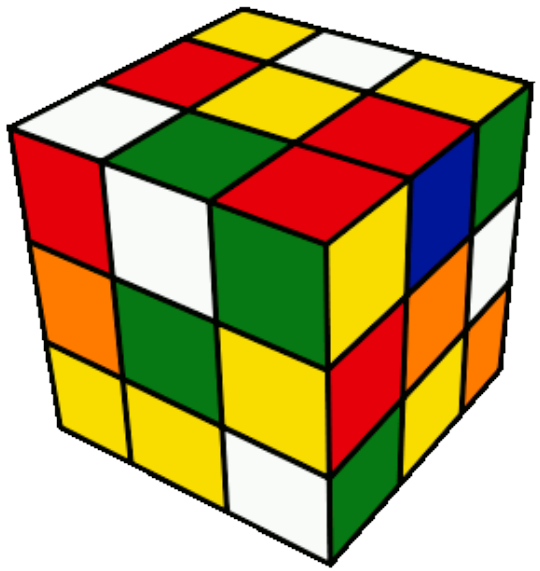
III Workshop de Álgebra da UFG-CAC

Minicurso 2

# O cubo mágico e a Teoria dos Grupos



Prof. Dr. Agnaldo José Ferrari
FC-UNESP-Bauru

# Tópicos

# Tópicos

- Histórias e curiosidades

# Tópicos

- Histórias e curiosidades
- Conhecendo o Cubo de Rubik

# Tópicos

- Histórias e curiosidades
- Conhecendo o Cubo de Rubik
- Métodos de resolução

# Tópicos

- Histórias e curiosidades
- Conhecendo o Cubo de Rubik
- Métodos de resolução
- Permutações e grupos

# Tópicos

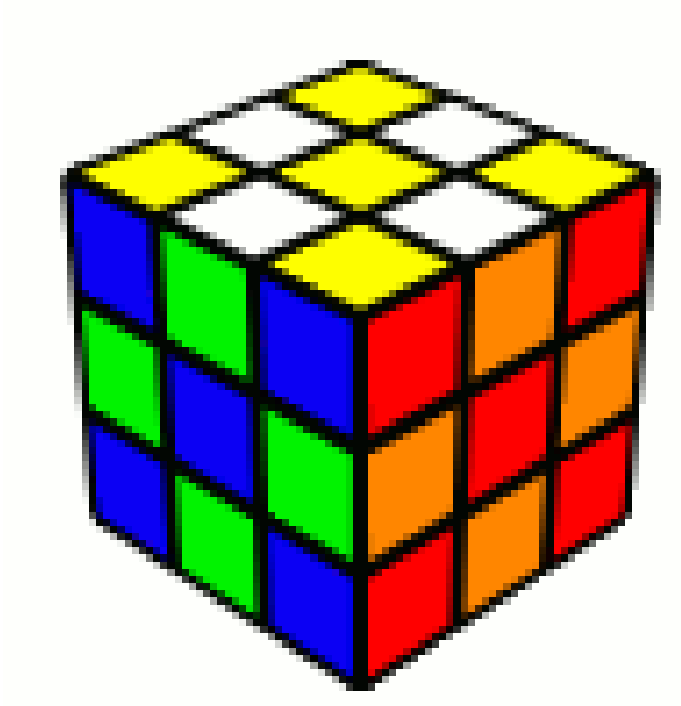
- Histórias e curiosidades
- Conhecendo o Cubo de Rubik
- Métodos de resolução
- Permutações e grupos
- Teoria de Grupos: Paridade no cubo

# Tópicos

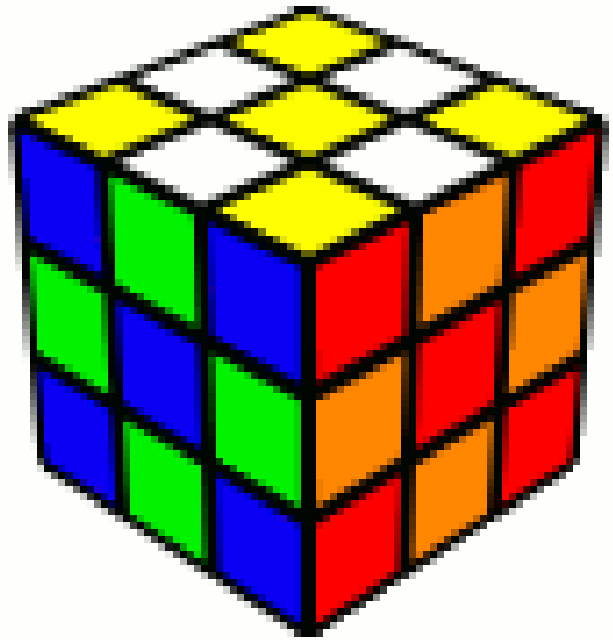
- Histórias e curiosidades
- Conhecendo o Cubo de Rubik
- Métodos de resolução
- Permutações e grupos
- Teoria de Grupos: Paridade no cubo
- Teoria de Grupos: Um passo no método de camadas

# Histórias e curiosidades

# Cubo de Rubik

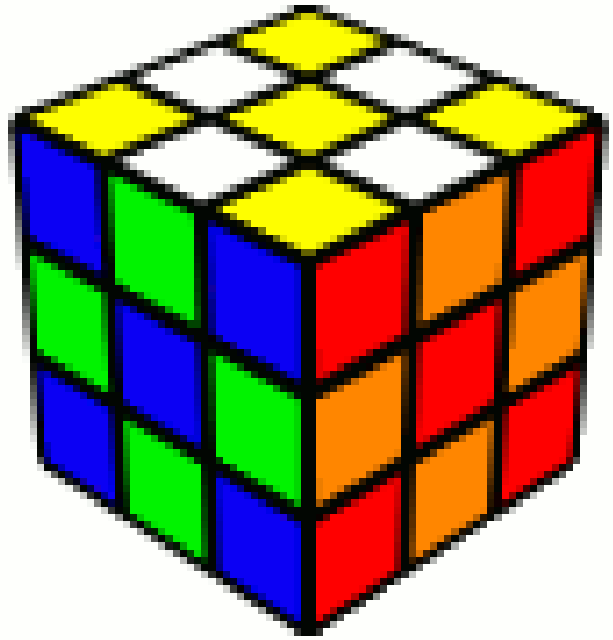


# Cubo de Rubik



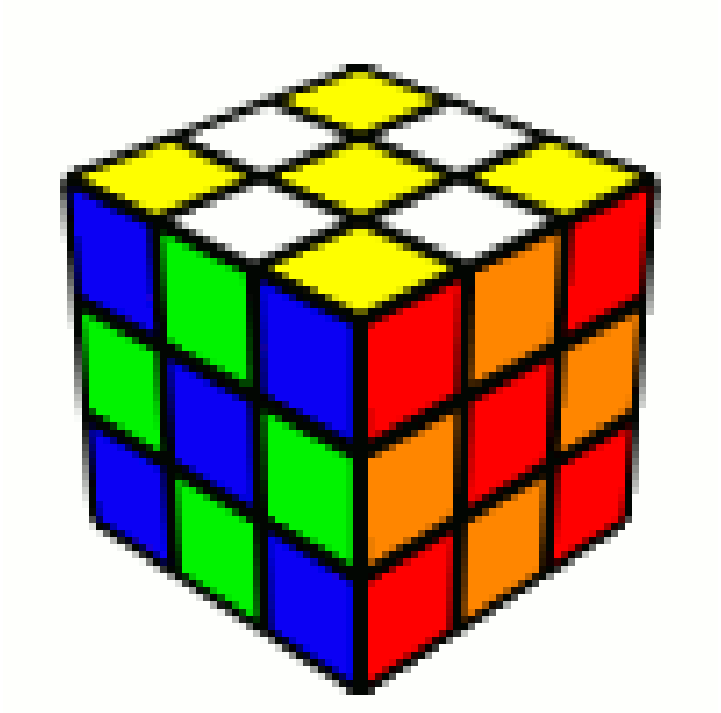
- Criado em 1974 pelo húngaro Ernst Rubik.

# Cubo de Rubik



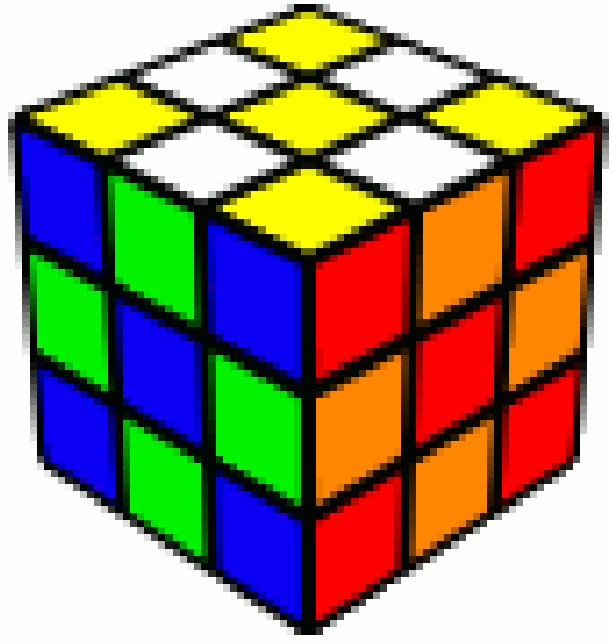
- Criado em 1974 pelo húngaro Ernst Rubik.
- Em 1980 inicia-se a produção industrial e a distribuição mundial do Cubo e 100 milhões de cubos são vendidos em 2 anos.

# Cubo de Rubik



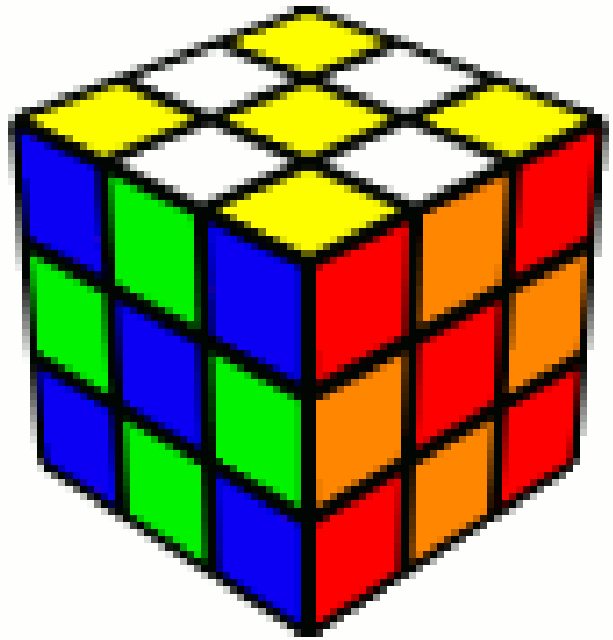
- O número de configurações possíveis para o cubo é $43.252.003.274.489.856.000$.

# Cubo de Rubik



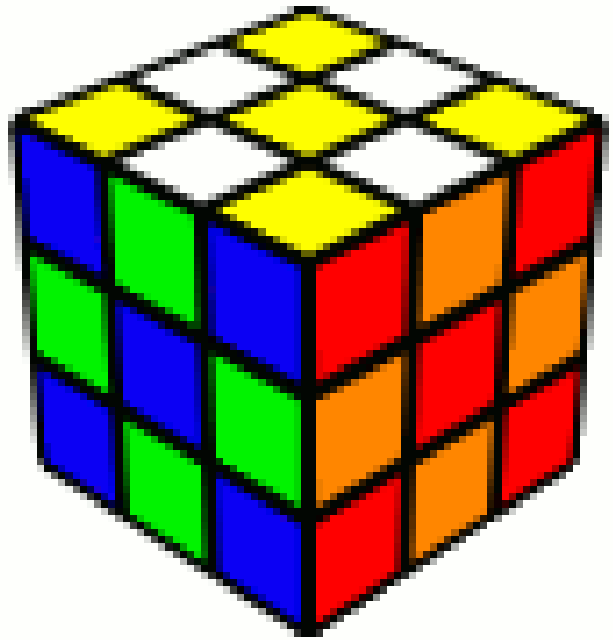
- O número de configurações possíveis para o cubo é $43.252.003.274.489.856.000$.
- Para a maioria das configurações são necessários de $15$ a $19$ movimentos para a resolução.

# Cubo de Rubik



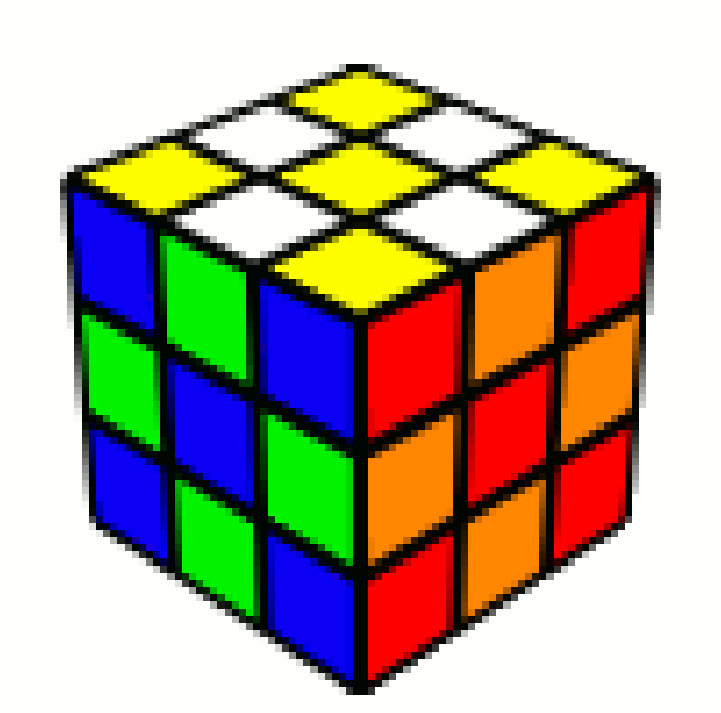
- Para $\pm 300$ milhões de configurações são necessários $20$ movimentos para a resolução.

# Cubo de Rubik



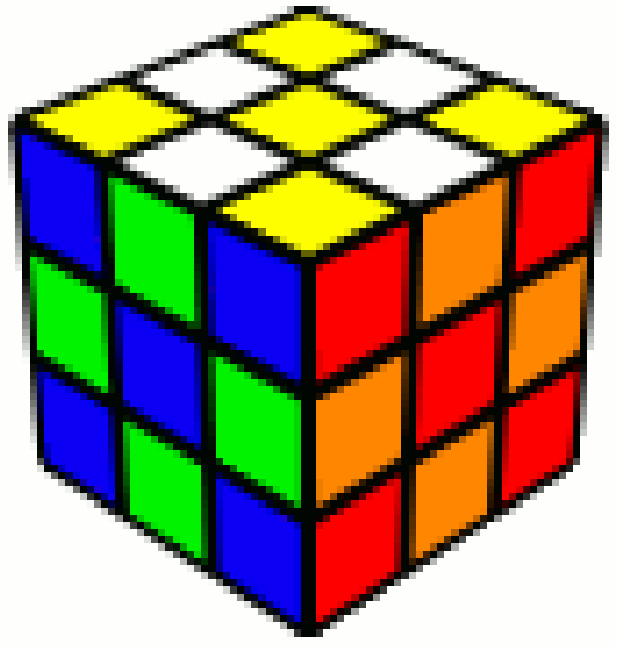
- Para $\pm 300$ milhões de configurações são necessários $20$ movimentos para a resolução.
- Foi provado que qualquer configuração do cubo pode ser resolvida com no máximo $20$ movimentos.

# Cubo de Rubik



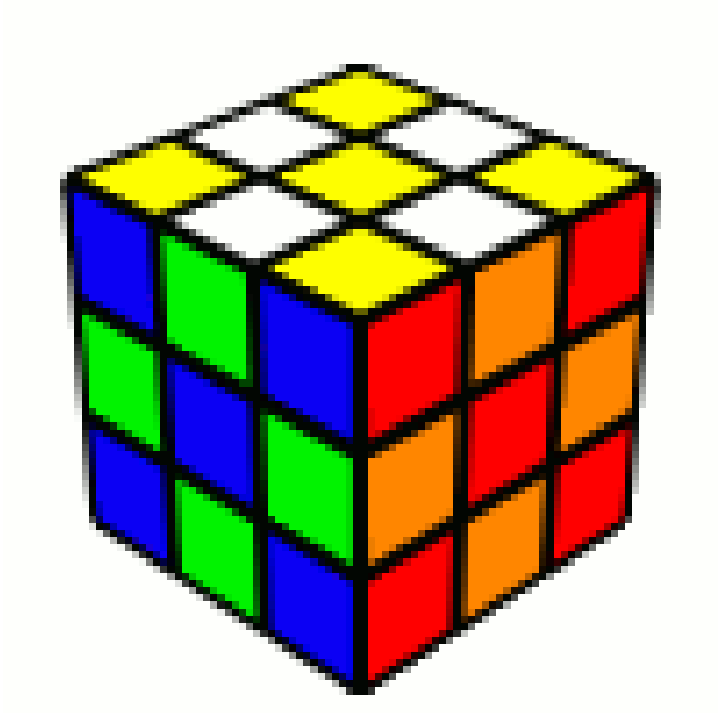
- A prova foi dada por Morley Davidson, John Dethridge, Herbert Kociemba e Tomas Rokicki.

# Cubo de Rubik



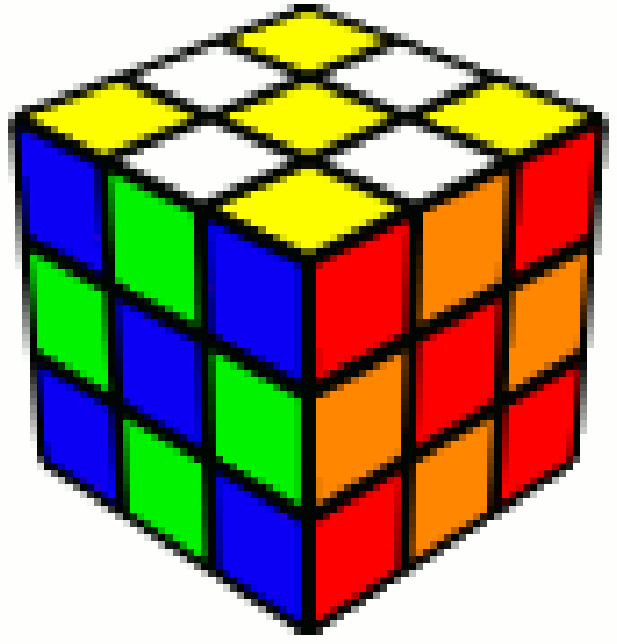
- A prova foi dada por Morley Davidson, John Dethridge, Herbert Kociemba e Tomas Rokicki.
- A ideia foi separar as configurações em grupos e resolver separadamente.

# Cubo de Rubik



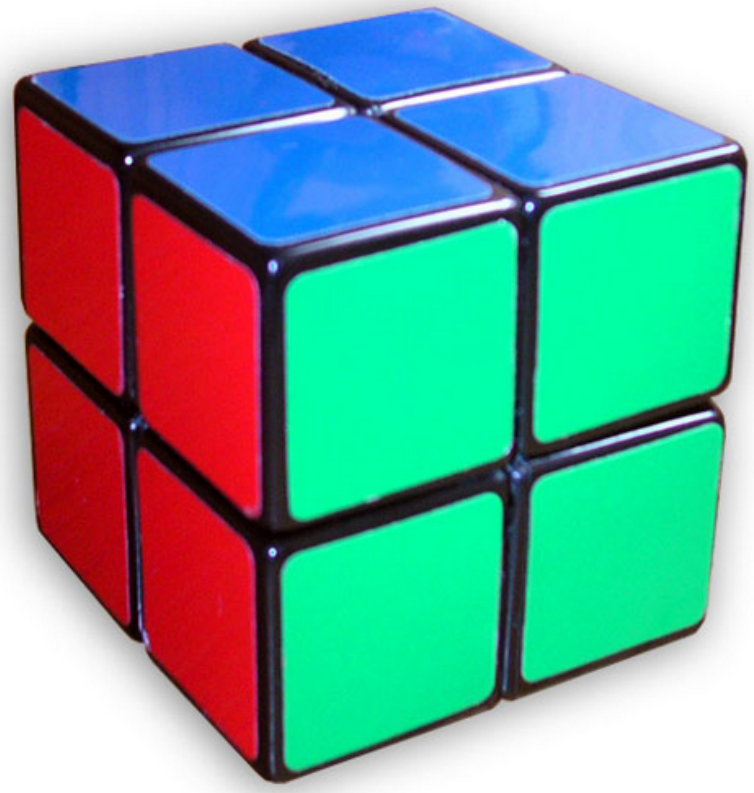
- O recorde de resolução do cubo por tempo é do holandes Mats Valk, com o tempo de $5,55$ segundos.

# Cubo de Rubik

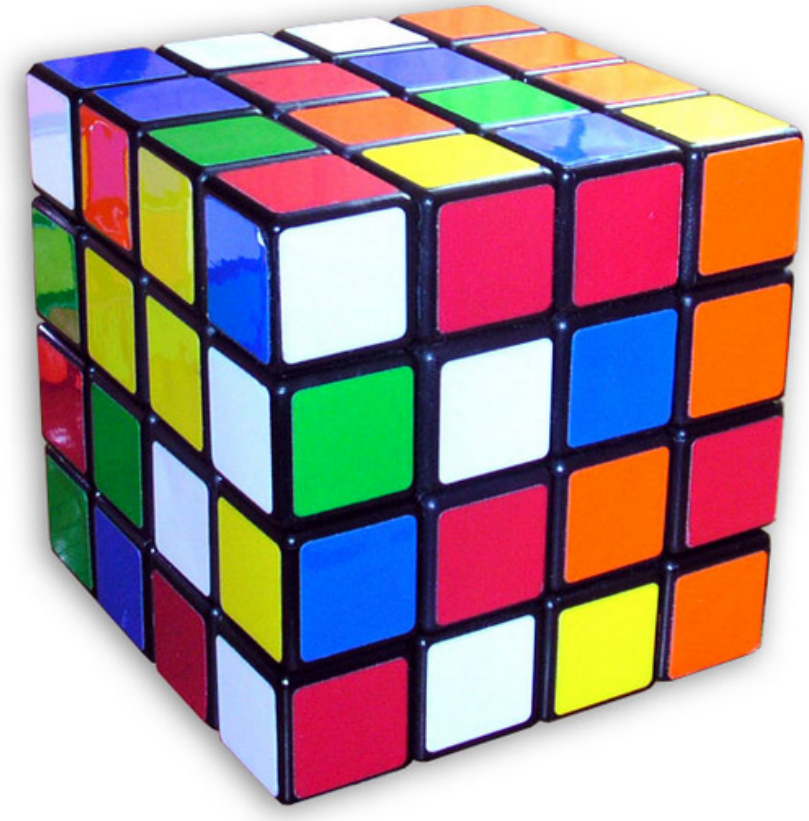


- O recorde de resolução do cubo por tempo é do holandes Mats Valk, com o tempo de $5,55$ segundos.
- Existem campeonatos em diversas outras modalidades: Resolução com os olhos vendados, resolução com os pés, etc.

