Dalle simmetrie alla crittografia

Francesco Matucci

francesco.matucci@unimib.it

Summer School

Una introduzione alla Matematica Universitaria

Milano-Bicocca, 27 giugno 2025

Idea intuitiva

Teoria dei gruppi è lo studio della simmetria

In modo intuitivo, possiamo definire un oggetto geometrico *simmetrico* se applicando qualche movimento su questo oggetto, lui rimane invariato.

Ad esempio, se ruotiamo un quadrato di 90 gradi attorno al suo centro, il quadrato si muove e torna a combaciare con sé stesso.

Simmetria

Figure con molta simmetria

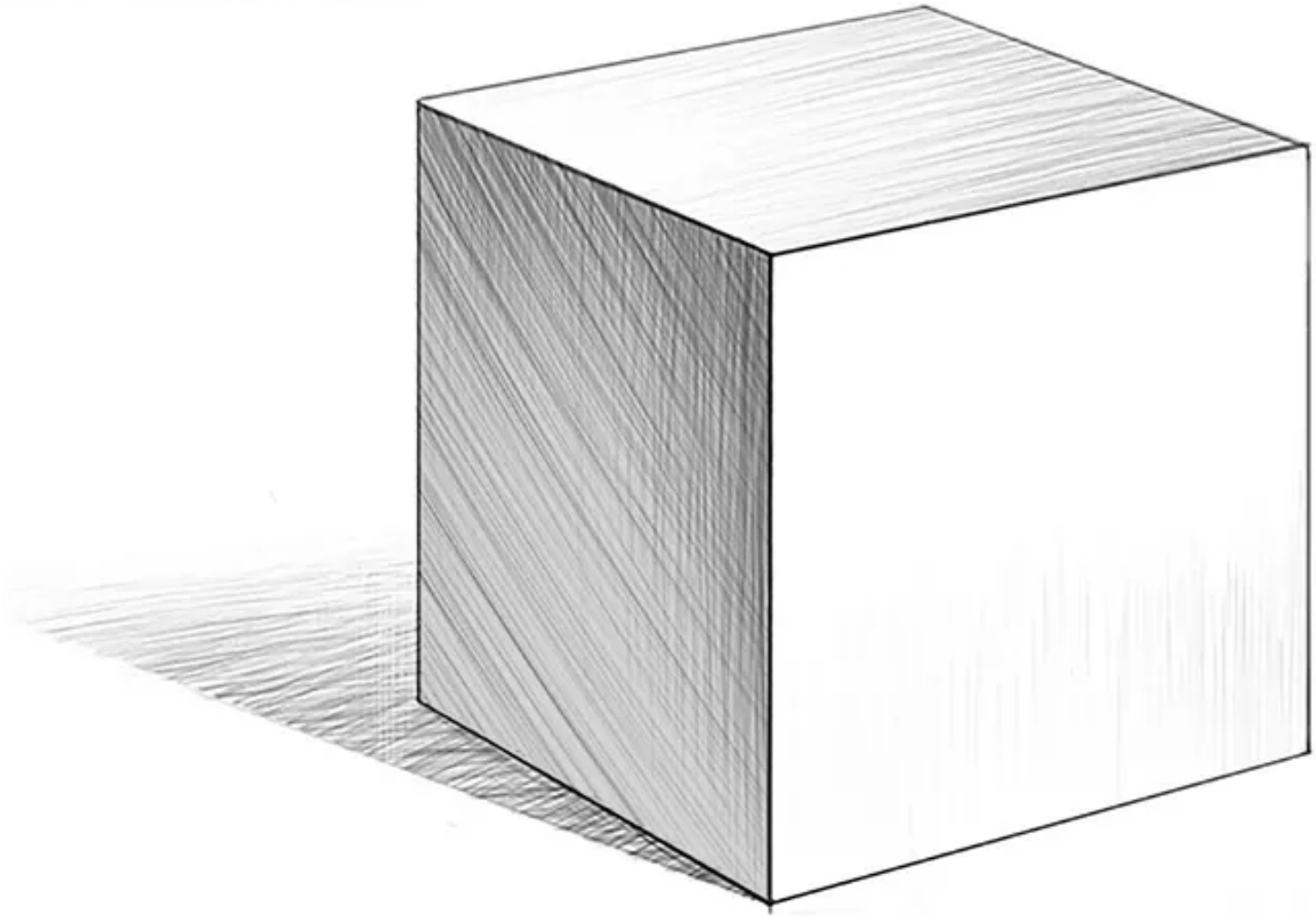


Figure con molta simmetria

