemáticos da época, talvez por desconfiarem da sua extrema juventude.

Quatorze anos após a sua morte, em 1846, foi publicado um texto, com cerca de 60 páginas, onde Galois esboçava a "Teoria de grupos", a chave da Álgebra e Geometria modernas, e abordava outros problemas clássicos.
A teoria dos grupos tem a sua origem também ligada a um outro jovem matemático norueguês Niels Henrik Abel $(1802-1829)$, principalmente pelos seus estudos sobre grupos comutativos. Em sua honra estes grupos são também chamados grupos abelianos.
Tal como Galois, publicou algumas memórias de Análise, com apenas 18 anos, em 1820.
Estes dois jovens contemporâneos apresentam estranhas coincidências nas suas vidas. Nomeadamente, ambos tentaram, sem êxito, que as suas descobertas fossem reconhecidas pelo meio científico de Paris, ambos viveram uma vida intensa e breve, morrendo antes dos 30 anos, e ambos alcançaram a celebridade postumamente: um é o francês Galois, o outro é o norueguês Abel.
Os grupos abelianos têm importância central em Álgebra Abstracta e noutros ramos da Matemática nomeadamente na Topologia Algébrica.

Após esta nota histórica[1], será feito um breve resumo de cada capítulo. Assim, no primeiro capítulo serão dadas algumas noções básicas sobre grupos, essenciais para os restantes capítulos.
No segundo capítulo, é feito um estudo do grupo geral linear, $\mathbb{GL}(n)$, grupo das matrizes invertíveis $n \times n$ com entradas reais. Existe um isomorfismo entre este grupo e o grupo das transformações lineares invertíveis em $\mathbb{R}^n$. Em particular, estudaremos o grupo ortogonal $\mathbb{O}(3)$ subgrupo de $\mathbb{GL}(3)$. Pretendemos identificar as transformações lineares de $\mathbb{R}^3$ em $\mathbb{R}^3$ que preservam distâncias e amplitudes de ângulos. Veremos que estas funções são rotações em torno de um eixo e formam um grupo, cuja operação é a

[1] ver, "A History of Mathematics", Jonh Wiley e Sons, Inc, 89, eyer, Carl e outros.

composição.

No terceiro capítulo, estudaremos o grupo das "Permutações" e veremos que qualquer grupo é isomorfo a um subgrupo de um grupo de permutações. Estudaremos, no quarto capítulo, as tabelas de caracteres de grupos e, como forma de aplicação de todos estes capítulos, teremos um último cujo tema é "Estudo dos grupos de rotações dos sólidos platónicos".

Ao longo destes capítulos, irá ser utilizado de forma progessiva o software "GAP"(Groups, Algorithms and Programming), que começou por ser um sistema computacional para lidar com grupos, mas o seu uso tem sido alargado devido ao elevado número de "share-packages"existente.

O mesmo software tem sido utilizado na realização de muitos trabalhos de investigação e, também, no ensino, especialmente para ensinar a "Teoria de Grupos".

A primeira versão da criação de tabelas de caracteres no "GAP"surgiu com o "GAP 3.1"em Março de 1992, para ser utilizado no estudo de grupos. Um outro aspecto foi a criação da biblioteca de tabelas de caracteres com todas as tabelas dos grupos finitos (ver [1], disponível na Internet).[2]

O software "GAP"começou a ser desenvolvido em 1984 em Aachen, na Alemanha, tendo o seu centro de desenvolvimento sido transferido para St. Andrews, na Escócia, em 1987. Existem pessoas a trabalhar no "GAP"um pouco por todo o mundo.

Na conclusão será elaborada uma pequena reflexão sobre o tema da tese.

[2] "The GAP caracter table library", version 1.1, maintained by Thomas Breuer

Capítulo 1

Noções básicas sobre grupos

Em matemática moderna chama-se estrutura algébrica a um conjunto munido com uma ou várias operações binárias (ou leis de composição interna) que obedece a um determinado sistema de leis axiomáticas.

A teoria que estuda as estruturas algébricas, dando ênfase às operações e leis que as definem e às consequências dessas leis, independentemente da natureza específica dos elementos que formam o conjunto, tem o nome de álgebra abstracta.

A álgebra abstracta constitui assim uma visão de síntese, unificadora, que revela as analogias estruturais de muitos conjuntos de seres matemáticos aparentemente desligados. Por exemplo, o conjunto dos vectores do plano,$\mathbb{V}_p$, associado à adição de vectores (+), goza das mesmas propriedades que o conjunto dos números inteiros, $\mathbb{Z}$, associado à adição usual (+).

1.1 Definição de grupo

Sejam x e y dois quaisquer elementos de um conjunto $\mathbb{G}$. Diz-se que φ é uma operação binária definida em $\mathbb{G}$, ou lei de composição interna em $\mathbb{G}$,

sse ao par ordenado (x,y) de $\mathbb{G} \times \mathbb{G}$ corresponde, pela operação φ, um único elemento de $\mathbb{G}$, que se designa por $x \ \varphi \ y$.

$$\varphi : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$$

$$(x, y) \mapsto z = x \ \varphi \ y$$

Exemplo 1.1 ***A adição usual em $\mathbb{Z}$ associa a cada par ordenado de números inteiros, (x,y), um número inteiro que é a sua soma, $x + y$.***

Exemplo 1.2 ***A adição de vectores de um plano $\mathbb{V}_p$ é uma operação binária definida em $\mathbb{V}_p$, porque a soma de dois vectores é um vector do mesmo plano.***

Exemplo 1.3 ***O produto escalar de dois vectores não é uma operação binária em $\mathbb{V}_p$, porque o produto escalar de dois vectores é um número real e não um vector. Por não ser lei de composição interna, ou operação interna, é que se abandonou a designação de produto interno.***

Sejam $\mathbb{G}$ um conjunto não vazio e φ uma operação binária definida em $\mathbb{G}$. Um conjunto $\mathbb{G}$ diz-se um grupóide relativamente à operação φ, ou $(\mathbb{G}, \varphi)$ é grupóide, sse φ é uma lei de composição interna em $\mathbb{G}$. O conjunto $\mathbb{G}$ é designado por conjunto suporte do grupóide.

Definição 1.1 ***[2], pág.28***
Um grupo é um par $(\mathbb{G}, \varphi)$, constituído por um conjunto $\mathbb{G}$ e uma operação binária:

$$\varphi : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$$

***que satisfaz os seguintes axiomas*:**
***Associatividade*: $\forall x,y,z \in \mathbb{G}$: $x \ \varphi \ (y \ \varphi \ z) = (x \ \varphi \ y) \ \varphi \ z$**

Existência de elemento neutro: $\exists e \in \mathbb{G}$, $\forall x \in \mathbb{G}$: $x \ \varphi \ e = e \ \varphi \ x = x$
Todo o elemento tem oposto: $\forall x \in \mathbb{G}$, $\exists x^{-1} \in \mathbb{G}$: $x \ \varphi \ x^{-1} = x^{-1} \ \varphi \ x = e$, e ***e*** x^{-1} ***são únicos.***

Diz-se que $(\mathbb{G}, \varphi)$ é abeliano ou comutativo se $(\mathbb{G}, \varphi)$ é grupo e φ é comutativa.

1.1.1 Exemplos de grupos

Definição 1.2 ***[3], pág.23***
Um subgrupo $\mathbb{H}$ ***de*** $\mathbb{G}$ ***é um subconjunto não vazio de um grupo*** $\mathbb{G}$ ***que segundo a lei de composição interna de*** $\mathbb{G}$ ***forma ele próprio um grupo.***

No caso do grupo ser finito uma definição equivalente, é que $\mathbb{H}$ deve ser fechado para a lei de composição interna, isto é

$$h_1 \ \varphi \ h_2 \in \mathbb{H}, \quad \forall h_1, \ h_2 \in \mathbb{H}$$

A associatividade é herdada do maior grupo $\mathbb{G}$ e, a existência da identidade em $\mathbb{H}$ vem do facto do grupo $\mathbb{G}$ ser finito e a operação ser uma lei de composição interna (fechada). Para justificar esta afirmação note-se que todo o elemento $h \in \mathbb{G}$, tem ordem finita r, portanto, $h^r = e$. Então por $\mathbb{H}$ ser fechado tem-se $e \in \mathbb{H}$. De igual modo,

$$h^{-1} = h^{r-1} \in \mathbb{H},$$

o que demonstra que o oposto de um elemento $h \in \mathbb{H}$ está também em $\mathbb{H}$. De acordo com a definição acima, {e} e $\mathbb{G}$ são subgrupos de $\mathbb{G}$. Estes subgrupos são designados de subgrupos triviais de $\mathbb{G}$. Um subgrupo $\mathbb{H}$ que não é trivial é chamado de subgrupo próprio e escreve-se $\mathbb{H} < \mathbb{G}$.

Teorema 1.1 ***[4], pág.136***
Um subconjunto $\mathbb{H}$ ***de um grupo*** $\mathbb{G}$ ***é um subgrupo de*** $\mathbb{G}$ ***sse*** $xy^{-1}\in\mathbb{H}$ ***sempre que*** x,$y\in\mathbb{H}$.

1.2 Conjugação e classes conjugadas

Definição 1.3 ***[3], pág.19***
Dois elementos x ***e*** y ***de um grupo*** $\mathbb{G}$ ***são conjugados se existe um elemento*** $g\in\mathbb{G}$ ***de modo que:***

$$x = g\ y\ g^{-1}$$

O elemento g ***é chamado de elemento conjugador.***

A conjugação é um exemplo de uma relação de equivalência, um dos conceitos fundamentais em Matemática. Uma relação é de equivalência se for: (i) **reflexiva (todo o elemento é equivalente a si próprio)**

$$x \sim x \text{ uma vez que } e \in \mathbb{G} \Rightarrow x = x^{-1}e$$

(ii) **simétrica (se** x **é equivalente a** y **então** y **é equivalente a** x**)**

$$x \sim y \Rightarrow y \sim x$$

$x \sim y$**, significa que** $x = g\ y\ g^{-1}$**, para algum** $g\in\mathbb{G}$**, pela existência de elemento oposto, podemos reescrever isto,** $y = g^{-1}\ x\ g$**, isto é,** $y \sim x$**, sendo** g^{-1} **um elemento conjugador.**

(iii) **transitiva (se** x **é equivalente a** y **e** y **é equivalente a** z **então** x **é equivalente a** z**)**

$$x \sim y \wedge y \sim z \Rightarrow x \sim z$$

Se $x \sim y \Rightarrow x = g\ y\ g^{-1}$**, para algum** $g\in\mathbb{G}$ **e** $y \sim z \Rightarrow y = hzh^{-1}$**, para algum** $h\in\mathbb{G}$ **então** $x = g\ y\ g^{-1} = (gh)z(h^{-1}g^{-1}) = (gh)z(hg)^{-1}$**, conclui-se que** $x \sim z$**, sendo** (gh) **um elemento conjugador.**

1.2.1 Classes de conjugação

Uma qualquer relação de equivalência definida num conjunto efectua uma partição do mesmo em classes de equivalência disjuntas. A classe de equivalência de um elemento x, escrevendo-se (x), é simplesmente o conjunto dos elementos equivalentes x:

$$(x) = \{\ y \mid y \sim x\}$$

Para construir classes de equivalêcia o procedimento é o seguinte: toma-se um elemento qualquer x do conjunto e constrói-se a sua classe (x). Se este processo não esgotar o conjunto, toma-se outro elemento y que não pertença a (x) e constrói-se a sua classe (y). Repete-se o mesmo processo até esgotar os elementos do conjunto. Pela natureza desta construção, as classes são necessariamente disjuntas. Para provar isto, suponhamos que (x) e (y) têm um elemento t em comum. Isto significa que $t \sim x$ e $t \sim y$, então pela propriedade transitiva, $x \sim y$, o que é uma contradição uma vez que y não pode ser elemento de (x).
Uma vez que a conjugação é uma relação de equivalência, então ela divide os elementos do grupo em classes de equivalência, designadas por classes de conjugação:

$$(x) = \{\ y \mid y = gxg^{-1},\ \forall g{\in}\mathbb{G}\ \}$$

1.2.2 Classes laterais

Seja $\mathbb{H} = \{\ h_1,\ h_2,\ ...,\ h_r\ \}$ um subgrupo finito do grupo $\mathbb{G}$. A classe esquerda de um elemento $g{\in}\mathbb{G}$, denotada por $g\mathbb{H}$, é definida como o conjunto de todos os elementos de $\mathbb{H}$ multiplicados à esquerda por g:

$$g\mathbb{H} = \{\ gh_1,\ gh_2,\ ...,\ gh_r\ \}$$

Estas classes ou coincidem, ou são disjuntas e fornecem outra partição do grupo $\mathbb{G}$, diferente da partição anterior. Para provar esta afirmação, vamos

estabelecer outra relação de equivalência. Dois elementos são equivalentes se:

$$x \sim y, \quad \textbf{se} \quad y \in x\mathbb{H}$$

Verificação da relação de equivalência:
(i) **reflexiva** **Será que** $x \in x\mathbb{H}$**?**

Sim, pois $x = xe$ **e** $e \in \mathbb{H}$ **(existência da identidade)**

(ii) **simétrica** **Se** $y \in x\mathbb{H}$ **então** $x \in y\mathbb{H}$ **?**
Se $y \in x\mathbb{H}$ **então** $y = xh$**, para um** $h \in \mathbb{H}$**, portanto,** $x = yh^{-1}$**, com** $h^{-1} \in \mathbb{H}$
(existência do elemento oposto)

(iii) **transitiva** **Se** $y \in x\mathbb{H}$ **e** $z \in y\mathbb{H}$ **então** $z \in x\mathbb{H}$ **?**
Se $y \in x\mathbb{H}$ **e** $z \in y\mathbb{H}$ **então** $y = xh$ **e** $z = yh'$**, para** h, $h' \in \mathbb{H}$**, portanto,** $z = xhh'$**, com** $hh' \in \mathbb{H}$ **(**$\mathbb{H}$ **fechado)**

Para um grupo finito $\mathbb{G}$ **podemos enumerar as classes da seguinte forma:**

$$g_1\mathbb{H},\ g_2\mathbb{H},\ ...,\ g_s\mathbb{H}$$

O conjunto das classes é designado por $\mathbb{G}/\mathbb{H}$**.**

Teorema 1.2 ***Teorema de Lagrange[3], pág.25***
A ordem de qualquer subgrupo de um grupo $\mathbb{G}$ ***é divisor da ordem de*** $\mathbb{G}$**.**

Demonstração Seja $g\mathbb{H}$ **uma classe esquerda de** $\mathbb{H}$**,**

$$g\mathbb{H} = \{gh_1, gh_2, ..., gh_r\}$$

O número de elementos distintos pode ser menor do que r **se** $gh_1 = gh_2$**. Mas multiplicando,** g^{-1}**, à esquerda, pode-se deduzir que** $h_1 = h_2$**, contrariando**

a hipótese. Sendo assim, todos os elementos de um grupo $\mathbb{G}$, que são em número $|\mathbb{G}|$, podem ser agrupados segundo s $(= |\mathbb{G}/\mathbb{H}|)$ classes contendo r $(= |\mathbb{H}|)$ elementos. Conclui-se que $|\mathbb{G}| = s|\mathbb{H}|$.
A ordem de qualquer subgrupo de $\mathbb{G}$ deve ser um divisor da ordem de $\mathbb{G}$.