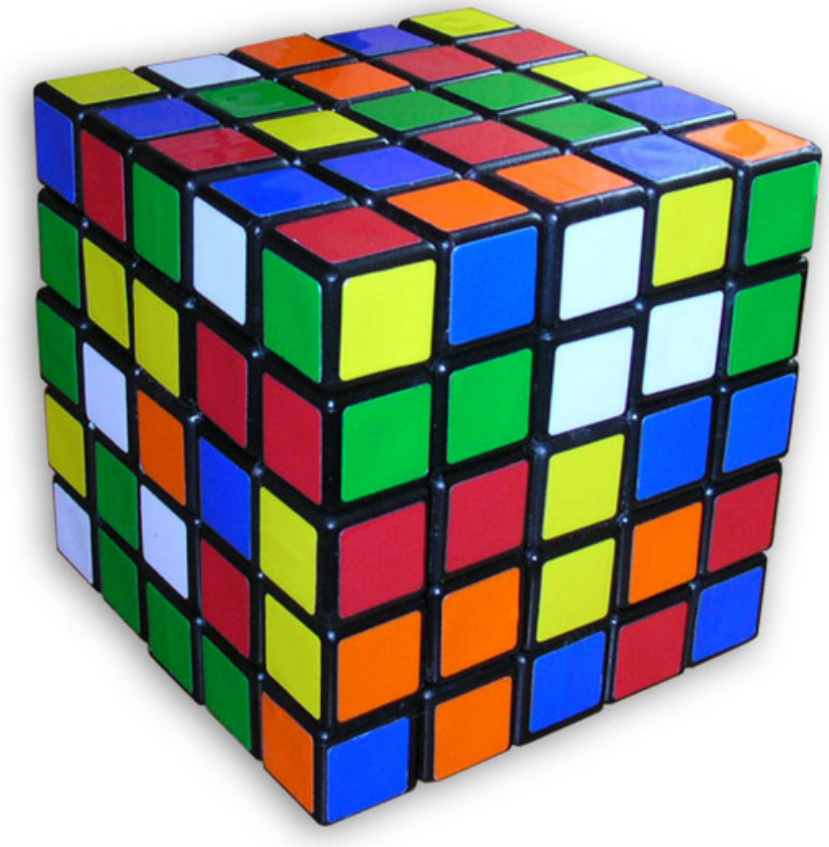
# Outras versões do cubo



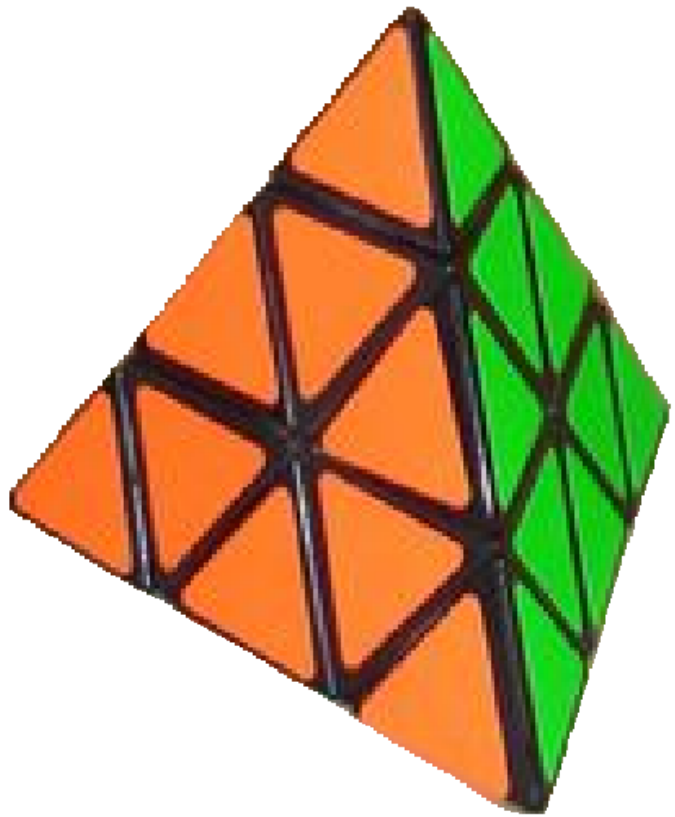
# Outras versões do cubo



# Outras versões do cubo



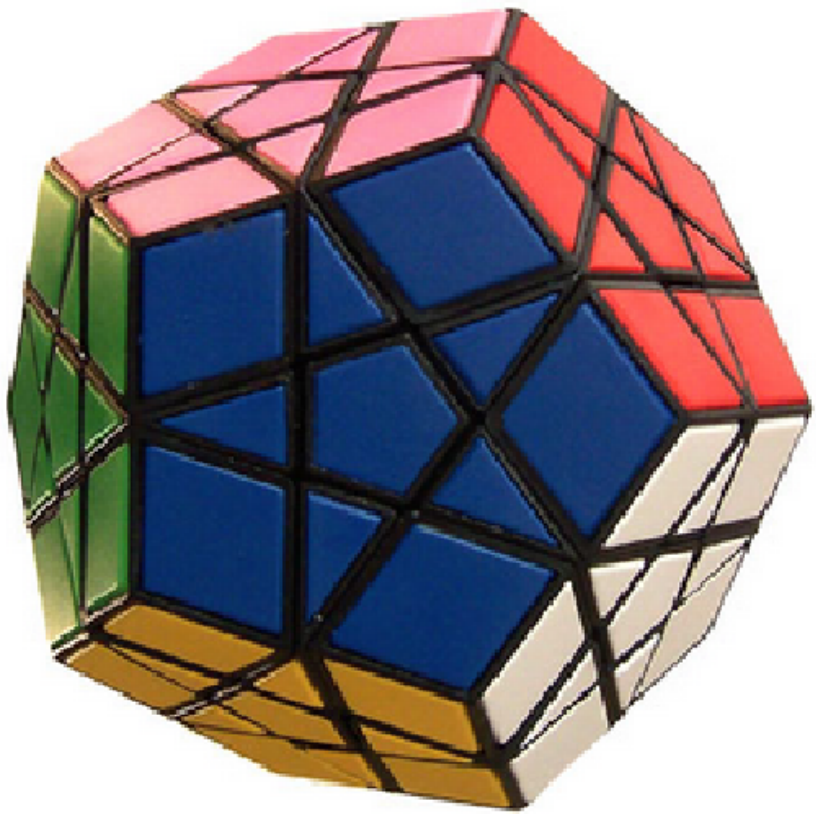
# Outras versões do cubo



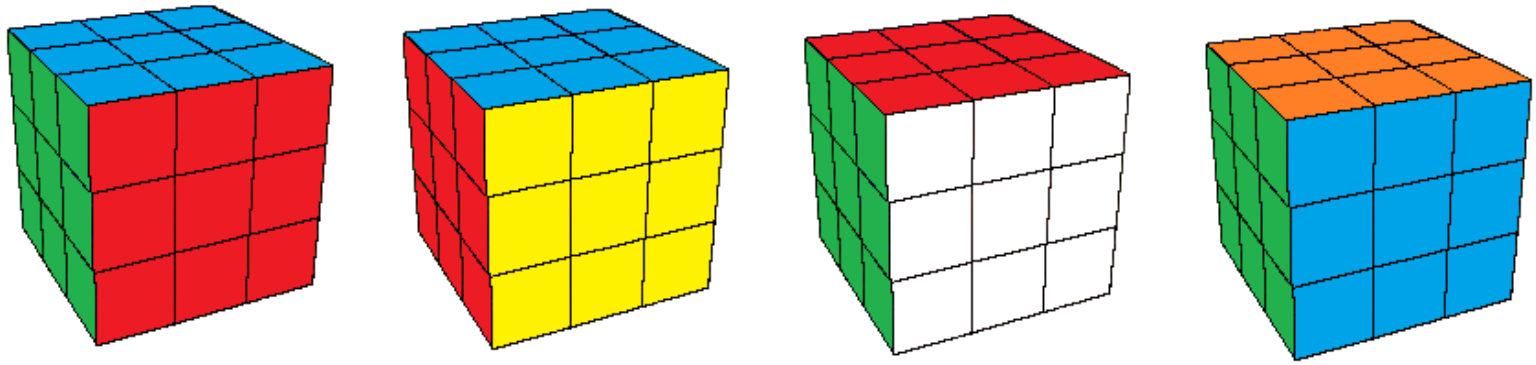
# Outras versões do cubo

# Outras versões do cubo

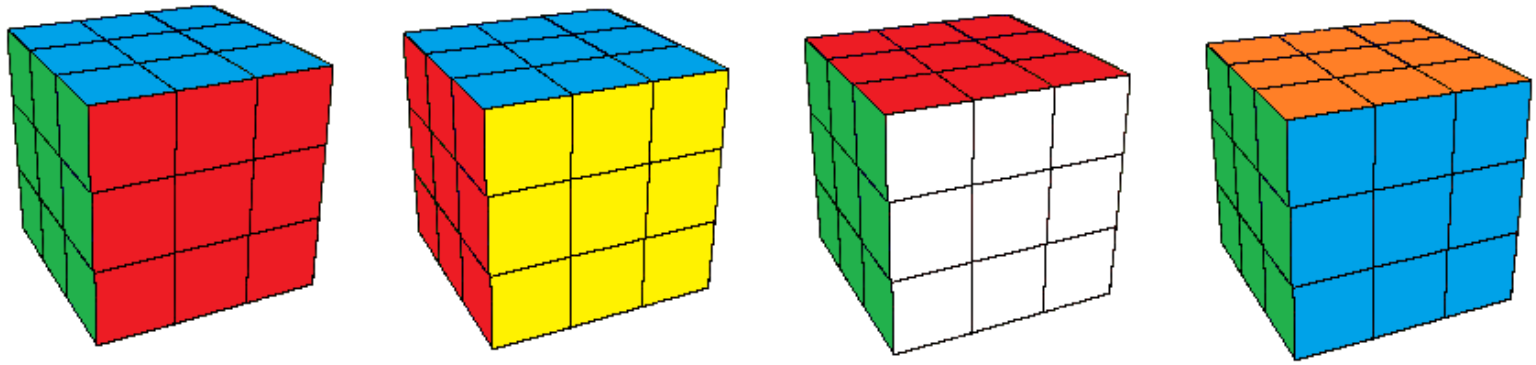
# Outras versões do cubo



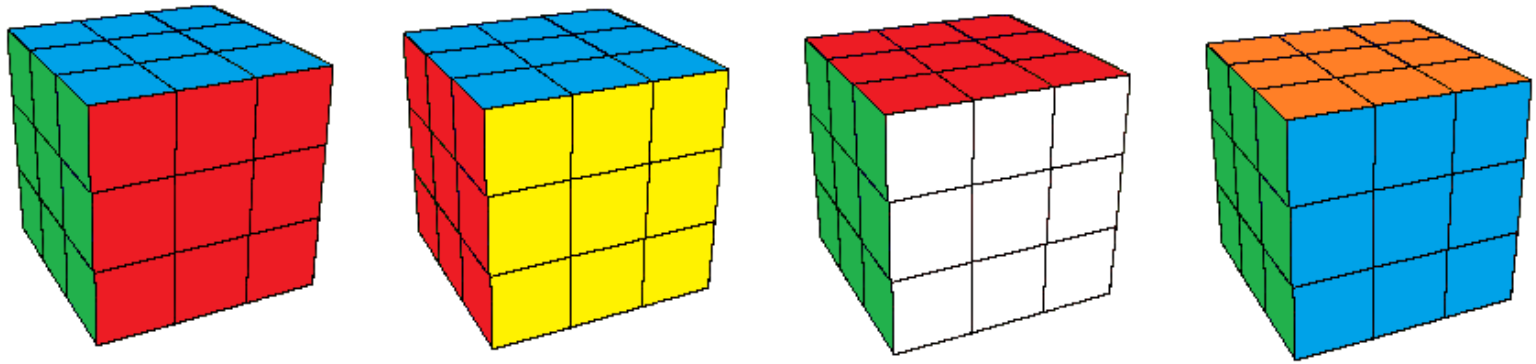
# Conhecendo o Cubo de Rubik



- O cubo possui 6 faces de cores distintas.



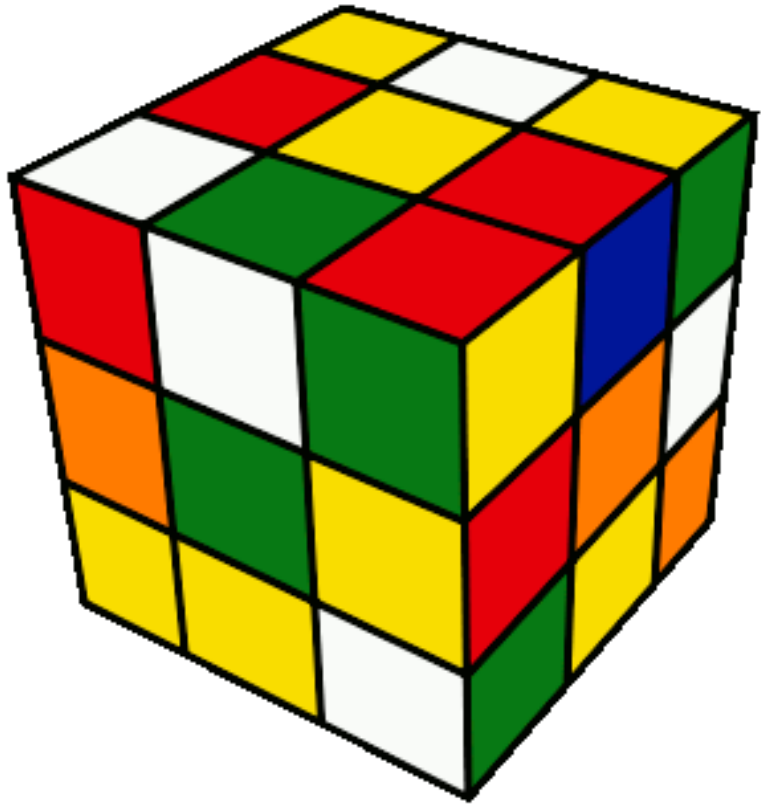
- O cubo possui 6 faces de cores distintas.
- Cada face possui 9 cubinhos, então o cubo possui 27 cubinhos (1 virtual).



- O cubo possui 6 faces de cores distintas.
- Cada face possui 9 cubinhos, então o cubo possui 27 cubinhos (1 virtual).
- Cada cubinho possui 6 facetas, mas somente são visíveis as que apontam para fora do cubo.