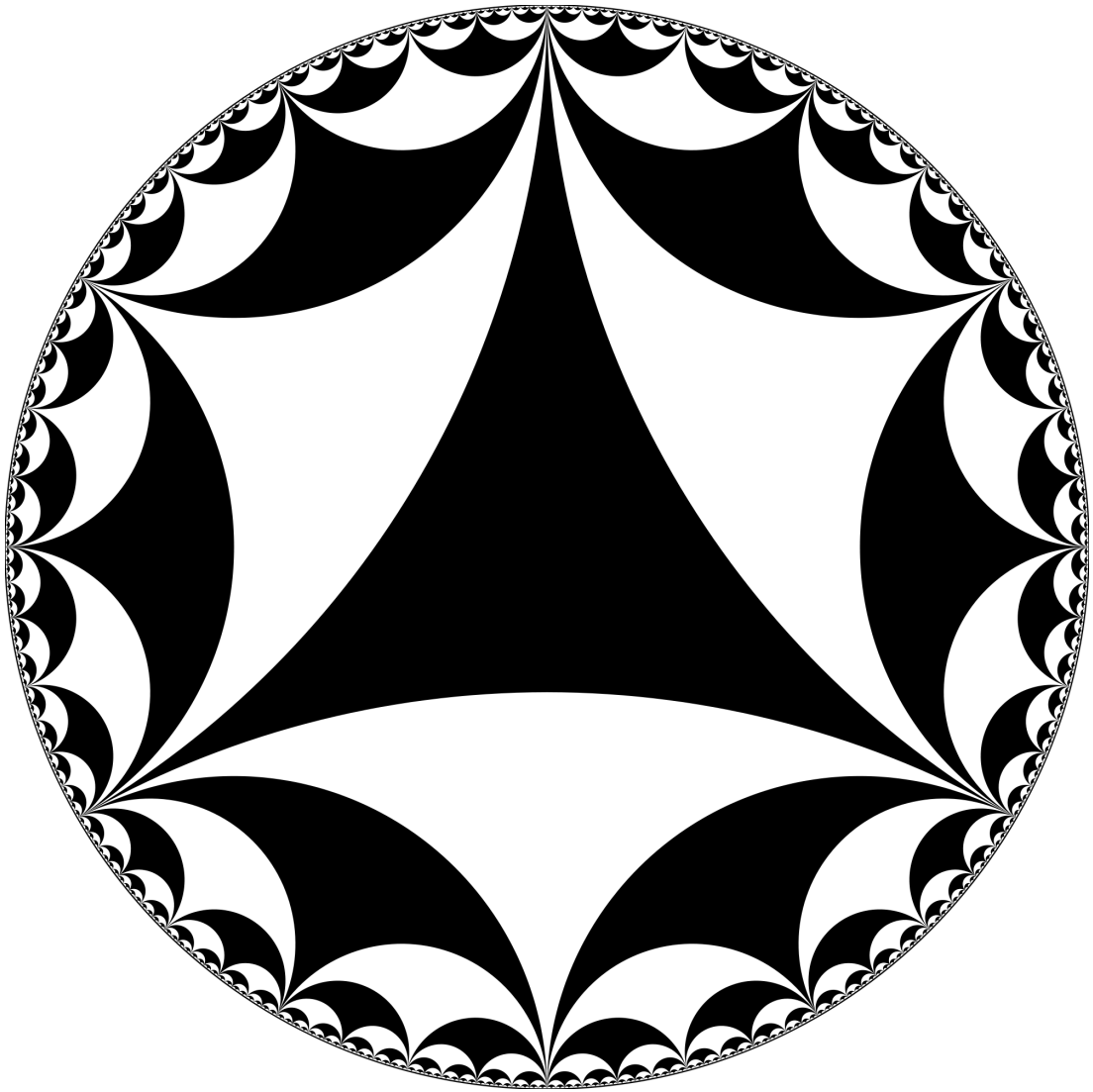


Figure con molta simmetria

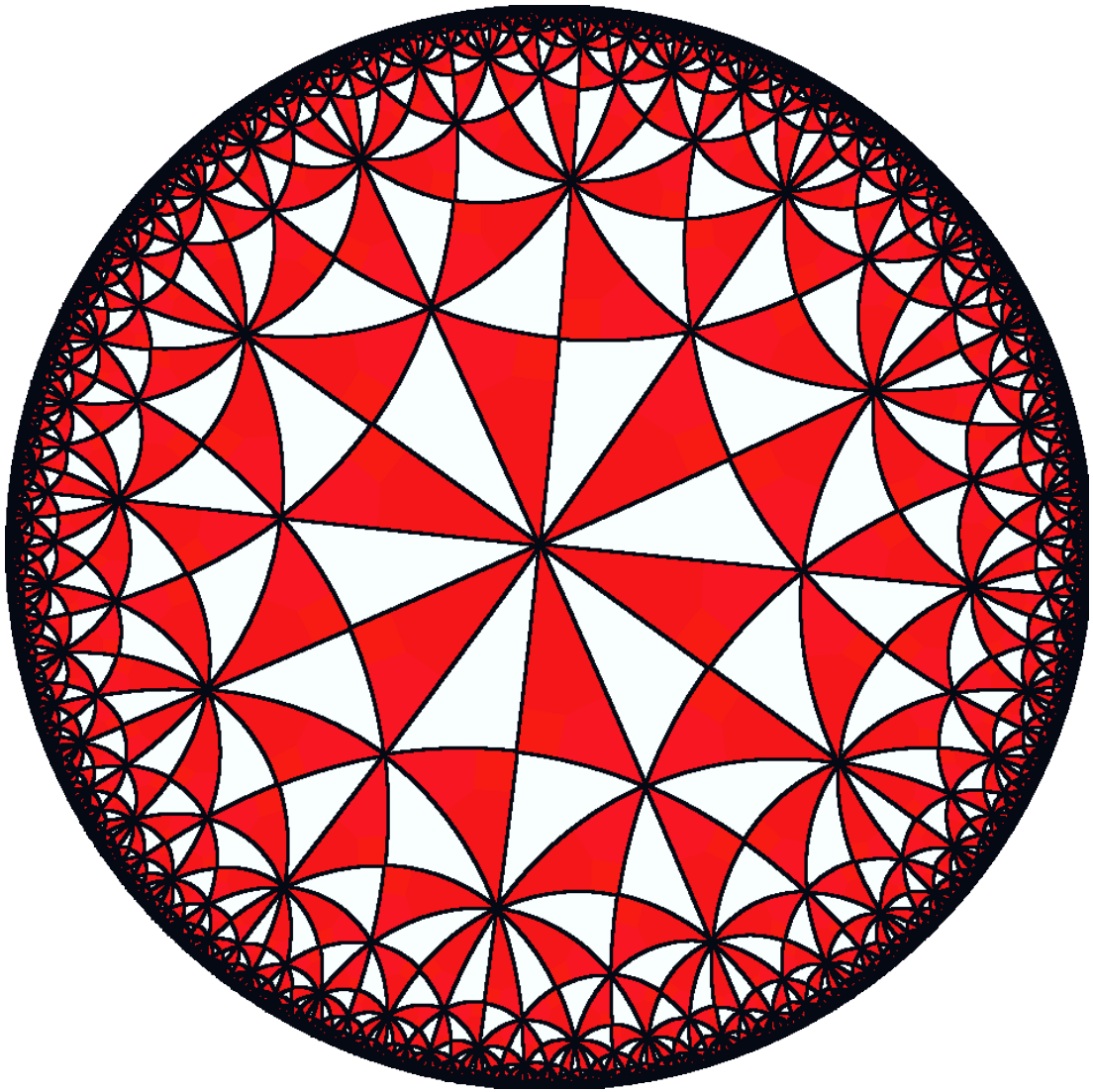


Figure con molta simmetria

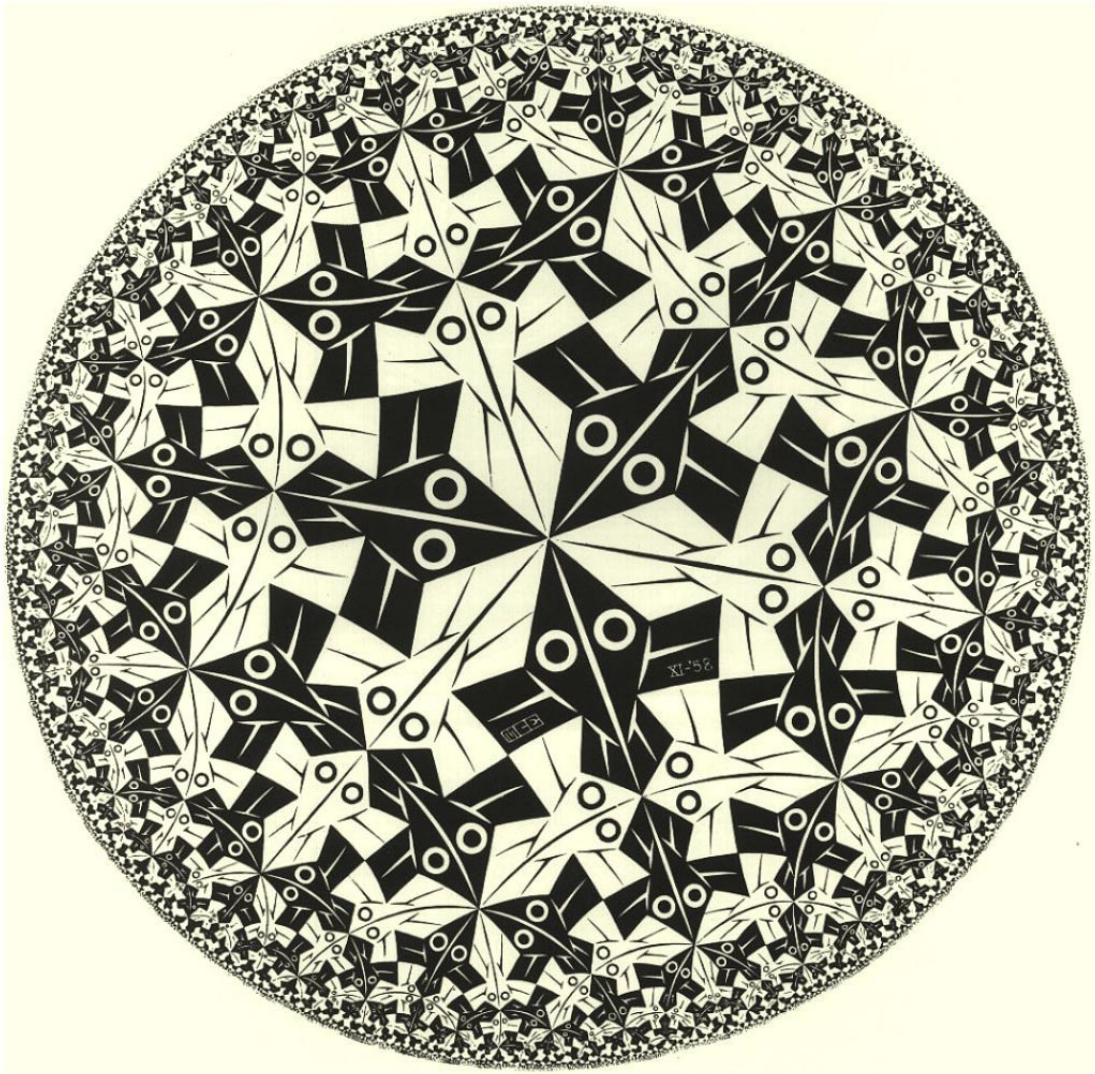