□

1.2.3 Subgrupo normal

Em geral os subgrupos e classes de conjugação têm pouco a ver uns com os outros. Contudo, os dois conceitos estão ligados segundo um tipo de subgrupo chamado de "normal", invariante ou subgrupo conjugado próprio. Apesar de especial, este tipo de subgrupo surge naturalmente num contexto de aplicações entre grupos. O subgrupo normal $\mathbb{H}$ de $\mathbb{G}$ satisfaz a seguinte condição:

$$g\mathbb{H}g^{-1} = \mathbb{H}, \quad \forall\ g{\in}\mathbb{G} \tag{1}$$

Existem várias formulações equivalentes a esta definição. Multiplicando por g à direita:

$$g\mathbb{H} = \mathbb{H}g$$

Aqui $\mathbb{H}g$ é uma classe à direita, consistindo nos elementos

$$\mathbb{H}g = \{\ h_1 g,\ h_2 g,\ \ldots\ ,\ h_r g\ \}$$

Assim, uma definição alternativa, um subgrupo normal é um subgrupo cujas classes à direita e à esquerda coincidem.
Pela primeira definição vê-se porque razão $\mathbb{H}$ é chamado conjugado próprio, por analogia com elemento conjugado próprio, satisfazendo,

$$ghg^{-1} = h$$

Contudo, em (1) o significado não é o mesmo. O significado é que todos os conjugados de h devem ser também elementos de $\mathbb{H}$, isto é

$$h \in \mathbb{H} \Rightarrow ghg^{-1} \in \mathbb{H}, \quad \forall g \in \mathbb{G}$$

Outra definição é, portanto, de que um subgrupo normal é um subgrupo formado por classes de conjugação completas.

Nota Se $\mathbb{H}$ é um subgrupo normal de $\mathbb{G}$ utiliza-se a seguinte notação:

$$\mathbb{H} \lhd \mathbb{G}.$$

1.2.4 Grupo quociente

Uma propriedade notável do subgrupo normal $\mathbb{H}$ é que o conjunto das classes $\mathbb{G}/\mathbb{H}$ pode ser munido da estrutura de grupo, usando uma definição adequada de produto de duas classes.

Definição 1.4 ***[3], pág.26***
O produto de duas classes $(g_1\mathbb{H})$ ***e*** $(g_2\mathbb{H})$ ***é definido como sendo a classe*** $(g_1g_2\mathbb{H})$***, ou seja***

$$(g_1\mathbb{H})(g_2\mathbb{H}) = (g_1g_2\mathbb{H})$$

Pode-se verificar que realmente esta operação satifaz os axiomas.

1.3 Homomorfismos

Seja θ uma operação binária de um conjunto $\mathbb{A}$ e φ uma operação de um conjunto $\mathbb{B}$. Um homomorfismo, f é uma aplicação

$$f : \mathbb{A} \to \mathbb{B}$$

tal que:

$$f(x\theta y) = f(x)\ \varphi\ f(y),\ \forall x,y\in\mathbb{A}$$

Os homomorfismos podem classificar-se em:
Monomorfismo se a função f é injectiva.
Epimorfismo se a função f é sobrejectiva.
Isomorfismo se a função f é bijectiva.

Definição 1.5 ***[4], pág.143***
Diz-se que a aplicação $f : \mathbb{A} \to \mathbb{B}$ ***é um isomorfismo do grupo*** $(\mathbb{A}, \theta)$ ***sobre o grupo*** $(\mathbb{B}, \varphi)$ ***sse:***
- f ***é bijectiva;***
- $f(x\theta y) = f(\boldsymbol{x})\ \varphi\ f(\boldsymbol{y}),\ \forall x,y\in\mathbb{A}$

Definição 1.6 ***[4], pág.143***
Dois grupos, $(\mathbb{A}, \theta)$ ***e*** $(\mathbb{B},\varphi)$ ***dizem-se isomorfos sse existe pelo menos um isomorfismo de*** $(\mathbb{A}, \theta)$ ***sobre*** $(\mathbb{B}, \varphi)$ ***e escreve-se:***

$$(\mathbb{A}, \theta) \simeq (\mathbb{B}, \varphi)$$

Quando existe um isomorfismo entre dois grupos, pode afirmar-se que eles têm a mesma estrutura. Consequentemente, estudadas as propriedades de um grupo, estão estudadas as propriedades de todos os grupos isomorfos, o que justifica o significado da palavra isomorfismo: etimologicamente - mesma forma.

Capítulo 2

Grupo Linear Geral, $\mathbb{GL}(n)$

O conjunto de todas as matrizes invertíveis, $n \times n$, com entradas reais, forma um grupo para a multiplicação de matrizes. Se $A = (a_{ij})$ e $B = (b_{ij})$ são duas matrizes, então cada elemento do produto é obtido através da soma:

$$a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{in}b_{nj}$$

A multiplicação de matrizes é associativa, tem como elemento neutro a matriz identidade, I_n, e o produto de AB tem inverso $(AB)^{-1} = B^{-1}A^{-1}$, pois

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$

Cada matriz A determina neste grupo uma transformação linear invertível,

$$f\colon \mathbb{R}^n \to \mathbb{R}^n$$

definida por:

$$f_A(X) = XA^t,$$

para todos os vectores $X = (x_1, ..., x_n)$ em $\mathbb{R}^n$, onde t significa a transposta.

O produto de matrizes, AB**, determina a composição de uma transformação linear** $f_A f_B$**:**

$$f_{AB}(X) = X(AB)^t = XB^tA^t = f_A(f_B(X))$$

Se f**:** $\mathbb{R}^n \to \mathbb{R}^n$ **é uma transformação linear invertível e, se** A **é uma matriz que a representa, então** A **é uma matriz invertível:** $f = f_A$**.**

Por estas razões, o grupo de todas as matrizes invertíveis $n \times n$ **com entradas reais é chamado de Grupo Linear Geral,** $\mathbb{GL}(\mathbf{n})$**,**

$$\mathbb{GL}(\mathbf{n}) = \{A \in M_{n\times n}\ (\mathbb{R})\text{: } \mathbf{det}(A) \neq \mathbf{0}\}$$

A multiplicação de matrizes não é comutativa para $n \geq 2$**. Assim, temos a família de grupos não comutativos infinitos:** $\mathbb{GL}(2)$, $\mathbb{GL}(3)$, ...

Quando $n = 1$**, cada matriz tem apenas uma entrada, não nula. Então o grupo** $\mathbb{GL}(\mathbf{1})$ **é isomorfo a** $\mathbb{R}\backslash\{\mathbf{0}\}$**.**

Dada a matriz $A \in \mathbb{GL}(n)$**, podemos construir a matriz:**

$$\tilde{A} = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

A colecção de matrizes desta forma é subgrupo de $\mathbb{GL}(n+1)$ **e a correspondência:** $A \mapsto \tilde{A}$ **mostra que** $\mathbb{GL}(n)$ **é isomorfo a este subgrupo.**
Em termos de transformações lineares, podemos identificar $\mathbb{R}^n$ **como o subespaço de** $\mathbb{R}^{n+1}$ **formado por todos os vectores cuja última coordenada é zero.**
Assim, $f_{\tilde{A}}$ **actua como** f_A **em** $\mathbb{R}^n$ **e deixa a última coordenada em cada ponto inalterada. Isto para dizer que:**

$$\mathbb{R}^{n+1} = \mathbb{R}^n \times \mathbb{R}$$

e

$$f_{\tilde{A}}\text{: } \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$$

dada por:

$$f_{\tilde{A}}(X,z) = (f_A(X),z)$$

2.1 Grupo ortogonal, $\mathbb{O}(n)$

Qualquer matriz, $A \in \mathbb{GL}(n)$**, diz-se ortogonal se**

$$A^tA = I_n \textbf{ ou, ainda, } A^t = A^{-1}$$

Note-se que: $(A^{-1})^{-1} = A = (A^t)^t$

Se A **e** B **são matrizes ortogonais, então,**

$$(AB^{-1})^tAB^{-1} = (B^{-1})^tA^tAB^{-1} = (B^{-1})^tIB^{-1} = I_n$$

Isto significa que AB^{-1} **é ortogonal. Pelo teorema 1.1 da página 7, o conjunto de todas as matrizes ortogonais forma um subgrupo de** $\mathbb{GL}(n)$**. Este subgrupo é chamado de grupo ortogonal,** $\mathbb{O}(n)$**, ou seja,**

$$\mathbb{O}(n) = \{A \in \mathbb{GL}(n) : A^tA = I_n\}$$

O determinante de uma matriz ortogonal é sempre $+1$ **ou** -1**, uma vez que**:

$$\textbf{det}(I_n) = \textbf{det}(A^tA) = (detA)^2$$

O conjunto de todos os elementos de $\mathbb{O}(n)$ **com determinante igual a** $+1$ **forma um subgrupo de** $\mathbb{O}(n)$ **chamado de Grupo Ortogonal Especial,** $\mathbb{SO}(n)$**, ou seja,**

$$\mathbb{SO}(n) = \{A \in \mathbb{O}(n)\text{: } \textbf{det}(A) = 1\}$$

Se $A \in \mathbb{O}(n)$, a correspondente transformação linear, f_A, preserva a distância e a ortogonalidade.
Para ver porquê, consideram-se X e Y pontos de $\mathbb{R}^n$ e considera-se o produto escalar de $f_A(X)$ por $f_A(Y)$.

Temos,

$$f_A(X)f_A(Y) = (XA^t)(YA^t)^t = XA^tAY^t = XY^t = XY \qquad (1)$$

Como $||X|| = \sqrt{X.X}$, substituindo em (1) Y por X verifica-se que:

$$||\mathbf{f}_A(X)|| = ||X||,$$

assim f_A preserva os comprimentos. Também,

$$||f_A(X) - f_A(Y)|| = ||f_A(X - Y)|| = ||X - Y||,$$

mostra-se que f_A preserva a distância entre dois quaisquer pontos.

Finalmente, o produto escalar $f_A(X)f_A(Y)$ é zero, quando o produto escalar XY é igual a zero. Assim se X e Y são vectores perpendiculares então as transformações lineares $f_A(X)$ e $f_A(Y)$ também são perpendiculares.

2.1.1 Grupo ortogonal, $\mathbb{O}(2)$

No plano $\mathbb{R}^2$ consideremos a origem. A rotação em torno da origem segundo um ângulo ou uma reflexão segundo um eixo que passa pela origem é uma transformação linear de $\mathbb{R}^2 \to \mathbb{R}^2$.

Se $A \in \mathbb{O}(2)$ as colunas da matriz A são vectores unitários e ortogonais. Supondo:

$$A = \begin{pmatrix} \mathbf{a} & \mathbf{c} \\ \mathbf{b} & \mathbf{d} \end{pmatrix}$$

Fazendo,

$a = cos\ \theta$ **,** $b = sen\ \theta$ **, para** $0 \leq \theta < 2\pi$

$c = cos\ \alpha$ **,** $d = sen\ \alpha$ **, para** $\alpha = \theta + \frac{\pi}{2}$ **ou** $\alpha = \theta - \frac{\pi}{2}$

No primeiro caso obtém-se:

$$A = \begin{pmatrix} \mathbf{cos}\,\theta & \mathbf{-\ sen}\,\theta \\ \mathbf{sen}\,\theta & \mathbf{cos}\,\theta \end{pmatrix}$$

$A \in \mathbb{SO}(2)$ **e representa uma rotação contrária à dos ponteiros do relógio, segundo o ângulo** θ**.**

Outra forma de descrever os elementos de $\mathbb{SO}(2)$ **é através da forma algébrica, ou seja, consideremos de novo a matriz,**

$$A = \begin{pmatrix} \mathbf{a} & \mathbf{c} \\ \mathbf{b} & \mathbf{d} \end{pmatrix} \in \mathbb{SO}(2)$$

sse

$$a^2 + b^2 = 1,$$
$$c^2 + d^2 = 1,$$
$$ac + bd = 0,$$
$$ad - bc = 1$$

A primeira equação diz-nos $(a,b) = r(cos\theta, sen\theta)$ **para algum** $r \in \mathbb{R}$**. A terceira equação implica** $(c,d) = r(-sen\theta, cos\theta)$ **para algum** $r \in \mathbb{R}$**. Da segunda conclui-se que** $r = \pm 1$ **e da quarta que** $r = 1$**.**

Então $a = cos\,\theta$**,** $b = sen\,\theta$**,** $c = -sen\,\theta$ **e** $d = cos\,\theta$**.**

O segundo caso dá-nos:

$$A = \begin{pmatrix} \mathbf{cos}\,\theta & \mathbf{sen}\,\theta \\ \mathbf{sen}\,\theta & \mathbf{-\ cos}\ \theta \end{pmatrix}$$

sendo o determinante igual a -1 e representa uma reflexão segundo o ângulo $\frac{\theta}{2}$. Assim, no segundo caso $A \notin \mathbb{SO}(2)$, pois o determinante é igual a -1. Algebricamente,

$$a^2 + b^2 = 1,$$
$$c^2 + d^2 = 1,$$
$$ac + bd = 0,$$
$$ad - bc = -1$$

A primeira equação diz-nos $(a,b) = r(cos\theta, sen\theta)$ para algum $r \in \mathbb{R}$. A terceira equação implica $(c,d) = r(sen\theta, -cos\theta)$ para algum $r \in \mathbb{R}$. Da segunda conclui-se que $r = \pm 1$ e da quarta que $r = -1$.
Então $a = cos\,\theta$, $b = sen\,\theta$, $c = sen\,\theta$ e $d = -cos\,\theta$.

