Notas de Álgebra I

Estas notas são sumários alargados do curso. Nelas pretendemos referir conceitos, resultados e exemplos apresentados nas aulas teóricas. Seguimos de perto o livro

M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, 1988, Cota 20F/ARM.

Neste texto incluiremos demonstrações que não constam ou são diferentes das apresentadas neste livro e faremos sugestões de leitura e consulta.

0. Introdução

O estudo de grupos é considerado como o início do estudo da álgebra abstracta. A passagem da aritmética para álgebra dá-se quando se passam a utilizar variáveis para representar números. Por exemplo, a proposição " Cada número primo que é um múltiplo de quatro mais um pode escrever-se, de forma única, como soma de dois quadrados"passa a escrever-se "$x^2 + y^2 = p$, com $p = 4n + 1$ primo, tem solução única".

A álgebra abstracta corresponde a deixar que a ou as operações envolvidas sejam variáveis: estudam-se as propriedades de um conjunto não especificado munido de uma ou mais operações satisfazendo determinadas propriedades tais como a associatividade, a existência de elemento neutro, etc..

As três principais áreas onde os estudos realizados originaram a definição de grupo, e o estudo da correspondente teoria, foram:

- A geometria do princípio do século XIX, quando as geometrias começaram a ser classificadas estudando as propriedades invariantes para um determindo grupo de transformações, tal como proposto por Klein no *Erlangen Program* de 1872.
- A teoria dos números do fim do século XVIII, com o estudo da aritmética modular, primeiro por Euler(1761), depois por Gauss(1801) e por muitos outros matemáticos e não matemáticos.
- A teoria das equações algébricas do fim do século século XVIII, que levou ao estudo das permutações.

A necessidade e utilidade da definição e estudo de uma determinado tipo de estrutura surge naturalmente quando ela aparece numa grande variedade de situações. Esse é o caso dos grupos. Eles surgem naturalmente em muitas áreas da matemática e têm numerosas aplicações, também noutras ciências.

Sugestões de consulta

História da teoria dos grupos:

http://pt.wikipedia.org/wiki/Teoria_de_grupos

Desenvolvimento do conceito de grupo:

http://turnbull.mcs.st-and.ac.uk/history/HistTopics/Development_group_theory.html

1. Axiomas: Definição de grupo

Um grupo é um conjunto munido de uma operação binária (uma regra que a cada par de elementos do conjunto faz corresponder um e um só elemento desse conjunto), que é associativa, tem elemento neutro, e tem inversos. De forma precisa:

Definição 1.1 *Um grupo é um par $(G, *)$, constituído por um conjunto G e uma operação binária $* : G \times G \to G$, que satisfaz os seguintes axiomas:*

- *Associatividade: se x, y, z são elementos de G então $x * (y * z) = (x * y) * z$.*
- *Elemento neutro: existe um elemento e em G tal que $x * e = e * x = x$.*
- *Inversos: para todo o elemento x de G existe um elemento x' em G tal que $x * x' = x' * x = e$.*

Se, além disso, $x * y = y * x$ para todos os elementos x e y de G, o grupo $(G, *)$ diz-se *abeliano* ou *comutativo*.

Em qualquer grupo
- *o elemento neutro é único*
e
- *cada elemento tem um único inverso.*

Os axiomas de grupo dão-nos exactamente o que necessitamos para poder resolver equações da forma $x * a = b$ e $a * x = b$, para quaisquer elementos a e b do grupo.

Exemplos 1.2 *São grupos*

1. $(\mathbb{Z}, +)$,
2. *Todos os espaços vectoriais para a adição,*
3. *O conjunto das simetrias de um triângulo equilátero,*
4. *O conjunto das matrizes reais invertíveis $n \times n$, com $n \geq 1$, para a multiplicação usual de matrizes, $(GL_n(\mathbb{R}), \times)$,*

sendo os dois primeiros grupos abelianos.

Não são grupos

1. $(\mathbb{N}, +)$,

2. $(\mathbb{N}, *)$, *sendo* $x * y = x^y$,

3. $(\mathbb{R}, \times)$,

4. *O conjunto das matrizes reais* $n \times n$ *para a multiplicação usual de matrizes,* $(M_n(\mathbb{R}), \times)$.

Várias simplificações vão ser a regra. Assim, em vez de $(G, *)$, falaremos no grupo G, sempre que não exista ambiguidade quanto à operação considerada.

Usaremos, em geral, notação multiplicativa, substituindo $x * y$ por $x \cdot y$ ou, simplesmente, por xy. Neste caso, o inverso de um elemento x será denotado por x^{-1}. Denotaremos o elemento neutro por e_G ou apenas por e.

A notação aditiva é usada, em geral, quando o grupo é abeliano. Nesse caso o elemento neutro é denotado por 0 e o inverso de x por $-x$, que se chama o simétrico de x.

Continuamos a apresentar propriedades básicas de um grupo G, usando agora a notação multiplicativa:

Se x *e* y *são elementos de um grupo* G*, então* $(xy)^{-1} = y^{-1}x^{-1}$

Se x*,* y *e* z *são elementos de um grupo* G *então*

$$xy = xz \Rightarrow y = z \qquad yx = zx \Rightarrow y = z,$$

as leis de cancelamento à esquerda e à direita.

Para qualquer conjunto finito $x_1, x_2, \cdots, x_n$ *de um grupo, qualquer forma de combinar estes elementos por esta ordem conduz-nos ao mesmo resultado*, isto é o produto $x_1 \cdot x_2 \cdots x_n$ faz sentido, sem a inserção de parêntesis. É a lei geral da associatidade que se prova por indução, a partir da associatividade para três elementos da definição de grupo.

Dado um elemento x de um grupo G, definimos x^n para todo o n inteiro da seguinte forma:

1. $x^0 = 1$

2. $x^n = xx^{n+1}$ e $x^{-n} = (x^n)^{-1}$, para $n \geq 1$.

Com esta notação temos as regras usuais dos expoentes:

Se x *é elemento de um grupo* G *então* $x^n x^m = x^{m+n}$ *e* $(x^m)^n = x^{mn}$

2. Grupos de Números

Vários conjuntos de números têm estrutura de grupo relativamente às operações de adição e multiplicação que nos são familiares.

Munidos da adição usual, são grupos os conjuntos $\mathbb{Z}$ dos inteiros, $\mathbb{Q}$ dos racionais, $\mathbb{R}$ dos reais, $\mathbb{C}$ dos números complexos e muitos outros tais como o conjunto dos inteiros pares. O mesmo já não sucede com os inteiros ímpares. (Porquê?)

São grupos multiplicativos os conjuntos $\mathbb{Q}-\{0\}$ dos racionais não nulos, $\mathbb{R}-\{0\}$ dos reais não nulos, $\mathbb{Q}^+$ dos racionais positivos, $\mathbb{R}^+$ dos reais positivos, $\{1,-1\}$, $\mathbb{C}-\{0\}$ dos números complexos não nulos, $\mathcal{C}$ dos complexos de módulo unitário, $\{\pm 1, \pm i\}$, etc..

Se n é um inteiro positivo, o conjunto $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ para a adição módulo n, $+_n$, é grupo abeliano.

Os elementos deste conjunto podem também ser multiplicados módulo n, operação que denotaremos por $._n$. Neste caso, se queremos obter um grupo, tal como fizemos noutros conjuntos, temos que remover o zero (Porquê?). Mesmo assim o resultado pode ser negativo: em $\mathbb{Z}_6 - \{0\} = \{1,2,3,4,5\}$ a multiplicação não é uma operação já que $2._6 3 = 0$ e o zero não pertence ao conjunto.

De facto, prova-se que $\mathbb{Z}_n - \{0\}$ é grupo para a multiplicação módulo n se e só se n é primo.

3. Grupos com quatro elementos

Exempos de grupos com quatro elementos são

1. O conjunto das raízes quartas da unidade, $\{1, i, -1, -i\}$, para a multiplicação de números complexos

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

2. O conjunto das simetrias de um rectângulo, que não é um quadrado, $\{e, r, s_1, s_2\}$ para a composição de simetrias, sendo e a transformação identidade, r a rotação de π e s_1, s_2 as reflexões em torno dos dois eixos de simetria:

$\circ$	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

Num conjunto com quatro elementos quantas operações binárias podemos definir que lhe confiram estrutura de grupo?

