Exemplo

Sabe-se que a mensagem "1727; 432; 2102" foi obtida por codificação usando o código RSA com a chave pública $m = 4037$ e $c = 523$. Sabe-se ainda que para a correspondência entre letras do alfabeto e números foi usado o código ASCII (em particular, as letras minúsculas correspondem, por ordem, aos números $97, \ldots, 122$). Por exemplo, a letra "n" corresponde ao número 110. Uma vez que m é pequeno, não deve ser difícil descodificar a mensagem. Consegue fazê-lo?

Verifica-se facilmente que $m = 11 \cdot 367$, sendo que 367 é primo. Então $\varphi(m) = 3660$ e $d = 7$. Obtém-se então "110; 97; 111" que corresponde à mensagem "nao".

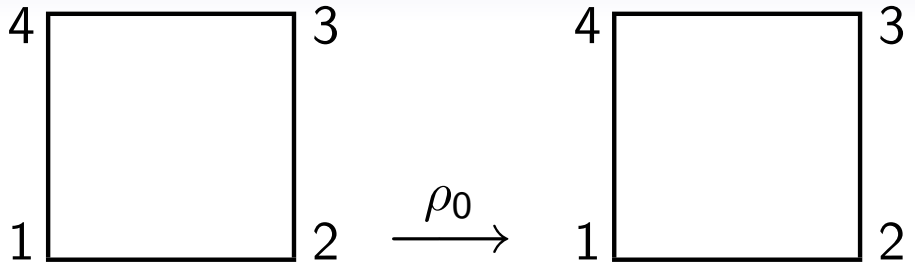
Teoria de Grupos

Damos agora início à parte principal do programa desta disciplina: uma introdução à teoria de grupos.

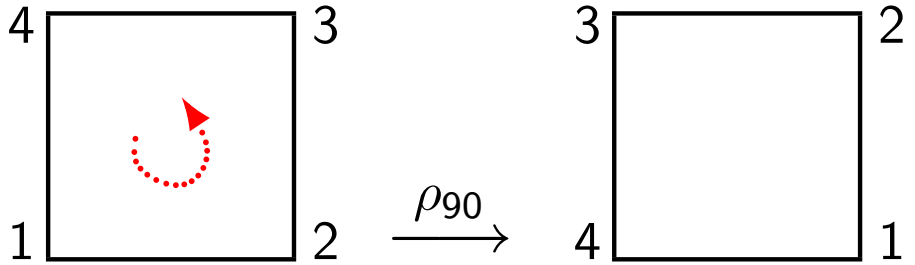
Simetrias do quadrado

Suponhamos que um quadrado é retirado de um plano, movimentado no espaço e depois recolocado no plano.
A recolocação do quadrado no plano pode ser feita de oito modos possíveis, pois a (nova) posição do quadrado no plano fica definida pela localização de um dos vértices (quatro possibilidades) e pela orientação (voltado para cima ou para baixo: duas possibilidades).
Assim, cada movimento que façamos com o quadrado no espaço será equivalente a um dos movimentos ilustrados a seguir.