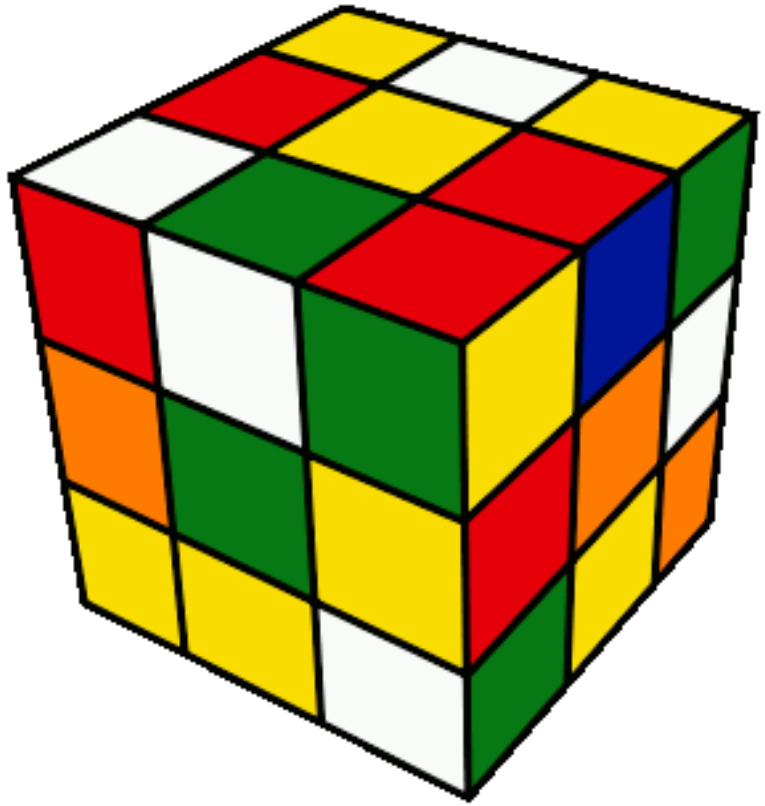
# Conhecendo o Cubo de Rubik

## FACES



# Conhecendo o Cubo de Rubik

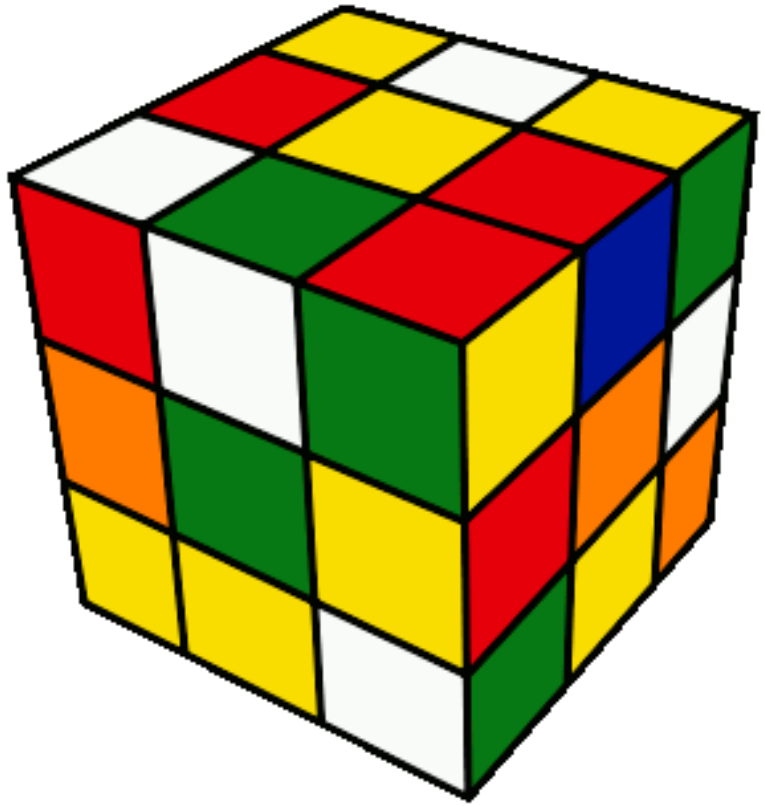
## FACES



**F** (Front)

# Conhecendo o Cubo de Rubik

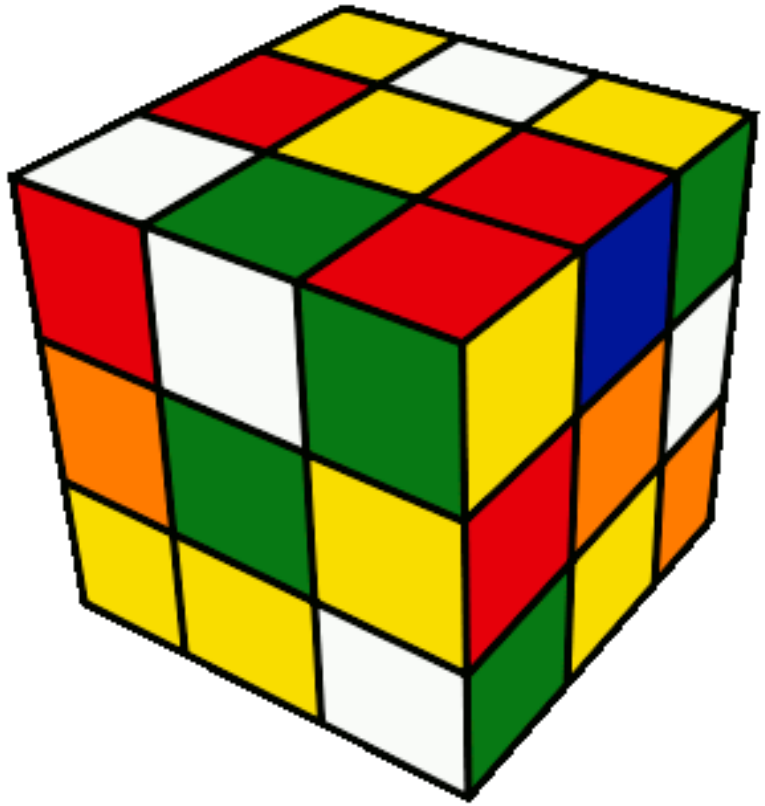
## FACES



**B** (Back)

# Conhecendo o Cubo de Rubik

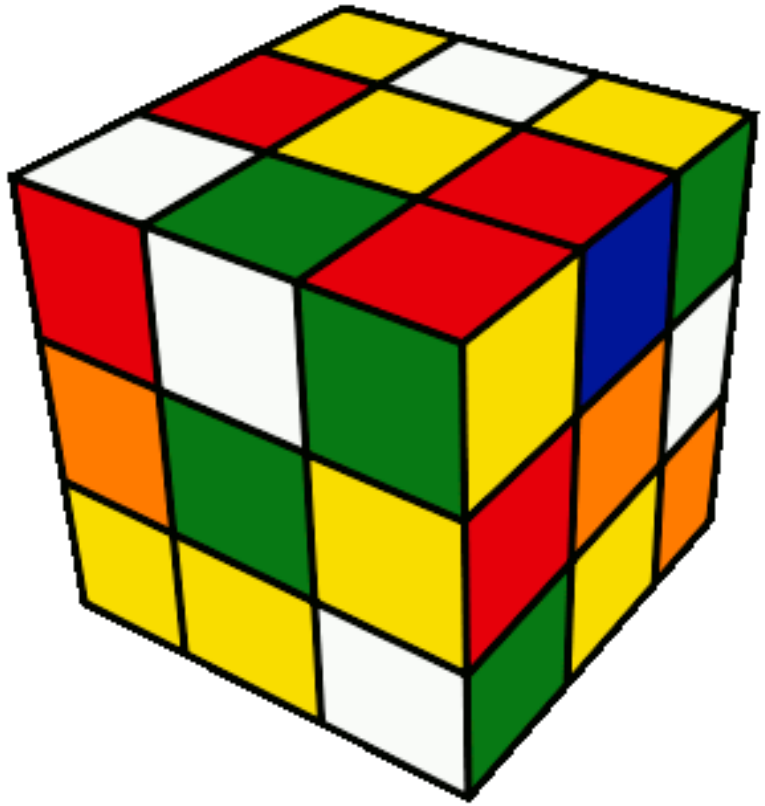
## FACES



**U** (Upper)

# Conhecendo o Cubo de Rubik

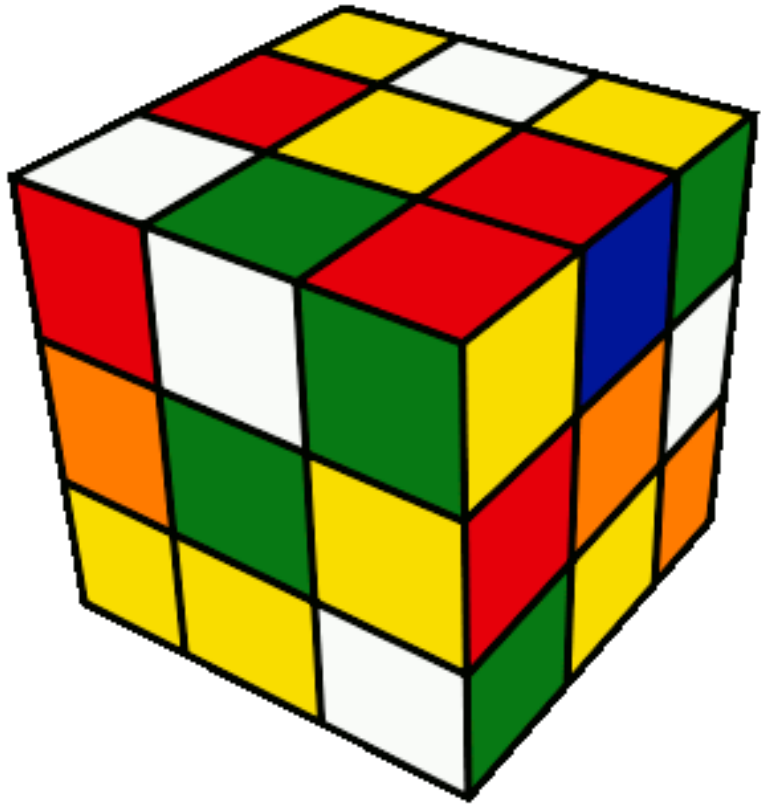
## FACES



**D** (Down)

# Conhecendo o Cubo de Rubik

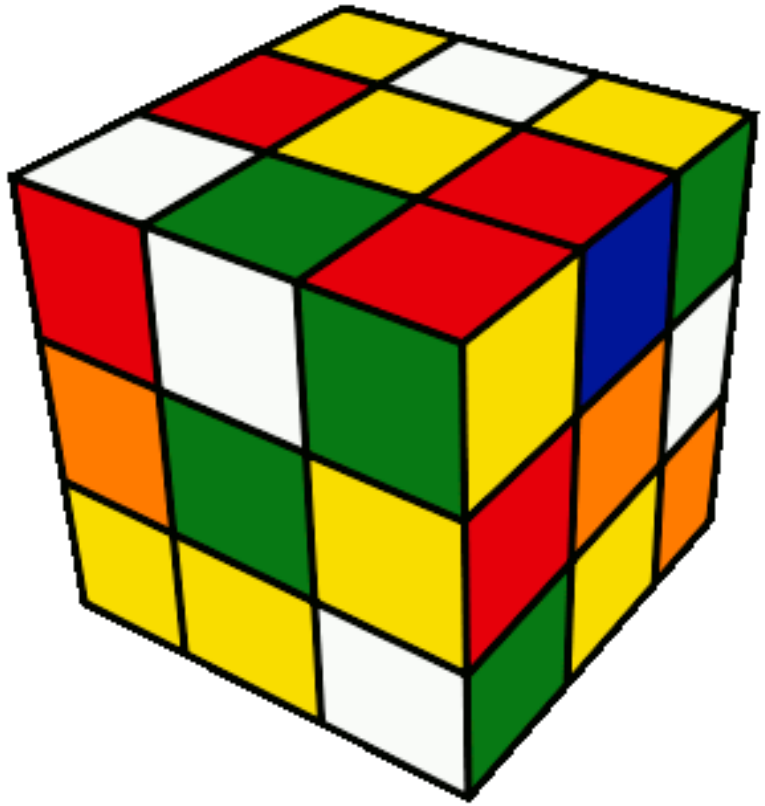
## FACES



**L** (Left)

# Conhecendo o Cubo de Rubik

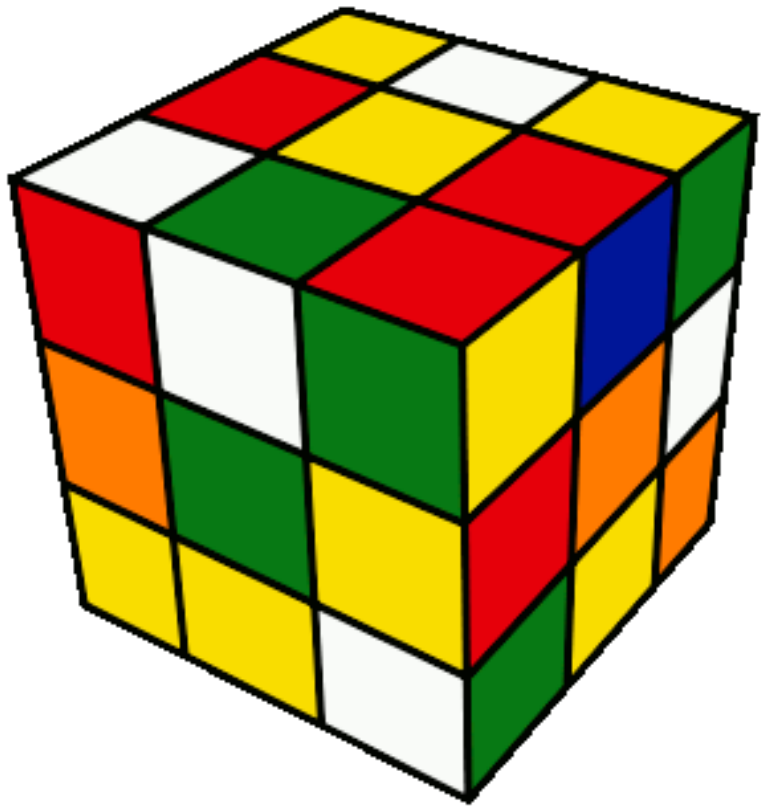
## FACES



**R** (Right)

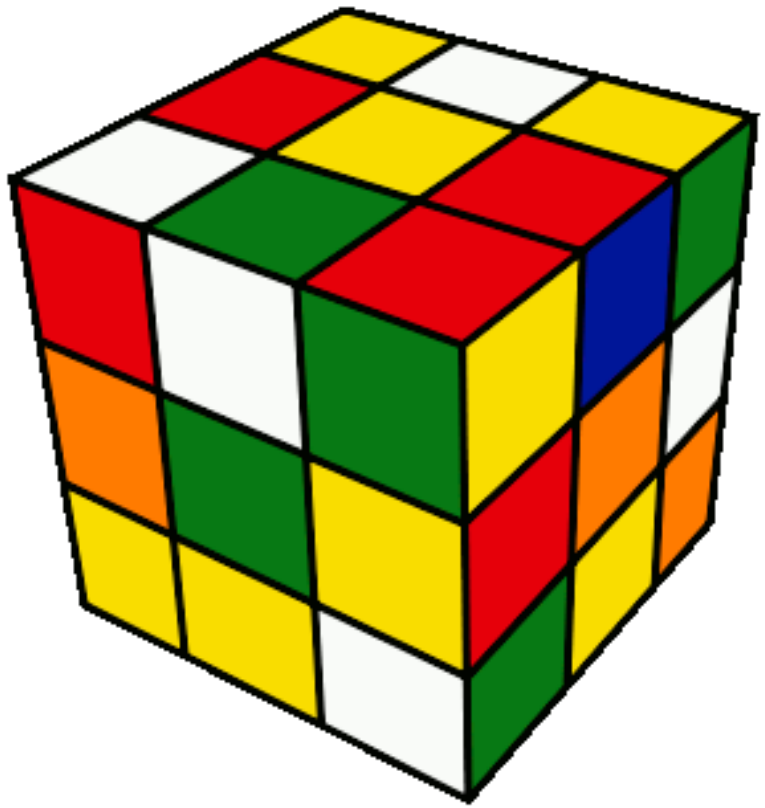
# Conhecendo o Cubo de Rubik

## CUBINHOS



# Conhecendo o Cubo de Rubik

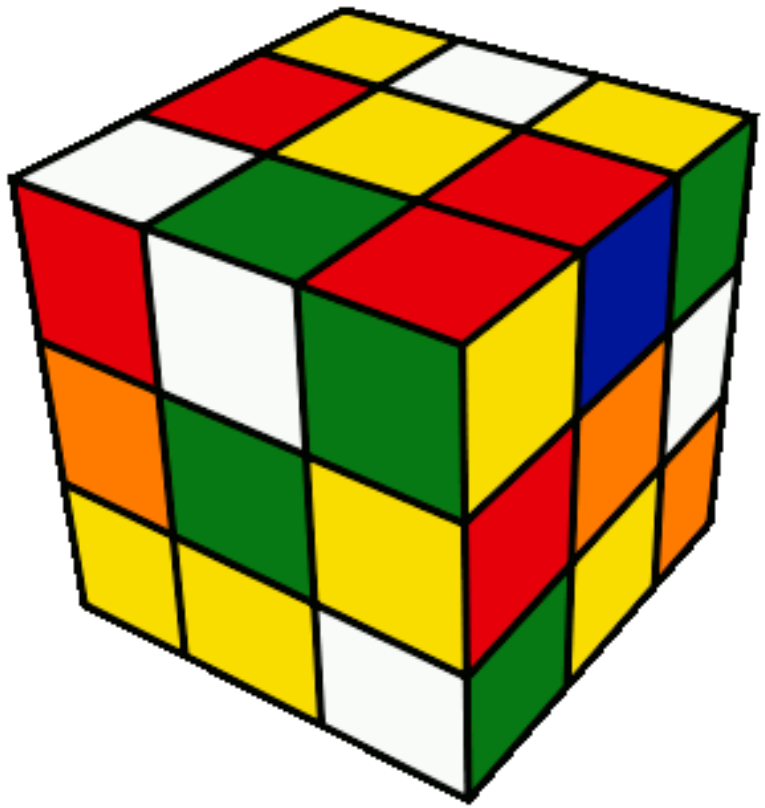
## CUBINHOS



cubinhos centrais

# Conhecendo o Cubo de Rubik

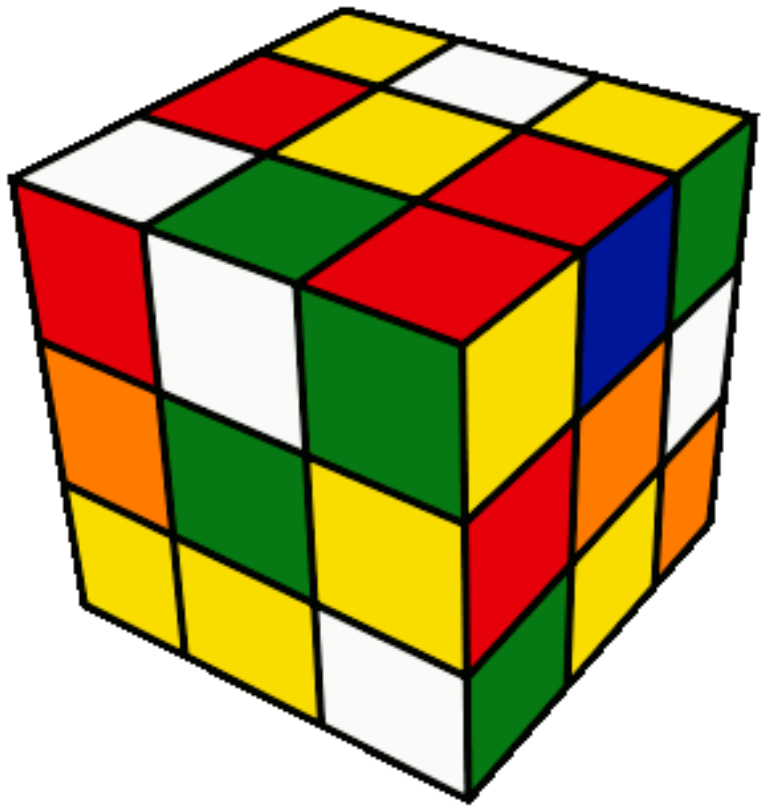
## CUBINHOS



cubinhos de aresta

# Conhecendo o Cubo de Rubik

## CUBINHOS



cubinhos de canto

# Movimentos do cubo

- Cada face pode ser girada um quarto de volta tanto no sentido horário quanto no anti-horário.

# Movimentos do cubo

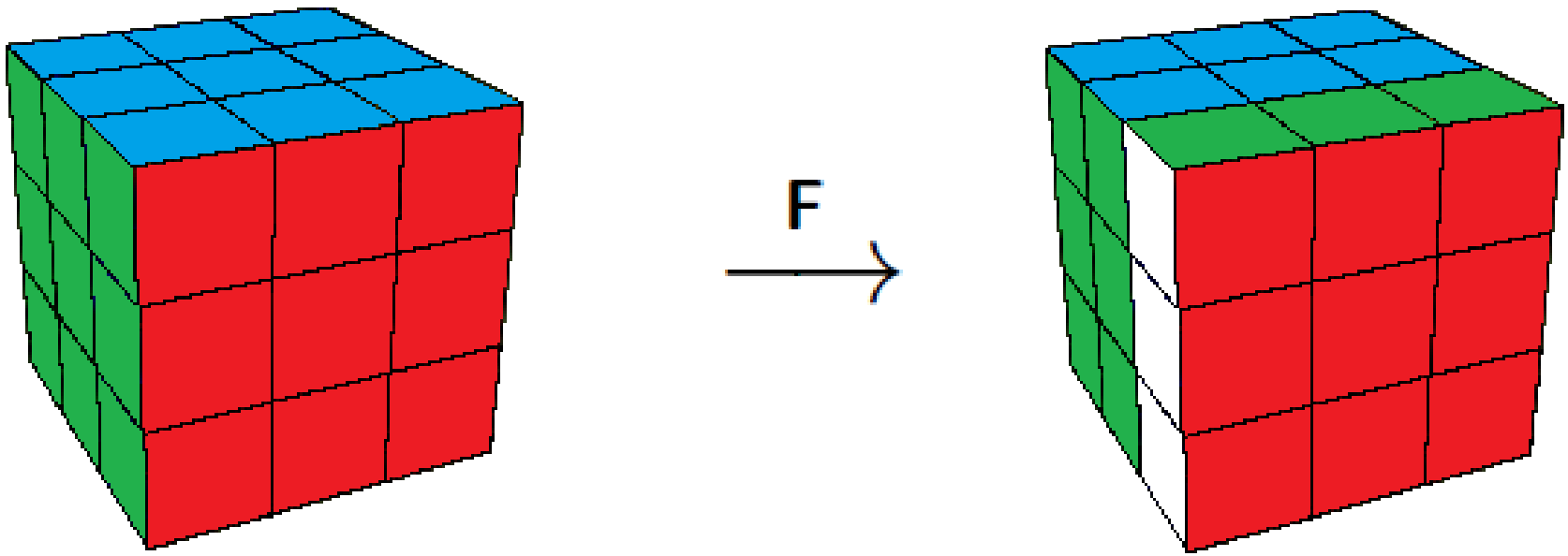
- Cada face pode ser girada um quarto de volta tanto no sentido horário quanto no anti-horário.
- Convencionaremos indicar os respectivos movimentos de **um quarto de volta no sentido horário** por F, B, U, D, L e R.

# Movimentos do cubo

- Cada face pode ser girada um quarto de volta tanto no sentido horário quanto no anti-horário.
- Convencionaremos indicar os respectivos movimentos de **um quarto de volta no sentido horário** por F, B, U, D, L e R.
- E os respectivos movimentos de **um quarto de volta no sentido anti-horário** por $F^{-1}$, $B^{-1}$, $U^{-1}$, $D^{-1}$, $L^{-1}$ e $R^{-1}$.

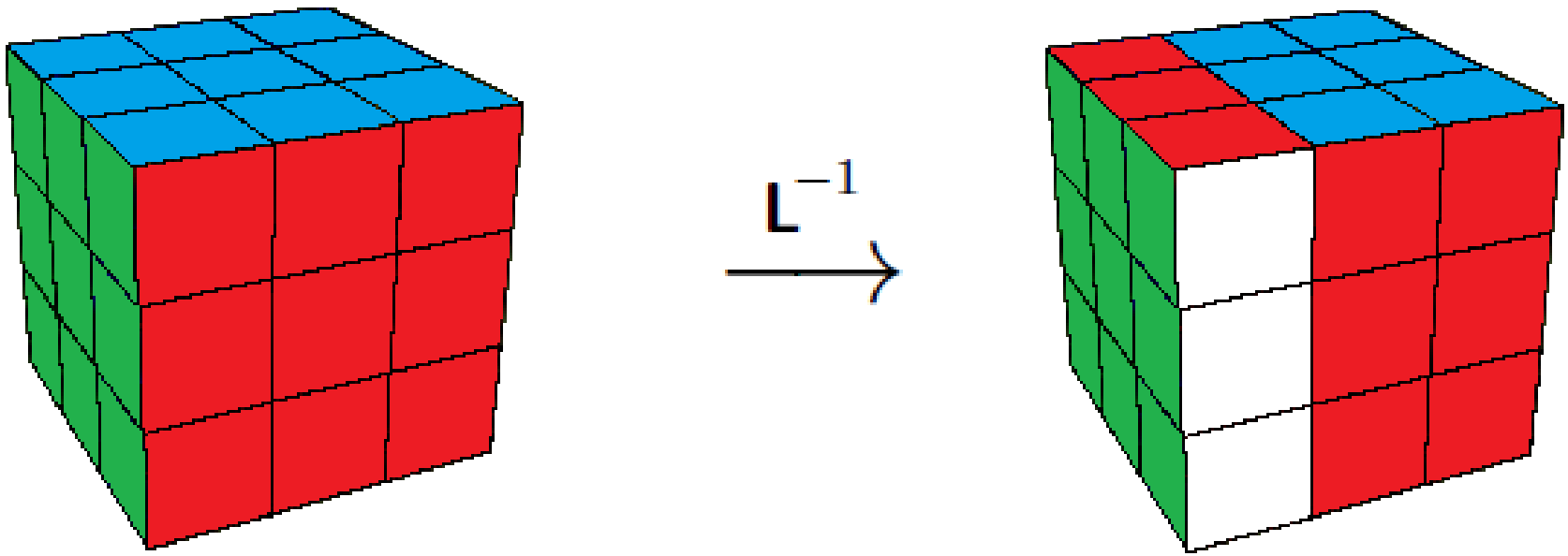
# Movimentos do cubo

## Exemplo 1



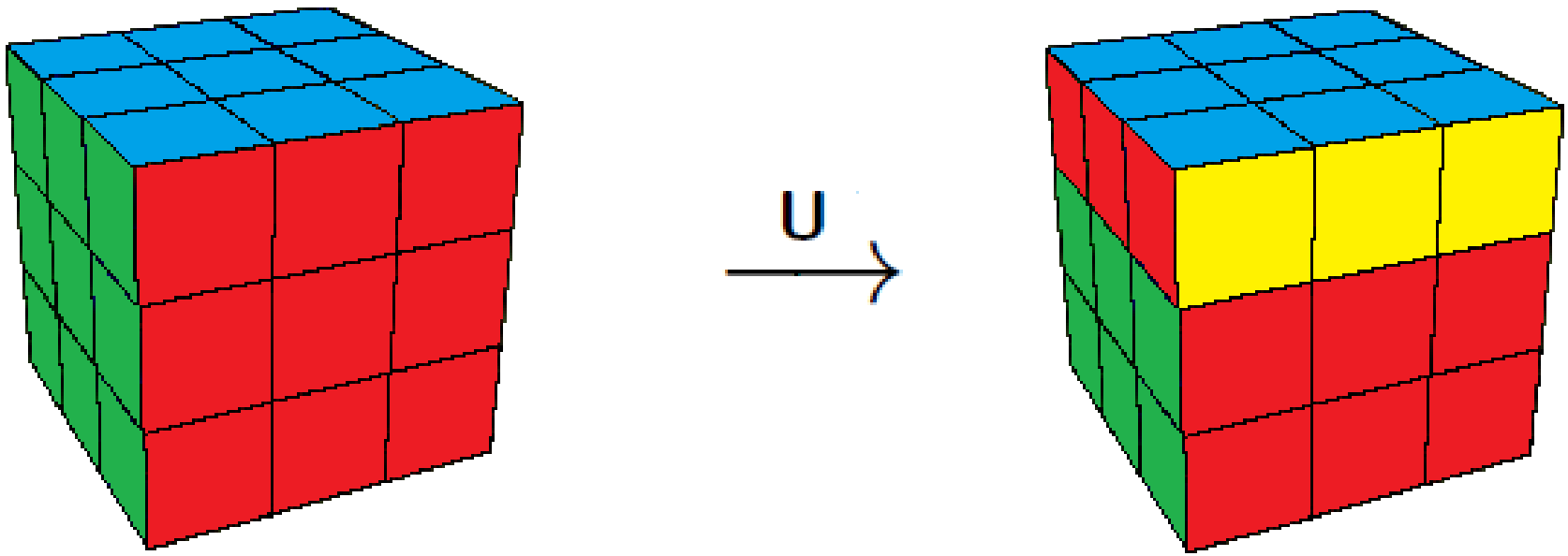
# Movimentos do cubo

## Exemplo 2



# Movimentos do cubo

## Exemplo 3



# Sequências de movimento

- Normalmente faremos várias sequências de movimento.

# Sequências de movimento

- Normalmente faremos várias sequências de movimento.
- Por exemplo, $S = LUB^{-1}$ significa que movemos a face da esquerda uma volta no sentido horário, depois movemos a face superior uma volta no sentido horário e finalmente movemos a face inferior uma volta no sentido anti-horário.