Figure con molta simmetria

Figure con molta simmetria

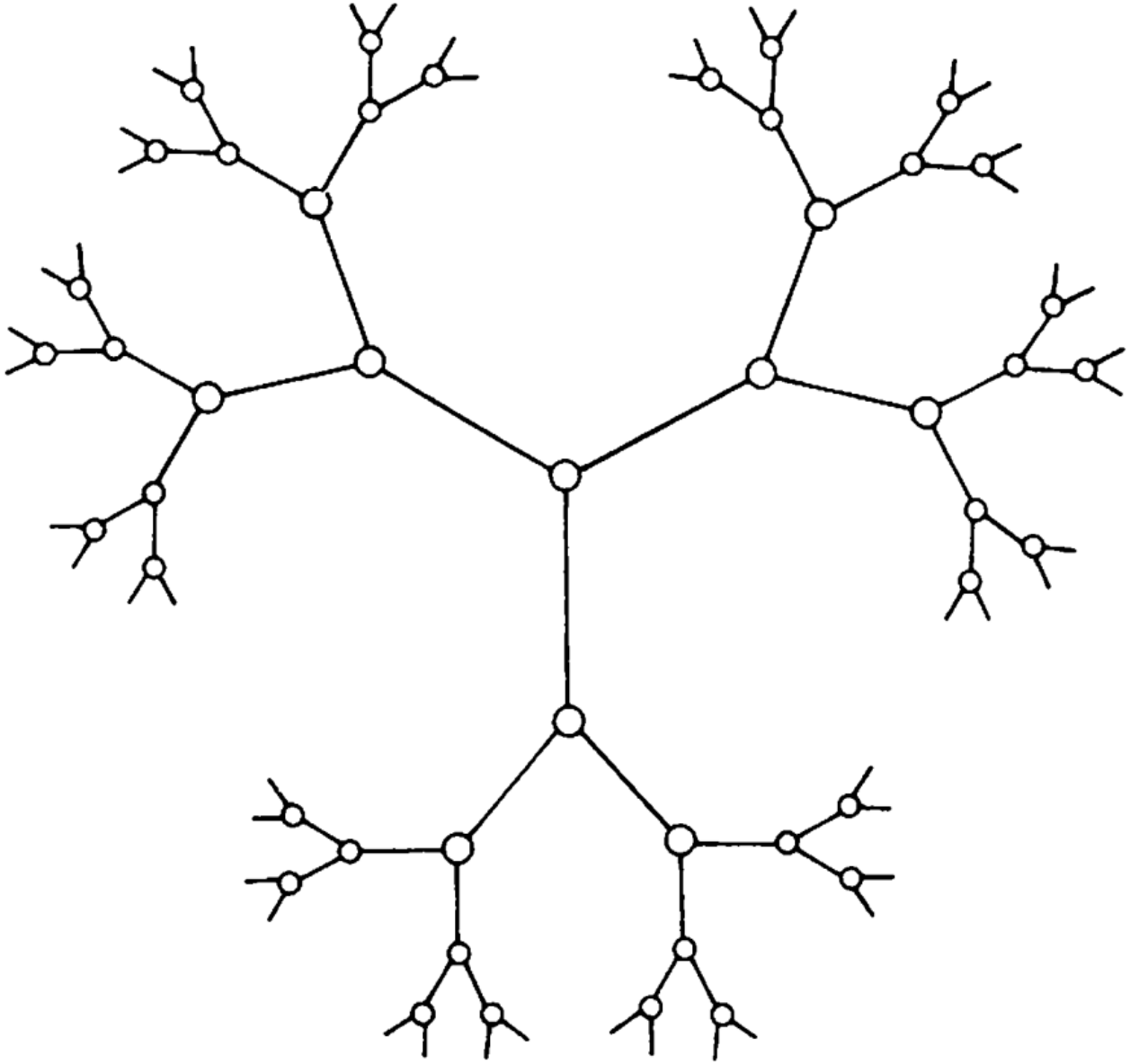


Figure con molta simmetria

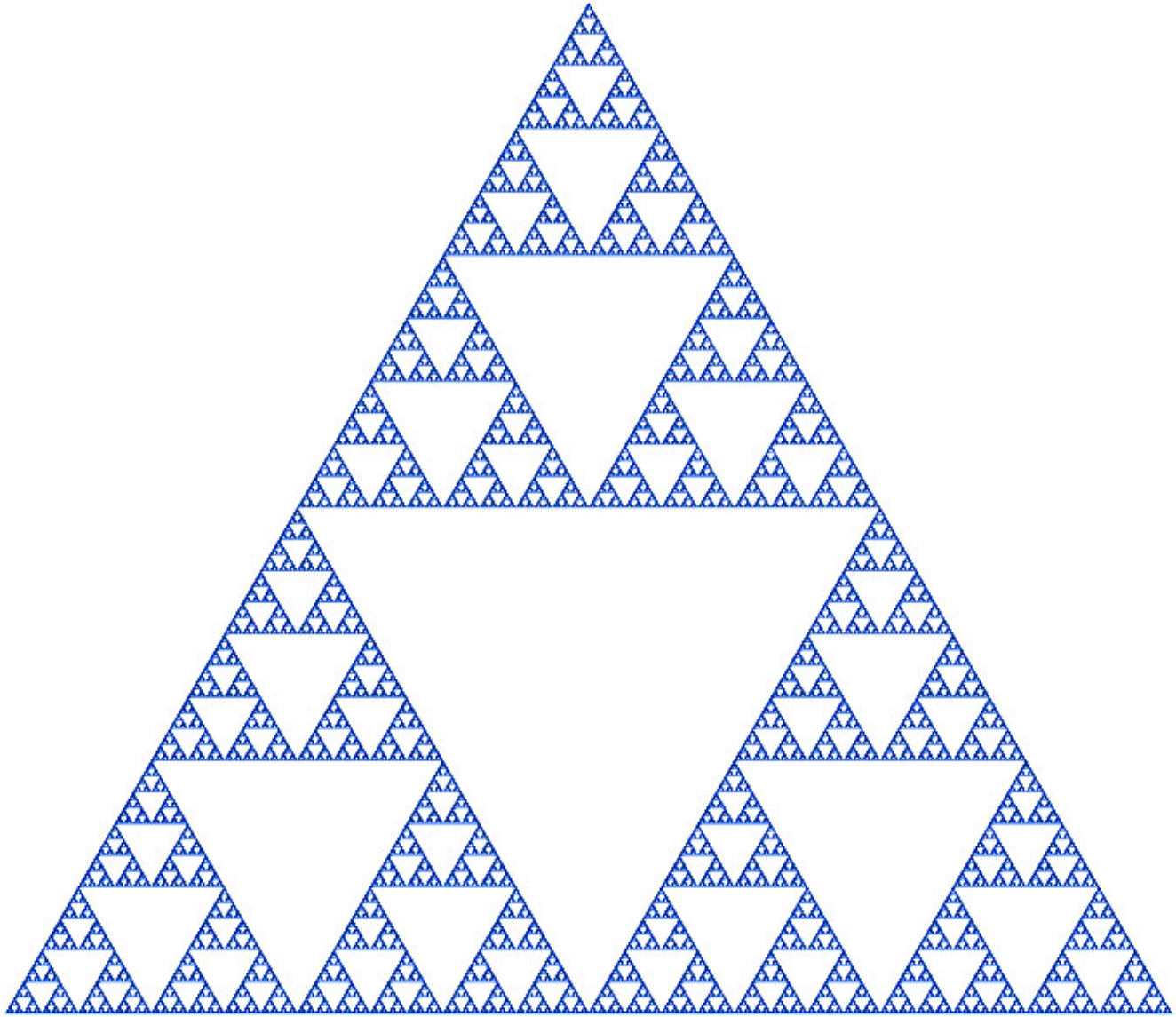
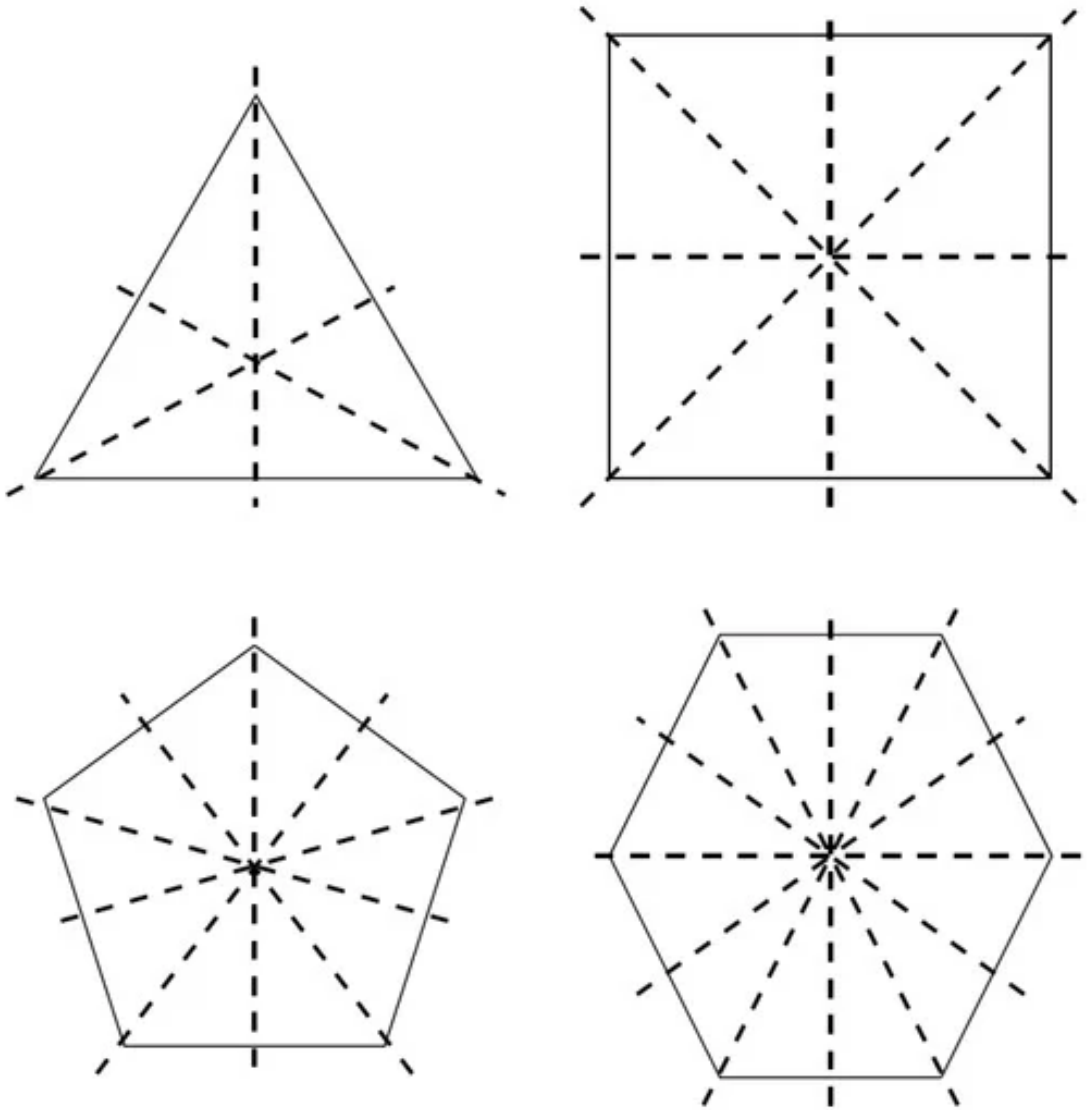


