CTC – 20
Estruturas Discretas para Computação

Prof. Armando Gouveia

Grupos

Definição

Um grupo é um par $(G, *)$

onde G é um conjunto não vazio

e $*$ é uma operação binária em G satisfazendo:

G1: $(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$

G2: Existe $e \in G$ tal que $\forall a \in G, e*a = a*e = a$

G3: Para todo $a \in G$ existe $a' \in G$ tq $a*a' = a'*a = e$

Nomes

G1: associatividade de $*$

G2: e = elemento neutro (ou unidade, ou identidade) para $*$

G3: a' = simétrico de a (ou inversa de a)

Exemplo 1

$(Z, +)$ é um grupo?

Sim, pois

$$\text{G1}: (a+b)+c = a+(b+c) \;\; \forall a,b,c \in Z$$

$$\text{G2}: \text{Existe elemento } 0 \in Z \text{ tal que } \forall a \in Z, 0+a = a+0 = a$$

$$\text{G3}: \text{Para todo } a \in Z \text{ existe } a' = (-1)\cdot a \in Z \text{ tq } a+a' = a'+a = 0$$

Exemplo 2

$(Z, \cdot)$ é um grupo?

Não.

$$\text{G1}: (a\cdot b)\cdot c = a\cdot(b\cdot c) \;\; \forall a,b,c \in Z$$

$$\text{G2}: \text{Existe elemento } 1 \in Z \text{ tal que } \forall a \in Z, 1\cdot a = a\cdot 1 = a$$

$$\text{G3}: \text{Não vale, pois para } 8 \in Z, \text{ não existe } a' \in Z \text{ tq } a'\cdot 8 = 1$$

Exemplo 3

$(Q, \cdot)$ é um grupo?

Não.

G1: associativa OK

G2: existe elemento neutro = 1

G3: NÃO VALE, pois o elemento zero não tem inversa!

Para $a = 0$ não existe $a' \in Q$ tq $a' \cdot 0 = 1 = e$

Exemplo 4

$(Q^*, \cdot)$ é um grupo?

Sim.

Exemplo 5

São grupos: $(Z, +)$, $(Q,+)$, $(IR, +)$, $(C,+)$,

$(Q^*, \cdot)$, $(IR^*, \cdot)$, $(C^*, \cdot)$

Exemplo 6

O conjunto dos irracionais, $I = IR - Q$, com operação multiplicação?

G1: associativa OK

G2: Falta o elemento neutro = 1

Pode haver outro elemento neutro?

Neste caso, não. Pois, em IR, $\pi * e = \pi \Rightarrow e = 1$

mas $1 \notin I$.

Então $(I, \cdot)$ não é grupo.

Exemplo 7

$J = (R - Q) \cup \{1\}$ com operação multiplicação

G1: OK associativa.

G2: OK elemento neutro = 1 está em J.

G3: OK pois 0 não está em J;

e todo elemento tem inversa em J

afinal $\begin{cases} \text{(a) } x \text{ irracional} \Rightarrow \frac{1}{x} \text{ irracional} \in J \\ \text{(b) } \frac{1}{1} = 1 \in J \end{cases}$

então J é grupo ???

Resposta: J **não** é grupo!

pois $\sqrt{2} \in J$ mas $\sqrt{2} \cdot \sqrt{2} = 2 \notin J$

Qual o problema?

É que a multiplicação não forma operação binária em J.

Definição: fechamento

Dada uma operação binária * em um conjunto A,

e dado S um subconjunto de A,

dizemos que * é fechada em S sse

$$\forall x, y \in S, \text{ vale } x * y \in S$$

Obs.:

Pela definição de operação binária, observamos que

toda operação binária * em A

é fechada no próprio conjunto A.

Definição: grupo abeliano

Um grupo $(G, *)$ é abeliano se,

além das propriedades de grupo, ele também satisfaz

G4 : $a * b = b * a \quad \forall a, b \in G$

Obs.:

A propriedade G4 é a propriedade comutativa.

Grupos abelianos também são chamados grupos comutativos.

Exemplo 8

$(Z, +)$ é abeliano

Exemplo 9

$(Q^*, \cdot)$ é abeliano.

Obs.:

Um grupo não abeliano?

Matrizes! Afinal, $A \cdot B$ nem sempre é igual a $B \cdot A$.

Vamos formalizar.

Exemplo 10

Seja M o conjunto de todas as matrizes sobre IR

e seja * a multiplicação de matrizes.

(M, *) é grupo não-abeliano?

FALSO, pois (M, *) não é grupo ☹

Vejamos: $A_{8\times5} * B_{5\times2} = C_{8\times2}$ está OK

mas $A_{8\times5} * D_{4\times4} = ?$ não está definido.

Portanto * não é operação binária em M.

Exemplo 11

Seja M_n o conjunto das matrizes quadradas $n \times n$ sobre IR.

$$\left.\begin{array}{l} A \in M_n \\ B \in M_n \end{array}\right\} \Rightarrow A * B \text{ existe e é quadrada } n \times n \text{ sobre } IR$$

$$\Rightarrow A * B \in M_n$$

→ ok operação binária em M_n

→ G1: $(AB)C = A(BC)$

→ G2: elemento neutro = matriz identidade $n \times n = I_n$

→ G3: elemento inverso?

$$\forall A, \exists A^{-1} \text{ tq } A * A^{-1} = I_n \text{ ? nem sempre!}$$

Portanto $(M_n , *)$ não é grupo.

Exemplo 12

Seja $M\,I_n$ o conjunto das matrizes quadradas $n \times n$ inversíveis sobre IR.

Agora G3 é válida ☺

Portanto $M\,I_n$ é grupo. ???