# Sequências de movimento

- Normalmente faremos várias sequências de movimento.
- Por exemplo, $S = LUB^{-1}$ significa que movemos a face da esquerda uma volta no sentido horário, depois movemos a face superior uma volta no sentido horário e finalmente movemos a face inferior uma volta no sentido anti-horário.
- A esta sequência atribuimos a letra $S$.

# Sequências de movimento

- O número de quartos de volta ($q$) da sequência é o seu comprimento, no exemplo acima o comprimento de $S$ é $3q$.

# Sequências de movimento

- O número de quartos de volta $(q)$ da sequência é o seu comprimento, no exemplo acima o comprimento de $S$ é $3q$.
- Uma seqüência longa finita S consistindo de dois ou mais movimentos é chamada **macro**.

# Sequências de movimento

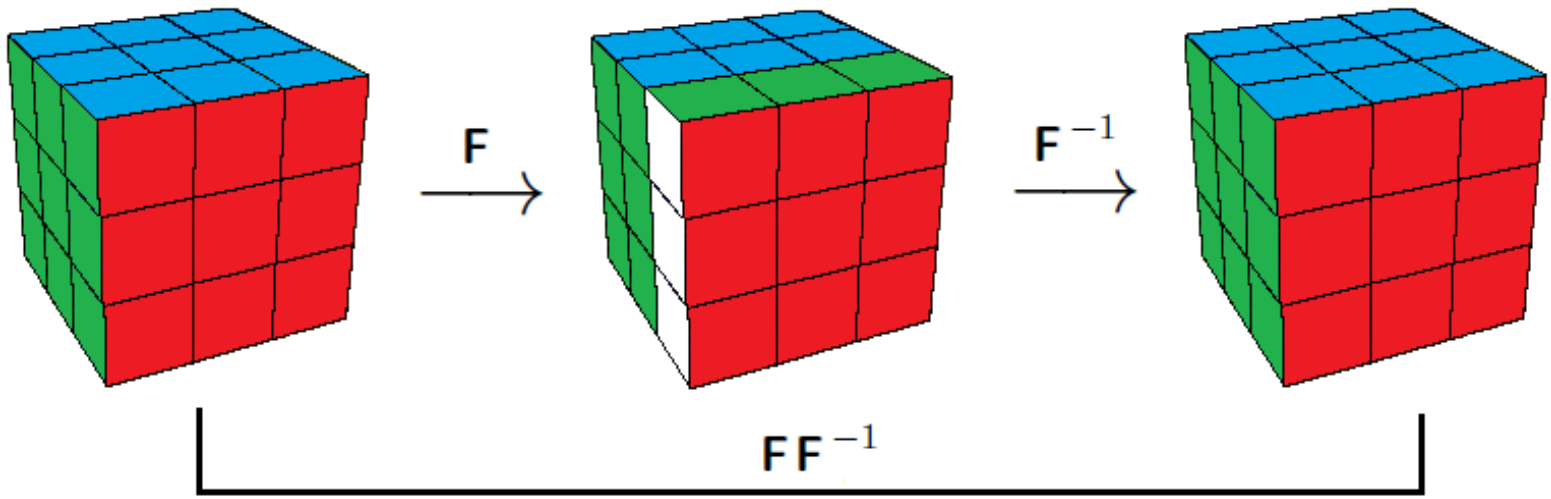
- O movimento **fazer nada** é deixar o cubo inalterado. Indicamos esse movimento por $I$, e o chamamos **identidade**.

# Sequências de movimento

- O movimento **fazer nada** é deixar o cubo inalterado. Indicamos esse movimento por $I$, e o chamamos **identidade**.
- Claramente, $FF^{-1} = I$, pois fazer $F$ seguido de $F^{-1}$ é o mesmo que não fazer nada com o cubo. Temos também que $F^{-1}F = I$, logo $(F^{-1})^{-1} = F$.

# Sequências de movimento

- O movimento **fazer nada** é deixar o cubo inalterado. Indicamos esse movimento por $I$, e o chamamos **identidade**.
- Claramente, $FF^{-1} = I$, pois fazer $F$ seguido de $F^{-1}$ é o mesmo que não fazer nada com o cubo. Temos também que $F^{-1}F = I$, logo $(F^{-1})^{-1} = F$.



# Comutatividade

# Comutatividade

Lei da aritmética: "A ordem dos fatores não altera o produto"

- No cubo alguns movimentos são **comutativos**, por exemplo, os movimentos que envolvem faces opostas: $FB = BF$, $RL = LR$ e $UD = DU$.

# Comutatividade

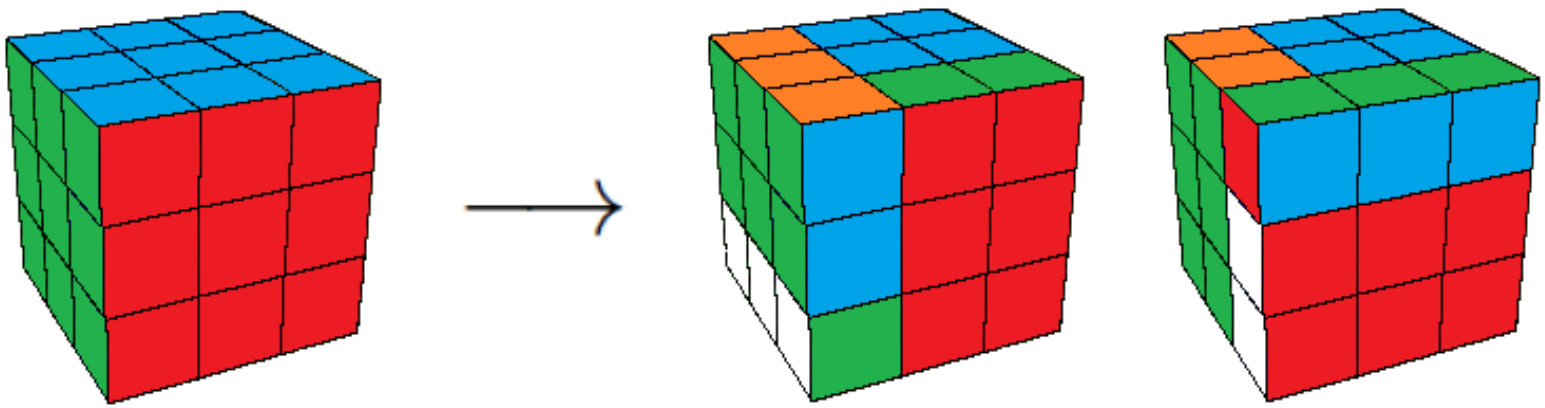
Lei da aritmética: "A ordem dos fatores não altera o produto"

- No cubo alguns movimentos são **comutativos**, por exemplo, os movimentos que envolvem faces opostas: $FB = BF$, $RL = LR$ e $UD = DU$.
- Mas existem movimentos **não-comutativos**, por exemplo, os movimentos que envolvem faces adjacentes: $UR \neq RU$, $FL \neq LF$, etc.

# Comutatividade

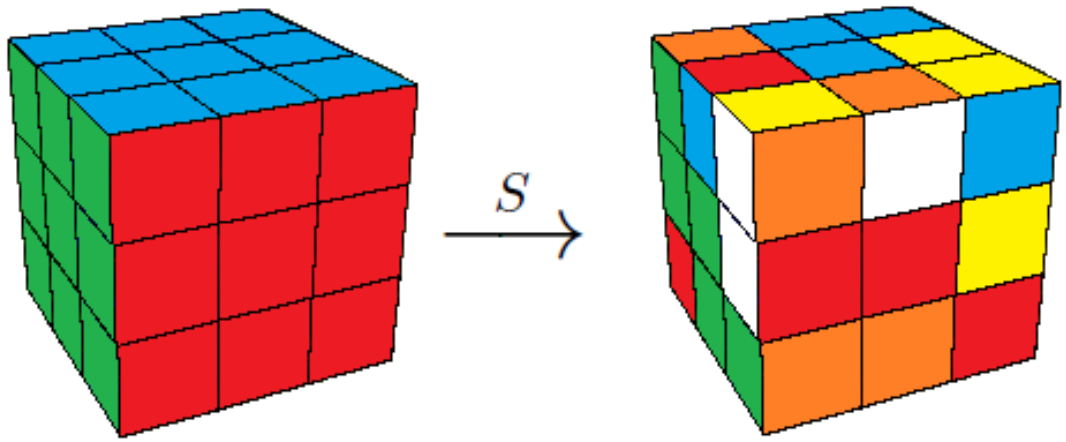
Lei da aritmética: "A ordem dos fatores não altera o produto"

- No cubo alguns movimentos são **comutativos**, por exemplo, os movimentos que envolvem faces opostas: $FB = BF$, $RL = LR$ e $UD = DU$.
- Mas existem movimentos **não-comutativos**, por exemplo, os movimentos que envolvem faces adjacentes: $UR \neq RU$, $FL \neq LF$, etc.



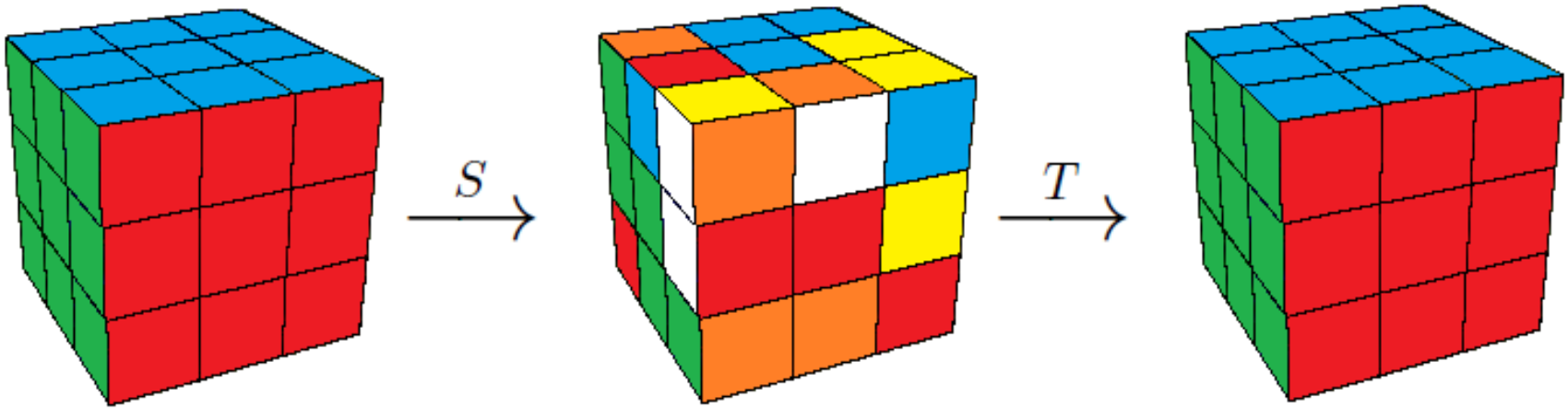
# Embaralhar e resolver o cubo

# Embaralhar e resolver o cubo




**Embaralhar o Cubo:** Aplicar uma macro aleatória de movimentos $S$ a um cubo resolvido.

# Embaralhar e resolver o cubo




**Resolver o Cubo:** Encontrar alguma macro $T$ tal que $ST = I$.

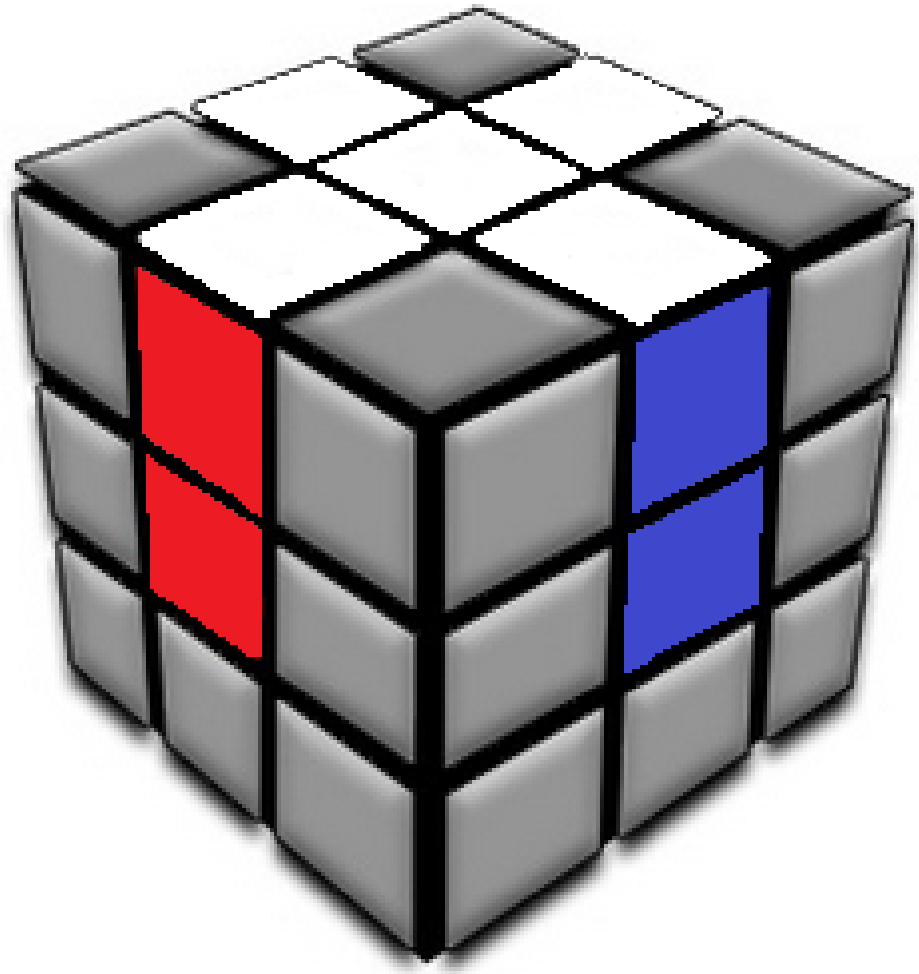
# Métodos de resolução

- Método de camadas

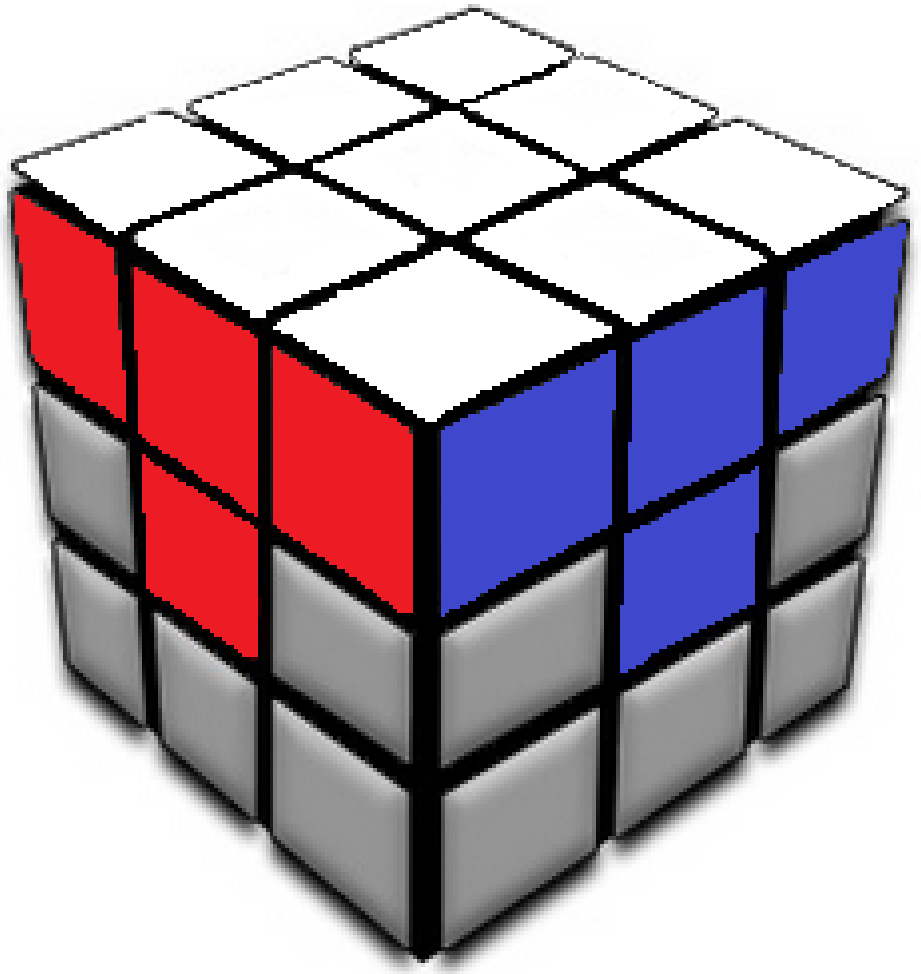
- Método de camadas
- Método de Fridrich

# Método de camadas

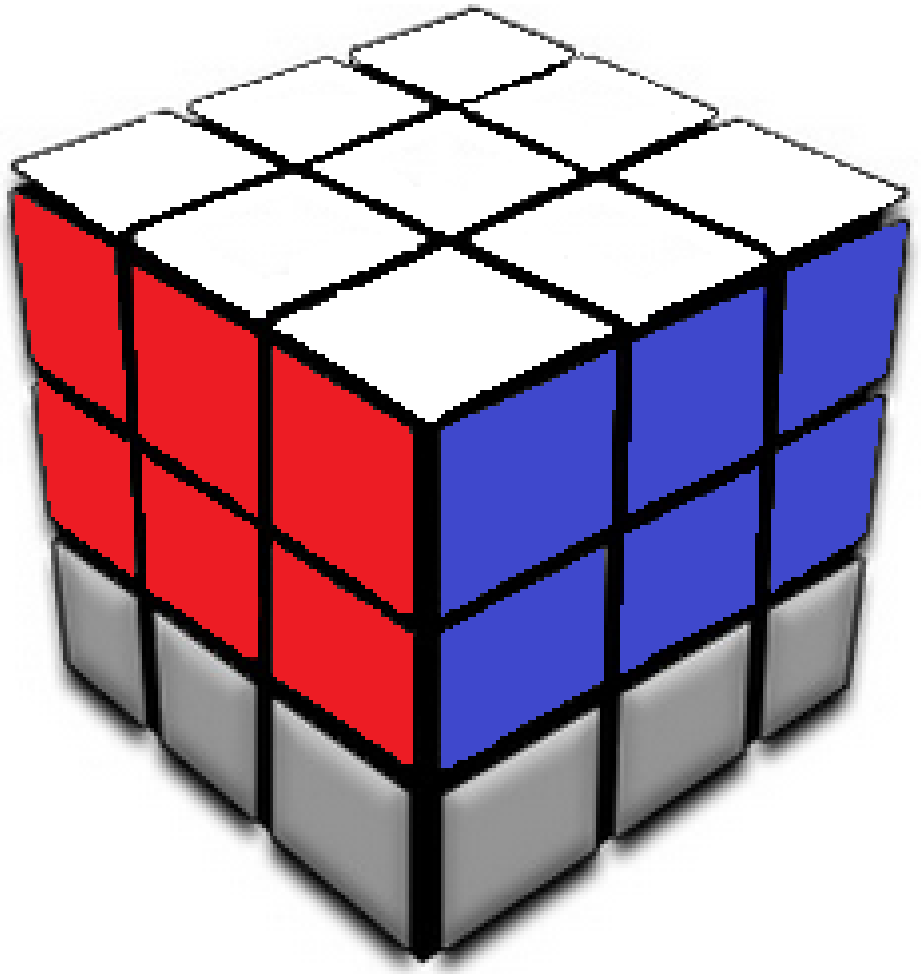
# Método de camadas



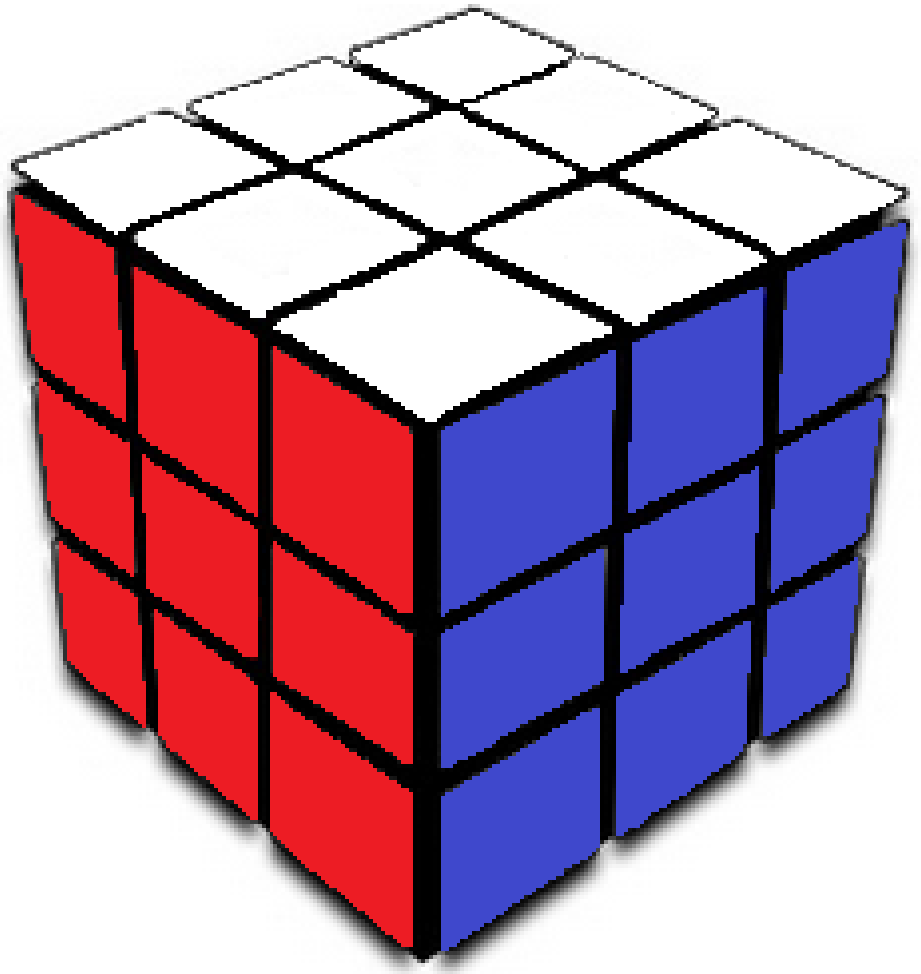
# Método de camadas



# Método de camadas



# Método de camadas



# Método de Fridrich

# Método de Fridrich

O método completo se divide em 4 passos

1. Cruz branca - solução intuitiva
2. F2L - Finish Two Layers / 41 casos
3. OLL - Orientation Last Layer / 57 casos
4. PLL - Permutation Last Layer / 21 casos

# Permutações e grupos

# Permutações

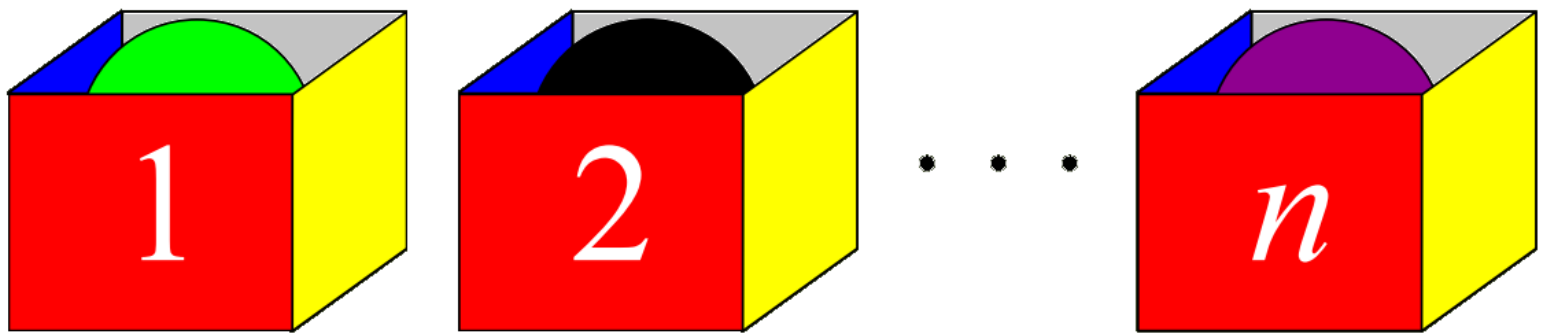
## Definição

Uma **permutação** é um rearranjo de um conjunto de objetos.

