INTRODUÇÃO A TEORIA DE GRUPOS – AULA 8

Até agora definimos um conjunto, falamos sobre o conceito de completude de um conjunto (sobre uma operação binária), de associatividade e falamos ainda da propriedade de existência de inversas e de identidades.

Com estas propriedades em mente, criamos um objeto chamado grupo, que não é mais que um par de um conjunto e uma operação binária com 4 propriedades ($(G1), (G2), (G3)$ $e(G4)$) . Se não te recordas destes quatro axiomas, então volte à Aula 5.

Demos três exemplos de estruturas que se conformam a esta definição. Falemos de um grupo muito simples, *o grupo de rotações de 90º num quadrado.* Prometimos que iria expandir mais e criar um verdadeiro grupo que represente todas as simetrias que podem ser encontradas num quadrado (e por generalização em qualquer polígono regular com n lados). Vamos deixar este grupo para mais tarde e vamos concentrar-nos em algo mais intuitivo. (Surpresa das surpresas, a estrutura que vamos descrever é um grupo).

Antes de começar, um novo conceito rápido: o de ordem de um grupo.

Definição 1: (Definição da ordem de um grupo G).

Um grupo G tem ordem n se o seu conjunto G tiver n elementos. A ordem de um grupo escreve-se $|G| = n$. Se G tiver infinitos elementos, o grupo é chamado de infinito e escreve-se $|G| = \infty$.

Esta é daquelas definições que seguramente entendeste de imediato. Como exemplos, podemos dar:

1. $(N, +)$ (O conjunto dos números naturais com a operação de adição) tem $|N| = \infty$. (1)
2. $(Z_2, +_2)$ (O conjunto dos números inteiros mod n com a operação de adição em módulo 2.Esta requer duas linhas, vemos que é fácil: $Z_2 = \{0, 1\}$. Repare que se este par de conjunto e operação é mesmo um grupo, ele tem de ser fechado. Conclusão: das $2 \times 2 = 4$ possibilidades de operares, 2 vão ter de ser necessariamente iguais! Calculemos: $0 + 0(mod\ 2) = 0(mod\ 2) = 0$ (lembra-te, 0 é par!)
   $1 + 0(mod\ 2) = 1(mod\ 2) = 1$ (1 é ímpar!)
   $0 + 1(mod\ 2) = 1(mod\ 2) = 1$ *(2)*
   $1 + 1(mod\ 2) = 2(mod\ 2) = 0$ (2 é par. Alternativamente, $2 = 2 \times 1 + 0 \ldots$ e então $(Z_2, +_2)$ *é um grupo. Que ordem tem ele? Bem,* $|Z_2| = 2$ *. (3)*
3. O nosso grupo $R_{90^\circ} = \{e, a, a^2, a^3\}$ tem, como se pode deduzir, $|R_{90^\circ}| = 4$

O Grupo Simétrico $Sym(\chi)$

Definição 2: (Definição de grupo simétrico)

O grupo simétrico $Sym(\chi)$ *ou* S_n *(em que* $n = |\chi|$ *é o conjunto de todas as permutações possíveis de se fazer com todos os elementos do conjunto* χ*, equipado com uma operação binária chamada de composição de permutações.*
Quanto o grupo é dado por $\chi = \{1, 2, 3, 4, 5, ..., n\}$ o grupo simétrico escreve-se S_n. Esta diferença é por precisão de notação, pois neste artigo veremos que o que importa desde conjunto χ é só mesmo o seu número de elementos. É intuitivo o que eu dissemos: permutares letras, números, bolas ou nomes de carros tem o mesmo valor para todos: é a mesma operação "disfarçada".

Desmistificando: ao aplicarmos uma operação muito parecida com a que usamos na definição do grupo de rotações do quadrado no conjunto de todas as permutações de todos os elementos de um certo conjunto, este par de conjunto e operação binária irão formar um grupo.
Um exemplo muito simples: Seja $\chi = \{Verde, Azul, Vermelho\}$
O grupo simétrico de χ, $Sym(\chi)$ é igual a $\{(Verde, Azul, Vermelho),$
$(Verde, Vermelho, Azul), (Azul, Verde, Vermelho)\ (Azul, Vermelho, Verde),$
$(Vermelho, Verde, Azul), (Vermelho, Azul, Verde)\}$