Figure con molta simmetria



Siamo più precisi

Simmetria come movimento rigido

I nostri occhi percepiscono una simmetria come un modo di muovere rigidamente una figura in sé stessa (ad esempio tramite una rotazione attorno ad un punto o una riflessione attorno ad una retta)

Più precisamente un movimento rigido è un movimento che non causa all'oggetto nessuna deformazione.

Ancora più precisamente, un **movimento rigido** è una funzione che conserva le distanze.

Simmetria come movimento rigido

I nostri occhi percepiscono una simmetria come un modo di muovere rigidamente una figura in sé stessa (ad esempio tramite una rotazione attorno ad un punto o una riflessione attorno ad una retta)

Più precisamente un movimento rigido è un movimento che non causa all'oggetto nessuna deformazione.

Ancora più precisamente, un **movimento rigido** è una funzione che conserva le distanze.

Cosa succede se eseguiamo due movimenti rigidi uno di seguito all'altro?

Simmetria come movimento rigido

I nostri occhi percepiscono una simmetria come un modo di muovere rigidamente una figura in sé stessa (ad esempio tramite una rotazione attorno ad un punto o una riflessione attorno ad una retta)

Più precisamente un movimento rigido è un movimento che non causa all'oggetto nessuna deformazione.

Ancora più precisamente, un **movimento rigido** è una funzione che conserva le distanze.

Cosa succede se eseguiamo due movimenti rigidi uno di seguito all'altro?

Il risultato finale è lui stesso un movimento rigido!