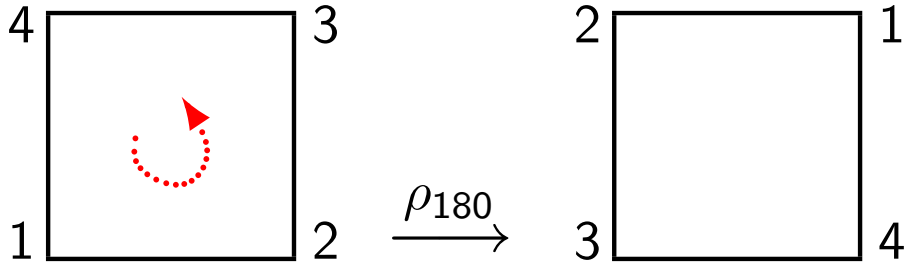
ρ_0 é a identidade



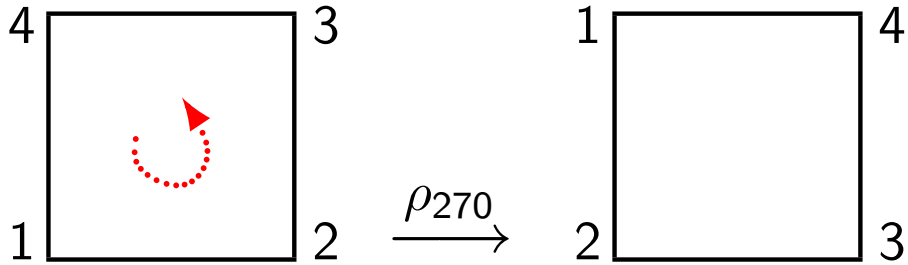
ρ_{90} é a rotação de 90°



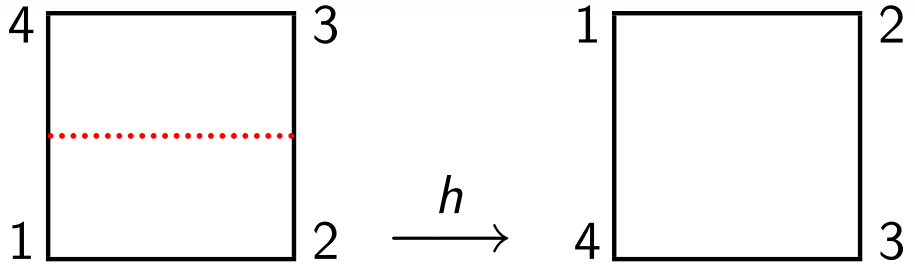
ρ_{180} é a rotação de 180°



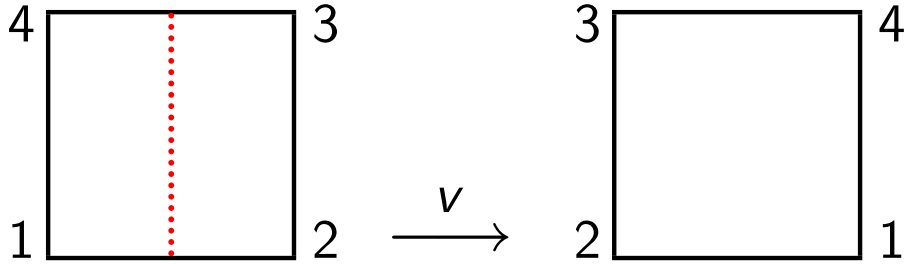
ρ_{270} é a rotação de 270°



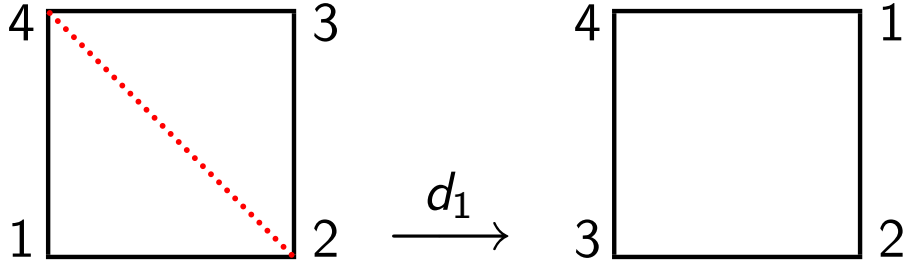
h reflexão sobre o eixo horizontal



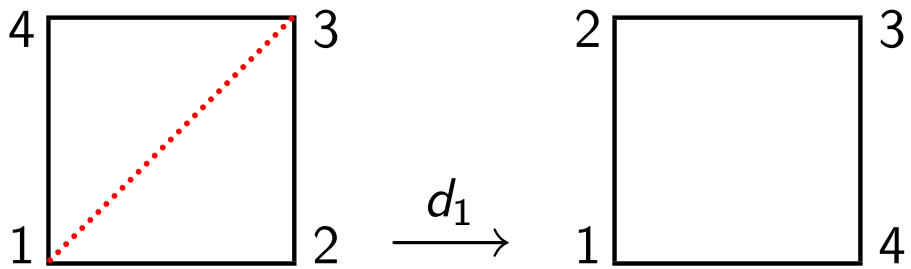
v reflexão sobre o eixo vertical



d_1 reflexão sobre diagonal principal

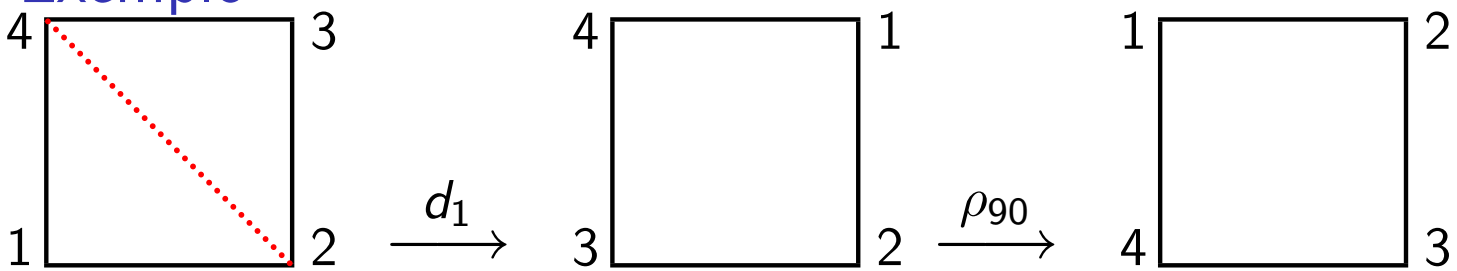


d_2 reflexão sobre diagonal secundária



Estes movimentos podem ser compostos.

