CTC – 20
Estruturas Discretas para Computação

Prof. Armando Gouveia

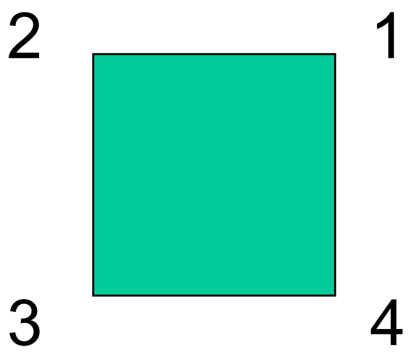
Tabelas

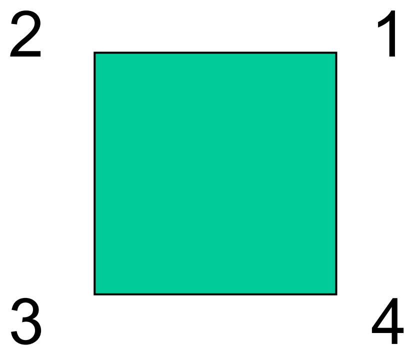
Questão

Existe algum grupo de ordem finita?

Exemplo

Quadrado de cartolina, com as pontas numeradas ☺





Seja R = rotação de 90º no sentido horário.

R' = rotação de 180º no sentido horário.

R'' = rotação de 270º no sentido horário.

H = reflexão no eixo horizontal

V = reflexão no eixo vertical

D = reflexão na diagonal /

D' = reflexão na diagonal \

$$R \rightarrow \begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix}$$

$$R' \rightarrow \begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$

$$R'' \rightarrow \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}$$

$$H \rightarrow \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}$$

$$V \rightarrow \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}$$

$$D \rightarrow \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$$

$$D' \rightarrow \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$$

Pensemos agora na “composição de movimentos”.

Por exemplo,

refletir na horizontal e depois fazer rotação de 90 º.

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \xrightarrow{H} \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \xrightarrow{R} \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$$ é igual a fazer reflexão D'

Chamemos * a essa operação “composição”.

Exemplo: $H*R = D'$.

Então * é operação binária?

É fechada?

– falta uma: I = identidade (mantém posição do quadrado)

Exemplos: $R*R'' = I$

$H*H = I$

– falta mais alguma?

– falta mais alguma?

$\begin{bmatrix} x & y \\ z & w \end{bmatrix}$ Exercício de contagem:

Preencher sem repetição.

Quantas possibilidades?

$4 \cdot 3 \cdot 2 \cdot 1 = 24$, mas só mostramos 8 operações.

Resposta: NÃO falta operação alguma,

pois as nossas operações sempre mantêm 1 e 3 na mesma diagonal

e idem para 2 e 4.

Como refazer a contagem?

$$\left.\begin{array}{l} \text{Fixo } x\text{, temos } w \text{ definido} \\ \text{fixo } y\text{, temos } z \text{ definido} \end{array}\right\} 4 \cdot 2 = 8 \ \text{possibilidades}$$

Conclusão:

esse conjunto de movimentos é fechado com operação * .

Agora vamos apresentar o grupo.

Seja M o conjunto $\{ I, R, R', R'', H, V, D, D' \}$

e * a composição de movimentos já descrita.

Então $(M, *)$ é um grupo de ordem 8.

Demonstração:

→ * é fechada: já mostramos.

→ G1: associativa: é complicado mostrar ☹

pois precisaria verificar TODAS as combinações.

→ G2: elem. neutro = I pois $X*I = X = I*X$ para todo X em M.

→ G3: existência de inversas:

podemos verificar para cada cada elemento:

a	I	R	R'	R''	H	V	D	D'
a^{-1}	I	R''	R'	R	H	V	D	D'

Tabelas

De modo geral, um grupo finito $G = \{ e, a_1 , a_2 , a_3 , \ldots , a_n \}$ pode ser apresentado através de uma tabela.