Um dos elementos do conjunto tem de ser o elemento neutro, cada elemento tem um inverso e, atendendo às leis de cancelamento, na tabela do grupo cada elemento aparece uma e uma só vez em cada linha e em cada coluna. Assim, considerando o conjunto $G = \{e, a, b, c\}$, onde e denota o elemento neutro, temos duas hipóteses relativamente aos inversos de a, b e c:

1. Um dos elemento é inverso de si próprio e os restantes elementos são inversos um do outro: por exemplo $b^{-1} = b$, $a^{-1} = c$ e, consequentemente, $c^{-1} = a$.

2. todos os elementos são inversos de si próprios.

Podemos construir duas tabelas diferentes que são, respectivamente,

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

e

$\diamond$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Falta averiguar se estas operações são associativas. Para cada uma das operações, isso corresponde a analisar 3^3 casos: todos os que resultam da inserção de parêntesis e da aplicação da operação, para as permutações com repetição dos elementos a, b e c.

Como a resposta é afirmativa, temos dois grupos distintos. Efectivamente, concluímos que, *num conjunto com quatro elementos podemos definir dois e apenas dois grupos distintos* $(G, \star)$ *e* $(G, \diamond)$.

Que podemos dizer sobre os grupos de quatro elementos anteriormente referidos? É fácil ver que *a menos da designação dos elementos*, $(G, \star)$ é o grupo $(\{1, i, -1, -i\}, \times)$ e $(G, \diamond)$ é o grupo das simetrias do rectângulo. Os conjuntos subjacentes têm o mesmo número de elementos e esses elementos combinam-se da mesma forma que os de $(G, \star)$ e que os de $(G, \diamond)$, respectivamente.

Como traduzir estes factos? No primeiro caso, dizemos que existe uma função bijectiva

$$f : G \to \{1, i, -1, -i\}$$

definida por $f(e) = 1, f(a) = i, f(b) = -1$ e $f(c) = -i$ que transforma o composto de quaisquer dois elementos $x, y \in G$ no composto das suas imagens, isto é tal que $f(x \star y) = f(x)f(y)$.

Analogamente, no segundo caso, é possível definir uma função bijectiva, $g : G \to \{e, r, s_1, s_2\}$, tomando $g(e) = e, g(a) = r, g(b) = s_1$ e $g(c) = s_2$, tal que $g(x \diamond y) = g(x) \circ g(y)$.

Descrevemos situações deste tipo dizendo que os grupos correspondentes são isomorfos.

Definição 3.1 *Dois grupos $(G, \star)$ e $(L, \ominus)$ dizem-se isomorfos, e escreve-se*

$$(G, \star) \cong (L, \ominus),$$

se existe uma função bijectiva $f : G \to L$ tal que $f(x \star y) = f(x) \ominus f(y)$ para todos os elementos x e y de G.

Sugestão de consulta

M. Sobral, *Álgebra*, Cota 20-01/SOB.

4. Grupos Diedrais

Para $n > 2$, o conjunto das simetrias de um polígono regular de n lados é um grupo para a composição de simetrias. Este tipo de grupo chama-se *grupo diedral de ordem n* e denota-se por D_n. Ele é constituído por n rotações de $\frac{2k\pi}{n}$ em torno do centro do polígono, para $k = 0, 1, 2, \cdots n-1$, 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

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

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

$$D_n = \{e, r, r^2, \cdots, r^{n-1}, s, rs, r^2 s, \cdots, r^{n-1}s\},$$

sendo $r^n = e$ e $s^2 = e$. Além disso, verifica-se que $sr = r^{n-1}s$ ou seja $sr = r^{-1}s$, visto que $r^{n-1} = r^{-1}$. Todos os outros produtos podem ser calculados a partir destas igualdades. Por exemplo,

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

.

Para n=3 temos o grupo

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

das simetrias do triângulo equilátero. (Veja tabela na página 17 do livro referido.)

Da mesma forma, $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$ é o grupo de simetrias do quadrado, $D_5 = \{e, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$ é o grupo de simetrias do pentágono regular, e assim sucessivamente.

Cada elemento do grupo D_n tem a forma r^k ou $r^k s$, onde $0 \leq k \leq n-1$, sendo

$$r^a r^b = r^k \text{ e } r^a(r^b s) = r^k s, \text{ com } k = a +_n b$$

$$(r^a s)r^b = r^l s \text{ e } (r^a s)(r^b s) = r^l, \text{ com} l = a +_n (n - b).$$

Diz-se que o conjunto $\{r, s\}$ *gera* o grupo D_n, num sentido óbvio que tornaremos preciso mais adiante.

A *ordem* de um grupo finito G é o número de elementos do conjunto subjacente que se denota por $|G|$. Um grupo com um número infinito de elementos diz-se que tem ordem infinita.

Para um elemento x de um grupo G, se $x^n = e$ para algum n natural diz-se que x tem ordem finita e o menor inteiro positivo que satisfaz essa igualdade chama-se a *ordem de* x. Caso contrário diz-se que x tem ordem infinita.

O único elemento de um grupo que tem ordem um é o elemento neutro. No grupo $\mathbb{Z}$ ele é o único elemento de ordem finita.

Todos os elementos de grupos finitos têm ordem finita.

No grupo infinito $\mathbb{C} - \{0\}$, existem elementos de ordem finita tais como i e $-i$ (que têm ordem quatro) e elementos de ordem infinita como $1 + i$ e muitos outros.

Sugestão de consulta

htttp://hemsindor.torget.se/users/m/mauritz/math/alg/dihed.htm

5. Subgrupos e Geradores

Existem subconjuntos do grupo

$$D_6 = \{e, r, r^2, r^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, r^5s\}$$

que são, eles próprios, grupos relativamente à composição de simetrias. Esse é o caso dos subconjuntos

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

e de

$$K = \{e, r^2, r^4, s, r^2s, r^4s\}.$$

Diz-se que H e K são subgrupos de D_6.

Definição 5.1 *Subgrupo de um grupo G é um subconjunto de G que tem, ele próprio, estrutura de grupo relativamente à operação que define o grupo G.*

Os grupos G e $\{e\}$ são subgrupos do grupo G, são os *subgrupos triviais* de G. Os restantes, caso existam, chamam-se *subgrupos próprios*. Escreve-se $H < G$ ou $H \leq G$, consoante H denota apenas um subgrupo próprio de G ou pode também ser subgrupo impróprio, respectivamente.

Um subconjunto H de G é subgrupo se e só se

1. o composto de dois elementos de H é um elemento de H;
2. o elemento neutro pertence a H;
3. o inverso de qualquer elemento de H também pertence a H.

A associatividade da operação em H vem imediamente da associatividade da operação em G.

Exemplos 5.2 *1. São subgrupos de $\mathbb{Z}$ todos os subconjuntos $n\mathbb{Z} = \{nx | x \in \mathbb{Z}\}$, com n inteiro não negativo.*

2. São subgrupos de $\mathbb{C} - \{0\}$ todos os conjuntos as raízes de índice $n \geq 1$ da unidade.

Teorema 5.3 *Um subconjunto não vazio H de um grupo G é subgrupo de G se e só se xy^{-1} pertence a H sempre que x e y são elementos de H.*

Para subconjuntos finitos de grupos, as propriedades elementares referidas permitem-nos concluir que:

Teorema 5.4 *Um subconjunto* finito *e não vazio H de um grupo G é subgrupo de G se e só se xy pertence a H sempre que x e y são elementos de H.*

Isto é falso para conjuntos infinitos (por exemplo, $\mathbb{N} \subset \mathbb{Z}$ satisfaz esta condição). No entanto, este critério permite-nos concluir que subconjuntos finitos de grupos finitos ou infinitos são subgrupos desde que sejam fechados para a operação. Exemplos de aplicação são os subconjuntos de $\mathbb{C} - \{0\}$ das raízes de índice n da unidade.