Alcuni ordini dei movimenti rigidi danno lo stesso risultato

Se a e b sono due movimenti rigidi del quadrato e scriviamo $a * b$ per intendere "prima fai il movimento b, poi fai il movimento a", allora non è difficile vedere che:

Alcuni ordini dei movimenti rigidi danno lo stesso risultato

Se a e b sono due movimenti rigidi del quadrato e scriviamo $a * b$ per intendere "prima fai il movimento b, poi fai il movimento a", allora non è difficile vedere che:

Se a, b, c sono elementi di G, allora

$$(a * b) * c = a * (b * c)$$

Il movimento rigido neutro

Esiste un movimento rigido speciale e (detto **neutro**) che non muove nessuno dei punti del quadrato.

Chiaramente se eseguiamo tale movimento e prima o dopo un movimento qualsiasi a, lasciamo invariato a, cioè

$$a * e = e * a = a$$

Il movimento rigido inverso

Se eseguiamo un movimento rigido g sul quadrato, spostiamo ogni vertice del quadrato in qualche altro vertice. Possiamo rimettere ogni vertice al suo posto iniziale invertendo ogni singolo spostamento.

Dato un movimento rigido g del quadrato, ne possiamo trovare uno g^{-1} tale che

$$g * g^{-1} = g^{-1} * g = e$$

Cos'è un gruppo?

Un **gruppo** è un insieme G assieme ad un'**operazione** $*$ (una macchina che prende due elementi di G e ne restituisce un altro, proprio come eseguire due movimenti rigidi uno dietro l'altro ne restituisce un altro)

Quindi se a, b sono elementi di G, allora $a * b$ è anch'esso elemento di G

Cos'è un gruppo?

Un **gruppo** è un insieme G assieme ad un'**operazione** $*$ (una macchina che prende due elementi di G e ne restituisce un altro, proprio come eseguire due movimenti rigidi uno dietro l'altro ne restituisce un altro)

Quindi se a, b sono elementi di G, allora $a * b$ è anch'esso elemento di G

... Tutto qua?

Cos'è un gruppo?

Un **gruppo** è un insieme G assieme ad un'**operazione** $*$ (una macchina che prende due elementi di G e ne restituisce un altro, proprio come eseguire due movimenti rigidi uno dietro l'altro ne restituisce un altro)

Quindi se a, b sono elementi di G, allora $a * b$ è anch'esso elemento di G

... Tutto qua?

No, abbiamo bisogno che G soddisfi anche le tre proprietà viste sul quadrato

Cos'è un gruppo?

Definizione

Un **gruppo** è un insieme G assieme ad un'**operazione** $*$ (una macchina che prende due elementi di G e ne restituisce un altro) tale che

1. Se a, b, c sono elementi di G, allora
$$(a * b) * c = a * (b * c)$$
2. Esiste un elemento e di G tale che, per ogni a elemento di G si ha
$$a * e = e * a = a$$
3. Per ogni elemento a di G, ne esiste sempre uno b di G tale che
$$a * b = b * a = e$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad a * b_2 = b_2 * a = e$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad a * b_2 = b_2 * a = e$$

Allora abbiamo che

$$b_1 =$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad a * b_2 = b_2 * a = e$$

Allora abbiamo che

$$b_1 = b_1 * e =$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad a * b_2 = b_2 * a = e$$

Allora abbiamo che

$$b_1 = b_1 * e = b_1 * (a * b_2) =$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad a * b_2 = b_2 * a = e$$

Allora abbiamo che

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 =$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad a * b_2 = b_2 * a = e$$

Allora abbiamo che

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 =$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad a * b_2 = b_2 * a = e$$

Allora abbiamo che

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

Proprietà di base di gruppo

Proprietà (Unicità dell'elemento inverso)

L'elemento b della proprietà di gruppo è unico.

Dimostrazione. Immaginiamo che ci siano due b_1 e b_2 tali che

$$a * b_1 = b_1 * a = e \qquad\qquad a * b_2 = b_2 * a = e$$

Allora abbiamo che

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

Dunque in un gruppo esiste sempre un solo elemento b tale che

$$a * b = b * a = e$$

e lo scriviamo come a^{-1} (**inverso** di a)

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

$a =$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

$a = e * a =$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

$$a = e * a = (c^{-1} * c) * a =$$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

$$a = e * a = (c^{-1} * c) * a = c^{-1} * (c * a) =$$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

$$a = e * a = (c^{-1} * c) * a = c^{-1} * (c * a) = c^{-1} * (c * b) =$$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

$$a = e * a = (c^{-1} * c) * a = c^{-1} * (c * a) = c^{-1} * (c * b) = (c^{-1} * c) * b =$$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

$$a = e * a = (c^{-1} * c) * a = c^{-1} * (c * a) = c^{-1} * (c * b) = (c^{-1} * c) * b = e * b =$$

Proprietà di base di un gruppo

Proprietà (Legge di cancellazione)

Sia $(G, *)$ un gruppo e siano a, b, c elementi tali che

$$c * a = c * b$$

allora $a = b$.