2.1.2 Grupo ortogonal especial, $\mathbb{SO}(3)$

Suponhamos que a matriz $A \in \mathbb{SO}(3)$. O polinómio característico, $\det(A - \lambda I)$, é cúbico e, portanto, a matriz A tem pelo menos um valor próprio real igual a 1 Como o $\det(A) = 1$ tem-se,

$$\det(A - I) = \det(A^t - I) =$$
$$= \det(A)\ \det(A^t - I) =$$
$$= \det(AA^t - A) =$$
$$= \det(I - A) =$$
$$= \text{- } \det(A - I),\ \lambda = 1$$

Conclui-se, assim, que o $\det(A - I) = 0$. Seja v é o vector próprio correspondente ao valor próprio igual a 1. A linha que passa pela origem e

é determinada pelo vector v **, é fixada pela função** f_A**. Também como** f_A **preserva os ângulos rectos, então** f_A **deve enviar o plano perpendicular a** v**, e passando pela origem, nele próprio. Vamos construir uma base ortonormal de** $\mathbb{R}^3$ **com vector unitário,** $v/||v||$**, como primeiro elemento. A matriz de** f_A **com respeito à nova base vai ser um elemento de** $\mathbb{SO}(3)$ **com a seguinte forma:**

$$A = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & & \\ \mathbf{0} & & \end{pmatrix} \quad \mathbf{B}$$

Claramente $B \in \mathbb{SO}(2)$**, portanto,** f_A **é uma rotação cujo eixo é determinado por** v**. Cada matriz de** $\mathbb{SO}(3)$ **representa uma rotação de** $\mathbb{R}^3$ **em volta de um eixo que passa pela origem. Prova-se também que, cada rotação de** $\mathbb{R}^3$ **que fixa a origem é representada por uma matriz de** $\mathbb{SO}(3)$**.**

Exemplo 2.1 ***Seja*** $A \in \mathbb{SO}(3)$

$$A - \lambda I = \begin{pmatrix} \mathbf{0} & \mathbf{-1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} \mathbf{-} \begin{pmatrix} \lambda & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \lambda \end{pmatrix} = \begin{pmatrix} \mathbf{-}\ \lambda & \mathbf{-1} & \mathbf{0} \\ \mathbf{1} & \mathbf{-}\ \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1}\ \mathbf{-}\ \lambda \end{pmatrix}$$

$P_A(\lambda) = \mathbf{det}(A - \lambda I) = -\lambda(-\lambda)(1-\lambda) + 1(1-\lambda)$

$$\begin{aligned} \mathbf{det}(A - \lambda I) = 0 &\Leftrightarrow (1-\lambda)(\lambda^2+1) = 0 \Leftrightarrow \\ &\Leftrightarrow 1 - \lambda = 0 \vee \lambda^2 + 1 = 0 \Leftrightarrow \\ &\Leftrightarrow \lambda = 1 \vee \lambda = \pm\sqrt{-1} = \pm\, i \end{aligned}$$

Assim, o produto dos valores próprios é igual ao $\mathbf{det}(A)$**:**

$$1 \times i \times(-i) = 1 \times -i^2 = 1 \times 1 = 1 \text{ , c.d.q.}$$

Seja

$$U = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{-1} \end{pmatrix}$$

A matriz U representa a reflexão no plano (x,y). Se $A \in \mathbb{O}(3)$ e $A \notin \mathbb{SO}(3)$, então $AU \in \mathbb{SO}(3)$, pois o determinante é igual a $+1$.

Escreve-se A como um produto:

$$(AU)U \text{ obtendo-se } f_A = f_{AU} f_U$$

Como f_{AU} é uma rotação, consequentemente, f_A é uma reflexão no plano (x,y) seguida de uma rotação. Normalmente referimos $\mathbb{SO}(3)$ como sendo o grupo das rotações a três dimensões. Se um sólido regular estiver posicionado em $\mathbb{R}^3$ com o centro de gravidade na origem, então cada simetria é representada por uma matriz de $\mathbb{O}(3)$. O grupo das simetrias rotacionais é, portanto, isomorfo ao subgrupo de $\mathbb{SO}(3)$, e o grupo de todas as simetrias é isomorfo ao grupo $\mathbb{O}(3)$.

2.1.3 Subgrupos finitos de $\mathbb{SO}(3)$

Teorema 2.1 ***[5], pág.104***
Seja $\mathbb{G}$ um subgrupo finito de $\mathbb{O}(2)$. Então $\mathbb{G}$ é cíclico ou diedral. Mais especificamente, se $\mathbb{G}$ for subgrupo de $\mathbb{SO}(2)$, então ele será cíclico, pois admite apenas rotações.

A ideia desta demonstração é dada a seguir.
Demonstração Seja $\mathbb{G}$ um subgrupo finito não trivial de $\mathbb{O}(2)$. Supondo primeiro que $\mathbb{G} \subset \mathbb{SO}(2)$, devemos olhar para a matriz da rotação de menor ângulo de $\mathbb{G}$, matriz para a qual temos uma caracterização em função do

ângulo. Assim, devemos concluir que esta matriz gera $\mathbb{G}$ e $\mathbb{G}$ é cíclico.
Se $\mathbb{G}$ não estiver contido em $\mathbb{SO}(2)$, então tomemos,

$$\mathbb{H} = \mathbb{G} \cap \mathbb{SO}(2)$$

Assim, $\mathbb{H}$ é um subgrupo de $\mathbb{G}$ cujo índice é igual a 2 e, pela primeira parte, $\mathbb{H}$ é cíclico porque está contido em $\mathbb{SO}(2)$. Escolhe-se um gerador a para $\mathbb{H}$ e um elemento b de $\mathbb{G} - \mathbb{H}$. Como b representa uma reflexão, temos $b^2 = I$. Se $a = I$, então $\mathbb{G}$ consiste em I e b e é um grupo cíclico de ordem 2. Aliás, a ordem de a é um inteiro para $n \geq 2$. Os elementos de $\mathbb{G}$ são agora:

$$I \ , \ a \ , \ ... \ , \ a^{n-1} \ , \ b \ , \ ab \ , \ ... \ , \ a^{n-1}b$$

e satisfazem $a^n = I$, $b^2 = I$, $ba = a^{-1}b$. Neste caso a correspondência:

$$a \to r \ , \ b \to s$$

determina um isomorfismo entre $\mathbb{G}$ e o grupo diedral $\mathbb{D}(n)$. $\square$

Teorema 2.2 ***[5], pág.105***
Um subgrupo finito de $\mathbb{SO}(3)$ ***é isomorfo a um grupo cíclico, ou a um grupo diedral,*** $\mathbb{D}(n)$***, ou ao grupo de rotações de um dos sólidos de Platão, ou seja,*** $\mathbb{A}_4$***,*** $\mathbb{S}_4$ ***ou*** $\mathbb{A}_5$***.***

A seguir, será descrito em pormenor cada um dos grupos ou família de grupos referidos no anterior teorema.

2.1.4 Grupos cíclicos

Se $\mathbb{G}$ é um grupo e $g \in \mathbb{G}$ então $< g > = \{g^n | \ n \in \mathbb{Z}\}$ é chamado de subgrupo cíclico gerado por g. Se $< g > = \mathbb{G}$, então $\mathbb{G}$ é um grupo cíclico.

Exemplo 2.2 ***[7], pág.51***
Para um hexágono regular, seja r ***uma rotação segundo um ângulo, no***

sentido contrário ao dos ponteiros do relógio, de amplitude igual a 60^0***. Assim, o grupo de todas as simetrias rotacionais do hexágono consiste em seis rotações,***

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

com $r^6 = e$***. O grupo é chamado de grupo cíclico de ordem*** 6***, gerado por*** r***.***

Exemplo 2.3 ***[7], pág.51***
Se L ***é uma linha infinita com todos os pontos inteiros, então uma simetria desta linha*** L ***é a translação*** T ***à direita segundo uma unidade. Todas as translações desta linha formam um grupo,***

$$\ldots\ ,\ T^{-3}\ ,\ T^{-2}\ ,\ T^{-1}\ ,\ 1\ ,\ T\ ,\ T^2\ ,\ T^3\ ,\ \ldots,$$

um grupo cíclico "infinito". Este grupo é isomorfo ao grupo aditivo de todos os inteiros.

Teorema 2.3 ***[6], pág.65***
Qualquer grupo cíclico infinito é isomorfo a $\mathbb{Z}$***. O grupo cíclico de ordem*** n ***é isomorfo a*** $\mathbb{Z}/n\mathbb{Z}$***.***

Demonstração Seja $\mathbb{G}$ **um grupo cíclico com gerador** g**. Define-se a função:**

$$f\colon \mathbb{Z} \to \mathbb{G} \qquad \textbf{por} \qquad f\colon m \mapsto g^m$$

para $m \in \mathbb{Z}$**. Uma vez que,**

$$f(m_1 + m_2) = g^{m_1+m_2} = g^{m_1}g^{m_2} = f(m_1)f(m_2),$$

f **é um isomorfismo. Uma vez que,** $\mathbb{G} = < g >$ **então** f **é sobrejectiva. Existem agora duas possibilidades. Uma supondo que** $|\mathbb{G}| = \infty$**. Então**

$$\alpha^m \neq 1,\ \forall_{m \neq 0}$$

Se existem m_1 **e** m_2 **tais que** $g^{m_1} = g^{m_2}$ **então** $g^{m_1-m_2} = 1$**. Sendo assim,**

$$m_1 - m_2 = 0$$

Assim, f é injectiva e, portanto, é um isomorfismo.
A segunda possibilidade é que $|\mathbb{G}| = n$, para algum $n \in \mathbb{N}$, isto é, a ordem de g é n. Ora,

$$f(m + sn) = g^{m+sn} = g^m = f(m), \forall_s$$

Assim, f define a função:

$$\overline{f}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{G}$$

o que é também um homomorfismo sobrejectivo. Uma vez que ambos os grupos têm ordem n, isto implica que f é injectiva e, assim, um isomorfismo.
□

Dois quaisquer grupos cíclicos com a mesma ordem são isomorfos. Não é verdade, em geral, que dois grupos com a mesma ordem sejam isomorfos.

Por exemplo, o grupo de Klein

$$\mathbb{K} = \{e, a, b, ab\},\ a^2 = b^2 = (ab)^2 = e$$

que tem ordem 4, não é isomorfo ao grupo cíclico de ordem 4,

$$\mathbb{C}_4 = \{e, r, r^2, r^3\},$$

porque não tem nenhum elemento de ordem 4.

Em geral, se $g \in \mathbb{G}$, então o subgrupo gerado por g, escrito $< g >$, é o subgrupo de todos os elementos de $\mathbb{G}$ que possam ser expressos em termos de elementos de g e seus inversos. De uma forma mais precisa, se $\mathbb{G}$ é finito, então temos,

$$< g >= \bigcup_{i=0}^{\infty} g^i.$$

Por outro lado se a descrição é mais complicada, deve-se incluir expressões com a forma: $\alpha_1^{e_1}\ \alpha_2^{e_2}\ ...\ \alpha_k^{e_k}$ onde $e_i = \pm 1$, $\forall_i$ e $\alpha_i \in g$. Este tipo de expressões são chamadas palavras em g.

Proposição 2.1 ***[7], pág.54***
Qualquer subgrupo de um grupo cíclico é cíclico.

Demonstração Para o grupo cíclico infinito $\mathbb{Z}$, demonstra-se que qualquer subgrupo de $\mathbb{Z}$ é um conjunto $n\mathbb{Z}$ de todos os múltiplos inteiros de um $n \geq 1$. Facilmente vemos que estes conjuntos $n\mathbb{Z}$ são subgrupos. Por outro lado, seja $\mathbb{S}$ um subgrupo próprio do grupo aditivo $\mathbb{Z}$. Considere-se o menor positivo $n \in \mathbb{S}$. Todo o inteiro múltiplo de n está em $\mathbb{S}$. Por outro lado, se $k \in \mathbb{S}$, o algoritmo da divisão dá-nos $k = qn + r$ com $0 \leq r < n$ e $k \in \mathbb{S}$, $qn \in \mathbb{S}$ implica $r \in \mathbb{S}$. Uma vez que n seja o menor elemento positivo de $\mathbb{S}$, relembrando que r deverá ser igual a zero e $k = qn$. Os elementos de $\mathbb{S}$ são exactamente os múltiplos de n.
Para um grupo cíclico finito $\mathbb{C}_n$ com gerador c de ordem n, demonstra-se que qualquer subgrupo de $\mathbb{C}_n$ é cíclico com gerador c^k de ordem n/k, onde k é um divisor positivo de n. Na verdade dado k tal que, $n = km$, as diferentes potências de c^k são 1, c^k, c^{2k},... , $c^{(m-1)k}$, com $c^{mk} = 1$. Elas formam um subgrupo de $\mathbb{C}_n$ cíclico de ordem m; ou seja, com m elementos. Por outro lado, se $\mathbb{S}$ é um qualquer subgrupo de $\mathbb{C}_n$, então existe um menor inteiro positivo k para o qual $c^k \in \mathbb{S}$. Uma que vez $1 = c^n \in \mathbb{S}$, o algoritmo de divisão mostra que k é um divisor de n e que $\mathbb{S}$ consiste exactamente em $m = n/k$ potências distintas de c^k, tal como queriamos demonstrar. □

2.1.5 Grupos diedrais

Vamos descrever os grupos diedrais de ordem n, denotados por $\mathbb{D}(n)$, sendo $n \in \mathbb{N}$.

Para $n = 1$, temos o grupo das simetrias de um triângulo isósceles:

$$\mathbb{D}(1) = \{e \ , \ s\},$$

onde e e s representam a identidade e a reflexão em torno do eixo que contém a altura relativa ao lado diferente, respectivamente.

$\mathbb{D}(1)$	e	s
e	e	s
s	(s)	e

Tabela 2.1: Tabela de Cayley para o grupo $\mathbb{D}(1)$

Para dispor os elementos do grupo acima foi utilizada uma tabela de multiplicação denominada por tabela de Cayley. Este tipo de tabela é quadrada, $n \times n$, e os produtos obtidos são o resultado da intersecção da linha pela coluna, por exemplo: $se = s$. Cada elemento aparece apenas uma vez em cada linha e em cada coluna da tabela. Em particular, a identidade ocorre exactamente uma vez em cada linha, o que corresponde ao facto de cada elemento do grupo ter um único inverso.

Para $n = 2$, temos o grupo das simetrias de um rectângulo:

$$\mathbb{D}(2) = \{e \ , \ r \ , \ s_1 \ , \ s_2\}$$

Na composição de isometrias, e representa a transformação identidade, r representa a rotação de π e s_1 e s_2 representam as reflexões em torno dos eixos de simetria do rectângulo.

$\mathbb{D}(2)$	e	r	s_1	s_2
e	e	r	s_1	s_2
r	r	e	s_2	s_1
s_1	s_1	s_2	e	r
s_2	s_2	s_1	r	e

Tabela 2.2: Tabela de Cayley para o grupo $\mathbb{D}(2)$

Analisando a tabela verifica-se que esta é simétrica, portanto o grupo é comutativo.