Se x é elemento de um grupo então

$$< x >= \{x^m | m \in \mathbb{Z}\}$$

é subgrupo de G. Ele é *o subgrupo gerado por x*. Se $G =< x >$, para algum dos seus elementos, diz-se que G é *grupo cíclico*.

Note que, se usarmos a notação aditiva,

$$< x >= \{mx | m \in \mathbb{Z}\}.$$

Exemplos 5.5 *São cíclicos os grupos*

1. $\mathbb{Z} =< 1 >=< -1 >$,
2. $n\mathbb{Z} =< n >=< -n >$,
3. $\mathbb{Z}_8 =< 1 >=< 3 >=< 5 >=< 7 >$,
4. *os subgrupos de* $\mathbb{C} - \{0\}$ *constituídos pelas raízes de índice* $n \geq 1$ *da unidade.*

Não são cíclicos

1. *os grupos aditivos* $\mathbb{Q}$, $\mathbb{R}$ *e* $\mathbb{C}$,
2. *os grupos multiplicativos* $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$ *e* $\mathbb{C} - \{0\}$.

Os grupos D_n também não são cíclicos. Basta ver que o máximo das ordens dos elementos do grupo é n. No entanto, todo o elemento de D_n se pode escrever como um produto de potências de r e de s.

Dado um subconjunto não vazio X de um grupo G, o conjunto

$$H = \{{x_1}^{m_1} {x_2}^{m_2} \cdots {x_k}^{m_k} | x_i \in X, m_j \in \mathbb{N}_0\}$$

é subgrupo de G. Ele é o menor subgrupo de G que contém X no seguinte sentido: se K é subgrupo de G e contém X então H está contido em K. Nesse caso, diz-se que H *é gerado por* X e escreve-se $H =< X >$.

O grupo $D_n =< X >$ para $X = \{r, s\}$. Ele é também gerado por $X = \{rs, s\}$ e por outros subconjuntos de D_n.

Conjuntos de geradores de um grupo G existem sempre. O próprio conjunto G é um deles, mas não acrescenta nada ao nosso conhecimento do grupo. Estamos, em geral, interessados em conjuntos de geradores com um número mínimo de elementos.

Por exemplo, $\mathbb{Z}_6 =< X >$ para $X = \{2, 3\}$. No entanto este grupo admite conjuntos singulares de geradores tais como $X = \{1\}$ ou $X = \{5\}$.

Um grupo G diz-se *finitamente gerado* se $G =< X >$ para algum subconjunto finito X de G.

Exemplo 5.6 *O grupo* G *das funções da recta real em si própria,* $f : \mathbb{R} \to \mathbb{R}$*, que preservam distâncias e transformam inteiros em inteiros, é finitamente gerado. De facto,* $G =< X >$ *sendo* $X = \{t, s\}$ *com* $t(x) = x + 1$ *e* $s(x) = -x$.

Este grupo é constituído por

$$\cdots t^{-2}, t^{-1}, e, t, t^2, \cdots$$

e por

$$\cdots t^{-2}s, t^{-1}s, s, ts, t^2s, \cdots$$

e, atendendo à sua semelhança com D_n*, chama-se* o grupo diedral infinito *e denota-se por* D_∞.

Teorema 5.7 *A intersecção de qualquer conjunto de subgrupos de um grupo G é subgrupo de G.*

Dado $X \subseteq G$,

$$< X >= \cap\{H | H \leq G \text{ e } X \subseteq H\},$$

uma outra forma de definir o subgrupo gerado por X.

Teorema 5.8 *(a) Todo o subgrupo de $\mathbb{Z}$ é cíclico;*
(b) Todo o subgrupo de um grupo cíclico é cíclico.

Concluímos assim que os subgrupos do grupo aditivo dos inteiros são exactamente os subgrupos da forma $n\mathbb{Z}$, para $n \in \mathbb{N}_0$, referidos em 5.2.1.

6. Permutações

Por *permutação* de um conjunto X entende-se uma função bijectiva $\alpha : X \to X$. O conjunto S_X das permutações de X é um grupo para a composição de funções.

Se X é infinito, S_X é um grupo infinito. Se X tem n elementos, por exemplo $X = \{1, 2, \cdots, n\}$, o grupo simétrico correspondente denota-se por S_n e tem ordem $n!$.

Subgrupos de grupos de permutações são exemplos universais de grupos no sentido que, como demonstraremos mais tarde, todo o grupo é isomorfo a um tal subgrupo.

Permutações $\alpha \in S_n$ podem ser representadas na forma

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}$$

Exemplo 6.1 *O grupo S_3 é constituído pelos elementos*

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

Se $a_1, a_2, \cdots a_n$ são elementos distintos de X, por $(a_1\ a_2\ \cdots a_k)$ denota-se a permutação que aplica a_1 em a_2, a_2 em $a_3, \cdots, a_{k-1}$ em a_k, a_k em a_1 e fixa os restantes elementos de X. Uma tal permutação chama-se *permutação cíclica* ou *ciclo* de comprimento k. Ciclos de comprimento $k = 2$ chamam-se *transposições*.

Os ciclos $(a_1\ a_2\ \cdots a_k)$ e $(b_1\ b_2\ \cdots b_s)$ dizem-se *disjuntos* se $\{a_1, a_2, \cdots a_k\} \cap \{b_1, b_2, \cdots b_s\} = \emptyset$.

Na permutação

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \\ 2 & 4 & 6 & 1 & 5 & 3 & 7 \end{bmatrix}$$

o ciclo que começa em 1,

$$1, \alpha(1) = 2, \alpha^2(1) = 4, \alpha^3(1) = 1,$$

é (124), o que começa em 3,

$$3, \alpha(3) = 6, \alpha^2(3) = 3,$$

é (36), portanto

$$\alpha = (124)(36)$$

visto que estas permutações têm o mesmo efeito sobre o conjunto dos sete primeiros números naturais. Ciclos de comprimento um não se escrevem, em geral.

Como $\beta = (124)$ e $\gamma = (36)$ são ciclos disjuntos, $\alpha = \beta\gamma = \gamma\beta$.

Usando esta notação

$$S_3 = \{\epsilon, (23), (13), (12), (123), (132)\},$$

que é um grupo não comutativo, pois $(12)(13) = (132)$ e $(13)(12) = (123)$. Daqui se conclui que, para $n \geq 3$, S_n não é comutativo: a composição das transposições (12) e (13) de S_n, por ordens diferentes, dá-nos ciclos diferentes de S_n.

Teorema 6.2 *Todo o elemento $\alpha \neq \epsilon$ de S_n se pode escrever de forma única, a menos da ordem dos factores, como um produto de ciclos disjuntos.*

Demonstração. Seja $X = \{1, 2, \cdots, n\}$ e $\alpha \in S_n$. Como X é finito, os termos da sucessão

$$1, \alpha(1), \alpha^2(1), \cdots$$

não podem ser todos distintos. Suponhamos que r é o menor inteiro positivo tal que $\alpha^r(1)$ coincide com um termo anteriormente obtido. Então $\alpha^r(1) = 1$ pois, caso contrário, se $\alpha^r(1) = \alpha^s(1) = m$, com $1 < s < r$, então

$$\alpha^{r-s}(1) = \alpha^{-s}\alpha^r(1) = \alpha^{-s}(m) = 1,$$

com $r - s < r$, o que contradiz a minimalidade de r. Desta forma, temos o ciclo

$$\sigma_1 = (1, \alpha(1), \cdots \alpha^{(r-1)}(1)).$$

Seja i o primeiro elemento de X que não aparece em σ_1. De forma análoga se obtém um novo ciclo

$$\sigma_2 = (i, \alpha(i), \cdots \alpha^{(t-1)}(i)).$$

Como X é finito, o processo tem de terminar em algum σ_k, sendo então $\alpha = \sigma_1\sigma_2\cdots\sigma_k$.

□

Como $(a_1\ a_2\ \cdots a_k) = (a_1a_k)\cdots(a_1a_3)(a_1a_2)$, toda a permutação se pode escrever como produto de transposições, ou seja

Teorema 6.3 *O conjunto das transposições de S_n gera S_n*

Toda a transposição se pode escrever na forma

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

portanto $\{(12), (13), \cdots, (1n)\}$ é um conjunto de geradores de S_n.