# Permutações

## Definição

Uma **permutação** é um rearranjo de um conjunto de objetos.



# Permutações

- Uma permutação pode ser descrita pelo seguinte esquema

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 1 & \cdots & n \end{pmatrix}$$

# Permutações

- Uma permutação pode ser descrita pelo seguinte esquema

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 1 & \cdots & n \end{pmatrix}$$

- Maneira mais simples para descrever uma permutação: **ciclos**

# Permutações

- Uma permutação pode ser descrita pelo seguinte esquema

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 1 & \cdots & n \end{pmatrix}$$

- Maneira mais simples para descrever uma permutação: **ciclos**
- Um **ciclo** pode ser pensado como uma série de transições de estado que acaba por retornar ao estado inicial.

$$S_1 \to S_2 \to \cdots \to S_n \to S_1$$

# Permutações

- Exemplo

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

# Permutações

- Exemplo

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

- Representando em ciclos

$$\sigma : 1 \to 3 \to 5 \to 1$$

$$2 \to 4 \to 2$$

# Permutações

- Exemplo

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

- Representando em ciclos

$$\sigma : 1 \to 3 \to 5 \to 1$$

$$2 \to 4 \to 2$$

- Simplificando

$$\sigma = (135)(24)$$

**Notação de ciclos de $\sigma$**

# Permutações

- Exemplo

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

# Permutações

- Exemplo

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

- Representando em ciclos

$$\sigma : 1 \to 5 \to 2 \to 4 \to 1$$

# Permutações

- Exemplo

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

- Representando em ciclos

$$\sigma : 1 \to 5 \to 2 \to 4 \to 1$$

- Simplificando

$$\sigma = (1524)$$

# Permutações

- Exemplo

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

- Representando em ciclos

$$\sigma : 1 \to 5 \to 2 \to 4 \to 1$$

- Simplificando

$$\sigma = (1524)$$

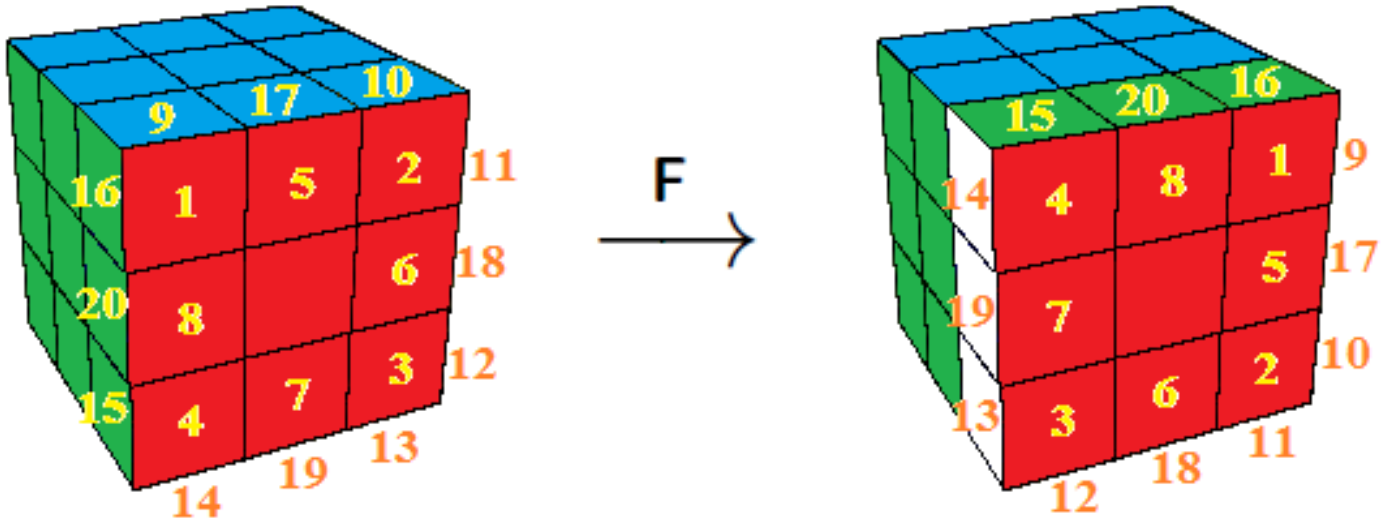
- Na notação canônica de ciclos o menor objeto entre parênteses deve iniciar o ciclo.

# Permutações das facetas do cubo

Os movimentos $R, L, F, B, U, D$ permutam o conjunto das facetas.

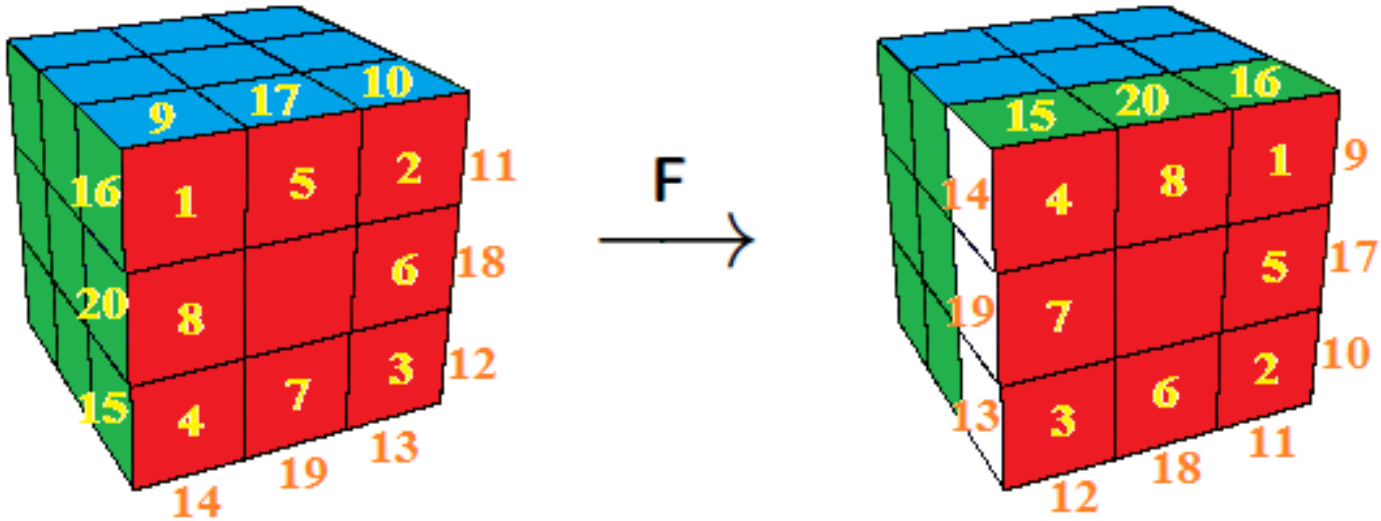
# Permutações das facetas do cubo

Os movimentos $R, L, F, B, U, D$ permutam o conjunto das facetas.



# Permutações das facetas do cubo

Os movimentos $R, L, F, B, U, D$ permutam o conjunto das facetas.




$$F = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 11\ 13\ 15)(10\ 12\ 14\ 16)(17\ 18\ 19\ 20)$$

# Decomposição em ciclos

- Fato: Toda permutação se decompõe como "produto" de ciclos disjuntos.

# Decomposição em ciclos

- Fato: Toda permutação se decompõe como "produto" de ciclos disjuntos.
- Repetição de ciclos:
  $I$
  $(1\ 2\ 3)$
  $(1\ 2\ 3)^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$
  $(1\ 2\ 3)^3 = (1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3) = I$

# Decomposição em ciclos

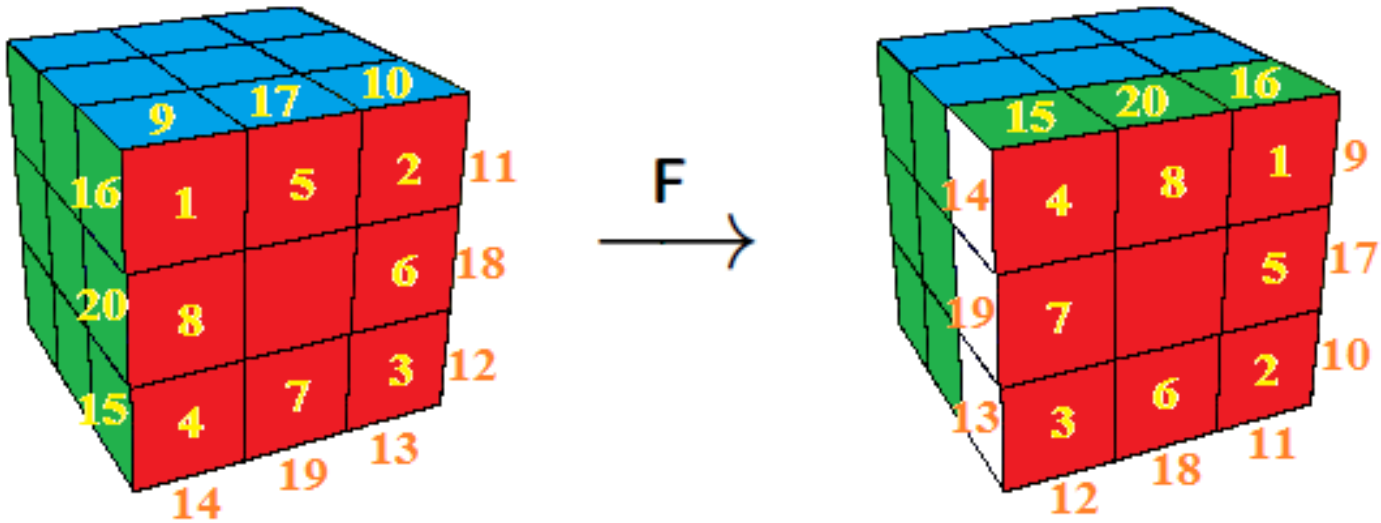
- Fato: Toda permutação se decompõe como "produto" de ciclos disjuntos.
- Repetição de ciclos:
  $I$
  $(1\ 2\ 3)$
  $(1\ 2\ 3)^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$
  $(1\ 2\ 3)^3 = (1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3) = I$
- Em geral a ordem do $n$-ciclo $(i_1\ i_2 \cdots i_n)$ é igual a $n$.

# Ordem de uma permutação qualquer

Se uma permutação $\sigma$ consiste de $m_1$-ciclos, $m_2$-ciclos, $\cdots$, $m_k$-ciclos, então sua ordem é o $MMC(m_1, m_2, \cdots, m_k)$.

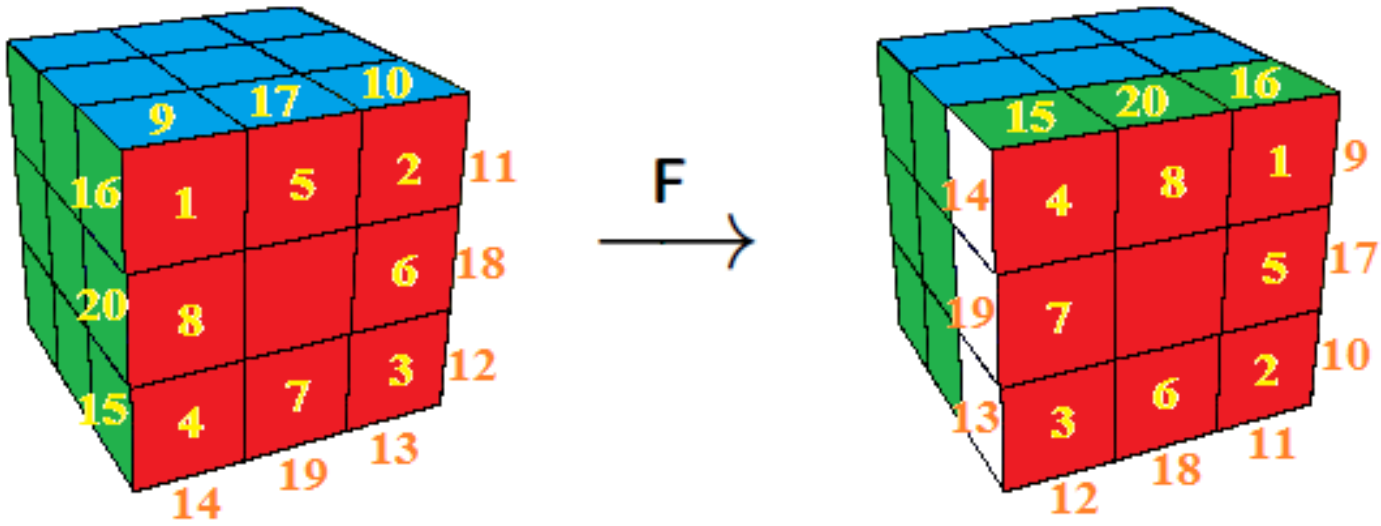
# Ordem de uma permutação qualquer

Se uma permutação $\sigma$ consiste de $m_1$-ciclos, $m_2$-ciclos, $\cdots$, $m_k$-ciclos, então sua ordem é o $MMC(m_1, m_2, \cdots, m_k)$.



# Ordem de uma permutação qualquer

Se uma permutação $\sigma$ consiste de $m_1$-ciclos, $m_2$-ciclos, $\cdots$, $m_k$-ciclos, então sua ordem é o $MMC(m_1, m_2, \cdots, m_k)$.




$$F = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 11\ 13\ 15)(10\ 12\ 14\ 16)(17\ 18\ 19\ 20)$$

$$\circ(F) = MMC(4, 4, 4, 4, 4) = 4$$

# Ordem de uma permutação qualquer

- Se $\sigma = (a\ b)(c\ d\ e)$ então $\circ(\sigma) = MMC(2,3) = 6$, isto é, $\sigma^6 = I$.

# Ordem de uma permutação qualquer

- Se $\sigma = (a\ b)(c\ d\ e)$ então $\circ(\sigma) = MMC(2,3) = 6$, isto é, $\sigma^6 = I$.

- Mas, $\sigma^3 = (a\ b)$, isto é, aplicando a permutação $\sigma$ três vezes faz com que o 3-ciclo $(c\ d\ e)$ volte à sua posição inicial, enquanto o 2-ciclo $(a\ b)$ é permutado um número ímpar de vezes, permanecendo como está.

# Grupos

# Grupos

Um grupo é um conjunto $G$ com uma operação binária $*$, satisfazendo as seguintes propriedades:

- Dados $g, h \in G$, temos que $g * h \in G$. (fechamento)

# Grupos

Um grupo é um conjunto $G$ com uma operação binária $*$, satisfazendo as seguintes propriedades:

- Dados $g, h \in G$, temos que $g * h \in G$. (fechamento)
- Dados $f, g, h \in G$, temos que $(f * g) * h = f * (g * h)$. (associativa)

# Grupos

Um grupo é um conjunto $G$ com uma operação binária $*$, satisfazendo as seguintes propriedades:

- Dados $g, h \in G$, temos que $g * h \in G$. (fechamento)
- Dados $f, g, h \in G$, temos que $(f * g) * h = f * (g * h)$. (associativa)
- Dado $g \in G$, existe $e \in G$ tal que $g * e = e * g = g$. (existência do elemento identidade)

# Grupos

Um grupo é um conjunto $G$ com uma operação binária $*$, satisfazendo as seguintes propriedades:

- Dados $g, h \in G$, temos que $g * h \in G$. (fechamento)
- Dados $f, g, h \in G$, temos que $(f * g) * h = f * (g * h)$. (associativa)
- Dado $g \in G$, existe $e \in G$ tal que $g * e = e * g = g$. (existência do elemento identidade)
- Dado $g \in G$, existe $g^{-1} \in G$ tal que $g * g^{-1} = g^{-1} * g = e$. (existência do elemento inverso)

# Grupos

- Para simplificar, denotaremos $gh$ (ao invés de $g * h$).

# Grupos

- Para simplificar, denotaremos $gh$ (ao invés de $g * h$).
- Definimos também
  $g^2 = gg$
  $g^3 = ggg$
  $g^0 = e$
  $g^{-n} = (g^n)^{-1}$

# Grupos

- Para simplificar, denotaremos $gh$ (ao invés de $g * h$).
- Definimos também
  $g^2 = gg$
  $g^3 = ggg$
  $g^0 = e$
  $g^{-n} = (g^n)^{-1}$
- O elemento identidade $e$ é único.

# Grupos

- Para simplificar, denotaremos $gh$ (ao invés de $g * h$).
- Definimos também
  $g^2 = gg$
  $g^3 = ggg$
  $g^0 = e$
  $g^{-n} = (g^n)^{-1}$
- O elemento identidade $e$ é único.
- Dado $g \in G$, o inverso $g^{-1}$ é único.

## Exemplos de grupos

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

## Exemplos de grupos

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- $(\mathbb{N}, +)$ não é grupo (dado $a \in N$, $a > 0$, $a$ não possui inverso em $\mathbb{N}$).

## Exemplos de grupos

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

- $(\mathbb{N}, +)$ não é grupo (dado $a \in N$, $a > 0$, $a$ não possui inverso em $\mathbb{N}$).
- $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$
  $\forall a, b \in \mathbb{Z}_n$, $a \oplus b$ é o resto da divisão de $a + b$ por $n$.
  $(\mathbb{Z}_n, \oplus)$ é um grupo.

## Exemplos de grupos

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

- $(\mathbb{N}, +)$ não é grupo (dado $a \in N$, $a > 0$, $a$ não possui inverso em $\mathbb{N}$).
- $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$
  $\forall a, b \in \mathbb{Z}_n$, $a \oplus b$ é o resto da divisão de $a + b$ por $n$.
  $(\mathbb{Z}_n, \oplus)$ é um grupo.
- $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$, $p$: primo
  $\forall a, b \in \mathbb{Z}_p^*$, $a \odot b$ é o resto da divisão de $ab$ por $n$.
  $(\mathbb{Z}_p^*, \odot)$ é um grupo.

## Exemplos de grupos

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

- $(\mathbb{N}, +)$ não é grupo (dado $a \in N$, $a > 0$, $a$ não possui inverso em $\mathbb{N}$).
- $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$
  $\forall a, b \in \mathbb{Z}_n$, $a \oplus b$ é o resto da divisão de $a + b$ por $n$.
  $(\mathbb{Z}_n, \oplus)$ é um grupo.
- $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$, $p$: primo
  $\forall a, b \in \mathbb{Z}_p^*$, $a \odot b$ é o resto da divisão de $ab$ por $n$.
  $(\mathbb{Z}_p^*, \odot)$ é um grupo.
- $\mathbb{Z}_n$ e $\mathbb{Z}_p^*$ são **grupos cíclicos**: seus elementos são da forma $e, a, a^2, \cdots$, para algum $a \neq e$.

# Grupos de Permutações

- Alguns conjuntos de permutações também formam grupos.

# Grupos de Permutações

- Alguns conjuntos de permutações também formam grupos.
- Sejam $a$ e $b$ permutações, então $a * b$ significa aplicar a permutação $a$ e em seguida aplicar a permutação $b$. (Simplificando: $ab$)

# Grupos de Permutações

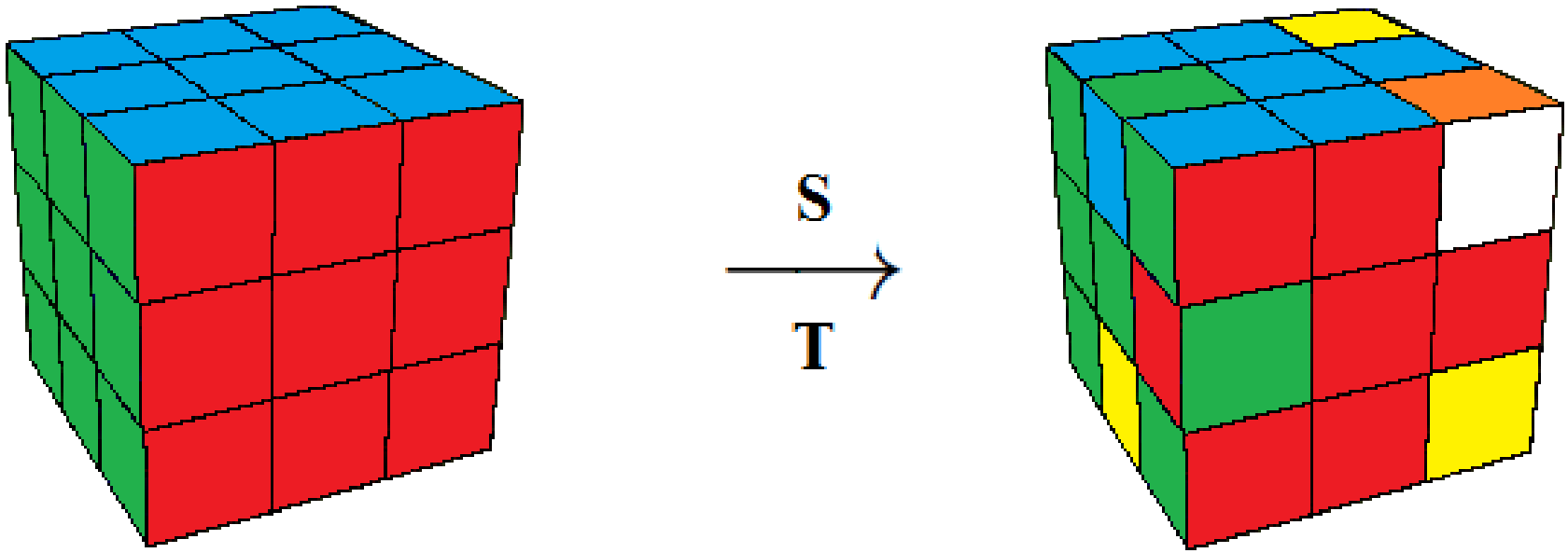
- Alguns conjuntos de permutações também formam grupos.
- Sejam $a$ e $b$ permutações, então $a * b$ significa aplicar a permutação $a$ e em seguida aplicar a permutação $b$. (Simplificando: $ab$)
- O conjunto de todas as permutações das facetas do cubo forma um grupo $\mathcal{R}$, chamado **Grupo de Rubik**.