Exemplo 2.4 ***Na composição das isometrias,*** $s_1 r$***, primeiro calcula-se a rotação,*** r***, e só depois a reflexão,*** s_1**.**

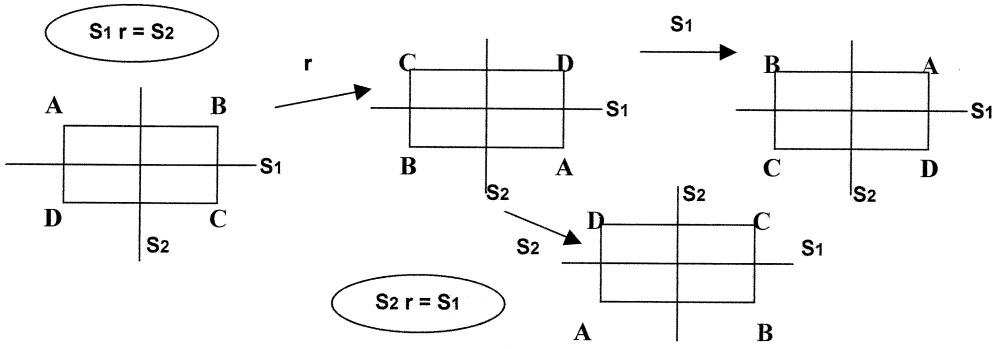

Figura 2.1: Composição de isometrias do rectângulo

Para $n > 2$, o grupo $\mathbb{D}(n)$ representa o conjunto das simetrias de um polígono regular de n lados. Trata-se de um grupo não abeliano, composto por $2n$ elementos, isto é, de ordem $2n$, para a composição de simetrias. Este grupo é constituído por n rotações de $\frac{2k\pi}{n}$ em torno do centro do polígono (para $k = 0, 1, 2, ..., n-1$), num dos sentidos (por exemplo, no sentido directo), e

por n reflexões em torno dos eixos de simetria do polígono. Denotando por r a rotação de $\frac{2\pi}{n}$, o conjunto das rotações é:

$$\{e \ , \ r \ , \ r^2 \ , \ ... \ , \ r^{n-1}\}$$

Se s é a reflexão de π em torno de um eixo de simetria, então todas as outras reflexões são da forma $r^i s$ para $i = 1 \ , \ ... \ , \ n-1$.

Assim, temos que:

$$\mathbb{D}(n) = \{e \ , \ r \ , \ r^2 \ , \ ... \ , \ r^{n-1} \ , \ s \ , \ rs \ , \ r^2 s \ , \ ... \ , \ r^{n-1}s\},$$

sendo $r^n = e$ e $s^2 = e$.

Verifica-se que $sr = r^{n-1}s$, ou seja, $sr = r^{-1}s$, visto que:

$$r^{n-1} = r^n \times r^{-1} = e \times r^{-1} = r^{-1}$$

Todos os outros produtos podem ser calculados a partir destas igualdades. Por exemplo,

$$sr^2 = (sr)r = (r^{-1}s)r = r^{-1}(sr) = r^{-1}r^{-1}s = r^{-2}s = r^{n-2}s$$

Para $n = 3$, temos o grupo das simetrias de um triângulo equilátero:

$$\mathbb{D}(3) = \{e \ , \ r \ , \ r^2 \ , \ s \ , \ rs \ , \ r^2 s\}$$

Na composição de isometrias, e representa a transformação identidade, r representa a rotação de $\frac{2\pi}{3}$ e s representa a reflexão de π em torno dos eixos.

Consideremos a figura a seguir:

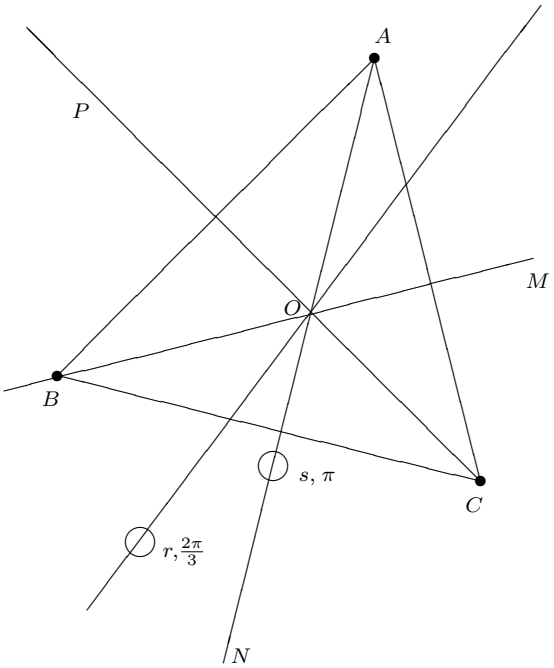

Figura 2.2: Simetrias do triângulo equilátero

Ao analisarmos a figura, verificamos que AN é um eixo de simetria e a recta que passa pelo ponto O é o eixo de rotação segundo o ângulo $\frac{2\pi}{3}$.

Ao combinarmos estes dois tipos de simetrias obtemos, por exemplo, um elemento pertencente a este grupo. Vamos algébrica e geometricamente verificar o que foi dito, considerando a figura[1] seguinte:

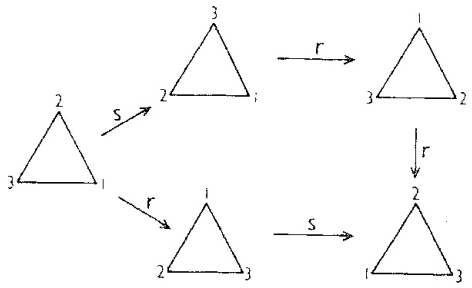

Figura 2.3: Composição de isometrias do triângulo equilátero

Verificamos geometricamente que:$rs = sr^2$ e, é um elemento de $\mathbb{D}(3)$.

[1]figura do livro, "Groups and Symmetry", M.A. Armstrong, Springer, 1988, pág.16

Algebricamente

$sr^2 = srr = (sr)r = (r^{-1}s)r =$

$=_{(1)}(r^2s)r = r^2(sr) = r^2(r^{-1}s) = r^2(r^2s) =$

$= r^4s = r^3(rs) =_{(2)} e(rs) = rs$

Nota

(1) $r^{-1} = r^{n-1} =_{(2)} r^{3-1} = r^2$

(2) $n = 3$

Na demonstração aplicou-se a propriedade associativa, várias vezes, e verificou-se a não existência da propriedade comutativa.

Consideremos, ainda, mais três exemplos:

Exemplo 2.5 $r(r^2s) = r^3s = es = s$

Exemplo 2.6 $(r^2s)(rs) = r^2(s(rs)) = r^2((sr)s) =$

$= r^2((r^2s)s) = r^2(r^2s^2) =$

$= r^4s^2 = r^3rs^2 = ere = r$

Exemplo 2.7 $(r^2s)(r^2s) = r^2(sr^2)s = r^2(rs)s = r^3s^2 = e$

Passemos agora à construção da tabela relativa ao grupo de simetrias do triângulo equilátero:

$\mathbb{D}(3)$	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	sr	sr^2	e	r^2	r
rs	rs	s	sr	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

Tabela 2.3: Tabela de Cayley para o grupo $\mathbb{D}(3)$

Conclusão Como se verifica pela tabela este grupo não goza da propriedade comutativa.

Para $n = 4$, temos o grupo das simetrias de um quadrado.
Quadrado centrado na origem e com os vértice sobre os eixos.

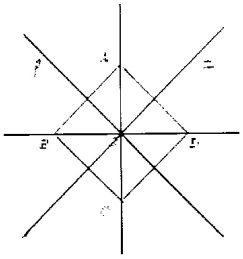

Figura 2.4: Simetrias do quadrado

Como as simetrias de um conjunto de pontos formam um grupo e

$$r^4 = s^2 = e,$$

podemos concluir que o quadrado é invariante pelas quatro rotações:

$$r, r^2, r^3, r^4,$$

designadas por simetrias pares, visto tratar-se de produtos de isometrias pares e para as quatro simetrias ímpares: rs , r^2s , r^3s , $r^4s = s$; **uma vez termos produtos de uma isometria par por uma isometria ímpar.**
Podemos assim garantir que o quadrado admite pelo menos as oito simetrias consideradas. No entanto, sendo A e B dois vértices adjacentes do quadrado, ao aplicarmos uma simetria ao quadrado, a imagem de A só pode ocupar quatro posições distintas (as que correspondem aos quatro vértices).

Ao fixarmos a posição da imagem de A, a imagem de B só pode ocupar duas posições, as dos vértices adjacentes à imagem de A. Ao fixarmos as posições das imagens de A e de B, as dos restantes vértices ficam univocamente determinadas.

Deste modo, concluímos que o quadrado admite no máximo $4 \times 2 = 8$ simetrias possíveis. Assim, existem exactamente 8 simetrias do quadrado, que são as anteriormente referidas.

Podemos então afirmar que o grupo das simetrias do quadrado é gerado por r e s. Este grupo é designado por $\mathbb{D}(4)$ e tem ordem 8:

$$\mathbb{D}(4) = \{\mathbf{e} \ , \ \mathbf{r} \ , \ \mathbf{r}^2 \ , \ r^3 \ , \ s \ , \ rs \ , \ r^2s \ , \ r^3s \ \}$$

A tabela de Cayley (transformações involutivas) associada ao grupo $\mathbb{D}(4)$ é:

$\mathbb{D}(4)$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	sr	sr^2	sr^3	e	r^3	r^2	r
rs	rs	s	sr	sr^2	r	e	r^3	r^2
r^2s	r^2s	sr^3	s	sr	r^2	r	e	r^3
r^3s	r^3s	sr^2	sr^3	s	r^3	r^2	r	e

Tabela 2.4: Tabela de Cayley para o grupo $\mathbb{D}(4)$

Mais uma vez se verifica que, para $n = 4$ o grupo $\mathbb{D}(4)$ é um grupo não abeliano.

2.1.6 Grupos de rotações dos sólidos de Platão

Existem cinco sólidos de Platão[2]: o tetraedro, o cubo, o octaedro, o dodecaedro e o icosaedro. São sólidos convexos que se diferenciam dos restantes por as suas faces serem polígonos regulares e cada um de seus vértices ter o mesmo número de arestas.

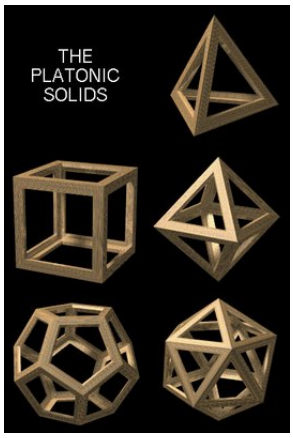

Figura 2.5: Sólidos platónicos

Às isometrias de $\mathbb{R}^3$ que deixam o poliedro invariante chamamos simetrias ou transformações de simetrias do poliedro.
As isometrias no espaço são designadas por: translação, reflexão(espacial), rotação(em torno de um eixo), parafuso(ou o deslocamento helicoidal), reflexão deslizante, reflexão rotativa e inversão central.
Como pretendemos as isometrias que deixam invariante um certo poliedro regular, devemos excluir imediatamente as translações e as isometrias que envolvam translações: o parafuso e a reflexão deslizante.
É entre as outras isometrias: rotação, reflexão, reflexão rotativa e inversão central que encontraremos as transformações de simetria do poliedro.
O tetraedro, por exemplo, é formado por quatro vértices equidistantes e, cada três vértices formam um triângulo equilátero. As simetrias obtidas

[2]Figura obtida através do site "Google"

serão fundamentais para a argumentação do teorema principal 2.2 referido na página 21.
Como já foi mencionado procuramos as rotações do espaço que levam cada sólido nele mesmo. Inicialmente vamos notar que o cubo é dual do octaedro, ou seja, podemos inscrever um cubo no octaedro de forma que cada vértice do cubo esteja no centro da face do octaedro e vice-versa. Da mesma forma o dodecaedro é dual do icosaedro e o tetraedro é dual de si próprio.
Este argumento, é importante pois ele, evidencia que o grupo de rotações do cubo é igual ao do octaedro e que o grupo de rotações do dodecaedro é igual ao do icosaedro.

2.1.6.1 Simetrias de rotação do tetraedro

Um tetraedro tem quatro faces iguais a triângulos equiláteros. Assim temos dois tipos de simetrias de rotação, ou seja, segundo um eixo de grau dois e segundo um eixo de grau três. Entendendo-se por eixo de grau dois, um eixo que intersecta os pontos médios de um par de arestas opostas, formando-se, assim, uma rotação segundo um ângulo π diferente da identidade.
Um eixo de grau três, entende-se como sendo um eixo que intersecta um vértice e um ponto no centro da face oposta, formado-se duas rotações diferentes da identidade, uma segundo um ângulo de $\frac{2\pi}{3}$ e outra segundo um ângulo de $\frac{4\pi}{3}$.

Assim, o número de simetrias de rotação do tetraedro é:

$$3 \times 1 + 4 \times 2 = 11$$

Com a identidade temos 12 simetrias de rotação, todas elas produzem permutações pares nas faces.

2.1.6.2 Simetrias de rotação do cubo

Um cubo tem seis faces iguais a quadrados. Assim temos três tipos de simetrias de rotação, ou seja, um eixo de grau dois, por cada par de arestas opostas, temos uma rotação segundo um ângulo π diferente da identidade; um eixo de grau três, por cada par de vértices opostos, temos duas rotações diferentes da identidade, uma segundo um ângulo de $\frac{2\pi}{3}$ e outra segundo um ângulo $\frac{4\pi}{3}$ por último, temos um eixo de grau quatro, por cada par de faces opostas, temos três rotações diferentes da identidade, uma segundo um ângulo de $\frac{\pi}{2}$, outra segundo um ângulo de $\frac{2\pi}{2}$ e, finalmente, segundo um ângulo de $\frac{3\pi}{2}$.
Assim, o número de simetrias de rotação do cubo é:

$$6 \times 1 + 4 \times 2 + 3 \times 3 = 23$$

Com a identidade temos 24 simetrias de rotação.

2.1.6.3 Simetrias de rotação do dodecaedro

Um dodecaedro tem doze faces iguais a pentágonos regulares. Assim temos três tipos de simetrias de rotação, ou seja, um eixo de grau dois, por cada par de arestas opostas, temos uma rotação segundo um ângulo de π diferente da identidade; um eixo de grau três, por cada par de vértices opostos, temos duas rotações diferentes da identidade, uma segundo um ângulo de $\frac{2\pi}{3}$ e outra segundo um ângulo $\frac{4\pi}{3}$ e, ainda, um eixo de grau cinco, por cada par de faces opostas, temos quatro rotações diferentes da identidade, uma segundo um ângulo de $\frac{2\pi}{5}$, segundo um ângulo de $\frac{4\pi}{5}$, segundo um ângulo de $\frac{6\pi}{5}$ e, por último, uma rotação segundo um ângulo de $\frac{8\pi}{5}$. Assim, o número de simetrias do dodecaedro é:

$$15 \times 1 + 10 \times 2 + 6 \times 4 = 59$$

Com a identidade temos 60 simetrias de rotação.

2.2 Introdução ao software GAP

O software "GAP"(Groups, Algorithms and Programing), começou por ser um sistema computacional para ser utilizado no estudo de grupos, mas o seu uso tem sido alargado devido ao elevado número "share-packages"existente. O mesmo software tem sido utilizado na realização de muitos trabalhos de investigação e, também, no uso do ensino, especialmente para ensinar a "Teoria de Grupos".

Após esta pequena introdução, iremos com um exemplo aplicar todas as noções sobre grupos mencionadas até aqui, assim como serão dadas algumas intruções básicas[3] necessárias à utilização do software "GAP".

Na área de trabalho da janela do GAP, a última linha que se visualiza

```
gap>
```

está pronta a receber instruções.

Instruções básicas

Para terminar uma sessão GAP basta escrever quit; seguido de return, ou pressionar em simultâneo as teclas ctrl-d.
Devido a erros, o GAP entra num break loop (ciclo vicioso). Isto é indicado por

```
brk>
```

[3] "Generalidades sobre o GAP", curso da faculdade de Ciências. E outros.