Também $\{(12), (23), \cdots, (n-1n)\}$ gera S_n já que

$$(1a) = (a-1a)\cdots(34)(23)(12)(23)(34)\cdots(a-1a).$$

Exemplo 6.4 *A permutação $\alpha = (123)(45)$ pode decompor-se no produto de 3, 5 ou 21 transposições:*

$$\begin{aligned}
\alpha &= (123)(45) \\
&= (13)(12)(45) \\
&= (13)(12)(14)(15)(14) \\
&= (23)(12)(23)(12)(34)(23)(12)(23)(34)(45)(34)(23)(12)(23)(34)(45)(34)(23)(12)(23)(34)
\end{aligned}$$

.

Todo o elemento de S_n se pode escrever de várias formas como produto de transposições, não sendo as transposições disjuntas, em geral.

Sejam A_n e B_n os subconjuntos de S_n constituídos pelas permutações que podem escrever-se como produto de um número par de transposições e de um número ímpar de transposições, respectivamente.

Prova-se que

$$S_n = A_n \cup B_n \text{ e } A_n \cap B_n = \emptyset$$

o que nos permite classificar as permutações em *permutações pares*, as que se podem escrever como produto de um número pares de transposições, e *permutações ímpares*, no caso contrário.

Teorema 6.5 *O subconjunto A_n é um subgrupo de S_n com ordem $n!/2$,* o grupo alternante de grau n.

O subgrupo A_n é gerado pelos ciclos de comprimento três. Mais do que isso, como toda a permutação $\alpha \in A_n$ se pode escrever como produto de um número par de permutações da forma $(1k)$e agrupando essas transposições duas a duas temos $(1a)(1b) = (1ba)$, concluímos que

Teorema 6.6 *Para $n \geq 3$, A_n é gerado pelos ciclos da forma $(1ab)$.*

7. Homomorfismos e Isomorfismos

Definição 7.1 *Uma função $\varphi : G \to G'$ de um grupo noutro diz-se um* homomorfismo *se $\varphi(xy) = \varphi(x)\varphi(y)$, para todo o elemento x, y de G. Um* isomorfismo *é um homomorfismo bijectivo.*

Exemplos 7.2 *São homomorfismos*

1. *a função $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ que a cada inteiro faz corresponder o seu resto na divisão por n, com n natural,*
2. *a função $\psi : \mathbb{R} \to \mathbb{C} - \{0\}$ definida por $\psi(x) = e^{2\pi xi}$,*
3. *a função $log : \mathbb{R}^{pos} \to \mathbb{R}$,*
4. *a função $D_3 \to S_3$ que a cada simetria faz corresponder a permutação dos vértices do triângulo,*
5. *a função de D_4 em S_4 definida de forma análoga à do exemplo anterior.*

Proposição 7.3 *Se $\varphi : G \to G'$ é homomorfismo então*

1. *$\varphi(e_G) = e_{G'}$;*
2. *$\varphi(x^{-1}) = (\varphi(x))^{-1}$ para todo o $x \in G$;*
3. *se $x \in G$ tem ordem m então a ordem de $\varphi(x)$ divide m.*

A função identidade $1_G : G \to G$ é um homomorfismo. De facto é um isomorfismo.

A função constante $\varphi : G \to G'$ definida por $\varphi(x) = e_{G'}$ é homomorfismo. Ele é o único homomorfismo de $\mathbb{Z}_8$ em $\mathbb{Z}_3$. (Porquê?)

A função composta $\psi\varphi$ de dois homomorfismos $\varphi : G_1 \to G_2$ e $\psi : G_2 \to G_3$ é um homomorfismo de G_1 em G_3. O mesmo se verifica se substituirmos homomorfismo por isomorfismo.

A relação "ser isomorfo a "é uma relação de equivalência:

1. $G \cong G$ (1_G é isomorfismo);

2. Se $G \cong G'$ então $G' \cong G$ (o inverso de um isomorfismo é um isomorfismo);

3. Se $G \cong G'$ e $G' \cong G''$ então $G \cong G''$ (o composto de isomorfismos é isomorfismo).

Proposição 7.4 *Se $\varphi : G \to G'$ é homomorfismo, H é subgrupo de G e K é subgrupo de G', então $\varphi(H)$ é subgrupo de G' e $\varphi^{-1}(K)$ é subgrupo de G.*

Em particular, se $\varphi : G \to G'$ é homomorfismo de grupos então a *imagem* de φ, $Im\varphi = \varphi(G)$, é subgrupo de G' e o *núcleo* de φ, $\varphi^{-1}(e_{G'}) = \{x | \varphi(x) = e_{G'}\}$ é subgrupo de G.

Proposição 7.5 *Grupos cíclicos infinitos são isomorfos ao grupo aditivo dos inteiros. Grupos cíclicos de ordem m são isomorfos a $\mathbb{Z}_m$.*

Exemplos 7.6 *São isomorfos*

1. *$\mathbb{Z}$ e $n\mathbb{Z}$ (isomorfismo definido por $\varphi(x) = nx$);*

2. *$\mathbb{R}^{pos}$ e $\mathbb{R}$ ($log : \mathbb{R}^{pos} \to \mathbb{R}$ é um isomorfismo);*

3. *D_3 e S_3(para o isomorfismo indicado, e.g. $\varphi(r) = (123)$);*

4. *S_6 e o subgrupo de S_7 constituído pelas permutações que deixam o 7 fixo.*

Não são isomorfos

1. *quaisquer dois grupos de ordem diferente;*

2. *um grupo abeliano e um não abeliano;*

3. *$\mathbb{Q}$ e $\mathbb{Q}^{pos}$ e pois a equação $2 + x = b$ tem solução em $\mathbb{Q}$ para todo o número racional b e $x^2 = b$ só tem solução em $\mathbb{Q}^{pos}$ se b for um quadrado perfeito;*

4. *$\mathbb{Z}$ e $\mathbb{Q}$ porque $\mathbb{Q}$ que não é cíclico;*

5. *$\mathbb{Z}_6$ e S_3 porque S_3 não é cíclico.*

8. Sólidos Platónicos e o Teorema de Cayley

Existem cinco sólidos regulares convexos, também chamados sólidos platónicos, que são o tetraedro, o cubo, o octaedro, o dodecaedro e o icosaedro.

O grupo das simetrias rotacionais do tetraedro é isomorfo a A_4.

Unindo os centros de cada par de faces adjacentes de um cubo obtemos um octaedro inscrito no cubo. Procedendo da mesma forma no octaedro produzimos um cubo inscrito no octaedro.

Diz-se que o cubo e o octaedtro são sólidos *duais*. Toda a simetria de um deles é também uma simetria do outro

O grupo das simetrias rotacionais do cubo, tal como o das simetrias rotacionais do octaedro, é isomorfo a S_4.

Também o dodecaedro e o icosaedro são sólidos duais no sentido referido. Os correspondentes grupos de simetrias rotacionais são isomorfos a A_5.

Representámos grupos de simetria de polígonos e de sólidos regulares através de grupos de permutações. Vamos ver que todo o grupo é, a menos de isomorfismo, um grupo de permutações.

Teorema 8.1 Teorema de Cayley *Se G é grupo então ele é isomorfo a um subgrupo de S_G. Em particular, se G tem ordem n então G é isomorfo a um subgrupo de S_n.*

Exemplo 8.2 *O grupo $\mathbb{Z}_4$ é isomorfo ao subgrupo de S_4 (das permutações do conjunto $\{0,1,2,3\}$) constituído por $L_0 = \varepsilon, L_1 = (0123), L_2 = (02)(13)$ e $L_3 = (0321)$, sendo $L_a(x) = a + x$.*

Sugestão de consulta
Sólidos Platónicos:
http: mathworld.wolfram.com/PlatonocSolid.html
http://math.ucr.edu/home/baez/platonic.html

9. Grupos de Matrizes

No conjunto M_n das matrizes $n \times n$ com elementos reais (ou complexos) a multiplicação de matrizes é uma operação binária e associativa que tem como elemento neutro a matriz identidade I_n. Ele não é um grupo visto que nem todas as matrizes têm inversa. Temos uma estrutura mais geral, que se chama *monóide*. O monóide multiplicativo M_n é isomorfo ao monóide das transformações lineares $\mathcal{T}_n$ de $\mathbb{R}^n$ em $\mathbb{R}^n$. De facto, existe uma função bijectiva

$$\varphi : M_n \to \mathcal{T}_n$$

que a cada matriz A faz corresponder a aplicação linear definida por $\varphi_A(\mathbf{x}) = \mathbf{x}A^t$, sendo $\mathbf{x}$ o vector $(x_1, x_2, \cdots x_n)$ e A^t a matriz transposta de A. Além disso, $\varphi(AB) = \varphi(A) \circ \varphi(B)$ visto que

$$\begin{aligned} \varphi_{AB}(\mathbf{x}) &= \mathbf{x}(AB)^t \\ &= \mathbf{x}B^tA^t \\ &= \varphi_A \circ \varphi_B(\mathbf{x}) \end{aligned}$$

e φ_{I_n} é a transformação identidade $id : \mathbb{R}^n \to \mathbb{R}^n$.