Exemplo



Conclui-se assim que $\rho_{90} d_1 = h$.

Procedendo como no exemplo anterior, não é difícil construir a tabela de Cayley (ou tabela de multiplicação) seguinte:

	ρ_0	ρ_{90}	ρ_{180}	ρ_{270}	h	v	d_1	d_2
ρ_0	ρ_0	ρ_{90}	ρ_{180}	ρ_{270}	h	v	d_1	d_2
ρ_{90}	ρ_{90}	ρ_{180}	ρ_{270}	ρ_0	d_2	d_1	h	v
ρ_{180}	ρ_{180}	ρ_{270}	ρ_0	ρ_{90}	v	h	d_2	d_1
ρ_{270}	ρ_{270}	ρ_0	ρ_{90}	ρ_{180}	d_1	d_2	v	h
h								ρ_{270}
v						ρ_0	ρ_{270}	
d_1					ρ_{270}			
d_2						ρ_{270}		ρ_0

Exercício

Complete a tabela anterior.

O que fizemos anteriormente para um quadrado pode ser feito para um triângulo equilátero ou mais geralmente para um n-ágono regular, com $n \geq 3$. A estrutura assim obtida representa-se por D_n e designa-se por *grupo diedral de ordem* $2n$.

Seja G um conjunto. Uma *operação binária* em G é uma função de $G \times G$ em G, isto é, uma função que a cada par ordenado de elementos de G associa um elemento de G.

Exemplo

Tanto a *adição módulo n* como a *multiplicação módulo n* são operações binárias sobre o conjunto $\{0, 1, \ldots, n-1\}$.

Lembramos que, por exemplo, a adição módulo n é definida por $a +_n b = a + b \pmod{n}$, sendo que $x \pmod{n}$ é o resto da divisão de x por n.

Definição (grupo)

Seja G um conjunto não vazio munido de uma operação binária (habitualmente designada por multiplicação*) que a cada par ordenado (a, b) de elementos de G associa um elemento de G (habitualmente denotado por ab).*
Dizemos que G é um grupo *com esta operação se forem satisfeitas as seguintes propriedades:*

1. *a operação é* associativa, *isto é,*
$$(ab)c = a(bc), \forall a, b, c \in G;$$
2. *existe* elemento neutro *para a operação em causa, isto é,*
$$\exists e \in G, \forall a \in G : ae = ea = a;$$
3. *cada elemento tem um inverso, isto é,*
$$\forall a \in G, \exists a' \in G : aa' = a'a = e.$$

Nalgumas situações é mais conveniente (ou mais comum...) chamar "adição" à operação binária, usando-se neste caso notação aditiva ($a+b$ em vez de ab). Neste caso usamos a terminologia "simétrico" em vez de "inverso".
Pode haver conveniência em explicitar a operação que estamos a considerar. Neste caso usaremos uma notação do tipo (G,θ) para indicar que θ é a operação que nos interessa.
É fácil verificar que existe um único elemento neutro de um grupo. É habitual designá-lo por *identidade* e representá-lo por 1 (no caso de estar a usar notação aditiva representa-se por 0). É também fácil verificar que cada elemento de um grupo tem um único inverso. O inverso do elemento a denota-se por a^{-1} (no caso de estar a usar notação aditiva representa-se por $-a$).

Exemplo

O conjunto $\mathbb{Z}$ dos inteiros com a adição usual é um grupo. A adição usual é associativa, 0 é o elemento neutro e $-a$ é o simétrico de a. Também $\mathbb{Q}$ e $\mathbb{R}$ são grupos com a adição usual.

Exemplo

Seja n um inteiro positivo. O conjunto $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ com a adição módulo n é um grupo, o *grupo dos inteiros módulo n*. O elemento neutro é 0 e o inverso de j é $n - j$.

Exemplo

O conjunto $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ dos números reais não nulos é um grupo para a multiplicação usual. 1 é o elemento neutro e $1/a$ é o inverso de a.

Exemplo

O conjunto $\mathbb{Z}$ dos inteiros não nulos não é um grupo para a multiplicação usual. 1 é elemento neutro, mas não existe $b \in \mathbb{Z}$ tal que $2b = 1$, logo 2 não tem inverso.