*	e	a_1	a_2	a_3	...	a_k	...	a_n
e	e	a_1	a_2	a_3	...	a_k	...	a_n
a_1	a_1					...		
a_2	a_2					...		
a_3	a_3					...		
...	...					...		
a_j	a_j	...	...	...	...	a_j*a_k	...	a_j*a_n
...	...							
a_n	a_n	...	...	...	...	a_n*a_k	...	a_n*a_n

Exemplo

Para o grupo dos movimentos no quadrado, temos

$*$	I	R	R'	R''	H	V	D	D'
I	I	R	R'	R''	H	V	D	D'
R	R	R'	R''	I	D			
R'	R'	R''	I	R				
R''	R''	I	R	R'				
H	H	D'			I			
V	V					I		
D	D						I	
D'	D'							I

Observação

O grupo $(M, *)$ não é abeliano,

pois $R*H = D \neq D' = H*R$

Obs. 2:

Se a tabela de um grupo é simétrica em relação à diagonal principal, então esse grupo é abeliano.

Grupo Diedral

O grupo $(M, *)$ dos movimentos no quadrado é conhecido como "grupo diedral D_4".

O grupo das simetrias em um n-ágono regular é chamado grupo diedral D_n.

Questão

Quais são TODOS os grupos de ordem pequena?

$|G| = 1$

Existe grupo de ordem um?

$G = \{ e \}$

$e * e = e$

Satisfaz as propriedades?

Sim.

É grupo. ☺

$|G| = 2$

$G = \{ e, a \}$

$e * e = e$

$e * a = a$

$a * e = a$

$a * a = \ (?)$

Pode ser e ou pode ser a.

Mas se for a

então teremos $\left.\begin{array}{l} a * a = a \\ a * e = a \end{array}\right\} \Rightarrow a = e$

(usamos a Lei do Cancelamento)

Portanto existe um único grupo de ordem 2,
pois só há uma tabela possível.

*	e	a
e	e	a
a	a	e

Observação.

Não é correto dizer que há um "único" grupo de ordem 2.

É mais exato dizer que há uma única "estrutura possível" para grupos de ordem 2, embora os elementos tenham outros nomes.

Isso será bem definido mais adiante no curso.

Exemplo

xor	0	1
0	0	1
1	1	0

$|G| = 3$

Exercício.

$|\,G\,| = 4$

$G = \{\, e, a, b, c \,\}$

Primeira tabela:

*	e	a	b	c
e	e	a	b	c
a	a	e		
b	b	(?)		
c	c			

$\longrightarrow$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Pode ser b? Não, pois $ba = be \Rightarrow a = e$

Pode ser a? Não, pois $ba = ea \Rightarrow b = e$

Pode ser e? Não, pois $ba = aa \Rightarrow b = a$

Obs.: Em cada linha/coluna, não pode haver repetição de elemento!

Segunda tabela:

$*_2$	e	a	b	c
e	e	a	b	c
a	a	b		
b	b	(?)		
c	c			

$\longrightarrow$

$*_2$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Terceira tabela:

$*_3$	e	a	b	c
e	e	a	b	c
a	a	c		
b	b	(?)		
c	c			

$\longrightarrow$

$*_3$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Observação.

A terceira tabela representa um novo grupo, diferente dos outros?

Sim. $(G, *_3)$ é diferente de $(G, *_2)$
porém... há uma grande semelhança!!
Afinal, se permutarmos as colunas b e c
e as linhas b e c na terceira tabela, veremos que
"essencialmente" obtivemos o <u>mesmo</u> grupo da segunda tabela,
a menos de mudança de nome dos seus elementos.

Importante

Mais tarde, essa "semelhança" será formalizada
com o conceito de isomorfismo.

Vamos agora verificar a alternativa que ficou pendente na construção da primeira tabela.

Quarta tabela:

$*_4$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	(?)	
c	c	b		

$\longrightarrow$

$*_4$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Sim. Forma grupo!

Exercício

Verificar que a a quarta tabela representa um grupo semelhante a algum dos grupos anteriores (a menos de "mudança de nome").

Conclusão

Encontramos no máximo dois grupos "distintos" de ordem 4.

Dúvida

Mas será que a primeira e a segunda tabela são mesmo distintas?

$*_1$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$*_2$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Resposta

Sim. Existe uma diferença essencial.

No primeiro grupo, temos $x * x = e \quad \forall x \in G$

Já no segundo, ocorre $x * x = e \Rightarrow x \in \{e, b\}$

Nomes

O primeiro grupo é chamado “grupo de Klein”.

O segundo é chamado “grupo cíclico de ordem 4”.

Conclusão

Existem exatamente dois grupos de ordem 4, estruturalmente distintos

Observação importante

Para ambos os casos, apresentamos as tabelas e afirmamos sem provar que formam grupos.

Pois não se fez verificação da propriedade associativa.