AINDA FALTA PROVAR ALGO ☹

Havíamos provado que M_n é fechado sob a operação *.

Isso não implica que $M\,I_n$ o seja.

$$A, B \in MI_n \Rightarrow A * B \in MI_n (?)$$

Se A e B inversíveis, então $A*B$ inversível?

Resposta: sim. Como provar?

Temos A, B inversíveis $\rightarrow \det(A) \neq 0$ e $\det(B) \neq 0$

$\rightarrow \det(A*B) = \det(A) * \det(B) \neq 0$

$\rightarrow A*B$ inversível.

Portanto $M\,I_n$ é grupo.

E sabemos que não é abeliano.

Sabemos mesmo???

Na verdade sabemos que * não é comutativa em M.

Isso não implica que em $M\,I_n$ não o seja.

Precisamos de algum contra-exemplo.

$$A * B = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 3 \end{bmatrix} \qquad A^{-1} = \begin{bmatrix} \frac{1}{2} & 0 \\ -\frac{1}{2} & 1 \end{bmatrix}$$

$$B * A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} * \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \qquad B^{-1} = \begin{bmatrix} 0 & -\frac{1}{2} \\ 1 & \frac{1}{2} \end{bmatrix}$$

Conclusão: $M\,I_n$ é grupo não-abeliano.

Está provado? ☺ Na verdade, só demonstramos para $n = 2$. ☺

Questões

- Em um grupo deve haver ao menos um elemento neutro.
  Será que pode haver mais de um?
- Inversa: dada uma matriz $A_{20\times 20}$,
  pode haver matrizes B e C, $B \neq C$ tq ambas são inversas de A?
- Estamos acostumados a fazer

$$ab = ac \Rightarrow b = c$$

  Será que isso vale nos grupos?
- Nos reais, vale a propriedade acima?

NÃO ! Pois $$ab = ac \Rightarrow \begin{cases} b = c \\ \text{ou} \\ a = 0 \end{cases}$$

Lei do Cancelamento

Seja $(G, *)$ um grupo.

Se $a*b = a*c$ então $b = c$.

Se $b*a = c*a$ então $b = c$.

Demonstração

$a*b = a*c$	
$a'*(a*b) = a'*(a*c)$	Usei G3 e fato de que G é fechado sob *
$(a'*a)*b = (a'*a)*c$	Usei G1
$e*b = e*c$	Usei G3
$b = c$	Usei G2

Teorema

Cada grupo possui um único elemento neutro.

Demonstração

Suponha que existam dois elementos neutros e_1 e e_2

então teríamos

$$\left.\begin{aligned} e_1 * e_2 &= e_1 \\ e_1 * e_2 &= e_2 \end{aligned}\right\} \Rightarrow e_1 = e_2$$

[CQD]

Teorema

Em um grupo $(G, *)$, para cada elemento $a \in G$
existe um único elemento inverso a'.

Demonstração

Seja $a \in G$ e suponha que a_1' e a_2' sejam inversas de a.

Temos

$$e = e$$

$$a * a_1' = a * a_2' \quad \text{(usamos G3)}$$

$$a_1' = a_2' \quad \text{(usamos a Lei do Cancelamento)}$$

[CQD]

Teorema

Em um grupo $(G, *)$,
se $a, b \in G$ então $(a*b)' = b'*a'$

Demonstração

Verifiquemos se o produto vale e

$$(a*b)*(b'*a') =$$

$$a*(b*b')*a' =$$

$$a*e*a' =$$

$$a*a' = e$$

Então $b'*a'$ é uma inversa de $a*b$

logo, pela unicidade, está provado.

Teorema

Em todo grupo $(G, *)$,

a equação $x*a = b$ tem uma única solução

e a equação $a*y = b$ tem uma única solução.

Demonstração

Qual é a solução?

$$x*a = b$$
$$(x*a)*a' = b*a'$$
$$x*(a*a') = b*a'$$
$$x*e = b*a'$$
$$x = b*a'$$

Verifiquemos:

$$x*a = $$
$$(b*a')*a = $$
$$b*(a'*a) = $$
$$b*e = b$$

[CQD]

Essa solução é única?

Supor que x_1 e x_2 são duas soluções. Então

$$\left.\begin{array}{l} x_1*a = b \\ x_2*a = b \end{array}\right\} \Rightarrow x_1*a = x_2*a$$

$$\Rightarrow x_1 = x_2$$

[CQD]

Analogamente para a equação $a*y = b$.

Convenções

	grupos em geral	grupo abeliano
$(G,*)$	G	G
$a*b$	ab	$a+b$
a'	a^{-1}	$-a$
e	1	0

Observação importante

Os axiomas de grupo podem ser apresentados de outra forma.

Exemplo:

$\text{G2}: \exists e \in G \text{ tal que } \forall a \in G \;\; e*a = a$ (elem. neutro à esquerda)

$\text{G3}: \forall a \in G \;\; \exists a' \in G \text{ tq } \;\; a'*a = e$ (inversa à esquerda)

Definição: ordem

A ordem de um grupo $(G, *)$
é o tamanho do conjunto G.

Notação

Ordem de $(G, *) = |G|$

Obs.:

Costuma-se escrever "ordem de G ".

Exemplos

$A = (Z, +)$ $\quad |A| = \infty$

$|(Q^*, \cdot)| = \infty$

Questão

Existe algum grupo de ordem finita?

Curiosidade

Alguns livros apresentam generalizações / particularizações do conceito de grupo:

- semi-grupo
- monóide
- quasi-grupo
- grupóide
- loop

  etc...

Tais conceitos **não** são sinônimos de grupo.