# Grupos de Permutações

- Alguns conjuntos de permutações também formam grupos.
- Sejam $a$ e $b$ permutações, então $a * b$ significa aplicar a permutação $a$ e em seguida aplicar a permutação $b$. (Simplificando: $ab$)
- O conjunto de todas as permutações das facetas do cubo forma um grupo $\mathcal{R}$, chamado **Grupo de Rubik**.
- O grupo $\mathcal{R}$ consiste dos movimentos $L, R, F, B, U, D$ e de todas as macros $S$, assumindo que duas macros que produzem o mesmo resultado são vistas como iguais.

# Grupos de Permutações

## Exemplo




$$S = (F\ L\ U)^{42}$$

$$T = U\ F^{-2}\ U^{-2}\ F^{-2}\ U^{-1}\ L\ U^{-2}\ F\ U^{-1}\ L^{-2}\ U^{-2}\ L^{-2}\ U\ L^{-1}\ F^{-1}$$

# Grupos de Permutações

- O número total de elementos do grupo $\mathcal{R}$ é exatamente o número de todas as possíveis configurações do cubo.

# Grupos de Permutações

- O número total de elementos do grupo $\mathcal{R}$ é exatamente o número de todas as possíveis configurações do cubo.
- Não significa que $\mathcal{R}$ deva conter todas as permutações das facetas, mas apenas aquelas que podem ser atingidas por meio dos movimentos acima.

  (Exemplo: A faceta de um cubinho de centro **não** pode permutar com a faceta de um cubinho de canto/aresta)

# Grupos de Permutações

- O número total de elementos do grupo $\mathcal{R}$ é exatamente o número de todas as possíveis configurações do cubo.
- Não significa que $\mathcal{R}$ deva conter todas as permutações das facetas, mas apenas aquelas que podem ser atingidas por meio dos movimentos acima.

  (Exemplo: A faceta de um cubinho de centro **não** pode permutar com a faceta de um cubinho de canto/aresta)
- Se uma permutação não está em $\mathcal{R}$ então a configuração correspondente é impossível no cubo.

# O grupo simétrico $S_n$

- **Grupo simétrico $S_n$:** grupo de todas as permutações do conjunto $\{1, 2, \cdots, n\}$. (Total: $n!$ permutações)

# O grupo simétrico $S_n$

- **Grupo simétrico $S_n$:** grupo de todas as permutações do conjunto $\{1, 2, \cdots, n\}$. (Total: $n!$ permutações)
- Todo $n$-ciclo, $n > 1$ se escreve como produto de 2-ciclos.

Se $n$ é par, o número de 2-ciclos é impar.
Se $n$ é impar, o número de 2-ciclos é par.

$$(12) = (12)$$
$$(12)(13) = (123)$$
$$(12)(13)(14) = (1234)$$
$$(12)(13)(14)(15) = (12345)$$

$$(12)(13)(14)(15)\cdots(1n) = (12345\cdots n)$$

# O grupo simétrico $S_n$

## Exemplo

# O grupo simétrico $S_n$

## Exemplo

$$(12)(13)(14) = (1234)$$

# O grupo simétrico $S_n$

## Exemplo

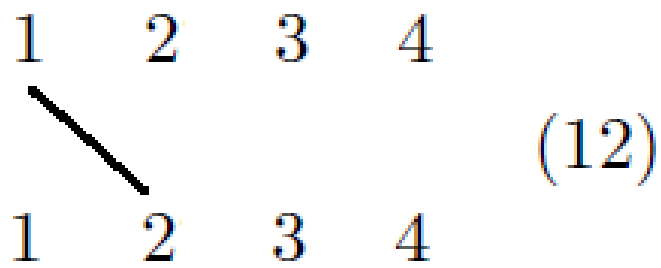
$$(12)(13)(14) = (1234)$$

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ & & & \\ & & & \\ 1 & 2 & 3 & 4 \end{array} \qquad (12)$$

# O grupo simétrico $S_n$

## Exemplo

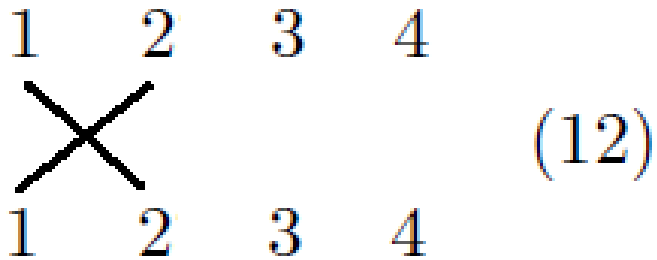
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

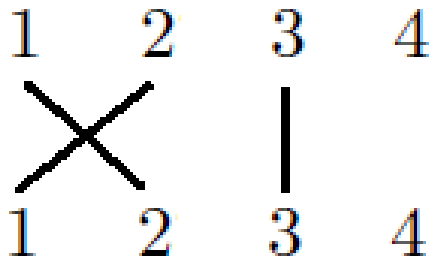
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

$$(12)(13)(14) = (1234)$$

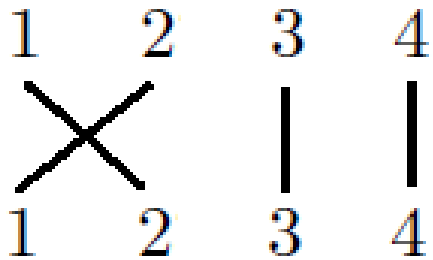



$(12)$

# O grupo simétrico $S_n$

## Exemplo

$$(12)(13)(14) = (1234)$$

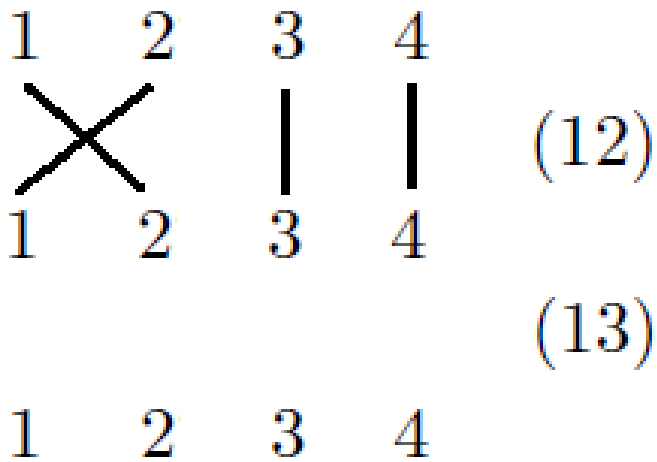



$(12)$

# O grupo simétrico $S_n$

## Exemplo

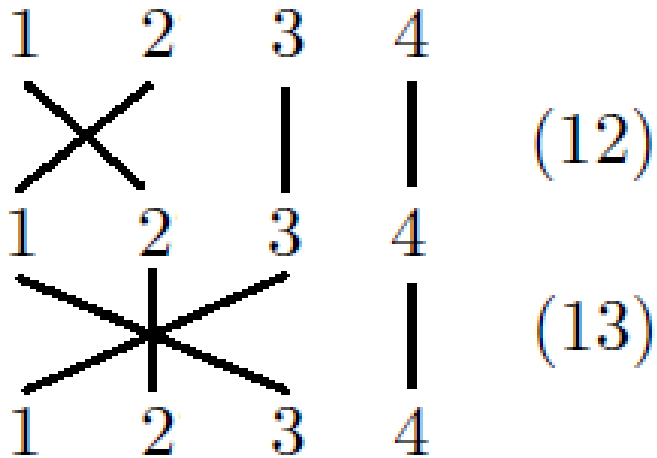
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

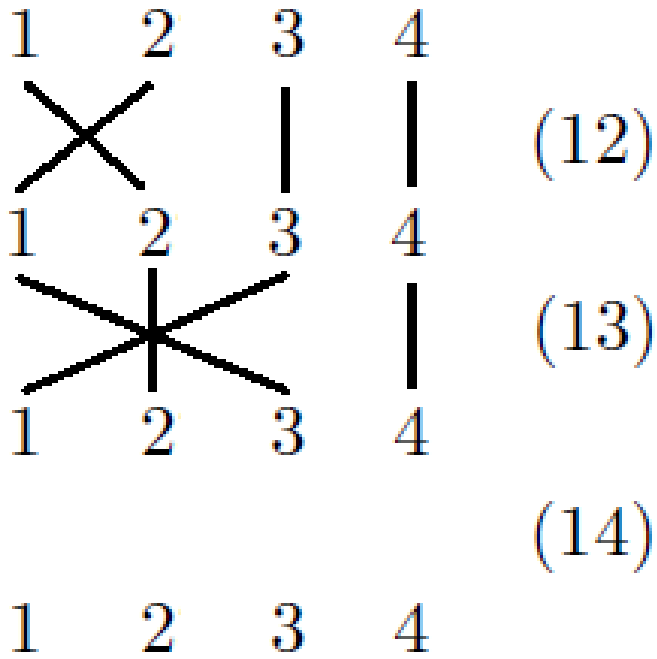
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

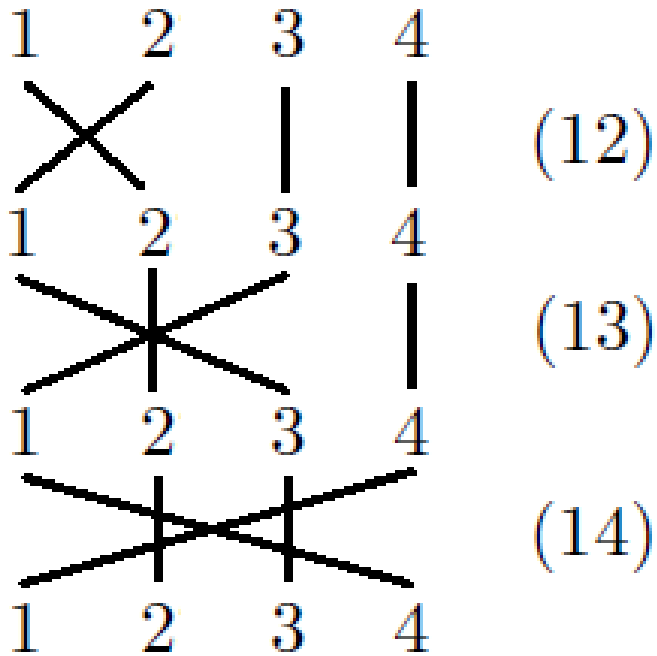
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

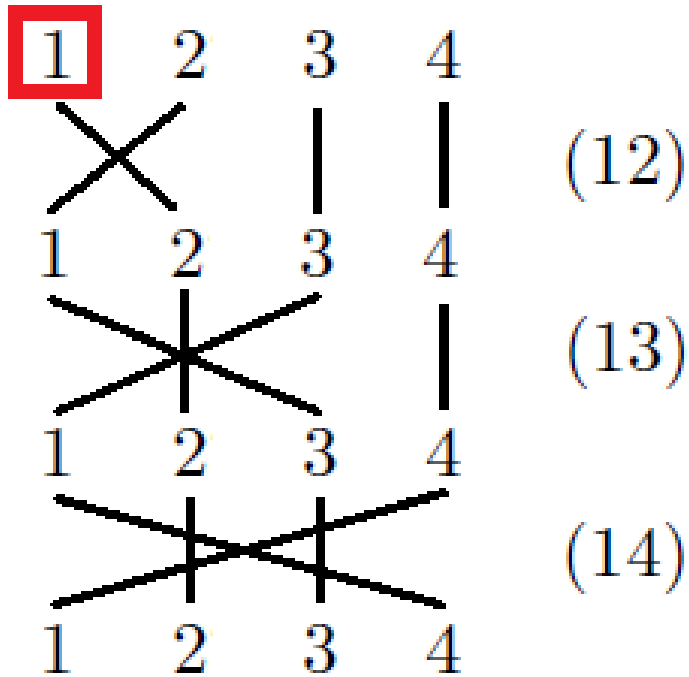
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

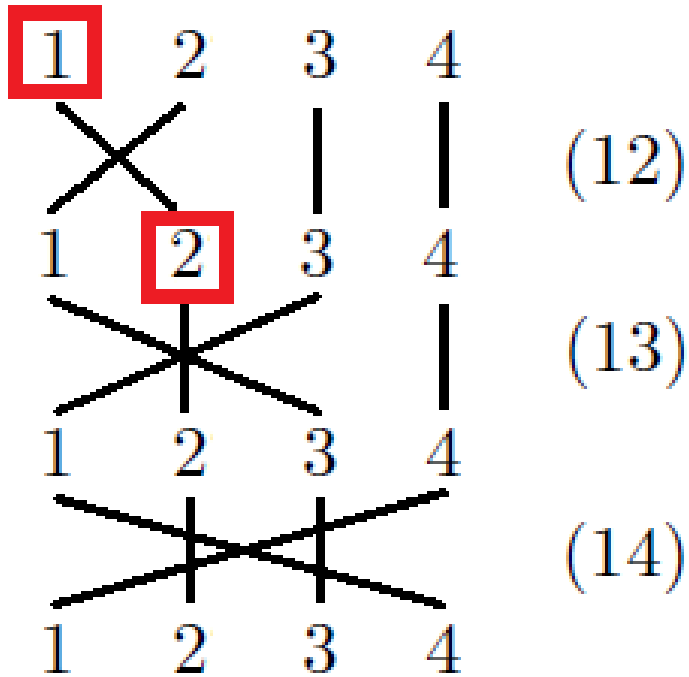
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

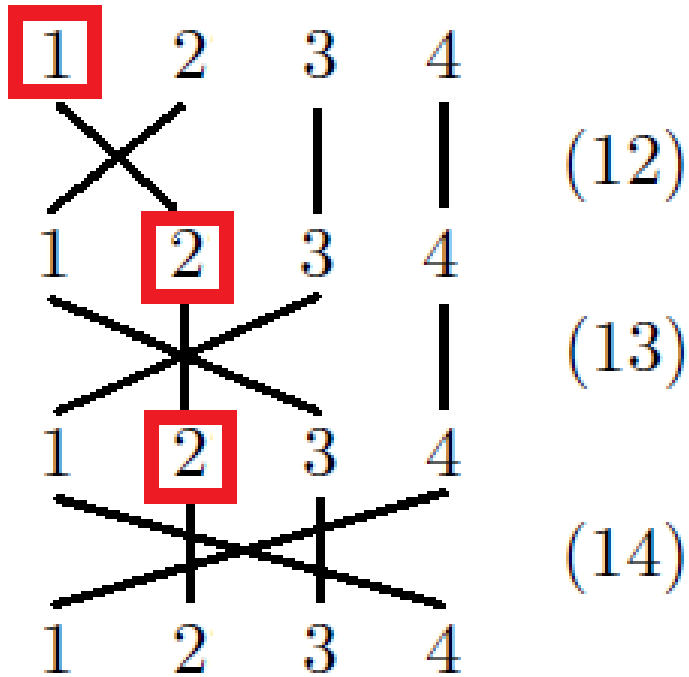
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

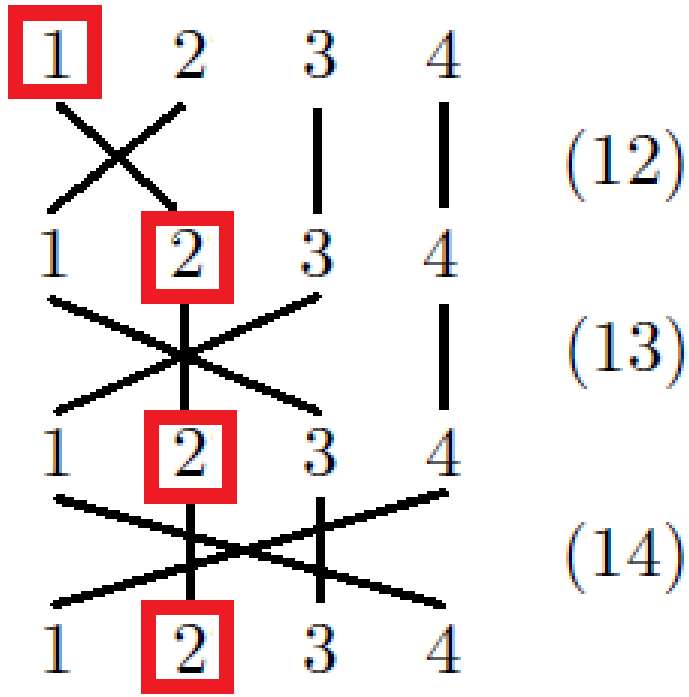
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

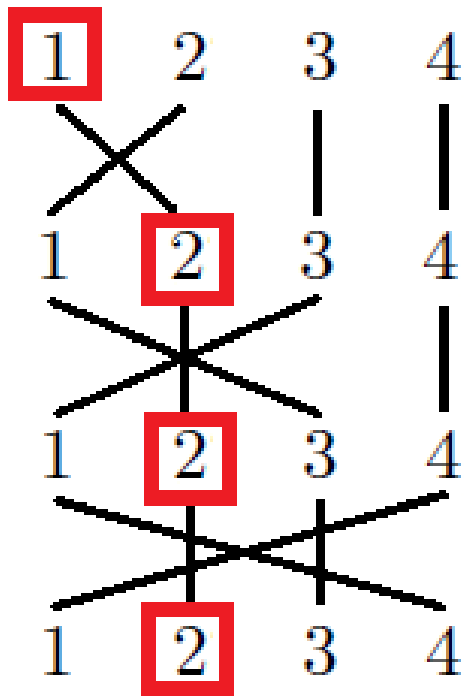
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

$$(12)(13)(14) = (1234)$$

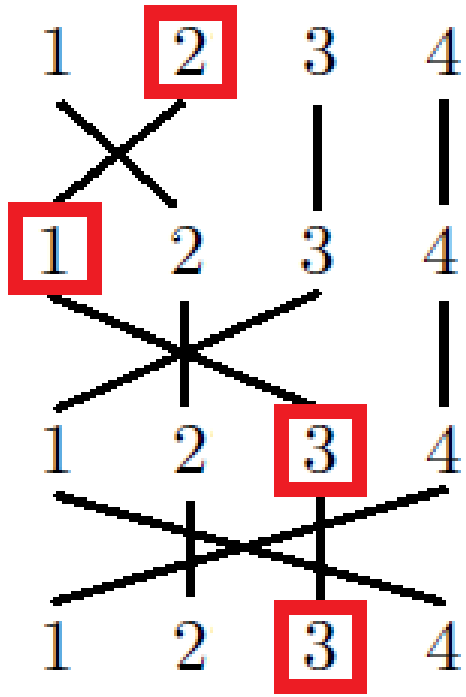



(12

# O grupo simétrico $S_n$

## Exemplo

$$(12)(13)(14) = (1234)$$

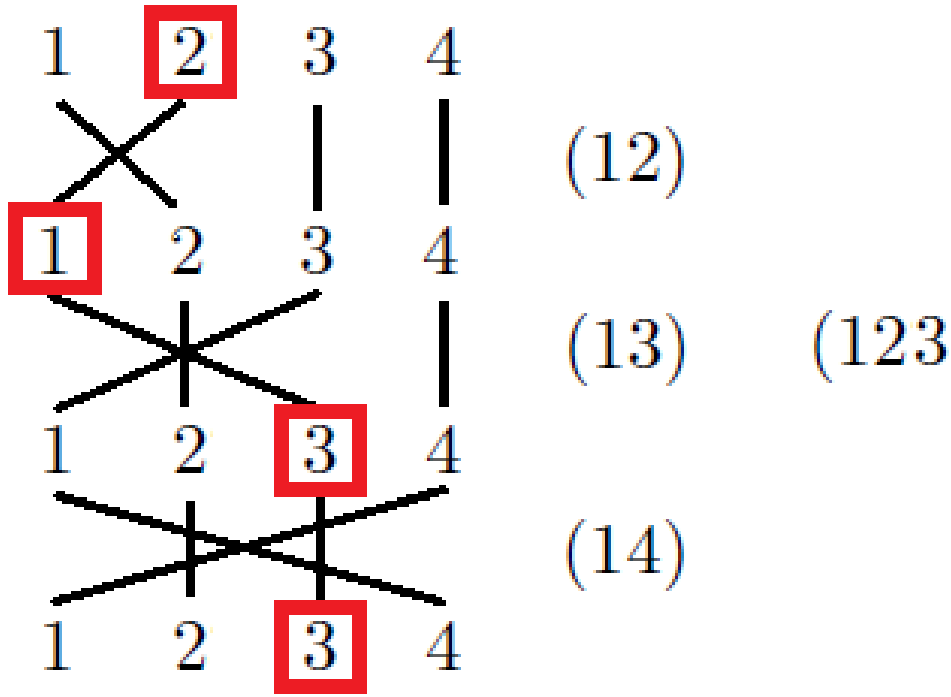



(12

# O grupo simétrico $S_n$

## Exemplo

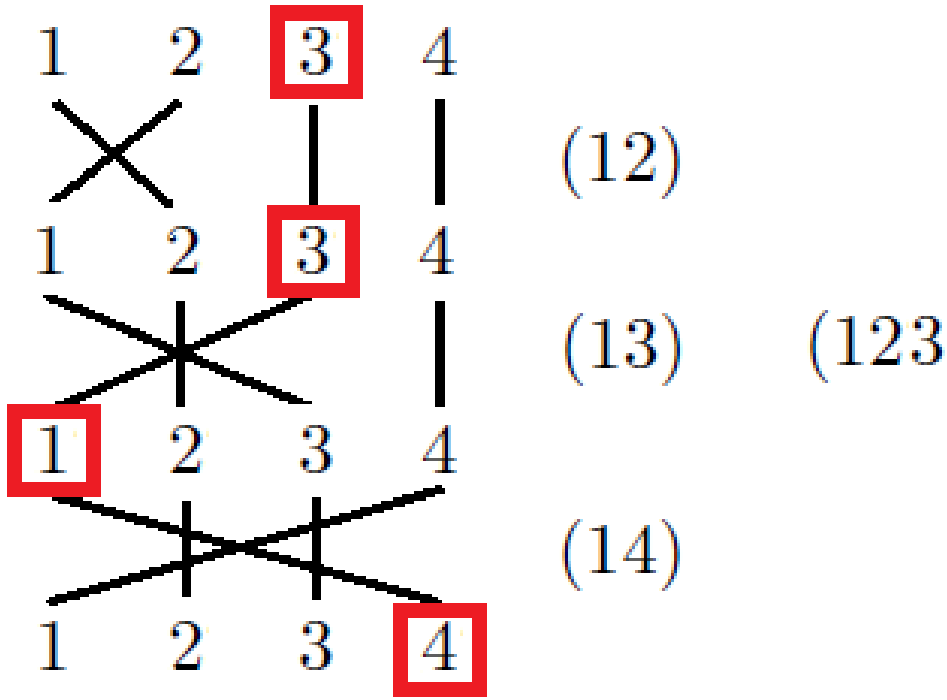
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