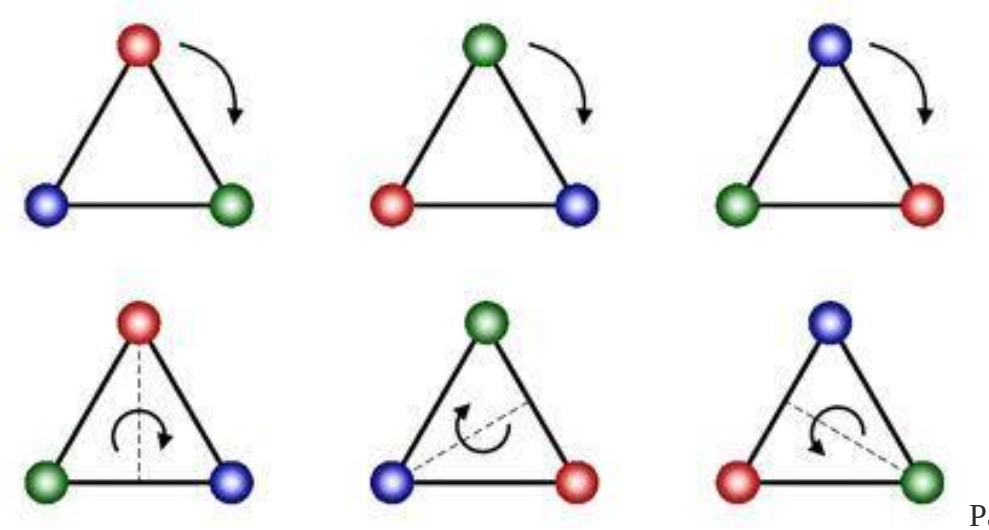
A diferença de notação é visível: $\{A, B, C\} = \{A, C, B\}$ porque se tratam de conjuntos e o que importa é apenas aquilo que contêm e não a sua ordem. Já com $(A, B, C) \neq (B, C, A)$ pois são permutações e claro que os seus efeitos são diferentes, pois são configurações diferentes. Veremos o que quero dizer.

Por conveniência, vamos também definir o conjunto $X_n = \{1, 2, 3, 4, ..., n\}$.

O que é uma permutação?

Como um exemplo simples, vamos escrever explicitamente os $3! = 3 \times 2 = 6$ elementos que fazem parte do grupo simétrico de ordem 3, S_3.

Reparemos configurações a seguir:



Para pensarmos em todas as permutações (as formas diferentes de trocar Verde Vermelho Azul) começa por fixar o triângulo num ponto e trocar os outros pontos restantes. Gira-se $60º$ e repete o processo, iremos ter de girar o triângulo 3 vezes e trocar os pontos restantes a cada etapa dando 2 resultados. Logo há $3 \times 2 = 6$ permutações com 3 elementos. Como vamos ver, isto justifica dizer que o grupo S_3 tem 6 elementos.
Ou seja, uma permutação é uma combinação possível dados n elementos. Escrevendo explicitamente todas as permutações de três elementos (que, afinal de contas é o que esse triângulo representa) (2), temos que as permutações de A, B, C são: $(A, B, C), (A, C, B), (C, A, B), (C, B, A), (B, A, C), (B, C, A)$

Pode-se pensar, por exemplo, numa estante de livros. Que sejam nos 10 livros no total. Pense agora em todas as possibilidades de reordenação. Seriam muitas ou poucas? Se lhe fosse dito que você tem 1 segundo para alterar para cada ordem, então você teria de o fazer 24 / 24h por 42 dias? São muitas possibilidades! São $10! = 3628800$ possibilidades.

Um ponto de exclamação numa expressão numérica? Que poderá representar?

Definição 3: (Definição de fatorial)

$n!$ *lê-se "n fatorial" ou "o fatorial de n". Representa a quantidade* $n! = n \times (n-1) \times (n-2) \times \ \ldots \ \times 2 \times 1$.
Como exemplos, tem-se que $3! = 3 \times 2 \times 1 = 6$
ou $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5040$. Certamente. sabemos que $1! = 1$. Será que é possível definir o fatorial de 0? Sim: $0! = 1$. Por quê? Intuitivamente, porque tens apenas 1 maneira de organizar um conjunto vazio: nele mesmo. *(4)*

Um matemático gosta de encontrar o padrão e estabelecer a generalização. Muitas vezes é da intuição que nasce conhecimento:

Será que se pode inferir $|S_n| = n!$ desta tabela? Não! Verifica-se que a relação é verdadeira para $1, 2, 3, 4, 5$ mas não se sabe sobre o resto. Pode bem ser, e parece que o é.
Vamos provar.

Demontração 1: (A ordem do grupo simétrico de nível n é igual a n!)