O subconjunto GL_n de M_n constituído pelas matrizes invertíveis é um grupo, o *Grupo Geral Linear*.

A restrição de φ a GL_n define um isomorfismo entre o grupo GL_n e o grupo das transformações lineares invertíveis de $\mathbb{R}^n$ em $\mathbb{R}^n$.

Para $n = 1$, GL_1 é isomorfo a $\mathbb{R}$. Para $n > 1$ temos uma sucessão de grupos não comutativos

$$GL_2, GL_3, \cdots GL_n, GL_{n+1}, \cdots,$$

em que cada GL_n é isomorfo ao subgrupo de GL_{n+1} constituído pelas matrizes da forma

$$\begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$$

para $A \in GL_n$.

Subgrupos importantes de GL_n são

- o *Grupo Ortogonal* $\mathcal{O}_n$ constituído pelas matrizes *ortogonais*, isto é pelas matrizes A tais que $A^t A = I_n$;

- o *Grupo Ortogonal Especial* das matrizes cujo determinante é $+1$, que é denotado por $\mathcal{SO}_n$.

Pelo isomorfismo φ a $\mathcal{O}_n$ corresponde o grupo das transformações lineares que preservam distâncias e ortogonalidade.

No caso de $n = 2$, $\mathcal{O}_2$ é constituído pelas matrizes

$$\begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix},$$

e

$$\begin{bmatrix} cos\theta & sin\theta \\ sin\theta & -cos\theta \end{bmatrix}$$

para $0 \leq \theta < 2\pi$.

As primeiras representam uma rotações do plano $\mathbb{R}^2$ em torno da origem, de ângulo θ no sentido directo. As matrizes de determinante -1 representam reflexões em torno de rectas que formam ângulos de $\theta/2$ com o semi-eixo positivo dos xx.

Cada matriz de $\mathcal{SO}_3$ representa uma rotação de $\mathbb{R}^3$ em torno de um eixo que passa pela origem de coordenadas.

10. Produtos Directos

Dados grupos G_1 e G_2 o produto cartesiano dos conjuntos subjacentes munido da operação

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

sendo $x_i y_i$ o produto em G_i, é um grupo. É o *produto directo* de G_1 e G_2 e denota-se por $G_1 \times G_2$.

A função $\varphi : G_1 \times G_2 \to G_2 \times G_1$, definida por $\varphi(g_1, g_2) = (g_2, g_1)$, é um isomorfismo.

O produto $G_1 \times G_2$ é grupo comutativo se os grupos G_1 e G_2 forem comutativos. O recíproco é também verdadeiro porque $G_1 \cong G_1 \times \{e_{G_2}\}$ e $G_2 \cong \{e_{G_1}\} \times G_2$ que, sendo subgrupos de $G_1 \times G_2$, são comutativos se este o for.

De forma análoga se define o produto directo $G_1 \times G_2 \times \cdots \times G_n$ de n grupos.

Exemplos 10.1 (i) $S_3 \times \mathbb{Z}_2$ é um grupo não comutativo de ordem 12;
(ii) $\mathbb{Z}_2 \times \mathbb{Z}_2$ é isomorfo ao grupo das simetrias do rectângulo;
(iii) $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$;
(iv) $\mathbb{Z} \times \mathbb{Z}$ não é cíclico.

Os grupos G_1 e G_2 são cíclicos se $G_1 \times G_2$ é cíclico. O recíproco é falso em geral. No entanto o produto directo de grupos cíclicos é cíclico se o máximo divisor comum dos ordens é igual a um.

Teorema 10.2 *$\mathbb{Z}_m \times \mathbb{Z}_n$ é isomorfo a $\mathbb{Z}_{mn}$ se e só se m e n são primos entre si.*

Corolário 10.3 *Se $m = {p_1}^{n_1}{p_2}^{n_2} \cdots {p_k}^{n_k}$ é a decomposição de m em primos distintos, então $\mathbb{Z}_m \cong \mathbb{Z}_{{p_1}^{n_1}} \times \mathbb{Z}_{{p_2}^{n_2}} \times \cdots \times \mathbb{Z}_{{p_k}^{n_k}}$.*

Exemplo 10.4 Sendo $J = -I$, a correspondência

$$\phi : \mathcal{SO}_3 \times \{I, J\} \to \mathcal{O}_3$$

definida por $\phi(A, U) = AU$ estabelece um isomorfismo entre estes grupos.

De forma semelhante se concluiu que, para n ímpar, $\mathcal{O}_n$ é isomorfo ao produto directo dos subgrupos $\mathcal{SO}_3$ e $\{I, J\}$.

Teorema 10.5 *se H e K são subgrupos de um grupo G tais que*

1. *$G = HK = \{hk | h \in H \text{ e } k \in K\}$,*
2. *$H \cap K = \{e\}$,*
3. *$hk = kh$ para todo o $h \in H$ e $k \in K$,*

então G é isomorfo a $H \times K$.

Exemplos 10.6 Exemplos de grupos indecomponíveis são
1. o grupo S_3: se $S_3 \cong H \times K$ então H ou K é o grupo identidade;
2. $\mathbb{Z}_p$ se p é primo.

11. Teorema de Lagrange

Se H é subgrupo de um grupo G, *classe lateral esquerda* de H em G é um subconjunto da forma

$$aH = \{ah \; h \in H\}$$

para algum elemento $a \in G$.

Classe lateral direita de H em G é

$$Ha = \{ha \; h \in H\},$$

para $a \in G$.

Teorema 11.1 *(***Teorema de Lagrange***) A ordem de qualquer subgrupo de um grupo finito divide a ordem do grupo.*

Corolário 11.2 *O ordem de qualquer elemento de um grupo finito é um divisor da ordem do grupo.*

Corolário 11.3 *Para $x \in G$ finito, temos que $x^{|G|} = e$.*

Corolário 11.4 *Se G tem ordem prima então G é cíclico.*

Exemplos 11.5 Além dos subgrupos triviais

(i) S_3 tem dois subgrupos de ordem dois e um de ordem três.

(ii) D_4 tem cinco subgrupos de ordem 2 e três subgrupos de ordem 4.

(iii) A_4 tem três subgrupos de ordem dois, quatro de ordem três, um de ordem quatro *mas não tem nenhum subgrupo de ordem seis.*

Se n é um inteiro positivo então $\mathbb{Z}_n - \{0\}$, que se representa por $\mathbb{Z}_n^*$, é grupo para a multiplicação módulo n se e só se n é primo. Por exemplo, em $\mathbb{Z}_8 - \{0\}$ a multiplicação módulo 8 não é uma operação que esteja definida no conjunto: $2 \times_8 4 = 0$.

No entanto, no subconjunto R_n constituído pelos inteiros $1 \leq m \leq n-1$ que são primos com n a multiplicação módulo n é fechada e R_n é grupo para essa operação. A ordem de R_n é $\varphi(n)$, a função φ de Euler.

