CTC – 20
Estruturas Discretas para Computação

Prof. Armando Gouveia

Permutações

Definição

Uma permutação de um conjunto A

é uma função $\sigma : A \to A$ bijetora.

Exemplo

$A = \{1,2,3,4,5\}$

$$\sigma = \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 4 \\ 3 \mapsto 2 \\ 4 \mapsto 1 \\ 5 \mapsto 5 \end{cases}$$

Ou seja, $\sigma(1) = 3$

$\sigma(2) = 4$

$\sigma(3) = 2$

$\sigma(4) = 1$

$\sigma(5) = 5$

Notação

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{bmatrix}$$

Outro exemplo

Conjunto Z.

função $x \mapsto x+1$

é uma permutação de um conjunto infinito.

Notação

S_A = conjunto de todas as funções bijetoras de A em A.

Observação

Se A é finito com $|A| = n$

então $|S_A| = n!$

Grupo de Permutações

S_A com operação "composição de funções" é um grupo.

Demonstração

- Fechamento

$$\left.\begin{array}{l}\sigma \in S_A \\ \mu \in S_A\end{array}\right\} \Rightarrow \sigma \circ \mu \in S_A$$ pois compostas de bijetoras é bijetora.

- Associativa

$(\sigma \circ \mu) \circ \nu = \sigma \circ (\mu \circ \nu)$

sempre vale, pois domínios e contra-domínios compatíveis.

- Elemento neutro

função identidade $\iota \in S_A$ tal que $\sigma \circ \iota = \sigma = \iota \circ \sigma \ \ \forall \sigma \in S_A$

pois ι é bijetora.

- Inversas

Sim, pois toda função bijetora σ possui inversa σ^{-1} tal que

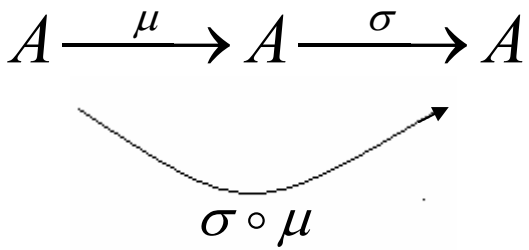
$$\sigma \circ \sigma^{-1} = \iota = \sigma^{-1} \circ \sigma \quad \forall \sigma \in S_A$$

e $\sigma^{-1} \in S_A$

pois inversa de função bijetora também é bijetora. [CQD]

Notação

$$\sigma\mu = (\sigma \circ \mu)(x) = \sigma(\mu(x))$$



Notação

S_A : grupo das permutações de A.

S_n : grupo das permutações de n símbolos. $\{ 1, 2, \ldots, n \}$

ou grupo simétrico de n elementos.

Exemplo

Grupo S_3

Os elementos do grupo são

$$\rho_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \qquad \mu_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

$$\rho_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \qquad \mu_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

$$\rho_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \qquad \mu_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

Há 6 elementos. São todas as permutações possíveis.

A operação no grupo é a função “composta”.

$$\mu_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \qquad \rho_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$\mu_1 \circ \rho_1 = ? \quad \begin{cases} \mu_1(\rho_1(1)) = \mu_1(2) = 3 \\ \mu_1(\rho_1(2)) = \mu_1(3) = 2 \\ \mu_1(\rho_1(3)) = \mu_1(1) = 1 \end{cases}$$

Portanto $\mu_1 \circ \rho_1 = \mu_2$

$$\rho_1 \circ \mu_1 = ? \quad \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \mu_3$$

Cuidado para fazer as operações na ordem correta.

Tabela

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Observação

Este é o menor grupo não-abeliano que existe ☺

Ou seja, os grupos de ordem 1, 2, 3, 4 e 5 são todos abelianos.

Teorema de Cayley

Dado um grupo G genérico,

G é isomorfo a um subgrupo de algum grupo de permutações S_A.

Intuição?

Lembrar que, quando estudamos "tabelas", percebemos
que em cada linha/coluna não aparecem elementos repetidos!
Ou seja, cada linha/coluna contém
uma permutação dos elementos do grupo ☺

Enunciado (outra forma de apresentar)

Todo grupo é isomorfo a algum grupo de permutações.

Demonstração

Idéia: considerar as funções $f_a(x) = ax$.

Formalmente: consideremos a função $f_a : G \to G$

tal que $f_a(x) = ax$, onde a é um elemento de G.

Provemos que é uma permutação.

(i) Sobrejetora:

Quero provar : $\forall x \in G \;\; \exists y \in G \;\; \text{tq} \;\; f_a(y) = x$

Basta tomar $y = a^{-1}x$ pois $f_a(y) = a(a^{-1}x) = x$

Mas $y \in G$?

Sim, pois $\left.\begin{array}{l} x \in G \\ a \in G \Rightarrow a^{-1} \in G \end{array}\right\} \Rightarrow a^{-1}x \in G$

(ii) Injetora:

Sejam $x_1, x_2 \in G$

então $f_a(x_1) = f_a(x_2) \Rightarrow ax_1 = ax_2 \underset{\text{Cancelamento}}{\Rightarrow} x_1 = x_2.$

Portanto, de (i) e (ii) temos que as funções f_a são permutações.

Consideremos agora o conjunto $H = \{f_a \mid a \in G\}$.

Obviamente, $H \subseteq S_G$ e S_G é grupo.

Queremos provar que H é subgrupo de S_G.

(a) fechamento

$$\left.\begin{array}{l} f_a \in H \\ f_b \in H \end{array}\right\} \Rightarrow \forall x \in G \text{ vale } f_a(f_b(x)) = a(bx) = (ab)x = f_{ab}(x)$$

e $f_{ab} \in H$ pois $ab \in G$ afinal $a, b \in G$ e G fechado.

Logo $f_a \circ f_b = f_{ab} \in H.$

(b) elemento neutro

Seja e o elemento neutro de G

Vamos provar que f_e é o elemento neutro de H.

$\forall f_a \in H$ temos $f_e \circ f_a = f_a$ pois

$\forall x \in G$ vale $f_e(f_a(x)) = e*(ax) = ax = f_a(x)$

(c) inversas

Dada $f_a \in H$ queremos provar $(f_a)^{-1} \in H$.

Temos $a \in G \Rightarrow a^{-1} \in G \Rightarrow f_{a^{-1}} \in H$

e temos $f_a \circ f_{a^{-1}} = f_e$ pois

$\forall x \in G \quad f_a \circ f_{a^{-1}}(x) = a(a^{-1}x) = ex = f_e(x)$

logo $\forall a \in G \quad (f_a)^{-1} = f_{a^{-1}} \in H$.

Ainda falta mostrar o isomorfismo.

Seja $\varphi : G \to H$

$$\varphi(a) = f_a$$

- Homomorfismo:

  $\varphi(ab) = f_{ab}$

  mas $f_{ab}(x) = (ab)x = a(bx) = f_a(f_b(x)) \quad \forall x \in G$

  logo $\varphi(ab) = f_a \circ f_b = \varphi(a)\varphi(b)$

- Bijetor

  Sobrejetor:

  $\forall f_a \in H \quad \exists a \in G$ tq $\varphi(a) = f_a$? Sim, por definição de H.

  Injetor:

  $\varphi(a) = \varphi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \quad \forall x \in G$

  $\Rightarrow ax = bx \quad \forall x \in G \Rightarrow ae = be \Rightarrow a = b$ [CQD (!)]