$|S_n| = n!$

Começa com n lugares vazios, e n elementos que vão ser permutados nessas posições. Coloca qualquer um no primeiro lugar. Então há n possibilidades para o primeiro lugar. Com o primeiro elemento no primeiro lugar fixo, coloca mais um elemento no segundo lugar. Seguramente que há $n - 1$ possibilidades de colocar lá (todos os elementos menos o primeiro que está fixo no primeiro lugar). Para o terceiro lugar, haverá $(n - 2)$ possibilidades. Continua o processo até só haver um elemento para colocar num lugar. Este tem de ir para o último necessariamente, logo há apenas 1 possibilidade. O número de todas as possibilidades tem de ser o produto de todos estes fatores:

Logo, $|S_n| = n!$ □

Será que é o grupo simétrico é um grupo? Embora possas pensar que "um grupo é um grupo" é sempre verdadeiro, as palavras podem ter significados diferentes. "Grupo Simétrico" podia ter sido genuinamente o nome que alguém se lembrou de chamar a este conjunto. Antes de provar, vamos fazer um pequeno reparo para que o entendimento do que está a ser feito. Que operação está a ser feita sobre este conjunto? O que é esta operação, "composição de permutações"?

Permutações como uma bijeção $X_n \to X_n$

Agora que já sabemos o que é uma permutação, é melhor tentarmos definir uma permutação de maneira mais rigorosamente. À medida que se vai avançado poderíamos nos concentrar em permutações mais decentemente, mas agora iremos só introduzir o básico para que se entenda a demonstração de que o grupo simétrico é de fato um grupo.

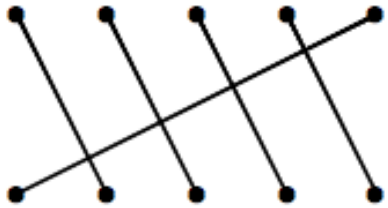
Lembremos que já introduzimos a notação $X_n = \{1, 2, 3, 4, 5, ..., n\}$ desde o início.

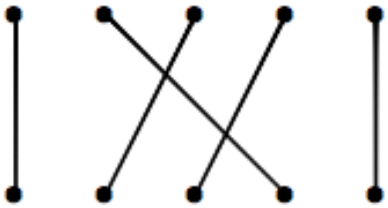
Definição 4: (Definição de uma permutação)

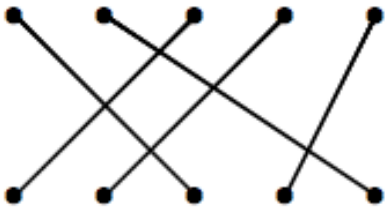
Uma permutação é uma função bijetora $\sigma : X \to X$

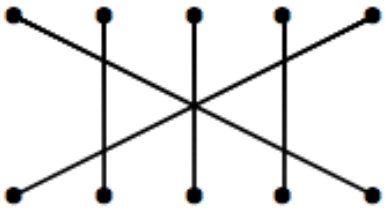
O que é que esta definição te diz? Uma permutação é uma função muito especial: considerando qualquer conjunto S, uma permutação altera a ordem dos mesmos elementos dentro do mesmo conjunto S. Informalmente, a cada vez que permutasse permuta um conjunto, se está a baralhar os seus elementos.

Por que é que tem de ser bijetora? Certamente que quando se troca dois elementos A, B entre si, $A \mapsto B$, $B \mapsto A$. Isto quer dizer que cada elemento $A \in S$ tem de ser transformado num outro. Isto quer dizer que a função é sobrejetora. Como cada lugar apenas pode ter um elemento, a cada elemento transformado há apenas um que o transformou. Isto significa que a função é injetora. Uma função que é injetora e sobrejetora tem de ser bijetora. Todos os seguintes diagramas ou configurações são exemplos de permutações para $X_5 = \{1, 2, 3, 4, 5\}$

$\alpha =$ 

$\beta =$ 

$\sigma =$ 

$\gamma =$ 

Reparemos em α. Esta permutação faz com que $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $5 \mapsto 1$. As outras permutações β σ γ são explicadas da mesma maneira. Fácil agora entender porque uma permutação tem de ser uma transformação bijetora? (Achas que se permutações não fossem bijetoras seria sempre garantido que se pudesse encontrar outra permutação que "desfizesse" a permutação e colocar os elementos na configuração inicial??