A saída do ciclo faz-se como a do próprio GAP: escreve-se quit; seguido de return, ou pressionam-se em simultâneo as teclas ctrl-d. Para fazer um comentário no GAP utiliza-se o símbolo

#

no início da linha.
Cada instrução dada deve terminar sempre com ; (ponto e vírgula) para que o GAP execute a instrução e dê a respectiva resposta. Dois pontos e vírgula ;; a seguir a uma instrução fazem com que o GAP execute a instrução mas não mostre a resposta ao utilizador.

2.2.1 Aplicação do software GAP no estudo de grupos

O nosso problema começa com a representação do grupo $\mathbb{D}(4)$. Assim, começamos por definir o primeiro e segundo comandos, com a atribuição das letras "a"e "b", às matrizes geradoras do grupo $\mathbb{D}(4)$:

```
gap> a:=[[0,-1,0],[1,0,0],[0,0,1]];
[ [ 0, -1, 0 ], [ 1, 0, 0 ], [ 0, 0, 1 ] ]

gap> b:=[[1,0,0],[0,-1,0],[0,0,-1]];
[ [ 1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, -1 ] ]
```

Determinação dos elementos do grupo $\mathbb{D}(4)$, através das matrizes geradoras

```
gap> D4:=Group(a,b);
Group([ [ [ 0, -1, 0 ], [ 1, 0, 0 ], [ 0, 0, 1 ] ],
  [ [ 1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, -1 ] ] ])

gap> Elements(D4);
[ [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ] ],
```

```
  [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
  [ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ],
  [ [ 0, -1, 0 ], [ 1, 0, 0 ], [ 0, 0, 1 ] ],
  [ [ 0, 1, 0 ], [ -1, 0, 0 ], [ 0, 0, 1 ] ],
  [ [ 0, 1, 0 ], [ 1, 0, 0 ], [ 0, 0, -1 ] ],
  [ [ 1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, -1 ] ],
  [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ] ]
```

Constatamos, assim, a existência de 8 matrizes, dado que o grupo tem ordem 8.

Determinação das classes de conjugação de $\mathbb{D}(4)$

```
gap> ConjugacyClasses(D4);
[ [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ]^G,
  [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ]^G,
  [ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ]^G,
  [ [ 0, -1, 0 ], [ 1, 0, 0 ], [ 0, 0, 1 ] ]^G,
  [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ] ]^G ]
```

Verificamos que existem 5 classes disjuntas, ou seja, não têm elementos em comum. A letra G **refere-se ao grupo** $\mathbb{D}(4)$**.**

Determinação dos elementos das classes de conjugação.

Classe de conjugação de: [[1,0,0],[0,1,0],[0,0,1]]

```
gap> c:=ConjugacyClass(d4,[[1,0,0],[0,1,0],[0,0,1]]);
[ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ]^G
gap> Elements(c);
[ [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ] ]
```

Classe de conjugação de : [[$-$1,0,0],[0,1,0],[0,0, $-$ 1]]

```
gap> d:=ConjugacyClass(d4,[[-1,0,0],[0,1,0],[0,0,-1]]);
[ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ]^G
gap> Elements(d);
[ [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
  [ [ 1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, -1 ] ] ]
```

Classe de conjugação de : $[[0,-1,0],[-1,0,0],[0,0,-1]]$

```
gap> e:=ConjugacyClass(d4,[[0,-1,0],[-1,0,0],[0,0,-1]]);
[ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ]^G
gap> Elements(e);
[ [ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ],
  [ [ 0, 1, 0 ], [ 1, 0, 0 ], [ 0, 0, -1 ] ] ]
```

Classe de conjugação de : $[[0,-1,0],[1,0,0],[0,0,1]]$

```
gap> f:=ConjugacyClass(d4,[[0,-1,0],[1,0,0],[0,0,1]]);
[ [ 0, -1, 0 ], [ 1, 0, 0 ], [ 0, 0, 1 ] ]^G
gap> Elements(f);
[ [ [ 0, -1, 0 ], [ 1, 0, 0 ], [ 0, 0, 1 ] ],
  [ [ 0, 1, 0 ], [ -1, 0, 0 ], [ 0, 0, 1 ] ] ]
```

Classe de conjugação de : $[[-1,0,0],[0,-1,0],[0,0,1]]$

```
gap> g:=ConjugacyClass(d4,[[-1,0,0],[0,-1,0],[0,0,1]]);
[ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ] ]^G
gap> Elements(g);
[ [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ] ] ]
```

Atribuição das letras h e i a dois geradores de um subgrupo de $\mathbb{D}(4)$

```
gap> h:=[[-1,0,0],[0,1,0],[0,0,-1]];
[ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ]
```

```
gap> i:=[[-1,0,0],[0,1,0],[0,0,1]];
[ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ]
```

Determinação dos elementos do subgrupo através dos geradores acima mencionados:

```
gap> C:=Group(h,i);
Group([ [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
  [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ] ])
```

```
gap> Elements(C);
[ [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
  [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ],
  [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
  [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ] ]
```

Será, C, um subgrupo Normal de $\mathbb{D}(4)$**?**

```
gap> IsNormal(D4,C);
false
```

Significa que não existem classes de conjugação completas que possam formar o subgrupo C.

Determinação de dois geradores do grupo inicial

```
gap> j:=[[0,-1,0],[-1,0,0],[0,0,-1]];
[ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ]
```

```
gap> l:=[[1,0,0],[0,-1,0],[0,0,-1]];
[ [ 1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, -1 ] ]
```

Determinação dos elementos de um subgrupo $\mathbb{H}\subset\mathbb{D}(4)$:

```
gap> j:=[[0,-1,0],[-1,0,0],[0,0,-1]];
[ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ]

gap> g:=[[0,1,0],[1,0,0],[0,0,-1]];
[ [ 0, 1, 0 ], [ 1, 0, 0 ], [ 0, 0, -1 ] ]

gap> H:=Group(j,g);
Group([ [ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ],
  [ [ 0, 1, 0 ], [ 1, 0, 0 ], [ 0, 0, -1 ] ] ])

gap> Elements(H);
[ [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ] ],
  [ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ],
  [ [ 0, 1, 0 ], [ 1, 0, 0 ], [ 0, 0, -1 ] ],
  [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ] ]
```

Será o subgrupo $\mathbb{H}$ **um subgrupo Normal**

```
gap> IsNormal(D4,H);
true
```

Capítulo 3

Permutações

Uma permutação de um conjunto $\mathbb{X}$ não é mais do que uma função bijectiva,

$$f\colon \mathbb{X} \to \mathbb{X}$$

O conjunto $\mathbb{S}_{\mathbb{X}}$, não vazio, das permutações de $\mathbb{X}$ é um grupo para a composição de funções, designado por grupo simétrico.

Se $\mathbb{X}$ é infinito então $\mathbb{S}_{\mathbb{X}}$ é um grupo infinito. Se $\mathbb{X}$ tem n elementos, por exemplo:

$$\mathbb{X} = \{\ 1\ ,\ 2\ ,\ 3\ ,\ \ldots\ ,\ n\ \},$$

o grupo simétrico correspondente denota-se por $\mathbb{S}_n$ e tem ordem $n!$.

Permutações $f \in \mathbb{S}_n$ podem ser representadas na forma:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$$

Exemplo 3.1 ***Se*** $\mathbb{X} = \{1\ ,\ 2\ ,\ 3\}$***, o grupo*** $\mathbb{S}_n = \mathbb{S}_3$ ***é constituído por*** $n! = 3! = 6$ ***elementos representados a seguir.***

$$f = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{1} & \mathbf{3} & \mathbf{2} \end{pmatrix}, \mathbf{g} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{2} & \mathbf{1} \end{pmatrix}, \mathbf{h} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{3} \end{pmatrix},$$

$$i = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} \end{pmatrix}, \mathbf{j} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{1} & \mathbf{2} \end{pmatrix}, \mathbf{l} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}$$

Teorema 3.1 ***[2] (Teorema de Cayley), pág.57***
Subgrupos de grupos de permutações são exemplos universais de grupos no sentido que, todo o grupo é isomorfo a um tal subgrupo.

3.1 Permutação cíclica

Uma permutação chama-se permutação cíclica ou ciclo de comprimento k **ou ciclo de ordem** k **, se aplica** a_1 **em** a_2**,** a_2 **em** a_3**, ...,** a_{k-1} **em** a_k**,** a_k **em** a_1 **sendo** a_1**,** a_2**, ... ,** a_n **elementos de** $\mathbb{X}$ **distintos. Este ciclo denota-se por,**

$$(\mathbf{a}_1,\ a_2,\ ...,\ a_k)$$

Ciclos de comprimento $k = 2$ **chamam-se transposições.**

Os ciclos $(a_1,\ a_2,\ ...,\ a_k)$ **e** $(b_1,\ b_2,\ ...,\ b_k)$ **dizem-se disjuntos se:**

$$\{\ a_1,\ a_2,\ ...,\ a_k\ \} \cap \{\ b_1,\ b_2,\ ...,\ b_k\ \} = \emptyset$$

Teorema 3.2 ***[2], pág.63***
Todo o elemento de $\mathbb{S}_n$ ***é um produto de transposições.***

Existem várias maneiras de escrever um elemento de $\mathbb{S}_n$ como um produto de transposições. Por exemplo, a identidade de $\mathbb{S}_5$ pode ser escrita como $(1,2)(1,2)$, ou $(1,2)(1,2)(1,3)(1,3)$. Mais, duas transposições não precisam, necessariamente, de comutar. Por exemplo, $(1,3)(1,2) \neq (1,2)(1,3)$. Contudo, existe uma propriedade importante acerca de qualquer representação de uma permutação como produto de transposições. Esta propriedade tem a ver com a paridade do número de transposições usadas. O número de transposições é sempre par ou sempre ímpar. Assim, se

$$a_1\ a_2\ ...\ a_j = b_1\ b_2\ ...\ b_k \textbf{ com } a_i\textbf{´s e } b_i\textbf{´s transposições,}$$

então j e k são ambos pares ou ambos ímpares. (ver [2], pág.63).

Exemplo 3.2 ***Transformação do ciclo de comprimento*** 3 ***num produto de transposições:***

$$(1,b,a) = (1,a)(1,b)$$

Exemplo 3.3 ***A permutação*** $(1,5)(2,4,6)$ ***pode escrever-se à custa de*** 3**,** 5**,** 7 ***ou*** 25 ***transposições:***

$(1,5)(2,4,6) = (1,5)(2,6)(2,4) = (1,5)(1,2)(1,6)(1,2)(2,4) =$
$= (1,5)(1,2)(1,6)(1,2)(1,2)(1,4)(1,2) =$
$= (4,5)(3,4)(2,3)(1,2)(2,3)(3,4)(4,5)(1,2)(5,6)(4,5)(3,4)(2,3)(1,2)(2,3)(3,4)$
$(4,5)(5,6)(1,2)(1,2)(3,4)(2,3)(1,2)(2,3)(3,4)(1,2)$

Para $n \geq 3$, $\mathbb{S}_n$ é um grupo não comutativo, pois, por exemplo, $(1,3)(1,2) \neq (1,2)(1,3)$, ou seja,

$$(1,3)(1,2) = (1,2,3) \quad \textbf{e} \quad (1,2)(1,3) = (1,3,2)$$

Conclui-se, assim, que a composição das transposições anteriores dá-nos ciclos diferentes, quando trocamos a ordem das transposições.

Cada elemento de $\mathbb{S}_3$ pode ser escrito como um produto de permutações cíclicas. Mais como transposições ou composição de transposições:

$$\mathbb{S}_3 = \{\ (1,2)\ ,\ (1,3)\ ,\ (2,3)\ ,\ (1,2,3)\ ,\ (1,3,2)\ ,\ e\ \} =$$
$$=\{\ (1,2)\ ,\ (1,3)\ ,\ (2,3)\ ,\ (1,3)(1,2)\ ,\ (1,2)(1,3)\ ,\ e\ \}$$

Exemplo 3.4 ***Decomposição de permutações cíclicas em produtos de transposições.***

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (1,5)\ (2,4,6) = (1,5)(2,6)(2,4)$$

Note-se que, $(2,4,6) = (6,2,4) = (4,6,2)$**, portanto**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (1,5)(6,2,4) = (1,5)(6,4)(6,2) = (1,5)(4,6)(2,6)$$

Por outro lado,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (1,5)(4,6,2) = (1,5)(4,2)(4,6) = (1,5)(2,4)(2,6)$$

Nota O mesmo ciclo pode ser escrito como um produto de transposições, não precisando estas de serem disjuntas e a sua decomposição não é única.

Teorema 3.3 ***[5], pág.28***
O conjunto das transposições de $\mathbb{S}_n$ ***gera*** $\mathbb{S}_n$**.**

Outros conjuntos de geradores de $\mathbb{S}_n$:

(i) $\{(1,2)(1,3)...(1,$ **n**$)\}$**, porque toda a transposição** (a,b) **se pode escrever na forma:** $(a,b) = (1,a)(1,b)(1,a)$

Usando o teorema 3.3, da página 44 fica provado que o conjunto dado gera $\mathbb{S}_n$.

(ii) $\{(1,2)(2,3)...(n-1,n)\}$ **, uma vez que,**

$$(1,k) = (k-1,k)...(3,4)(2,3)(1,2)(2,3)(3,4) \text{ ... } (k-1,k)$$

Usando (i), verifica-se que este conjunto gera $\mathbb{S}_n$.

(iii) A transposição $(1,2)$ e o ciclo de ordem n, $(1,2,$ ...$,n)$ juntos geram $\mathbb{S}_n$, pois por (ii) basta escrever cada transposição da forma $(k,k+1)$ em termos de $(1,2)$ e $(1,2,...,n)$. Isto pode ser feito do seguinte modo. Note-se que,

$$(2,3) = (1,2, \text{...},n)^{2-1}(1,2)(1,2, \text{...},n)^{1-2} = (1,2, \text{... },n)^1(1,2)(1,2, \text{... },n)^{-1}$$

De uma forma geral:

$$(k,k+1) = (1,2, \text{... },n)^{k-1}\ (1,2)(1,2, \text{... },n)^{1-k} \text{ , } 2 \leq k < n$$

3.2 Subconjuntos de $\mathbb{S}_n$

Sejam $\mathbb{A}_n$ e $\mathbb{B}_n$ os subconjuntos de $\mathbb{S}_n$ constituídos pelas permutações que se podem escrever como um produto de um número par de transposições, as permutações pares, e as que se podem factorizar num número ímpar de transposições, as permutações ímpares, respectivamente.
Estas designações fazem sentido porque $\mathbb{A}_n$ e $\mathbb{B}_n$ são conjuntos disjuntos. (ver [2], pág.63).

A função φ: $\mathbb{A}_n \to \mathbb{B}_n$ definida por:

$$\varphi\ (f) = (1,2)f$$

é bijectiva, (ver teorema seguinte), o que prova que o número de permutações pares de $\mathbb{S}_n$ é igual ao número de permutações ímpares.