Se x é primo com n então o resto da sua divisão por n, $x(modn)$, pertence a R_n. Atendendo a que $\varphi(n) = |R_n|$ e que $\varphi(p) = p - 1$ se p é primo, por 11.3, obtêm-se os seguintes resultados:

Teorema 11.6 *(***Teorema de Euler***) Se x é primo com n então $x^{\varphi(n)}$ é congruente com 1 módulo n.*

Teorema 11.7 *(***Pequeno Teorema de Fermat***) Se p é primo e x não é múltiplo de p, então x^{p-1} é congruente com 1 módulo p.*

12. Partições/Relações de equivalência

Uma *partição* de um conjunto X é uma decomposição do conjunto numa reunião de subconjuntos não vazios e disjuntos dois a dois.

A relação binária em X definida por $x \sim y$ *se* x *e* y *pertencem ao mesmo elemento da partição* é uma relação de equivalência, portanto uma relação reflexiva, simétrica e transitiva. O conjunto quociente $X/\sim$ é constituído pelos elementos da partição de que partimos.

Toda a relação de equivalência $\sim$ num conjunto X define uma partição de X em classes de equivalência distintas.

Exemplos 12.1 Exemplos de partições/relações de equivalência importantes neste contexto são:

1. À partição dos inteiros
$$\mathbb{Z} = 4\mathbb{Z} \cup 4\mathbb{Z}+1 \cup 4\mathbb{Z}+2 \cup 4\mathbb{Z}+3$$
corresponde a relação de equivalência $x \sim y$ se $x-y$ é um múltiplo de quatro, a *relação de congruência módulo 4*, $\equiv (mod 4)$.

2. Para qualquer inteiro positivo n *a relação de congruência módulo* n, $\equiv (mod n)$, determina uma partição de $\mathbb{Z}$ em n classes de equivalência:
$$\mathbb{Z} = n\mathbb{Z} \cup n\mathbb{Z}+1 \cup \cdots \cup n\mathbb{Z}+(n-1).$$

3. Se H é subgrupo de G, a relação binária $\sim$ definida por $a \sim b$ se $a^{-1}b \in H$ (se $ab^{-1} \in H$) é uma relação de equivalência. Nesse caso, as classes de equivalência de são exactamente as classes laterais esquerdas aH (as classes laterais direitas Ha, respectivamente). Propriedades referidas para classes laterais são apenas consequência deste facto. Já o mesmo não é o caso com a cardinalidade das classes de equivalência: todas as classes laterais esquerdas e direitas têm o mesmo cardinal que H pois as funções $L_a : H \to aH$ definidas por $L_a(h) = ah$ e $R_a : H \to Ha$ definidas por $R_a(h) = ha$ são bijectivas, para todo o $a \in G$.

   O recíproco é também verdadeiro: um subconjunto não vazio $H \subseteq G$ é subgrupo se $a \sim b$ se $a^{-1}b \in H$ (ou se $ab^{-1} \in H$) é uma relação de equivalência em G.

4. Num grupo G diz-se que x *é conjugado* de y se $gxg^{-1} = y$ para algum $g \in G$. A relação binária assim definida é uma relação de equivalência e as classes de equivalência chamam-se *classes de conjugação*. A classe de equivalência do elemento neutro é $\{e\}$ e G é abeliano se e só se todas as suas classes de equivalência são conjuntos singulares.

   Em S_3 as classes de conjugação são os conjuntos
$$\{\epsilon\}, \{(12),(13),(23)\}, \{(123),(132)\}.$$

13. Teorema de Cauchy

Teorema 13.1 *(**Teorema de Cauchy**) Se p é um divisor primo da ordem de um grupo G então G tem um subgrupo de ordem p.*

Usando este facto prova-se que:

Teorema 13.2 *Um grupo de ordem 6 é isomorfo a $\mathbb{Z}_6$ ou a D_3.*

Teorema 13.3 *Um grupo de ordem 8 é isomorfo a $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4 ou a Q, sendo Q o grupo dos quaterniões.*

14. Conjugação

Dois elementos x e y de um grupo G são *conjugados* se $gxg^{-1} = y$, para algum $g \in G$. A relação de conjugação é uma relação de equivalência cujas classes de equivalência se designam por *classes de conjugação* (Exemplo 12.1.4).

Para um elemento $g \in G$ a função $\varphi_g : G \to G$ definida por $\phi_g(x) = gxg^{-1}$ é um isomorfismo chamado *conjugação por g*. Como isomorfismos preservam a ordem dos elementos do grupo, elementos da mesma classe de conjugação têm a mesma ordem.

Se H é subgrupo de G então $gHg^{-1} = \{ghg^{-1} | h \in H\}$ é também subgrupo de G.

Dois subgrupos H e K de um grupo G dizem-se *conjugados* se $K = gHg^{-1}$ para algum elemento $g \in G$. A relação assim definida é também uma relação de equivalência no conjunto dos subgrupos de um grupo G.

Exemplos 14.1 São exemplos de classes de conjugação de grupos

1. Os conjuntos singulares se (e só se) o grupo é abeliano.
2. Em D_6 as classes de conjugação são

   $\{e\}$, $\{r, r^5\}, \{r^2, r^4\}\{r^3\}$, e $\{s, r^2s, r^4s\}, \{rs, r^3s, r^5s\}$.
3. Em S_n são os subconjuntos contendo permutações com a mesma estrutura de ciclo.

   Dizemos que dois elementos de S_n têm a mesma *estrutura de ciclo* quando se podem decompor no mesmo número de ciclos disjuntos com o mesmo comprimento. Por exemplo em S_7, as permutações

   $$\alpha = (1)(2)(37)(564)$$

   $$\beta = (6)(7)(12)(345)$$

   têm a mesma estrutura de ciclo pois têm dois ciclos de comprimento 1, um de comprimento 2 e um de comprimento 3 na decomposição (única) de cada uma delas em ciclos disjuntos.

O elemento g de S_7 que aplica cada elemento de α no elemento de β que fica por baixo na vertical, isto é a permutação $g = (16453)(27)$, satisfaz a condição $g\alpha g^{-1} = \beta$ (note que g não é única).

De uma forma geral, para permutações α e β de S_n com a mesma estrutura de ciclo, escritas por ordem crescente dos comprimentos dos seus ciclos, sem omitir os ciclos de comprimento 1, um elemento $g \in S_n$ tal que $g\alpha g^{-1} = \beta$ obtém-se da forma indicada acima. *Portanto, permutações com a mesma estrutura de ciclo são conjugadas.*

Reciprocamente, prova-se que permutações conjugadas têm a mesma estrutura de ciclo.

4. Do exemplo anterior conclui-se que as classes de conjugação de S_4 são

$$\{\epsilon\},$$

$$\{(12),(13),(14),(23),(24),(34)\},$$

$$\{(123),(132),(124),(142),(134),(143),(234),(243)\},$$

$$\{(1234),(1432),(1342),(1324),(1423)(1243)\},$$

$$\{(12)(34),(13)(24),(14)(23)\}$$

5. As classes de conjugação em A_4 são

$$\{\epsilon\},$$

$$\{(123),(142),(134),(243)\},$$

$$\{(132),(124),(143),(234)\}.$$

Por exemplo, não existe $g \in A_4$ para o qual $g(123)g^{-1} = (132)$: uma tal permutação seria, por exemplo, (23) que é ímpar.

6. Sendo

$$A_\theta = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix},$$

$$B_\varphi = \begin{bmatrix} cos\varphi & sin\varphi \\ sin\varphi & -cos\varphi \end{bmatrix}$$

as classes de conjugação de $\mathcal{O}_2$ são

$\{I\}$, $\{A_\theta, A_{-\theta}\}$, $\{A_\pi\}$ e $\{B_\varphi\}$, para $0 < \theta < \pi$ e $0 \leq \varphi < 2\pi$.

O *centro* de um grupo G é o conjunto $Z(G)$ dos elementos que comutam com todos o elemento de G:

$$Z(G) = \{g | gx = xg \text{ para todo o } x \in G\}.$$

Ele é a reunião de todas as classes de conjugação singulares.

Teorema 14.2 *O centro é um subgrupo de G.*

Exemplos 14.3 O centro

1. de S_n, para $n > 2$, é $\{\epsilon\}$;
2. de D_6 é $\{e, r^3\}$;
3. de GL_n é o conjunto das matrizes da forma λI para $\lambda \neq 0$.