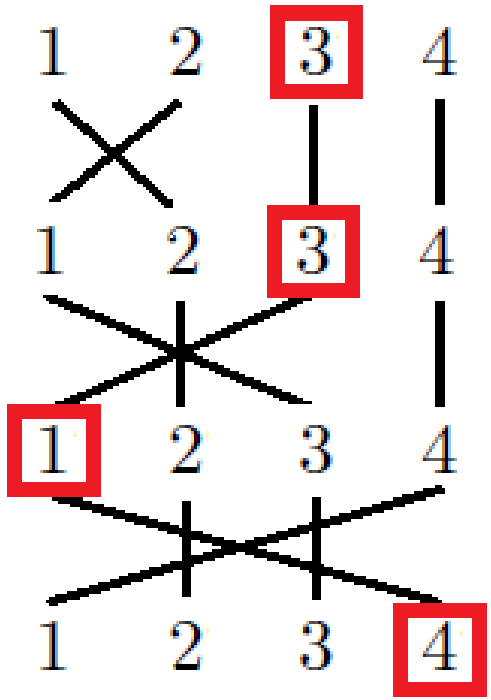
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

$$(12)(13)(14) = (1234)$$

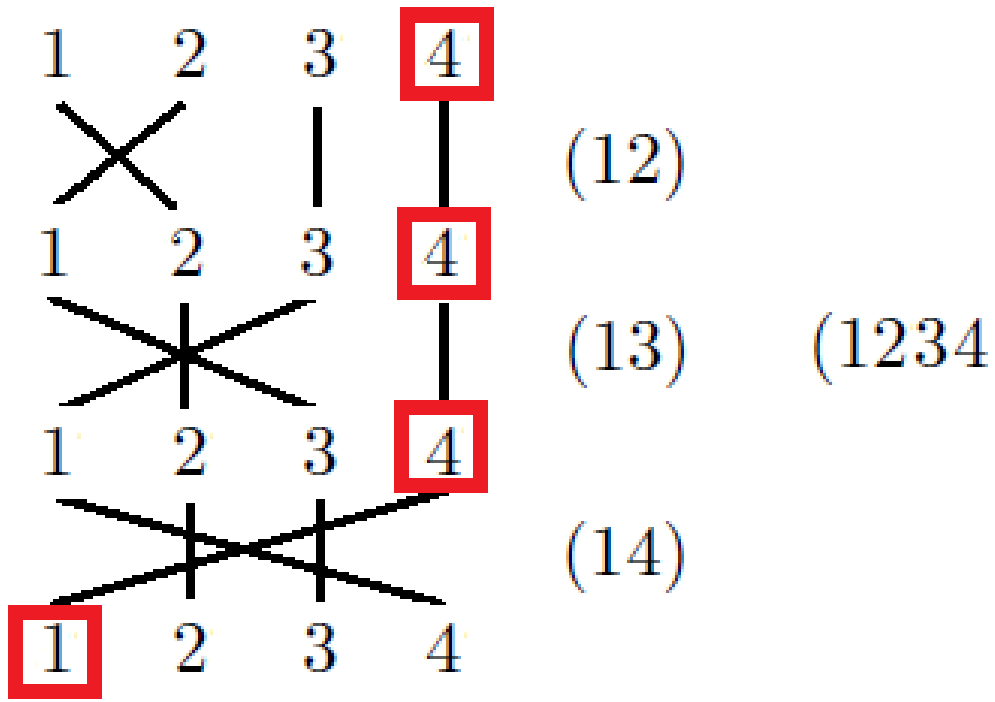



$(1234$

# O grupo simétrico $S_n$

## Exemplo

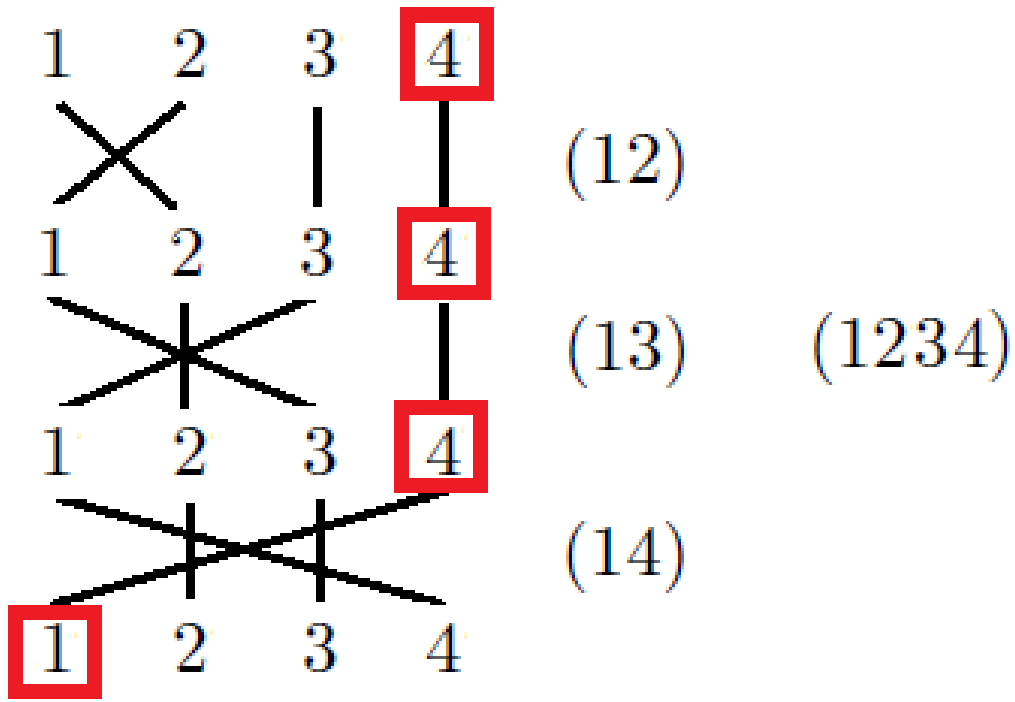
$$(12)(13)(14) = (1234)$$



# O grupo simétrico $S_n$

## Exemplo

$$(12)(13)(14) = (1234)$$



# Permutação par/impar

- **Permutação par:** Que se escreve com produto par de $2$-ciclos.

  **Permutação ímpar:** Que se escreve com produto ímpar de $2$-ciclos.

# Permutação par/impar

- **Permutação par:** Que se escreve com produto par de $2$-ciclos.

  **Permutação ímpar:** Que se escreve com produto ímpar de $2$-ciclos.
- Metade dos elementos de $S_n$ é par e a outra metade é ímpar.

# Permutação par/impar

- **Permutação par:** Que se escreve com produto par de $2$-ciclos.
  **Permutação ímpar:** Que se escreve com produto ímpar de $2$-ciclos.
- Metade dos elementos de $S_n$ é par e a outra metade é ímpar.
- A metade par, chamada $A_n$, forma um grupo chamado de **grupo alternante**.

# Teoria de Grupos: Paridade no cubo

- Vimos que somente podemos trocar cubinhos que tenham o mesmo “gênero”.

  central $\longleftrightarrow$ central
  aresta $\longleftrightarrow$ aresta
  canto $\longleftrightarrow$ canto

- Vimos que somente podemos trocar cubinhos que tenham o mesmo "gênero".

  central $\longleftrightarrow$ central
  aresta $\longleftrightarrow$ aresta
  canto $\longleftrightarrow$ canto

- Qual a relação de paridade entre cada tipo de cubinho?

# Teoria de Grupos: Paridade no cubo

É possivel trocar $2$ pares de cubinhos (de mesmo gênero) deixando os demais como estão.

# Teoria de Grupos: Paridade no cubo

É possivel trocar $2$ pares de cubinhos (de mesmo gênero) deixando os demais como estão.

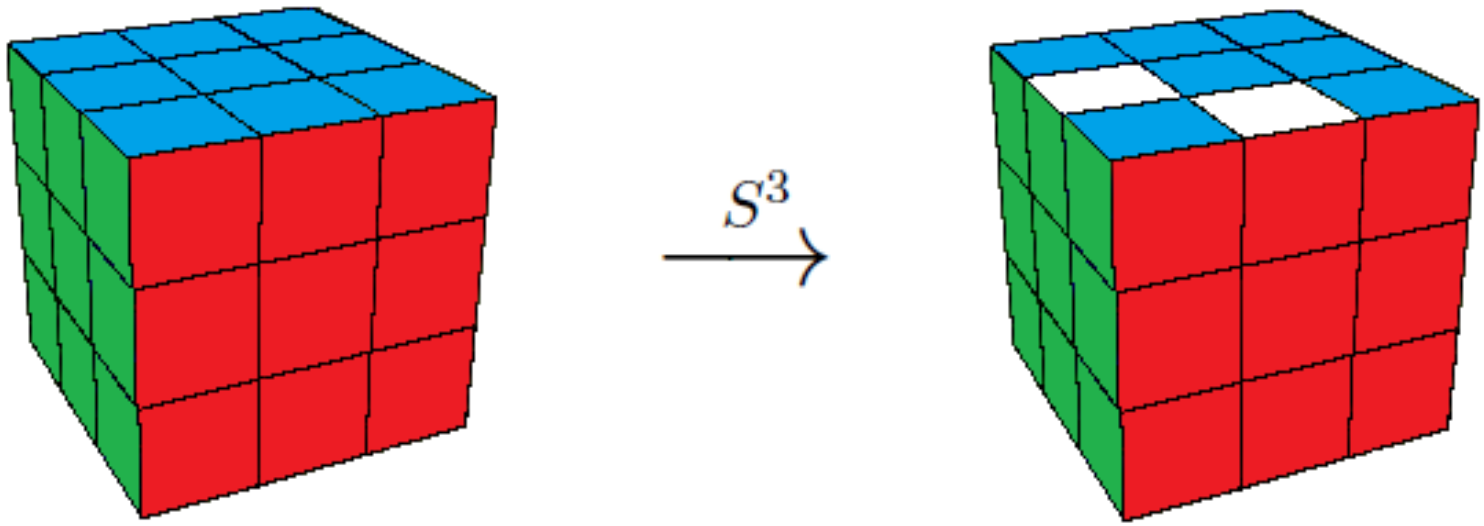
# Teoria de Grupos: Paridade no cubo

É possivel trocar $2$ pares de cubinhos (de mesmo gênero) deixando os demais como estão.


$$S = F^2L^2 = (a_1\ a_2)(b_1\ b_2)(c_1\ c_2\ c_3)(d_1\ d_2\ d_3)(e_1\ e_2\ e_3)$$

# Teoria de Grupos: Paridade no cubo

É possivel trocar $2$ pares de cubinhos (de mesmo gênero) deixando os demais como estão.

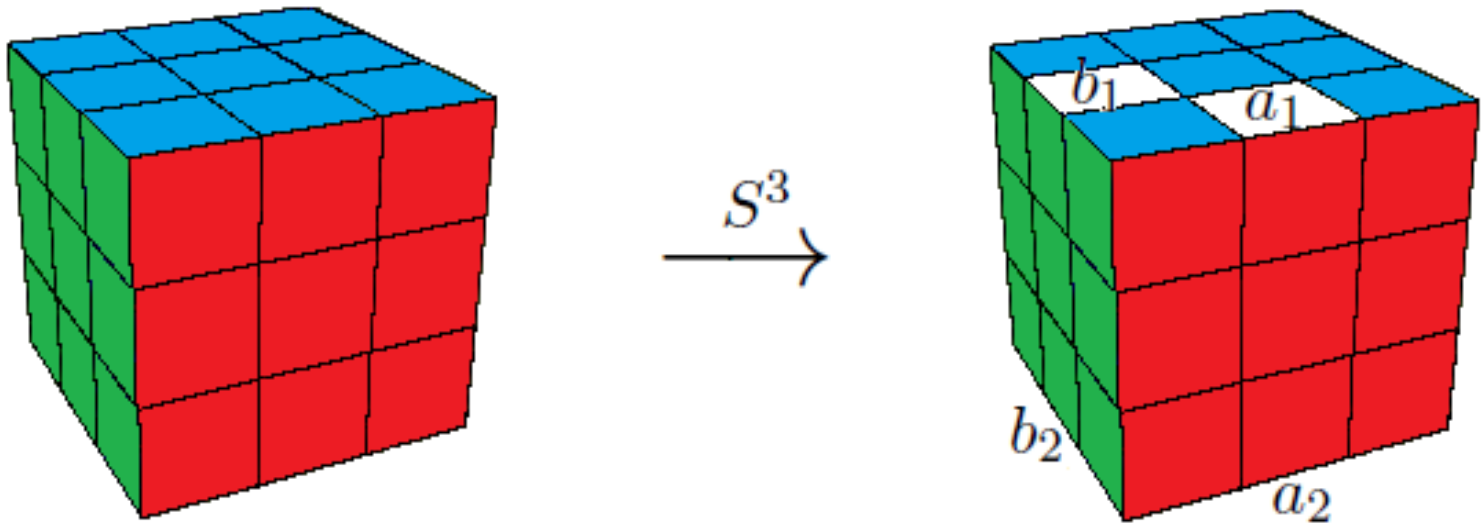



$$S = F^2L^2 = (a_1\ a_2)(b_1\ b_2)(c_1\ c_2\ c_3)(d_1\ d_2\ d_3)(e_1\ e_2\ e_3)$$

$$S^3 = (F^2L^2)^3 = (a_1\ a_2)(b_1\ b_2)$$

# Teoria de Grupos: Paridade no cubo

É possivel trocar $2$ pares de cubinhos (de mesmo gênero) deixando os demais como estão.



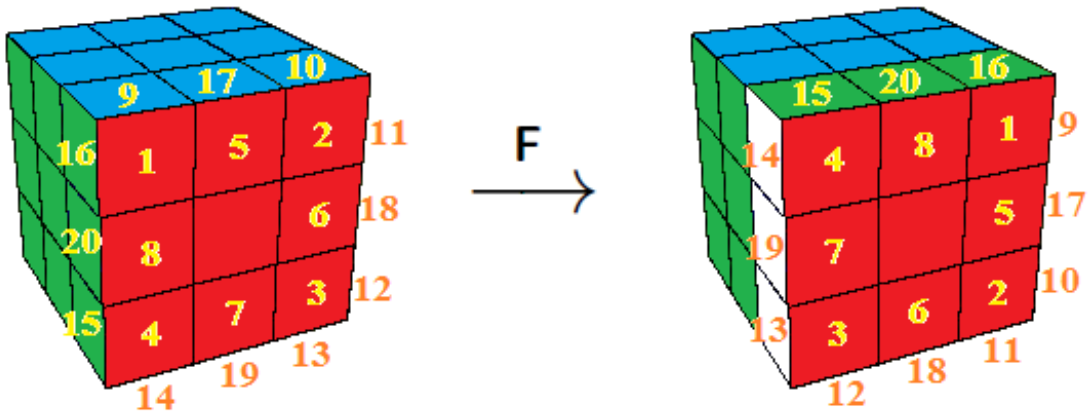

$$S = F^2L^2 = (a_1\ a_2)(b_1\ b_2)(c_1\ c_2\ c_3)(d_1\ d_2\ d_3)(e_1\ e_2\ e_3)$$

$$S^3 = (F^2L^2)^3 = (a_1\ a_2)(b_1\ b_2)$$

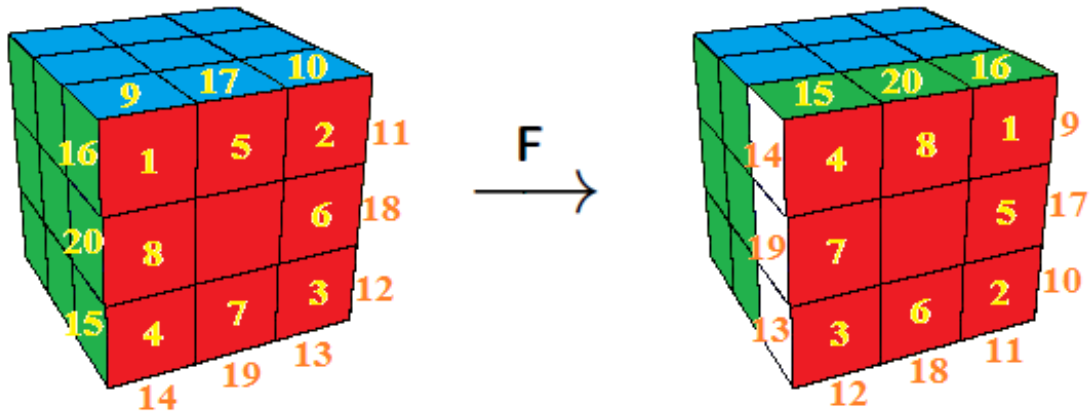
# Teoria de Grupos: Paridade no cubo

Não existe nenhuma combinação de movimentos que consiga trocar apenas um par de cubinhos.

# Teoria de Grupos: Paridade no cubo

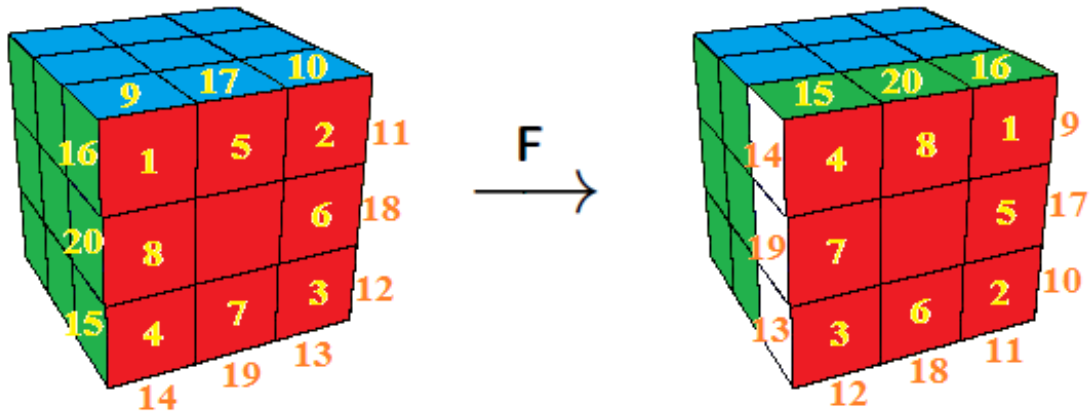


# Teoria de Grupos: Paridade no cubo




$$F = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 11\ 13\ 15)(10\ 12\ 14\ 16)(17\ 18\ 19\ 20) \qquad \textbf{(IMPAR)}$$

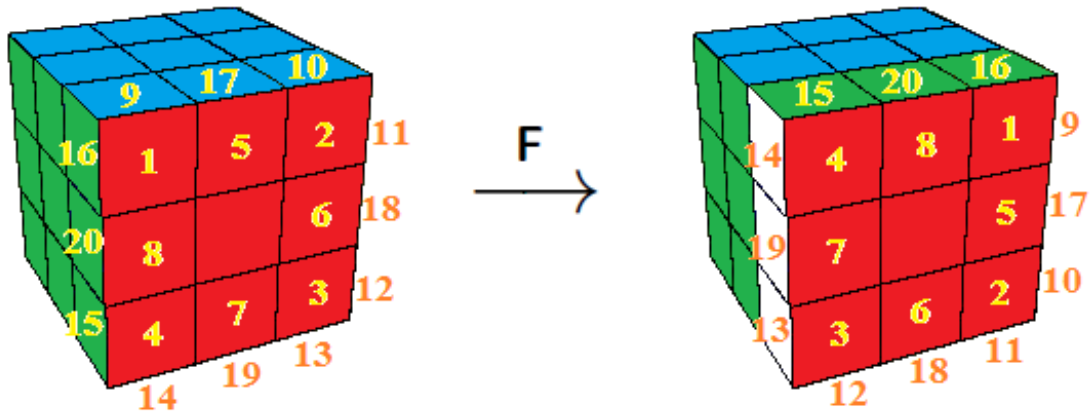
# Teoria de Grupos: Paridade no cubo




$F = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 11\ 13\ 15)(10\ 12\ 14\ 16)(17\ 18\ 19\ 20)$ **( IMPAR )**

$R = (1\ 27\ 30\ 11)(5\ 26\ 29\ 32)(2\ 16\ 28\ 31)(9\ 22\ 24\ 10)(21\ 23\ 25\ 17)$ **( IMPAR )**

# Teoria de Grupos: Paridade no cubo

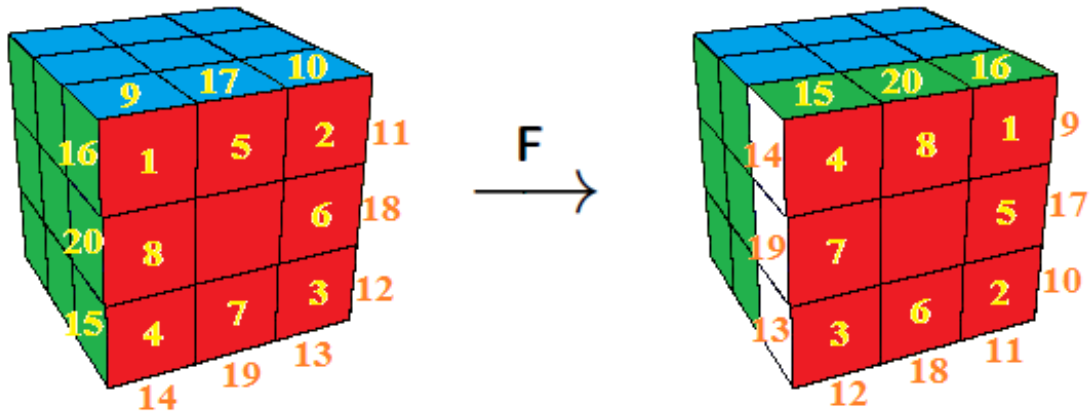



$F = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 11\ 13\ 15)(10\ 12\ 14\ 16)(17\ 18\ 19\ 20)$ **( IMPAR )**

$R = (1\ 27\ 30\ 11)(5\ 26\ 29\ 32)(2\ 16\ 28\ 31)(9\ 22\ 24\ 10)(21\ 23\ 25\ 17)$ **( IMPAR )**

$FR = (1\ 16\ 9)(2\ 3\ 4\ 27\ 30\ 11\ 13\ 15\ 22\ 24\ 10\ 12\ 14\ 28\ 31)$
$(5\ 6\ 7\ 8\ 26\ 29\ 32)(17\ 18\ 19\ 20\ 21\ 23\ 25)$ **( PAR )**

# Teoria de Grupos: Paridade no cubo




$F = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 11\ 13\ 15)(10\ 12\ 14\ 16)(17\ 18\ 19\ 20)$ **( IMPAR )**

$R = (1\ 27\ 30\ 11)(5\ 26\ 29\ 32)(2\ 16\ 28\ 31)(9\ 22\ 24\ 10)(21\ 23\ 25\ 17)$ **( IMPAR )**

$FR = (1\ 16\ 9)(2\ 3\ 4\ 27\ 30\ 11\ 13\ 15\ 22\ 24\ 10\ 12\ 14\ 28\ 31)$
$(5\ 6\ 7\ 8\ 26\ 29\ 32)(17\ 18\ 19\ 20\ 21\ 23\ 25)$ **( PAR )**

$\tau = (a\ b)$ **( IMPAR )**

# Teoria de Grupos: Um passo no método de camadas

# Subgrupo

- Sejam $(G, *)$ um grupo e $H \subseteq G$. Dizemos que $H$ é **subgrupo** de $G$ se $H$ com a operação $*$ for um grupo.