3.3 Subgrupo alterno

Teorema 3.4 ***[5], pág.29***
O subconjunto $\mathbb{A}_n$ das permutações pares é um subgrupo de $\mathbb{S}_n$ com ordem $\frac{n!}{2}$ e chama-se grupo alterno de grau n.

Demonstração Se f e g são permutações pares, escrevemos cada uma delas como um produto de um número par de transposições. O produto de f por g, fg, é par. Ao escrevermos o produto das transposições de f em ordem inversa, obtemos f^{-1} e, portanto, verifica-se que f^{-1} é par. A identidade é par, pois $e = (1,2)(1,2)$. Assim, as permutações pares formam um subgrupo de $\mathbb{S}_n$. Se f é par então $(1,2)f$ é ímpar. Isto emparelha os elementos de $\mathbb{S}_n$ e mostra que precisamente que metade deles é par. (Note-se que toda a permutação ímpar pode ser escrita como uma permutação par seguida de $(1,2)$). □

Teorema 3.5 ***[5], pág.30***
Para $n \geq 3$, $\mathbb{A}_n$ é gerado pelos ciclos da forma $(1, a, b)$.
Demonstração O subgrupo $\mathbb{A}_n$ é gerado pelos ciclos de comprimento três pois, como toda a permutação $f \in \mathbb{A}_n$ se pode escrever como produto de um número par de transposições da forma $(1, k)$, agrupando essas transposições duas a duas temos: $(1, a)(1, b) = (1, b, a)$ □

Exemplo 3.5

$$\textbf{Se} \quad |\mathbb{S}_3| = 3! = 6 \quad \textbf{então} \quad |\mathbb{A}_3| = \frac{3!}{2} = \frac{6}{2} = 3,$$

o que significa que temos 3 permutações pares.

Todos os elementos de $\mathbb{S}_3$:

$(2,3) = (1,2)(1,3)(1,2) = (1,2)(2,3)(1,2)(2,3)(1,2)$

$(1,3) = (2,3)(1,2)(2,3)$

$(1,2)$

$(1,2,3) = (1,3)(1,2)$

$(1,3,2) = (1,2)(1,3)$

$(1)(2)(3) = e$

Todos os elementos de $\mathbb{A}_3$ (grupo alterno de grau 3):

$(1,2,3) = (1,3)(1,2)$

$(1,3,2) = (1,2)(1,3)$

$(1)(2)(3) = e$

Todos os elementos de $\mathbb{B}_3$ (conjunto das permutações ímpares):

$(2,3) = (1,2)(1,3)(1,2) = (1,2)(2,3)(1,2)(2,3)(1,2)$

$(1,3) = (2,3)(1,2)(2,3)$

$(1,2)$

3.4 Sólidos de Platão e grupos simétricos

Os grupos de rotações dos sólidos platónicos, já mencionados no capítulo anterior, podem ser vistos como grupos de permutações. Pelo teorema de Cayley,

Teorema 3.6 ***[5], pág.41***

Se $\mathbb{H}$ é um grupo finito de ordem n, então $\mathbb{H}$ é isomorfo a um subgrupo

de $\mathbb{S}_n$**.**

3.4.1 Simetrias do tetraedro

Comecemos pelo tetraedro regular. Existem dois tipos de rotações, o primeiro tipo segundo os ângulos $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ **e o segundo tipo segundo o ângulo** π**. Desde que existam quatro vértices existem oito rotações do primeiro tipo e três rotações do segundo tipo. Juntos com a identidade o grupo simétrico tem assim 12 elementos.**
Tal como nos polígonos regulares, podemos recordar estas simetrias como permutações dos vértices do tetraedro. Assim o primeiro tipo de rotações correspondem ao ciclo de comprimento três e, o segundo ao produto de duas transposições disjuntas. Assim, estas com a identidade, são precisamente as doze permutações pares em $\mathbb{S}_4$**. Esta função é um homomorfismo e, portanto, o grupo próprio das simetrias de um tetraedro regular, que denotamos por** $\mathbb{T}$**, é isomorfo a** $\mathbb{A}_4$**.**

3.4.1.1 Determinação do número de elementos de $\mathbb{A}_4$ através do GAP

Os geradores de $\mathbb{A}_4$ **são ciclos de comprimento** 3 **de** $\mathbb{S}_4$**, pois podem ser escritos como um produto par de transposições (ver teorema 3.5 da página 46).**

```
gap> A4:=Group((2,3,4),(2,4,3),(1,2,3),(1,2,4),(1,3,2),(1,3,4),
(1,4,3),(1,4,2));(8 ciclos de ordem 3)

Group([ (2,3,4), (2,4,3), (1,2,3), (1,2,4), (1,3,2), (1,3,4), (1,4,2),
  (1,4,3) ])

gap> Size(a4);
```

```
12

gap> Elements(a4);
[ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2), (1,3,4),
  (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ]
```

Assim, pelo teorema 3.6 da página 47

$$|\mathbb{A}_4| = 12 \textbf{ então } |\mathbb{T}| = |\mathbb{A}_4| = 24$$

3.4.2 Simetrias do cubo

A seguir vamos olhar para as simetrias próprias do cubo. Denotemos este por $\mathbb{O}$.

Primeiro existem rotações segundo os centros e pares das faces opostas, segundo os ângulos $\frac{\pi}{2}$, $\frac{2\pi}{2}$ e $\frac{3\pi}{2}$. Segundo, através da diagonal, podemos rodar o cubo segundo os ângulos $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ juntando o par de vértices opostos. Terceiro, podemos rodar qualquer ângulo π segundo os pontos médios pares de arestas. Se recordarmos estas simetrias como permutações dos oito vértices, conseguimos o homomorfismo de $\mathbb{O}$ em $\mathbb{S}_8$, que certamente é injectivo. Agora, $|\mathbb{S}_8| = 40320$. Assim, a imagem é relativamente um grupo pequeno e, este homomorfismo não nos diz muito acerca de $\mathbb{O}$. Contudo, existem outras formas esclarecedoras de identificar $\mathbb{O}$ com o grupo de permutação. Em vez, de oito vértices, vamos tomar as quatro diagonais como objectos permutados. Vamos provar que esta função, segundo $\mathbb{S}_4$, é injectiva. Uma vez que $|\mathbb{S}_4| = 24$, o nosso homomorfismo é então um isomorfismo. Supondo que as simetrias próprias fixam as quatro diagonais. As rotações do primeiro tipo não fixam qualquer diagonal. As do segundo tipo fixam apenas a diagonal formada por um par de vértices. O terceiro tipo de simetrias não fixa diagonais, logo a rotação que fixa as quatro

diagonais é a identidade. Assim, o núcleo do nosso homomorfismo é trivial e, portanto, é injectivo.

3.4.2.1 Determinação do número de elementos de $\mathbb{S}_4$ através do GAP

```
Geradores de S4
gap> s4:=Group((1,2),(1,2,3,4));
Group([ (1,2), (1,2,3,4) ])

Número de elementos de S4
gap> Size(s4);
24

gap> Elements(s4);
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2), (1,2)(3,4), (1,2,3),
  (1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2), (1,3,4,2), (1,3), (1,3,4),
  (1,3)(2,4), (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3), (1,4), (1,4,2,3),
  (1,4)(2,3) ]
```

Assim, pelo teorema 3.6 da página 47

$$|\mathbb{S}_4| = 24 \textbf{ então } |\mathbb{O}| = |\mathbb{S}_4| = 24$$

3.4.3 Simetrias do dodecaedro

Finalmente, consideremos as simetrias próprias do dodecaedro regular, ou do seu dual, o icosaedro regular.
Existem três tipos de simetrias rotacionais. Primeiro, podemos rodar segundo os ângulos $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ através de um par de vértices opostos. Existem

vinte rotações deste tipo. Segundo, podemos rodar segundo qualquer ângulo de π, que passa pelos pontos médios de um par antipodal de arestas. Temos quinze destas rotações. E, finalmente, podemos rodar segundo uma linha que passa pelos centros de um par de faces opostos, segundo os ângulos $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$ e $\frac{8\pi}{5}$. Estas dão-nos mais vinte e quatro rotações. Ao todo existem sessenta simetrias próprias.

Seja $\mathbb{I}$ a designação do grupo próprio das simetrias de um dodecaedro regular ou icosaedro.

Podemos novamente recordar estas simetrias como permutações. As rotações de ordem três correspondem aos ciclos de comprimento três, as de ordem dois correspondem ao produto de duas transposições disjuntas e, as restantes rotações são de ordem cinco e correspondem aos ciclos de comprimento cinco. Repare-se que todas as permutações são pares. Como $\mathbb{A}_5$ tem sessenta elementos e estes escrevem-se à custa do produto de um número par de transposições, então $\mathbb{I}$ é isomorfo a $\mathbb{A}_5$.

3.4.3.1 Determinação do número de elementos de $\mathbb{S}_5$ através do GAP

```
gap> s5:=Group((1,2),(1,2,3,4,5));
Group([ (1,2), (1,2,3,4,5) ])

gap> Size(s5);
120

gap> Elements(s5);
[ (), (4,5), (3,4), (3,4,5), (3,5,4), (3,5), (2,3), (2,3)(4,5), (2,3,4),
  (2,3,4,5), (2,3,5,4), (2,3,5), (2,4,3), (2,4,5,3), (2,4), (2,4,5),
  (2,4)(3,5), (2,4,3,5), (2,5,4,3), (2,5,3), (2,5,4), (2,5), (2,5,3,4),
  (2,5)(3,4), (1,2), (1,2)(4,5), (1,2)(3,4), (1,2)(3,4,5), (1,2)(3,5,4),
  (1,2)(3,5), (1,2,3), (1,2,3)(4,5), (1,2,3,4), (1,2,3,4,5), (1,2,3,5,4),
```

```
(1,2,3,5), (1,2,4,3), (1,2,4,5,3), (1,2,4), (1,2,4,5), (1,2,4)(3,5),
(1,2,4,3,5), (1,2,5,4,3), (1,2,5,3), (1,2,5,4), (1,2,5), (1,2,5,3,4),
(1,2,5)(3,4), (1,3,2), (1,3,2)(4,5), (1,3,4,2), (1,3,4,5,2), (1,3,5,4,2),
(1,3,5,2), (1,3), (1,3)(4,5), (1,3,4), (1,3,4,5), (1,3,5,4), (1,3,5),
(1,3)(2,4), (1,3)(2,4,5), (1,3,2,4), (1,3,2,4,5), (1,3,5,2,4),
(1,3,5)(2,4), (1,3)(2,5,4), (1,3)(2,5), (1,3,2,5,4), (1,3,2,5),
(1,3,4)(2,5), (1,3,4,2,5), (1,4,3,2), (1,4,5,3,2), (1,4,2), (1,4,5,2),
(1,4,2)(3,5), (1,4,3,5,2), (1,4,3), (1,4,5,3), (1,4), (1,4,5), (1,4)(3,5),
(1,4,3,5), (1,4,2,3), (1,4,5,2,3), (1,4)(2,3), (1,4,5)(2,3), (1,4)(2,3,5),
(1,4,2,3,5), (1,4,2,5,3), (1,4,3)(2,5), (1,4)(2,5,3), (1,4,3,2,5),
(1,4)(2,5), (1,4,2,5), (1,5,4,3,2), (1,5,3,2), (1,5,4,2), (1,5,2),
(1,5,3,4,2), (1,5,2)(3,4), (1,5,4,3), (1,5,3), (1,5,4), (1,5), (1,5,3,4),
(1,5)(3,4), (1,5,4,2,3), (1,5,2,3), (1,5,4)(2,3), (1,5)(2,3), (1,5,2,3,4),
(1,5)(2,3,4), (1,5,3)(2,4), (1,5,2,4,3), (1,5,3,2,4), (1,5)(2,4,3),
(1,5,2,4), (1,5)(2,4) ]
```

3.4.3.2 Determinação do número de elementos do subgrupo alterno $\mathbb{A}_5$ através do GAP

Os geradores deste subgrupo são ciclos de ordem 3, pois só podem ser escritos como um produto par de transposições. (ver teorema 3.5 da página 46)

```
gap> a5:=Group((3,4,5),(3,5,4),(2,3,4),(2,3,5),(2,4,3),(2,4,5),(2,5,3),
(2,5,4),(1,2,3),(1,2,4),(1,2,5),(1,3,2),(1,3,4),(1,3,5),(1,4,2),(1,5,3),
(1,5,4));
```

```
Group([ (3,4,5), (3,5,4), (2,3,4), (2,3,5), (2,4,3), (2,4,5), (2,5,3),
(2,5,4), (1,2,3), (1,2,4), (1,2,5), (1,3,2), (1,3,4), (1,3,5), (1,4,2),
(1,5,3), (1,5,4) ])
```

```
gap> Size(a5);
60
```

```
gap> Elements(a5);
[ (), (3,4,5), (3,5,4), (2,3)(4,5), (2,3,4), (2,3,5), (2,4,3), (2,4,5),
(2,4)(3,5), (2,5,3), (2,5,4), (2,5)(3,4), (1,2)(4,5), (1,2)(3,4),
(1,2)(3,5), (1,2,3), (1,2,3,4,5), (1,2,3,5,4), (1,2,4,5,3), (1,2,4),
(1,2,4,3,5), (1,2,5,4,3), (1,2,5), (1,2,5,3,4), (1,3,2), (1,3,4,5,2),
(1,3,5,4,2), (1,3)(4,5), (1,3,4), (1,3,5), (1,3)(2,4), (1,3,2,4,5),
(1,3,5,2,4), (1,3)(2,5), (1,3,2,5,4), (1,3,4,2,5), (1,4,5,3,2),
(1,4,2), (1,4,3,5,2), (1,4,3), (1,4,5), (1,4)(3,5), (1,4,5,2,3),
(1,4)(2,3), (1,4,2,3,5), (1,4,2,5,3), (1,4,3,2,5), (1,4)(2,5),
(1,5,4,3,2), (1,5,2), (1,5,3,4,2), (1,5,3), (1,5,4), (1,5)(3,4),
(1,5,4,2,3), (1,5)(2,3), (1,5,2,3,4), (1,5,2,4,3), (1,5,3,2,4), (1,5)(2,4) ]
```

Assim, pelo teorema 3.6 da página 47

$$|\mathbb{A}_5| = 60 \textbf{ então } |\mathbb{H}| = |\mathbb{A}_5| = 60$$

Capítulo 4

Tabelas de caracteres

Neste capítulo vamos fazer um resumo da teoria de caracteres de grupos, com o objectivo de construir tabelas de caracteres.
Na secção 4.1. indicamos as ferramentas básicas para o estudo das representações de grupos. Este assunto leva-nos à teoria de caracteres (secção 4.2.), que é o estudo das representações através do traço. Um dos resultados fundamentais é o Teorema de Maschke, que implica que toda a representação linear é a soma directa de representações irredutíveis.

4.1 Representação de grupos

Nesta secção definimos representação de um grupo sobre o corpo $\mathbb{R}$ ou $\mathbb{C}$ e estudamos as suas propriedades básicas, tendo em vista o Teorema de Maschke. O grupo será sempre denotado por $\mathbb{G}$, com a operação escrita como multiplicação e o elemento identidade escrito como e. Focaremos o nosso estudo nos grupos finitos. Em particular, no fim, daremos ênfase ao grupo simétrico, $\mathbb{S}_n$.