15. Grupos quocientes

Um subgrupo H de G diz-se normal se H é reunião de classes de conjugação.

Exemplo 15.1 O subgrupo $H = \{\epsilon, (13)\}$ de S_3 não é normal pois não contém a classe de conjugação de (13).

Já $K = \{\epsilon, (123), (132)\}$ é subgrupo normal de S_3: ele é constituído por duas classes de conjugação.

Este tipo de subgrupo é muito importante porque o conjunto das suas classes laterais esquerdas, que neste caso são também classes laterais direitas, tem uma estrutura natural de grupo, o que significa que $aH \cdot bH = abH$ é uma operação nesse conjunto.

Todo o subgrupo de um grupo abeliano é normal visto que, para grupos deste tipo, as classes de conjugação são conjuntos singulares.

Proposição 15.2 *Para um subgrupo H de um grupo G são equivalentes:*
(i) H é subgrupo normal de G;
(ii) $gHg^{-1} \subseteq H$ para todo o $g \in G$;
(iii) $gH = Hg$ para todo o $g \in G$.

Se H é subgrupo normal de G escreve-se se $H \lhd G$.

Por (iii), um subgrupo é normal se e só se toda a classe lateral esquerda é também classe lateral direita pelo que, para subgrupos normais, falaremos apenas em classes laterais.

Teorema 15.3 *Se H é subgrupo normal de G, então o conjunto das classes laterais é grupo para a multiplicação definida por $aH \cdot bH = abH$. O subgrupo H é o elemento neutro deste grupo e o inverso de aH é $a^{-1}H$.*

O grupo das casses laterais chama-se o *grupo quociente* de G por H e denota-se por G/H.

Exemplo 15.4 *No grupo diedral D_4 o subgrupo $H = \{\epsilon, r^2\}$ é subgrupo normal: ele é reunião das classes de conjugação $\{\epsilon\}$ e $\{r^2\}$. As suas classes laterais são*

$$H, Hr = \{r, r^3\} = rH, Hs = \{s, r^2 s\} = sH, Hrs = \{rs, r^3 s\} = rsH.$$

Assim, o grupo quociente tem ordem quatro $G/H = \{H, rH, sH, rsH\}$ e é fácil ver que é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Teorema 15.5 *Todo o subgrupo de índice dois de um grupo é subgrupo normal.*

Exemplos 15.6 *Temos que $[G : H] = 2$ para os grupos e subgrupos a seguir indicados, pelo que concluimos que*

1. *A_n é subgrupo normal de S_n;*
2. *$< r >$ é subgrupo normal de D_n;*
3. *$\mathcal{SO}_n$ é subgrupo normal em $\mathcal{O}_n$.*

Podemos agora caracterizar, a menos de isomorfismo, os grupos de ordem $2p$, para $p > 2$ primo.

Teorema 15.7 *Se p é primo ímpar, um grupo de ordem $2p$ é cíclico ou diedral.*

Um elemento da forma $xyx^{-1}y^{-1}$, para $x, y \in G$ chama-se um *comutador*. O subgrupo do grupo G gerado pelo conjunto dos comutadores é o *subgrupo comutador* de G e denota-se por $[G, G]$.

O grupo comutador de um grupo abeliano é $\{e\}$ e $xy = yx$ exactamente quando $xyx^{-1}y^{-1} = e$. Para "abelianisar"um grupo G vamos considerar o grupo $G/[G, G]$ pois [G, G] é o menor subgrupo normal cujo grupo quociente é abeliano.

Teorema 15.8 *O subgrupo comutador $[G, G]$ é subgrupo normal de G e $G/[G, G]$ é abeliano. Além disso, se $H \lhd G$ então G/H é abeliano se e só se $[G, G] \subseteq H$.*

Exemplos 15.9 *São grupos comutadores*

1. $[S_n, S_n] = A_n$ *e* S_n/A_n *é isomorfo a* $\mathbb{Z}_2$.
2. $[D_n, D_n] =< r^2 >$, *sendo* $D_n/ < r^2 >$ *isomorfo* $\mathbb{Z}_2$ *se* n *ímpar e isomorfo a* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *se* n *par.*
3. $[Q, Q] = \{-1, 1\}$ *e* $Q/\{\pm 1\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, *sendo* Q *o grupo dos quaterniões.*

16. Os Teoremas de Isomorfismo

Homomorfismo $\varphi : G \to L$ é uma função que satisfaz a condição $\varphi(xy) = \varphi(x)\varphi(y)$ (Veja 7.1) .

Dois subgrupos fundamentais definidos por um homomorfismo $\varphi : G \to L$ são:

- o *núcleo* $N = \{x | \varphi(x) = e_L\}$, que é subgrupo normal de G e
- a *imagem* $\varphi(G) = \{\varphi(x) | x \in G\}$, que é subgrupo de L.

Teorema 16.1 *(***Primeiro Teorema de Isomorfismo***) Se* N *é o núcleo de* $\varphi : G \to L$ *então existe um isomorfismo* $\overline{\varphi} : G/N \to \varphi(G)$ *definido por* $\overline{\varphi}(xN) = \varphi(x)$.

Corolário 16.2 *Se* $\varphi : G \to L$ *é homomorfismo sobrejectivo de núcleo* N, *então* $G/N \cong L$

Exemplos 16.3 O Primeiro Teorema de Isomorfismo diz-nos que

1. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, porque $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ definido por $\varphi(x) = x(mod n)$ é um homomorfismo sobrejectivo de núcleo $n\mathbb{Z}$;
2. $\mathbb{R}/\mathbb{Z} \cong \mathcal{C}$, porque $\psi : \mathbb{R} \to \mathbb{C}^*$ definido por $\psi(x) = cos 2\pi x + i sen 2\pi x$ é um homomorfismo cuja imagem é o subgrupo dos complexos de módulo unitário $\mathcal{C}$, sendo o núcleo $\mathbb{Z}$.

Não é possível definir um homomorfismo sobrejectivo
- de A_4 em $\mathbb{Z}_2$, porque A_4 não tem subgrupos de ordem 6;
- de $\mathbb{Z}_8$ em $\mathbb{Z}_5$, porque 5 não divide 8.

Grupos cíclicos finitos $\mathbb{Z}_n$ tem imagens homomorfas de ordem d para todo o divisor d de n. De facto, se $n = md$,

- $\mathbb{Z}_n$ tem um, e um só, subgrupo H de ordem m que é o subgrupo gerado por d (e $< d > \cong \mathbb{Z}_m$);
- H é normal porque $\mathbb{Z}_n$ é abeliano;
- a *projecção canónica* $p : \mathbb{Z}_n \to \mathbb{Z}_n/H$ definida por $p(x) = x + H$ é um homomorfismo sobrejectivo cuja imagem tem ordem

$$[\mathbb{Z}_n : H] = \frac{|\mathbb{Z}_n|}{|H|} = p.$$

Teorema 16.4 *(***Segundo Teorema de Isomorfismo***) Sejam H e K subgrupos de G. Se K é subgrupo normal, então*

- *HK é subgrupo de G,*
- *$H \cap K$ é subgrupo normal de H,*
- *$\varphi : H \to HK/K$, definido por $\varphi(x) = xK$ é um homomorfismo sobrejectivo de núcleo $H \cap K$*

portanto, $H/H \cap K \cong HK/K$

Teorema 16.5 *(***Terceiro Teorema de Isomorfismo***) Se $H \subseteq K$ são subgrupos normais de G então K/H é subrupo normal de G/H e a função $\varphi : G/H \to G/K$ definida por $\varphi(xH) = xK$ é um homomorfismo de núcleo K/H, portanto $(G/H)/(H/K) \cong G/K$.*

17. Acções, Órbitas e Estabilizadores

Uma *acção* de um grupo G num conjunto X é uma função $G \times X \to X$, que escrevemos $(g, x) \rightarrowtail g \cdot x$, tal que, para todo o x em X, $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ e $e \cdot x = x$, sendo o "produto"denotado por $g \cdot x$ para distinguir do produto $g_1 g_2$ de G.

Isto é equivalente a dizer que

Uma acção de G em X é um homomorfismo de G em S_X.