Como é que é possível escrever uma permutação? A notação que vamos usar vai ser a seguinte: uma tabela com 2 linhas e n colunas. Escrevendo α como permutação, então $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$; já γ é escrita como: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$

Em geral, uma permutação $\phi : X_n \to X_n$ é escrita como:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \phi(1) & \phi(2) & \phi(3) & \dots & \phi(n) \end{pmatrix}$$

Existe algo interessante nas permutações que vimos. Existem ciclos – permutações "consecutivas" em que o último elemento é transformado no primeiro.

Observemos α: $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1$; este caso é um caso extremo: a permutação é o ciclo todo. *(6)*
Observemos, agora, que γ: existem 4 ciclos: $1 \mapsto 5 \mapsto 1$, $2 \mapsto 2$, e ainda $3 \mapsto 3$ e $4 \mapsto 4$. Que quer isto dizer? O primeiro ciclo representa uma transposição: a permutação de 2 elementos , um com o outro; os restantes três são permutações "nulas" – os elementos mantêm-se na mesma posição, não sofrendo alteração.
Como representar um ciclo? Nada melhor que veres com um exemplo:

α pode ser escrita em notação de ciclos como (12345) (um ciclo único)

Já γ pode ser escrita em notação de ciclos como (15): apenas 1 e o 5 permutam (uma transposição) e as restantes formam ciclos sobre si mesmos (não se escrevem).

Pode-se notar que os ciclos têm de ser disjuntos uns dos outros. Isto quer dizer que não pode haver um elemento em dois ciclos diferentes. Então se assumirmos isto como verdadeiro, já temos uma maneira fácil de calcular o produto de ciclos!

Exemplo: em $\sigma = (13) \circ (45) = (13)(45)$ tem de ser igual à permutação $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$
Para terminar, iremos citar um resultado importante sobre permutações. Observe-se que muitos dos ciclos que fomos obtendo eram transposições (permutações de dois elementos, um com o outro). Será que é sempre possível escrever uma permutação como um produto de transposições? A resposta não deve surpreender (basta ver no teorema a seguir, ele faz sentido).

Teorema 1: (Toda a permutação num conjunto χ pode ser escrita como um produto de ciclos (disjuntos))

$\forall \sigma \in Sym(\chi)$, $\sigma = c_1 \circ c_2 \circ \ \ldots \ \circ c_n$, c_i sendo ciclos disjuntos.

Teorema 2: (Toda o ciclo $c \in \chi$ pode ser escrito como um produto de transposições.)

$\forall c \in Sym(\chi)\ C = \tau_1 \circ \tau_2 \circ \ \ldots . \tau_n$, τ_i sendo transposições

O resultado, como corolário, segue:

Corolário 1: (Toda a permutação num conjunto χ pode ser escrita como um produto de transposições)

Iremos falar mais sobre permutações em outra ocasião e iremos mostrar, também, que este grupo (depois de provar que o é) é o primeiro que trabalhamos aqui que não é abeliano. Aplicar uma duas permutações em ordens diferentes resulta em respostas diferentes.

---

(1) – Relembremos que quando se diz $|N| = \infty$ estamos nos referindo a um grupo. E um grupo, por definição, é equipado de uma operação binária. Neste caso, a operação binária não influencia em nada o número de elementos do conjunto; é apenas um reparo técnico.

(2) Porque é que o resultado é igual? Porque é que $0 + 1 = 1 + 0 mod(n)$. Que tal uma sugestão? $(a + b)(mod\ n) = a(mod\ n) + b(mod\ n)$

(3) Em geral, como dever ter adivinhado, $|Z_n| = n$.

(4) Rigorosamente falando, porque é um resultado que segue da generalização de fatoriais a números complexos onde a Função Gama desempenha este papel.
(5) Se tivesses numa sala e tivesses de cumprimentar toda a gente com um aperto de mão, n pessoas, quantos apertos de mão seriam necessários ser dados?

(6) Acabamos de afirmar que o grupo de permutações de um triângulo tem a mesma estrutura que o grupo de permutações de 3 elementos A, B, C. Será que dá para provar? Haveremos de provar que se dois grupos têm o mesmo número de elementos, então o seu grupo simétrico tem de ser essencialmente o mesmo. Simbolicamente: se G, H são grupos, e $|G| = |H| = n$ então $Sym(G) \cong Sym(H)$.

(7) Não confundir a notação de ciclos com uma permutação em si. (A, B, C) significa a ordem A, B, C. Já a notação de ciclos $(123)(45)$ quer dizer: ” $1 \mapsto 2,\ 2 \mapsto 3$ e $3 \mapsto 1$ e $4 \mapsto 5,\ 5 \mapsto 4$.

Fonte Original: https://paralysisbyanalysis52.wordpress.com/