Definição 4.1 ***[9], pág.198***
Uma representação de dimensão n ***de um grupo*** $\mathbb{G}$ ***abstracto é um homomorfismo de grupos***

$$D\colon \mathbb{G} \to \mathbb{GL}(n).$$

Nota A representação é designada de real, pois as entradas das matrizes de $\mathbb{GL}(n)$ são reais. Se as entradas fossem complexas a representação seria designada por representação complexa.

O núcleo da representação D, denotado $\ker(D)$, mede a quantidade de informação que é perdida ao passar para $\mathbb{GL}(n)$. Uma representação com núcleo {e} é designada de "faithful".

Definição 4.2 ***[8], pág.119***
Seja $\mathbb{D}$ ***uma representação de um grupo*** $\mathbb{G}$ ***num espaço vectorial*** $(\mathbb{R}^n ou \mathbb{C}_n)$***. Um subespaço*** $\mathbb{W}$ ***contido no espaço vectorial é designado por invariante se para qualquer*** $g{\in}\mathbb{G}$ ***tivermos*** $D(g)\mathbb{W}{\subset}\mathbb{W}$***.***

Definição 4.3 ***[8], pág.119***
Uma representação $D\colon \mathbb{G} \to \mathbb{GL}(n)$ ***é chamada irredutível se os únicos subespaços invariantes forem*** $\{0\}$ ***e*** $\mathbb{R}^n$ ***ou*** $\mathbb{C}_n$***.***

Definição 4.4 ***Uma representação diz-se redutível se não for irredutível.***

Definição 4.5 ***[3], pág.43***
Duas representações de ordem n***,*** $D^{(1)}$ ***e*** $D^{(2)}$ ***de um grupo*** $\mathbb{G}$ ***são equivalentes se todas as matrizes*** $D^{(1)}(g)$ ***e*** $D^{(2)}(g)$ ***estiverem relacionadas segundo a mesma transformação de semelhança:***

$$D^{(1)}(g) = SD^{(2)}(g)S^{-1}, \quad \forall g{\in}\mathbb{G} \text{ , com } S \text{ independente de } g.$$

Na classificação de representações, as representações equivalentes são consideradas como sendo as mesmas, ou seja, têm a mesma transformação de semelhança, mas com diferentes bases. Apenas consideramos as classes de equivalência distintas.
Se queremos um modo de distinguir entre representações que trata representações equivalentes como a mesma, somos naturalmente conduzidos à noção de caracter.

Definição 4.6 ***[3], pág.43***
O caracter de uma representação D ***de um grupo*** $\mathbb{G}$ ***é o conjunto:***

$$\chi = \{\ \chi(g) \mid g \in \mathbb{G}\ \},$$

onde $\chi(g)$ **é o traço da matriz da representação** $D(g)$**:**

$$\chi(g) = \mathbf{Tr}(D(g))$$

O traço da matriz é soma dos elementos da diagonal principal:

$$\mathbf{Tr}(A) = \Sigma_i A_{ii}$$

O facto de que o caracter não faz distinção entre representações equivalentes, (isto é, é uma função de classes de equivalência), segue da propriedade cíclica do traço. Ou seja, para quaisquer matrizes A, B e C tem-se:

$$\mathbf{Tr}(ABC) = \Sigma_{ijk} A_{ij} B_{jk} C_{ki} =$$

$$= \Sigma_{ijk} B_{jk} C_{ki} A_{ij} =$$

$$= \mathbf{Tr}(BCA)$$

Em particular,

$$\mathbf{Tr}(SD(g)S^{-1}) = \mathbf{Tr}(D(g)S^{-1}S) = \mathbf{Tr}(D(\mathbf{g}))$$

Conclusão Se $D^{(1)}(g)$ e $D^{(2)}(g)$ forem representações equivalentes têm o mesmo caracter:

$$\{\ \chi^{(1)}(g)\} = \{\ \chi^{(2)}(g)\}$$

O recíproco também é verdadeiro, ou seja, se duas representações têm o mesmo caracter são equivalentes.

Corolário 4.1 ***[8], pág.129***
Seja $D^{(1)}$, ... , $D^{(r)}$ o conjunto representativo de todas as representações irredutíveis não equivalentes de um grupo finito $\mathbb{G}$ num espaço vectorial $\mathbb{V}_i$ com dimensão d_i. Então,

$$\Sigma_{i=1}^{r} d_i^2 = |\mathbb{G}|$$

Demonstração Seja χ_i o caracter de $D^{(i)}$. Sabe-se que:

$$\chi_{\mathbb{G}} = \Sigma_{i=1}^{r} d_i \chi_i$$

Devido a

$$|\mathbb{G}| = \tfrac{1}{|\mathbb{G}|}\chi_{\mathbb{G}}(e)^2 = (\chi_{\mathbb{G}}|\chi_{\mathbb{G}})$$

tem-se,

$$|\mathbb{G}| = <\chi_{\mathbb{G}}|\chi_{\mathbb{G}}> = \Sigma_{i=1}^{r} d_i^2(\chi_i|\chi_i) = \Sigma_{i=1}^{r} d_i^2$$

□

Teorema 4.1 ***[8], pág.130***
Cada d_i ***divide*** $|\mathbb{G}|$

Teorema 4.2 ***[8], pág.121***
As representações irredutíveis complexas de um grupo abeliano são de dimensão um.

Demonstração Para toda a representação D **de um grupo** $|\mathbb{G}|$ **compacto, cada elemento** $D(g)$ **pode ser diagonalizado. Mais, se** A **e** B **são duas matrizes diagonalizáveis comutam. Então uma pode diagonalizar as duas em simultâneo. Isto quer dizer que todos os elementos de** $D(g)$ **podem ser diagonalizados, o que implica que todos os subespaços irredutíveis são de dimensão um.** □

Exemplo 4.1 ***[8], pág.122***

Grupos cíclicos
Os grupos cíclicos $\mathbb{Z}_n$ **e** $\mathbb{C}_n$ **são isomorfos,** $\forall n \in \mathbb{N}$, $n > 1$.
São representações típicas de $\mathbb{R}^2$**, segundo rotações de** $\frac{2\pi}{n}$**. A representação é irredutível se** $n > 2$**. Pelo teorema** 4.2**, conclui-se que toda a representação irredutível é um complexo de dimensão um. Seja** ρ **um elemento geral para** $\mathbb{C}_n$**. É fácil verificar que:**

$$D_k\text{: } \mathbb{G} \to \mathbb{C} = \mathbb{GL}(1,\mathbb{C})\text{: } \rho \mapsto e^{\frac{2\pi ki}{n}}$$

para $k = 1$, ..., n **define** n **representações não equivalentes.**

Exemplo 4.2 ***[8], pág.130***

Grupos Diedrais
O grupo diedral $\mathbb{D}_n$ é gerado pela rotação de $\frac{2\pi}{n}$ e pela reflexão de π, já mencio-nado anteriormente. Se $n = 2$ então $\mathbb{D}_n$ tem uma representação irredutível. Se $n > 2$ não é irredutível.

Exemplo 4.3 ***[8], pág.130***

O grupo $\mathbb{D}_n$ tem:
(i) Se n é ímpar, duas representações de dimensão igual a um e $\frac{n-1}{2}$ representações de dimensão igual a dois,
(ii) Se n é par, quatro representações de dimensão igual a um e $\frac{n-2}{2}$ representações de dimensão igual a dois,
representações irredutíveis.

No final deste capítulo serão dados dois exemplos de construção de tabelas: de um grupo cíclico e de um grupo diedral.

4.1.1 Redutibilidade

Teorema 4.3 (Teorema de Maschke) ***[3], pág.56***
Todas as representações redutíveis de um grupo finito são completamente redutíveis, ou seja, decomponíveis.

Exemplo 4.4 ***[3] , pág.44*** $\mathbb{C}_3$
No caso de $\mathbb{C}_3$***, tem-se as matrizes com a forma***:

$$R(c) = \begin{pmatrix} . & . & 0 \\ . & . & 0 \\ 0 & 0 & 1 \end{pmatrix} \textbf{, etc.}$$

A diagonal formada é devido ao z ***ser invariante segundo as transformações de*** $\mathbb{C}_3$***. Apenas*** x ***e*** y ***mudam, ou seja, o vector*** $x = x_i + y_j + z_k$ ***é decomposto em dois vectores***:

$$x = u + v,$$

onde $u = x_i + y_j$ ***e*** $v = z_k$***.***

A representação é efectivamente decomposta em duas representações separáveis, a de dimensão dois, $D^{(2)}$***, actua em*** u ***e a representação trivial de dimensão um,*** $D^{(1)}$ ***actua em*** v***, sendo ambos completamente independentes***:

$$RR' = \begin{pmatrix} A & O \\ O & 1 \end{pmatrix} \begin{pmatrix} A' & O \\ O & 1 \end{pmatrix} = \begin{pmatrix} AA' & O \\ O & 1 \end{pmatrix}$$

O símbolo especial $\oplus$ ***é usado na decomposição da diagonal e, escreve-se:***

$$R(c) = D^{(1)}(c) \oplus D^{(2)}(c)$$

Definição 4.7 ***[3], pág.45***
A representação de dimensão $n + m$ ***é dita como sendo redutível se*** $D(g)$ ***toma a forma:***

$$D(g) = \begin{pmatrix} A(g) & C(g) \\ O & B(g) \end{pmatrix}, \forall\ g \in \mathbb{G}$$

onde A**,** C **e** B **são submatrizes de dimensão** $m \times m$**,** $m \times n$ **e** $n \times n$**, respectivamente, e** O **representa a matriz nula de dimensão** $n \times m$**.**
Ao multiplicar-se as duas matrizes vê-se:

$$D(g)D(g') = D(gg') = \begin{pmatrix} A(g) & C(g) \\ O & B(g) \end{pmatrix} \begin{pmatrix} A(g') & C(g') \\ O & B(g') \end{pmatrix} =$$

$$= \begin{pmatrix} A(g)A(g') & A(g)C(g') + C(g)B(g) \\ O & B(g)B(g') \end{pmatrix}$$

Assim,

$$A(gg') = A(g)A(g')$$
$$B(gg') = B(g)B(g')$$

e, também,

$$C(gg') = A(g)C(g') + C(g)B(g')$$

Assim, { $\mathbf{A}(g)$} e { $\mathbf{B}(g)$} são representações de $\mathbb{G}$ de ordem m e n, respectivamente.

Para grupos finitos a equivalência C pode ser a matriz nula, como no caso de $\mathbb{C}_3$. A representação $D(g)$ é dita como sendo uma redutibilidade completa ou decomponível se:

$$D(g) = A(g) \oplus B(g)$$

As representações A e B são elas próprias decomponíveis, sendo natural a continuação do processo, que termina quando se alcança o nível de representações irredutíveis, chamadas de representações que já não podem ser mais reduzidas. Não existe limite no número e dimensões de representações redutíveis, o que significa que as representações irredutíveis podem ser classificadas pelos caracteres e numeradas.
Uma representação irredutível pode aparecer mais do que uma vez na decomposição e, escreve-se:

$$D = \Sigma_{\oplus} a_v D^{(v)}$$

onde, o número inteiro não negativo, a_v representa o número de vezes que a representação irredutível, $D^{(v)}$, aparece na decomposição.
Para encontrar o coeficiente, a_v, usam-se as propriedades de ortogonalidade dos caracteres. (ver secção seguinte)
Tomando o traço de um elemento do grupo, g, verifica-se que o caracter, $\chi(g)$ de D é decomposto segundo uma soma de caracteres $\chi^{(v)}(g)$:

$$\chi(g) = \Sigma_v a_v \chi^{(v)}(g)$$

4.1.2 Ortogonalidade dos caracteres

Como já foi mencionado anteriormente, o caracter de uma representação D é o conjunto $\{\chi(g)\}$, onde $\chi(g)$ é o traço da matriz $D(g)$. O traço de uma matriz tem as seguintes propriedades:
(i) **χ é o mesmo quando as representações são equivalentes, ou seja,**

$$D'(g) = SD(g)S^{-1}$$

(ii) **χ é o mesmo para elementos conjugados, uma vez que,**

$$D(hgh^{-1}) = D(h)D(g)(D(h))^{-1}$$

(iii) **Se D é unitária, ou seja, $D^{-1} = D^{\star}$, então**

$$\chi(g^{-1}) = \mathbf{Tr}((D(g))^{-1}) = \mathbf{Tr}(D(g)^{\star}) = \chi^{*}(g)$$

Assim, é sempre verdade que para um grupo finito ou compacto, qualquer representação é equivalente a uma representação unitária, ou seja, tem o mesmo traço da representação unitária.
A relação de ortogonalidade de caracteres é obtida através do teorema fundamental de ortogonalidade de caracteres [3], pág.62:

$$\Sigma_g \ \chi^{(i)}(g)\chi^{(v)}(g^{-1}) = \frac{|\mathbb{G}|}{d_i} \ \delta^{iv} \ \delta_{kj} \ \delta_{kj}$$

onde, $\delta_{kj} \ \delta_{kj} = \delta_{kk} = d_i$**, dimensão da representação irredutível. Assim,**

$$\frac{1}{|\mathbb{G}|}\Sigma_g \ \chi^{(i)}(g)\chi^{(v)}(g^{-1}) = \delta^{iv} \ (1)$$

Por (iii) **tem-se uma forma alternativa,**

$$\frac{1}{|\mathbb{G}|} \ \Sigma_g \ \chi^{(i)}(g)\chi^{(v)*}(g) = \delta^{iv}$$

Assim, por (1) **é definido o produto escalar de dois caracteres de duas representações não equivalentes, em que estes dois caracteres são ortonormais, se,**

$$< \chi^{(i)}, \chi^{(v)} > = \delta^{iv}$$

Por (ii) **os elementos de uma mesma classe de conjugação têm o mesmo caracter, assim os caracteres distintos são classificados como** χ_j**,** $j = 1, \ldots,$ k**; correspondente a** k**, ao número de classes de conjugação,** K_j**.**
Seja k_j **o número de elementos da classe de conjugação** K_j**. Então a soma segundo** g **em** (1) **pode ser escrita como a soma de** j**:**

$$\frac{1}{|\mathbb{G}|} \ \Sigma_j \ k_j\chi_j^{(i)}(g)\chi_j^{(v)*}(g) = \delta^{iv}$$

Uma vez que não podem existir mais do que k **vectores ortogonais, temos novamente uma desigualdade no número** r **de diferentes representações irredutíveis. Normalmente, o número de representações irredutíveis é menor ou igual ao número de classes de conjugação:**

$$r \leq k$$

4.2 Construção de tabelas de caracteres

É possível na maioria das aplicações físicas determinar os caracteres das representações irredutíveis de um grupo finito. Os caracteres são apresentados numa tabela com a seguinte forma: as linhas correspondem às diferentes representações irredutíveis e as colunas correspondem às classes de conjugação do grupo.