Um homomorfismo $\varphi : G \to S_X$ associa a cada $g \in G$ uma função bijectiva $\varphi_g : X \to X$. Denotaremos $\varphi_g(x)$ apenas por $g(x)$.

Exemplos 17.1 Actuam sobre o plano $\mathbb{R}^2$

1. o grupo das translações;
2. o grupo das rotações em torno de um ponto fixo.

Dada uma acção de G em X, a *órbita* de $x \in X$ é o subconjunto $\{g(x) : g \in G\}$, que denotamos por $G(x)$. O *estabilizador* de x é o conjunto $G_x = \{g | g \in G \text{ e } g(x) = x\}$ que é subgrupo de G.

A relação binária definida em X por $x \sim y$ se $g(x) = y$ para algum elemento $g \in G$ é uma relação de equivalência. As classes de equivalência são as órbitas dos elementos de X. Portanto, órbitas distintas definem uma partição de X. Se existe uma única órbita diz-se que acção é *transitiva*. Esse é o caso do primeiro exemplo referido: todo o ponto de $\mathbb{R}^2$ pode ser obtido de outro ponto de $\mathbb{R}^2$ por uma translação.

O mesmo grupo G pode actuar sobre um conjunto X de mais do que uma forma.

Exemplos 17.2 Seja G um grupo e X o conjunto subjacente.

1. G actua sobre X por multiplicação à esquerda: $g(x) = gx$;
2. G actua sobre X por conjugação: $g(x) = gxg^{-1}$.

Dada uma acção do grupo G num conjunto X, se x, y pertencem à mesma órbita então existe um elemento $g \in G$ tal que $gG_xg^{-1} = G_y$, isto é:

Teorema 17.3 *Elementos da mesma órbita têm estabilizadores conjugados.*

Teorema 17.4 *Para cada elemento $x \in X$, a função que a cada $g(x)$ faz corresponder a classe lateral gG_x é bijectiva, portanto $|G(x)| = [G : G_x]$.*

Corolário 17.5 *Se G é finito o número de elementos de cada órbita $|G(x)|$ divide a ordem de G.*

Teorema 17.6 *Se p é primo e a ordem de G é uma potência de p, então G tem um centro não trivial, isto é $Z(G) \neq \{e\}$.*

Teorema 17.7 *Se p é primo, um grupo de ordem p^2 é cíclico ou isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

18. Teoremas de Sylow

Seja p um primo e p^m a maior potência de p que divide a ordem do grupo G. Então $|G| = p^m k$, sendo p primo com k.

Teorema 18.1 *O grupo G contém pelo menos um subgrupo de ordem p^m.*

Se $g \in G$, $\varphi_g : G \to G$ definida por $\varphi_g(h) = ghg^{-1}$é um isomorfismo (Secção 14). Então, se $H < G$, $\varphi_g(H) = gHg^{-1}$ é um subgrupo de G isomorfo a H, um subgrupo conjugado de H. Em particular, subgrupos conjugados têm a mesma ordem. O resultado seguinte diz-nos que estes são exactamente os subgrupos de ordem p^m.

Teorema 18.2 *Dois subgrupos da ordem p^m de G são conjugados.*

Exemplo 18.3 É fácil ver que os três subrupos de ordem dois de S_3 são conjugados: se, além do elemento neutro, H_1, H_2 e H_3 contêm $(12), (13)$ e (23), respectivamente, então

$$(23)H_1(23) = H_2, (12)H_1(12) = H_3 \text{ e } (123)H_2(123) = H_3$$

Teorema 18.4 *O número t de subgrupos de G de ordem p^m é congruente com 1 módulo p e é um divisor de k.*

Exemplo 18.5 Se $|G| = 6$, o número de subgrupos de ordem dois é $t \equiv 1(mod 2)$ tal que $t|3$. Então $t = 1$ ou $t = 3$. No primeiro caso $G \cong \mathbb{Z}_6$ e no segundo $G \equiv S_3$.

Exemplo 18.6 Todo o grupo de ordem 45 tem um subgrupo normal. Se $|G| = 45 = 3^2 \times 5$, por 18.1, G tem pelo menos um subgrupo H de ordem $3^2 = 9$. O Teorema 18.3 diz-nos que o número t de subgrupos dessa ordem tem de verificar

$$t \equiv 1(mod\ 3) \text{ e } t|5,$$

e o único número da forma $3k + 1$ que divide 5 é 1. Como $t = 1$, para todo o elemento $g \in G$, gHg^{-1} coincide com H. Portanto H é normal.

Proposição 18.7 *Se $|G| = pq$ com p e q primos, $p < q$ e $q \not\equiv 1(mod\ p)$ então $G \cong \mathbb{Z}_{pq}$.*

Exemplo 18.8 Pelo resultado anterior, concluímos que são cíclicos os grupos de ordem 15, 33, 35, 51, 65, 69, 85, etc..

Grupos dicíclicos

Se $m > 2$ é um inteiro, no conjunto de $4m$ elementos

$$\{e, x, \cdots x^{2m-1}, y, xy, \cdots, x^{2m-1}y\},$$

com uma multiplicação definida por

$$x^a x^b = x^{a+b}, x^a(x^b y) = x^{a+b}y,$$

$$(x^a y)x^b = x^{a-b}y \text{ e } (x^a y)(x^b y) = x^{a-b+m},$$

sendo $0 \leq a, b \leq 2m - 1$ e as potências de x consideradas módulo $2m$, é um grupo G. É o *grupo dicíclico* de ordem $4m$. No caso $m = 2$, G é isomorfo ao grupo dos quaterniões.

Classificação dos grupos de ordem 12:

Teorema 18.9 *Um grupo de ordem 12 é isomorfo a um dos seguintes grupos: $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, D_6, o grupo dicíclico de ordem 12 e A_4.*

19. Grupos Abelianos Finitamente Gerados

Teorema 19.1 *Todo o grupo abeliano finitamente gerado é isomorfo a um produto directo de grupos cíclicos*

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^s,$$

tal que $n_1|n_2|\cdots|n_k$.

A potência s chama-se a *característica* do grupo e os n_i são chamados os *coeficientes de torção* ou os *factores invariantes* do grupo.

Corolário 19.2 *Todo o grupo abeliano finito é isomorfo a um produto directo de grupos cíclicos*

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

tal que $n_1|n_2|\cdots|n_k$.

Corolário 19.3 *Todo o grupo abeliano finitamente gerado que não tenha elementos de ordem finita é isomorfo ao produto directo de um número finito de cópias de* $\mathbb{Z}$.

Estes resultados dão-nos uma classificação completa dos grupos abelianos finitamente gerados. De facto a decomposição indicada é única:

Teorema 19.4 *Se* $G_1 = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^s$ *e* $G_2 = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_l} \times \mathbb{Z}^t$ *são isomorfos então* $s = t, k = l$ *e* $n_i = m_i$.

Um grupo abeliano finito G, por 19.2 e 10.3, é isomorfo a dois tipos diferentes de produtos directos de grupos cíclicos:

1. $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, sendo $n_1|n_2|\cdots|n_k$ os seus factores invariantes;
2. $\mathbb{Z}_{{p_1}^{\alpha_1}} \times \mathbb{Z}_{{p_2}^{\alpha_2}} \times \cdots \times \mathbb{Z}_{{p_s}^{\alpha_s}}$, onde os primos p_i, não necessáriamente distintos, se chamam os *divisores elementares* de G.

Os factores invariantes de um grupo determinam os correspondentes divisores elementares e vice-versa. Portanto, *dois grupos abelianos finitos são isomorfos se e só se têm os mesmos divisores elementares.*

Exemplo 19.5 A menos de isomorfismo, existem três grupos abelianos de ordem $40 = 2^3 \times 5$ com as factorizações indicadas:

1. Divisores elementares $2, 2, 2, 5$: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$. Factores invariantes $2, 2, 10$: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{10}$.
2. Divisores elementares $2, 2^2, 5$: $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$. Factores invariantes $2, 20$: $\mathbb{Z}_2 \times \mathbb{Z}_{20}$.
3. Divisores elementares $2^3, 5$: $\mathbb{Z}_8 \times \mathbb{Z}_5$. Factor invariante 40: $\mathbb{Z}_{40}$.