# Subgrupo

- Sejam $(G, *)$ um grupo e $H \subseteq G$. Dizemos que $H$ é **subgrupo** de $G$ se $H$ com a operação $*$ for um grupo.
- Sejam $g_1, g_2, \cdots, g_k \in G$. O **subgrupo gerado** por $g_1, g_2, \cdots, g_k$ é o menor subgrupo de $G$ contendo $g_1, g_2, \cdots, g_k$.

$$H = < g_1, g_2, \cdots, g_k >$$

# Comutador

- Dados $g, h \in G$, o elemento

$$[g, h] = ghg^{-1}h^{-1}$$

é chamado de **comutador**. O conjunto

$$[G, G] = \{[g, h];\ g, h \in G\}$$

é um subgrupo de $G$ chamado de **grupo dos comutadores de G**.

# Homomorfismo de grupos

- Sejam $(G, *)$ e $(H, \#)$ grupos. A função

$$\varphi : G \to H$$

é um **homomorfismo de grupos** se para todo $g, h \in G$, tivermos
(i) $\varphi(e_G) = e_H$.
(ii) $\varphi(g * h) = \varphi(g) \# \varphi(h)$.

# Homomorfismo de grupos

- Sejam $(G, *)$ e $(H, \#)$ grupos. A função

$$\varphi : G \to H$$

é um **homomorfismo de grupos** se para todo $g, h \in G$, tivermos
(i) $\varphi(e_G) = e_H$.
(ii) $\varphi(g * h) = \varphi(g) \# \varphi(h)$.

- Se $\varphi$ é bijetora, então $\varphi$ é um isomorfismo, e dizemos que $G$ é isomorfo a $H$.

$$G \cong H$$

- Vimos que

  $S_4$: Grupo de todas as permutações do conjunto $\{1, 2, 3, 4\}$.
  (Total: $24$ permutações)

- Vimos que

  $S_4$: Grupo de todas as permutações do conjunto $\{1, 2, 3, 4\}$. (Total: $24$ permutações)

- Em $S_4$, temos que

$$A_4 =< (1\ 2\ 3), (1\ 2\ 4) >$$

Em geral, se $n \geq 3$, $A_n$ é gerado por $3$-ciclos.

Tomando,

$$S = L^{-1}URU^{-1}LUR^{-1}U^{-1}$$

$$T = F^{-1}UBU^{-1}FUB^{-1}U^{-1},$$

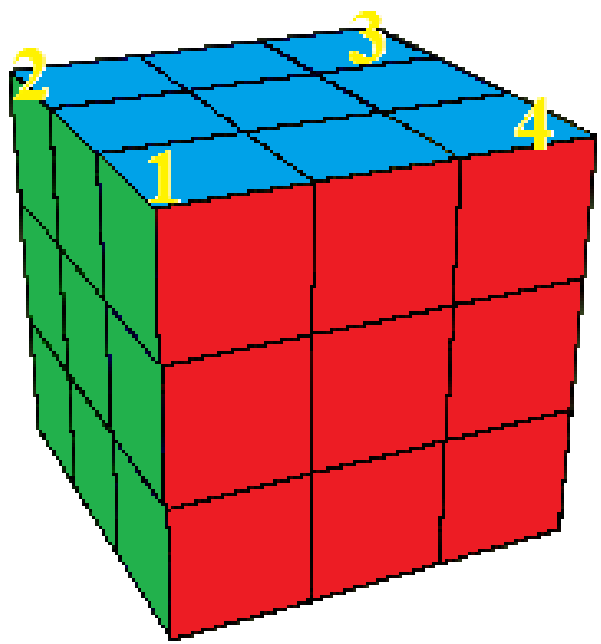
e definindo

$$\rho : A_4 \rightarrow < S, T > \subset \mathcal{R}$$

tal que $\rho(1\ 2\ 3) = S$ e $\rho(1\ 2\ 4) = T$, temos que

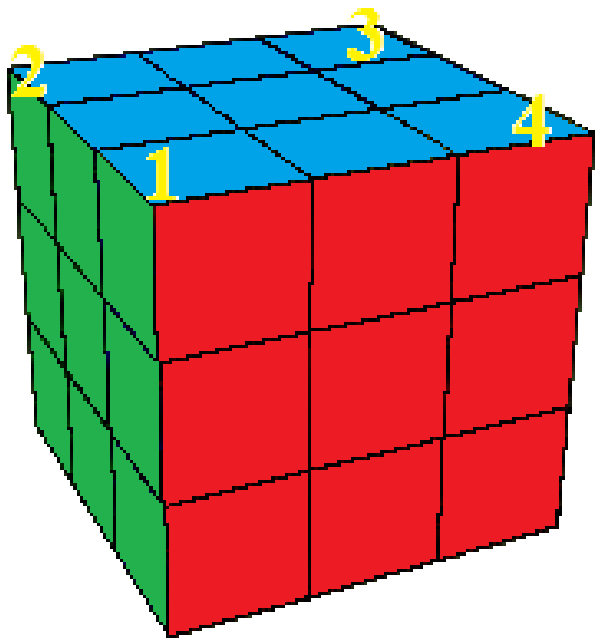
$$A_4 \cong < S, T >$$

# Permutação dos cantos numa camada



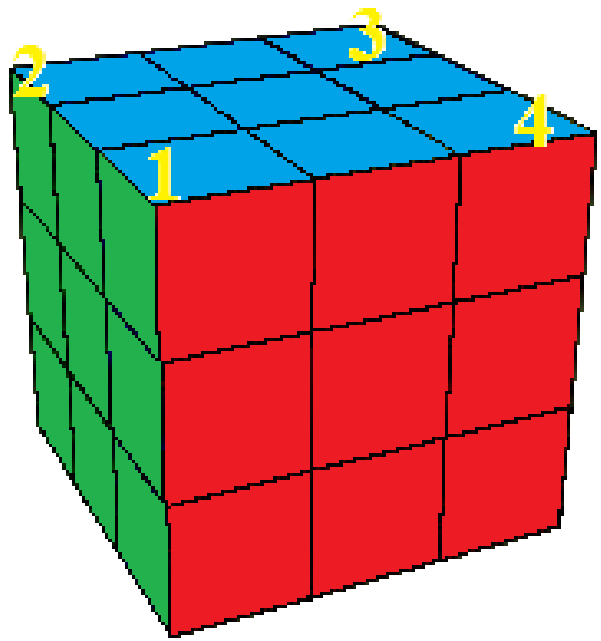
# Permutação dos cantos numa camada

- $S$ e $T$ são permutações pares.



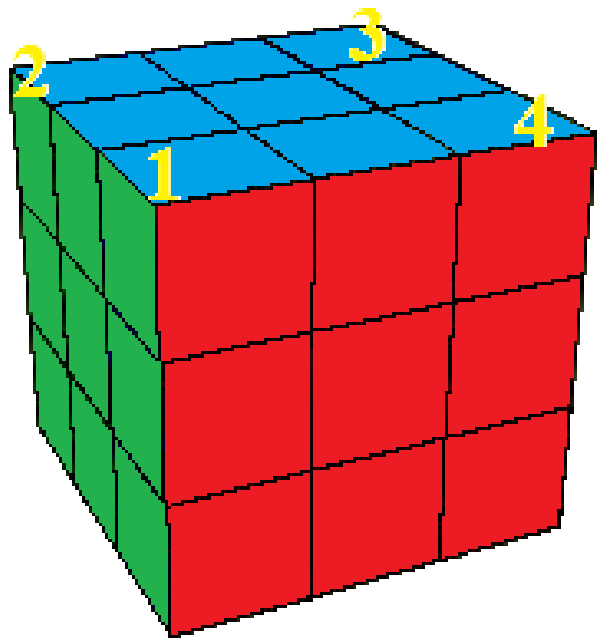
# Permutação dos cantos numa camada

- $S$ e $T$ são permutações pares.
- $A_4 \cong < S, T >$.



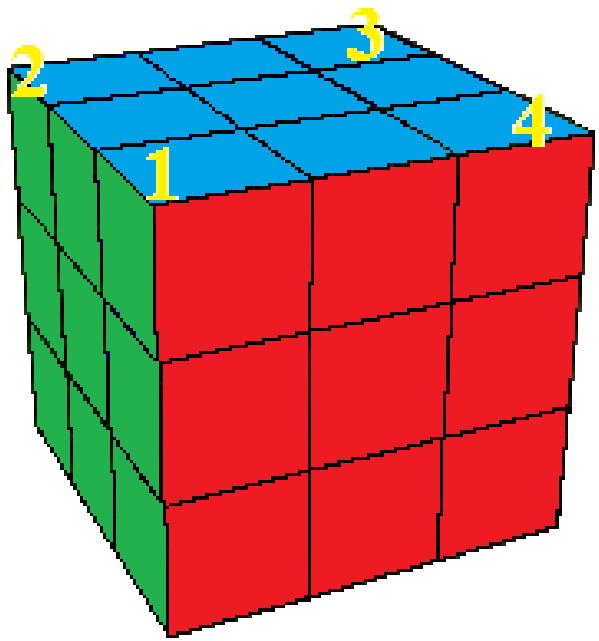
# Permutação dos cantos numa camada

- $S$ e $T$ são permutações pares.
- $A_4 \cong < S, T >$.
- $S = (1\ 2\ 3)$ e $T = (1\ 2\ 4)$.

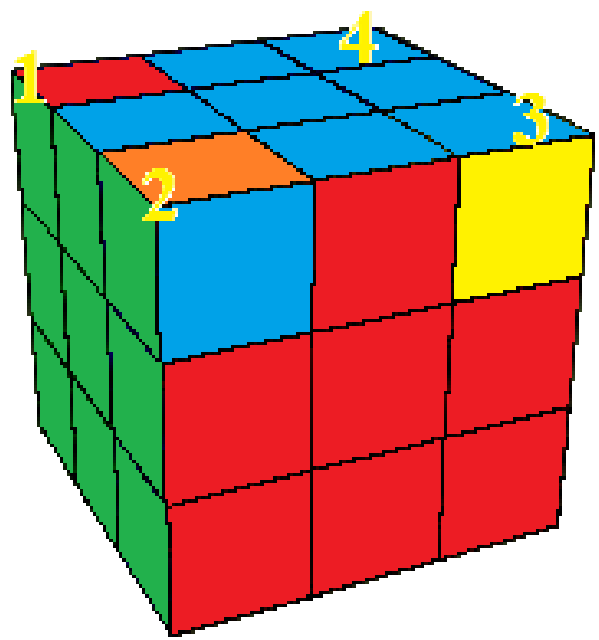


# Permutação dos cantos numa camada

- $S$ e $T$ são permutações pares.
- $A_4 \cong < S, T >$.
- $S = (1\ 2\ 3)$ e $T = (1\ 2\ 4)$.
- Permutações dos cantos em uma camada tem que ser uma permutação par de $\{1, 2, 3, 4\}$, isto é, tem que corresponder a um elemento de $A_4$.

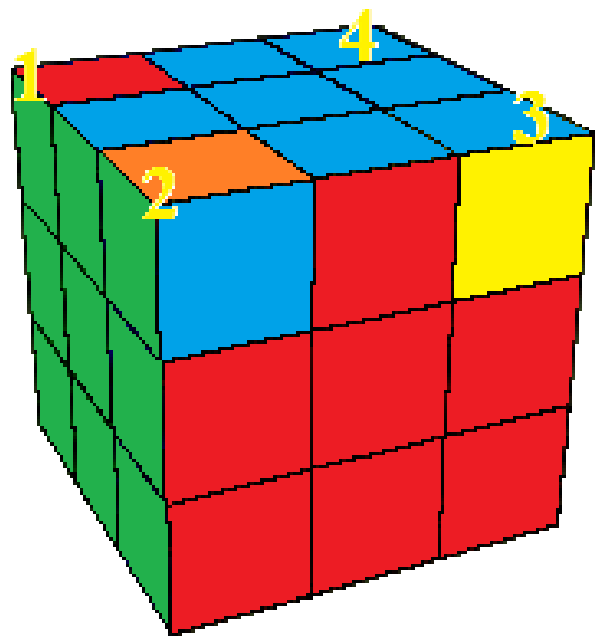


# Permutação dos cantos numa camada



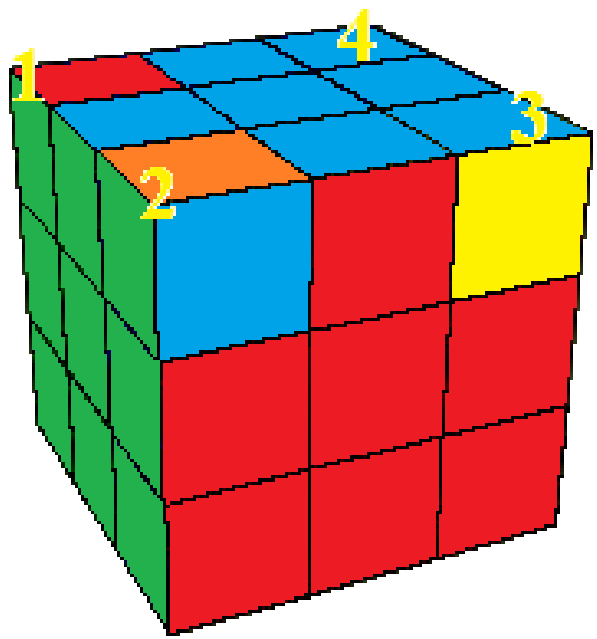
# Permutação dos cantos numa camada

- $\sigma = (1\ 2)(3\ 4)$.



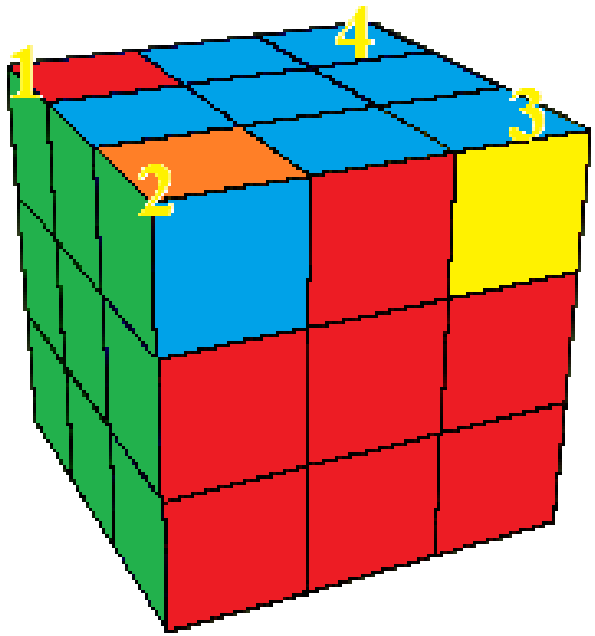
# Permutação dos cantos numa camada

- $\sigma = (1\ 2)(3\ 4)$.
- $(1\ 2)(3\ 4) = (1\ 2\ 3)(1\ 2\ 4)^2(1\ 2\ 3) = ST^2S$.



# Permutação dos cantos numa camada

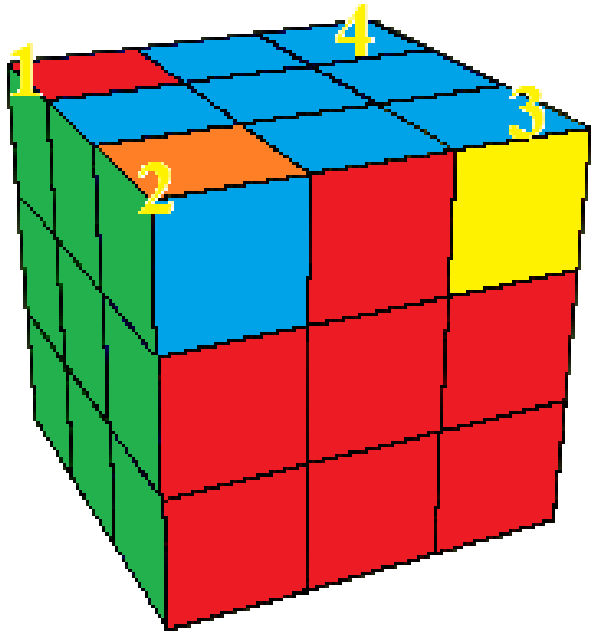
- $\sigma = (1\ 2)(3\ 4)$.
- $(1\ 2)(3\ 4) = (1\ 2\ 3)(1\ 2\ 4)^2(1\ 2\ 3) = ST^2S$.
- Como $(1\ 2)(3\ 4)$ tem ordem 2, então $(ST^2S)^2 = I$.



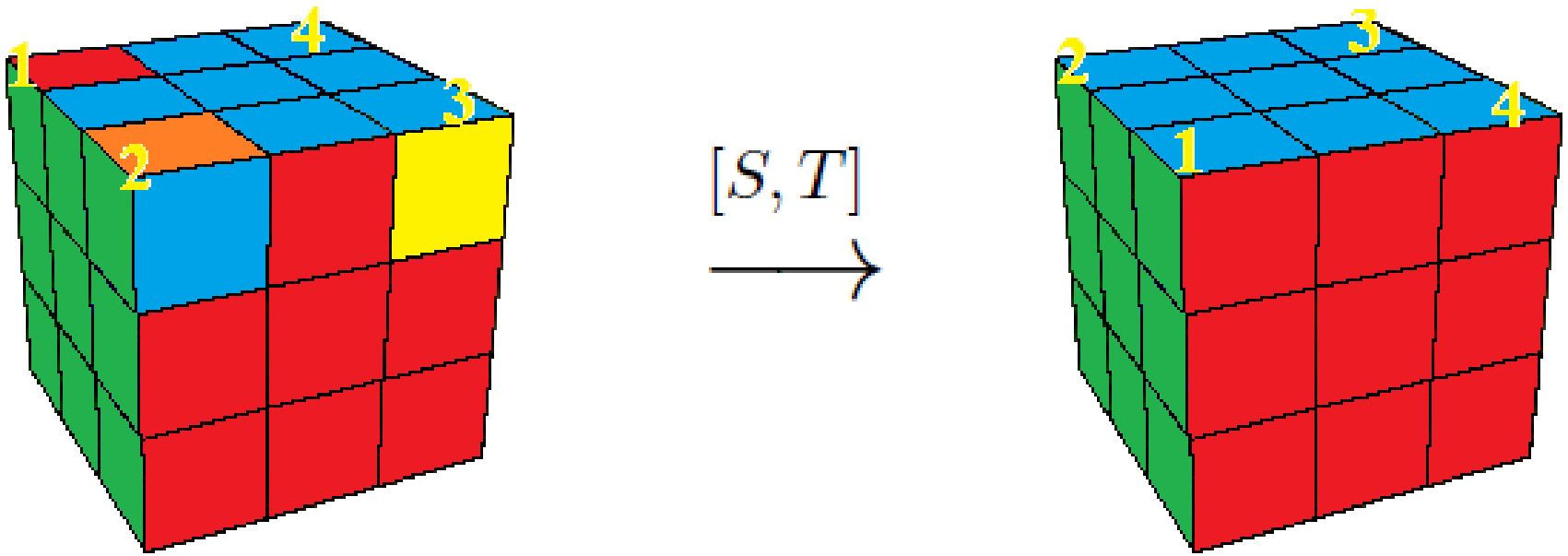
# Permutação dos cantos numa camada

- $\sigma = (1\ 2)(3\ 4)$.
- $(1\ 2)(3\ 4) = (1\ 2\ 3)(1\ 2\ 4)^2(1\ 2\ 3) = ST^2S$.
- Como $(1\ 2)(3\ 4)$ tem ordem 2, então $(ST^2S)^2 = I$.
- Para resolver o cubo abaixo, basta aplicar a macro $ST^2S$, que é um **comutador**, pois

$$[S, T] = STS^{-1}T^{-1} = STS^2T^2 = ST^2S.$$



# Permutação dos cantos numa camada



# Referências


- Waldeck Schützer, "Aprendendo Algebra com o cubo mágico", V Semana da Matemática da UFU, 2005
- Tom Davis, "Group Theory via Rubik's Cube", draft, http://www.geometer.org/rubik.
- Nathan Jacobson, "Basic Abstract Algebra", 2nd Ed., W. H. Freeman and Co., 1996.
- Edward C. Turner  Karen F. Gold, "Rubik's Groups", The American Mathematical Monthly, Vol. 92, No. 9, 1985.

Obrigado!