Na construção da tabela as principais ferramentas a serem usadas são:
(1) **O número de representações irredutíveis = ao número de classes de conjugação**: $r = k$**;**

(2) **A soma dos quadrados das dimensões das representações irredutíveis, é igual à ordem do grupo, isto é**: $\Sigma_{i=1}^{r} d_i^2 = |\mathbb{G}|$**;**

(3) **Ortogonalidade**: $\Sigma_j k_j \chi_j^{(i)} \chi_j^{(v)*} = |\mathbb{G}|$

(4) **Qualquer informação vem com** (!)**.**

Nas representações de dimensão um, os caracteres são o mesmo que as matrizes e, eles próprios devem imitar as propriedades da operação do grupo (multiplicação).
No caso do grupo ser abeliano, todas as representações irredutíveis são de facto de dimensão um.
Para grupos finitos isto pode ser provado usando (1), (2) **e o facto de que as classes de conjugação consistem em um único elemento. Sendo assim, o número de classes,** k**, é igual à ordem do grupo,** $|\mathbb{G}|$**, e** (2) **fica:**

$$\Sigma_{i=1}^{|\mathbb{G}|} d_i^2 = |\mathbb{G}|$$

cuja única solução é $d_i = 1$**,** $\forall_i$**.**

4.2.1 Exemplos de tabelas de caracteres

Exemplo 4.5 ***Tabela de caracteres de*** $\mathbb{C}_3$

A tabela quadrada 3×3 **é formada por três representações irredutíveis** $D^{(1)}$ ... $D^{(3)}$ **e por três classes de conjugação, cada uma com um elemento** e, r, r^2**.**

Os caracteres das representações irredutíveis são de dimensão um e devem "imitar"o grupo multiplicativo. Em particular,

$$\chi(r^2)=(\chi(r))^2 \qquad \text{e} \qquad (\chi(r))^3 = \chi(r^3) = \chi(e) = 1.$$

O $\chi(r)$ **deve, portanto, ser uma das raizes cúbicas unitárias, nomeadamente,**

$$1,\ w = e^{\frac{2\pi i}{3}} \text{ ou } w^2 = e^{\frac{4\pi i}{3}}$$

e, podemos construir a tabela da seguinte forma:

$\mathbb{C}_3$	e	r	r^2
$D^{(1)}$	1	1	1
$D^{(2)}$	1	w	w^2
$D^{(3)}$	1	w^2	w

Tabela 4.1: Tabela de caracteres de $\mathbb{C}_3$

$D^{(1)}$ **é uma representação trivial, onde cada elemento é uma função unitária.** $D^{(2)}$ **e** $D^{(3)}$ **são representações de dimensão um, são complexos conjugados. Pensando nas representações como funções de** $\mathbb{C}_3$ **para** $\mathbb{GL}(1,\mathbb{C})$**, de números complexos diferentes de zero, podemos identificar diferentes núcleos. Estes podem ser subgrupos normais de** $\mathbb{C}_3$**. Uma vez que** $\mathbb{C}_3$ **não tem subgrupos próprios, as únicas possibilidades são os subgrupos impróprios, ou seja,** $\mathbb{C}_3$ **e** $\{e\}$**. Para** $D^{(1)}$ **é uma das primeiras destas possibilidades que são**

realizadas, enquanto que para $D^{(2)}$ e $D^{(3)}$ o núcleo é justamente o elemento unitário, o que significa que são representações "faithful".Vamos verificar a ortogonalidade das linhas, segundo a equação abaixo,

$$< \chi^{(1)}, \chi^{(2)} > = \tfrac{1}{3}(1 + w^2 + w) = 0,$$

em virtude da factorização de $(z^3 - 1)$ em $(z-1)(z^2+z+1)$. De igual forma o mesmo para $< \chi^{(1)}, \chi^{(3)} >$ e $< \chi^{(2)}, \chi^{(3)} >$. A normalização é assegurada pelo facto dos caracteres terem módulo unitário (isto é, os números unitários, convêm à representação unitária).
Finalmente, vamos usar a tabela de caracteres para ver como actua o vector nas componentes x, y e z e, as decompõe em representações irredutíveis. O caracter é

$$\chi^V = (\chi^V(e), \chi^V(c), \chi^V(c^2)) = (3,0,0)$$

o que significa que

$$\chi^V = a_1\chi^{(1)} + a_2\chi^{(2)} + a_3\chi^{(3)}$$

Como o grupo é abeliano

$$\chi^V = \chi^{(1)} + \chi^{(2)} + \chi^{(3)}$$

O coeficiente é dado através

$$a_v = < \chi^V, \chi^{(v)} > = \tfrac{1}{3}\ (3\chi^{(v)}(e)) = 1$$

Assim, o vector da representação D^V é decomposto através de uma soma directa

$$D^V = D^{(1)} \oplus D^{(2)} \oplus D^{(3)}$$

Pelo exemplo 4.4 da página 59, z é invariante segundo qualquer rotação de $\mathbb{C}_3$, isto é, z forma a base da representação trivial $D^{(1)}$. Para $D^{(2)}$ e $D^{(3)}$, considera-se a transformação como sendo a combinação de $x \pm iy$.

Ficam, assim, explicados todos os passos necessários para a construção de uma tabela de um grupo abeliano.

Exemplo 4.6 ***Tabela de caracteres de*** $\mathbb{D}(3)$

As classes de conjugação de $\mathbb{D}(3)$ são: (e), (r, r^2) e (s, sr, sr^2), que denotamos por k_1, k_2 e k_3, respectivamente. Assim, temos três classes de conjugação e três representações irredutíveis.
Como a ordem do grupo é igual à soma dos quadrados das dimensões das representações irredutíveis, temos: $d_1^2 + d_2^2 + d_3^2 = 6$.
Existe sempre uma representação trivial $D^{(1)}(g) = 1$, com $d_1 =1$, obtendo-se, assim, $d_2^2 + d_3^2 = 5$.
Apenas as soluções inteiras da equação são: $d_2 = 1$, $d_3 = 2$. É importante, para preencher a primeira coluna da tabela de caracteres, uma vez

$$\chi^{(i)}(e) = d_i$$

Para as representações de dimensão um, χ' devem traduzir o grupo estrutura. Assim,

$$\chi(sr) = \chi(s)\chi(r).$$

Mas,

$$\chi(s) = \chi(sr) = \chi_3, \text{ uma vez } \chi(r) = \chi_2 = 1.$$

Portanto,

$$\chi(s)^2 = \chi(s^2) = \chi(e) = 1, \textbf{ dá-nos } \chi_3 = \pm 1.$$

O sinal superior dá a representação trivial, obtendo-se $\chi_3 = -1$ para $D^{(2)}$. Usando (1), (2) **e** (4) **determinamos a tabela de caracteres, a seguir,**

$\mathbb{D}(3)$	K_1	K_2	K_3
$D^{(1)}$	1	1	1
$D^{(2)}$	1	1	-1
$D^{(3)}$	2	-1	0

Tabela 4.2: Tabela de caracteres de $\mathbb{D}(3)$

Finalmente, usando (3)**, a ortogonalidade de caracteres, verificamos a ortogonalidade entre $\chi^{(3)}$ e $\chi^{(1)}$, entre $\chi^{(3)}$ e $\chi^{(2)}$ e, ainda, entre $\chi^{(1)}$ e $\chi^{(2)}$.**
No caso dos grupos rotacionais existe uma outra notação usada com frequência nas classes de conjugação que se reflecte no número e na natureza dos seus elementos.

Capítulo 5

Estudo dos grupos de rotações dos sólidos platónicos

A primeira versão da criação de tabelas de caracteres no "GAP"surgiu com o "GAP 3.1"em Março de 1992, para ser utilizado estudo nos grupos. Um outro aspecto foi a criação da biblioteca de tabelas de caracteres com todas as tabelas dos grupos finitos (ver [1], disponível na Internet).[1]

Vamos apresentar tabelas de caracteres obtidas através do software GAP, para os grupos de rotações dos sólidos platónicos.

5.1 Subgrupo alterno $\mathbb{A}4$

```
gap> a4:=CharacterTable("Alternating",4);
CharacterTable( "Alt(4)" )
gap> Display(a4);
Alt(4)
```

[1] "The GAP caracter table library", version 1.1, maintained by Thomas Breuer

```
     2  2  2  .  .
     3  1  .  1  1

       1a 2a 3a 3b
    2P 1a 1a 3b 3a
    3P 1a 2a 1a 1a

X.1     1  1  1  1
X.2     3 -1  .  .
X.3     1  1  A /A
X.4     1  1 /A  A

A = E(3)
  = (-1+ER(-3))/2 = b3
```

Nota: $A = e^{2\pi i/3}$

A tabela dada pelo software "GAP"não é a melhor para apresentar resultados, assim os seus resultados foram colocados numa tabela, de forma a que a sua leitura seja mais compreensível.

Elementos	1	3	4	4
Ordem	1	2	3	3
1	1	1	1	1
2	1	1	$e^{2\pi i/3}$	$e^{-2\pi i/3}$
3	1	1	$e^{-2\pi i/3}$	$e^{2\pi i/3}$
$4F$	3	-1	0	0

Tabela 5.1: Tabela de caracteres do grupo $\mathbb{A}4$

Passemos então a explicar cada linha obtida. A primeira linha dá-nos o

número de elementos de cada classe de conjugação, número de simetrias do subgrupo $\mathbb{A}(4)$, e a segunda a ordem dos elementos das classes. Assim, para comprovar o número de elementos de cada classe, assim como a ordem dos elementos, utilizamos, novamente, o software GAP.

5.1.1 Determinação do número de elementos do subgrupo alterno $\mathbb{A}(4)$, através de ciclos de comprimento 3 através software GAP

```
gap> A4:=Group((2,3,4),(2,4,3),(1,2,3),(1,2,4),(1,3,2),(1,3,4),
(1,4,3),(1,4,2));(8 ciclos de ordem 3)

Group([ (2,3,4), (2,4,3), (1,2,3), (1,2,4), (1,3,2), (1,3,4), (1,4,2),
  (1,4,3) ])

gap> Size(a4);
12

gap> Elements(a4);
[ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2), (1,3,4),
  (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ]
```

Determinação do número de classes de conjugação

```
gap> ConjugacyClasses(a4);
[ ()^G, (1,2)(3,4)^G, (1,2,3)^G, (1,2,4)^G ]
```

Classes de conjugação e número de elementos de cada classe

```
gap> e:=ConjugacyClass(a4,());
()^G
```

```
gap> Elements(e);
[ () ]

gap> ap> q:=ConjugacyClass(a4,(1,2)(3,4));
(1,2)(3,4)^G
gap> Elements(q);
[ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]

gap> n:=ConjugacyClass(a4,(1,2,3));
(1,2,3)^G
gap> Elements(e);
[ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ]

gap> s:=ConjugacyClass(a4,(1,2,4));
(1,2,4)^G
gap> Elements(s);
[ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ]
```

Após uma leitura dos dados, verifica-se que existem quatro classes de conjugação,

$$(), (1,2)(3,4), (1,2,3), (1,2,4).$$

Como se verifica, a 1^a classe de conjugação tem um elemento, a 2^a tem três elementos e as duas últimas têm quatro elementos, 1^a linha da tabela. As linhas a seguir representam o número de representações irredutíveis.

O caracter assinalado com o F significa que é uma representação irredutível "faithful", ou seja, a identidade é o único elemento do núcleo.
As representações irredutíveis sob a forma de complexos são de dimensão um e pertencem ao grupo cíclico $\mathbb{C}_2$, na tabela $A = e^{2\pi i/3}$.

5.2 Subgrupo alterno $\mathbb{A}5$

```
 gap> a5:=CharacterTable("Alternating",5);
CharacterTable( "Alt(5)" )
gap> Display(a5);
Alt(5)

     2  2  2  .  .  .
     3  1  .  1  .  .
     5  1  .  .  1  1

       1a 2a 3a 5a 5b
    2P 1a 1a 3a 5b 5a
    3P 1a 2a 1a 5b 5a
    5P 1a 2a 3a 1a 1a

X.1     1  1  1  1  1
X.2     4  .  1 -1 -1
X.3     5  1 -1  .  .
X.4     3 -1  .  A *A
X.5     3 -1  . *A  A

A = -E(5)-E(5)^4
  = (1-ER(5))/2 = -b5
```

5.3 Grupo Simétrico $\mathbb{S}4$

```
gap> s4:=CharacterTableSpecialized(CharacterTable("Symmetric"),4);
CharacterTable( "Sym(4)" )
gap> Display(s4);
Sym(4)

     2  3  2  3  .  2
     3  1  .  .  1  .

       1a 2a 2b 3a 4a
    2P 1a 1a 1a 3a 2b
    3P 1a 2a 2b 1a 4a

X.1     1 -1  1  1 -1
X.2     3 -1 -1  .  1
X.3     2  .  2 -1  .
X.4     3  1 -1  . -1
X.5     1  1  1  1  1
```

Conclusão

Como o tema geral deste trabalho se denomina por "Grupos e Simetrias", cada capítulo foi sendo elaborado em função do que era necessário para relacionar os dois sub-temas, ou seja, primeiro entender o significado de grupo, segundo entender o significado de simetria e, após este entendimento, como relacionar os dois sub-temas.

A sua relação é conseguida através de tabelas de caracteres. Estas tabelas fazem o estudo das representações de grupos.

Na construção destas tabelas e, mesmo ao longo de todos os capítulos, foi sendo utilizado, de forma progessiva, o software "GAP"(Groups, Algorithms and Programming), que começou por ser um sistema computacional para ser usado no estudo de grupos, mas o seu uso tem sido alargado devido ao elevado número de"share-packages"existente. No entanto, este software não foi utilizado tanto como gostariamos, devido ao tempo permitido para a elaboração da tese, ou seja, foi pouco. Por último, espero que a estrutura da tese esteja adequada ao tema aqui tratado.

Bibliografia

[1] **Breuer, T.** *The GAP character table library* **version 1.1, Copyright 2003**

[2] **Walker, E.A.,** *Introduction to Abstract Algebra*, **Random House, inc., 1987.**

[3] **Jones, H.F.,** *Groups, Representations and Physics*, **Adam Hilger, 1990.**

[4] **Rotman, J.J.,** *A First Course in Abstract Algebra*, 2^a **edição, Prentice Hall, 2000.**

[5] **Armstrong, M.A.,** *Groups and Symmetry*, **Springer, 1988.**

[6] **Scherk, J.,** *Algebra, A Computacional Introduction*, 2^a **edição, Chapman and Hall/CRC, 2000.**

[7] **Birkhoff, M.,** *Algebra*, 3^a **edição, Chelsea Publishing Company, New York, 1988.**

[8] **Chossat, P. e Lauterbach, R.,** *Methods in Equivariant Bifurcations and Dynamical Systems*, **World Scientific, 2000.**

[9] **Rowen, L.H.,** *Graduate Algebra: Noncommutative View*, **American Mathematical Society, Providence, Rhode Island, vol.91, 2008.**