Dimostrazione. Dall'unicità dell'inverso, sappiamo che esiste un solo c^{-1} tale che

$$c^{-1} * c = e$$

Vale anche $c * c^{-1} = e$ ma non ci serve qua!

Moltiplichiamo l'equazione $c * a = c * b$ a sinistra per c^{-1} e abbiamo

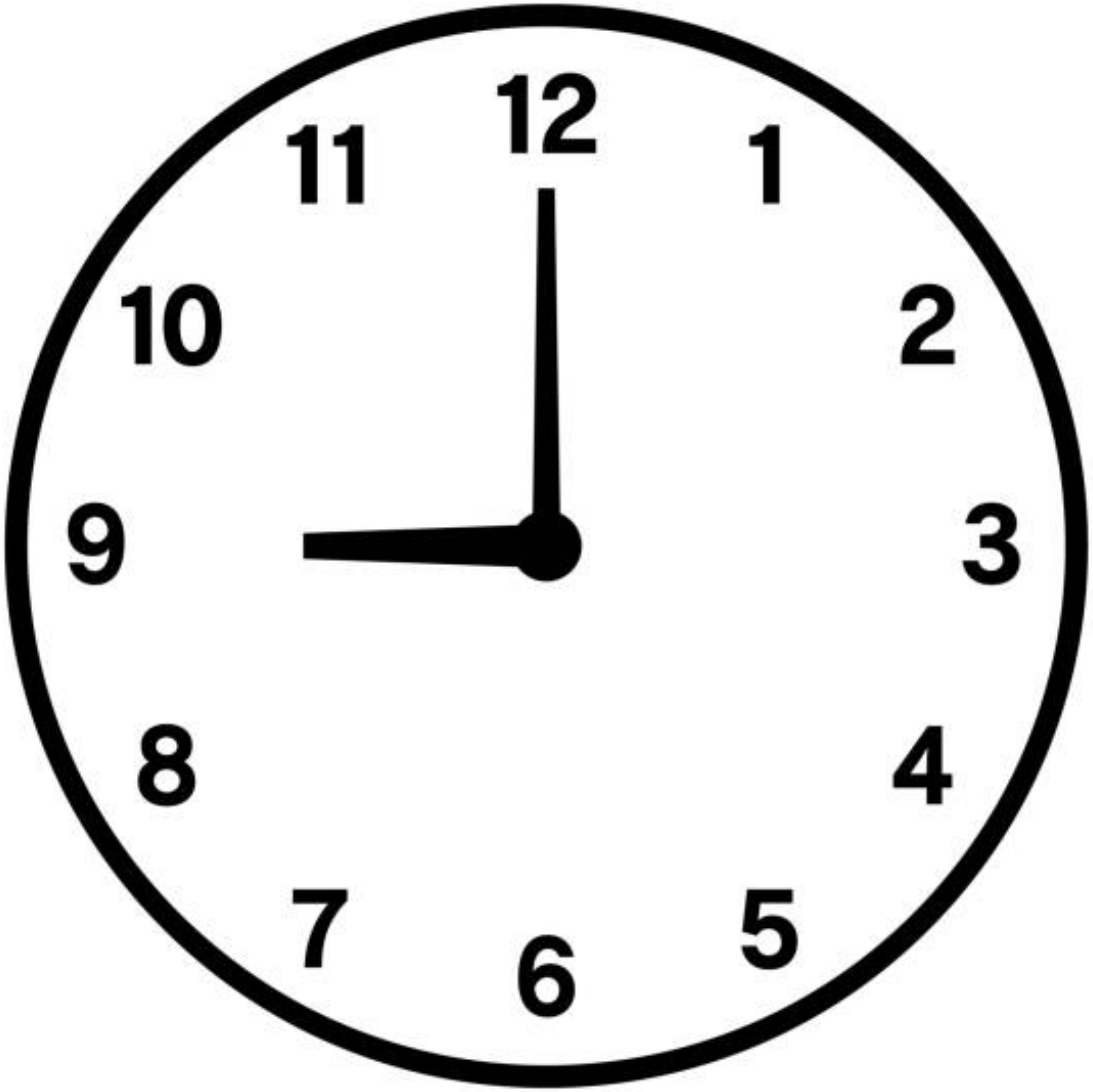
$$a = e * a = (c^{-1} * c) * a = c^{-1} * (c * a) = c^{-1} * (c * b) = (c^{-1} * c) * b = e * b = b$$

Gruppi abeliani o commutativi

Un gruppo $(G, *)$ è **abeliano** se per ogni due elementi a, b in G si ha che

$$a * b = b * a$$

L'orologio è un gruppo abeliano



L'orologio è un gruppo abeliano

Il **gruppo dell'orologio** si chiama $(\mathbb{Z}_{12}, +)$ e ha come elementi

$$\{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}, \underline{9}, \underline{10}, \underline{11}\}$$

dove la somma è semplicemente la somma di ore sull'orologio.

Si hanno quindi equazioni come

$$\underline{10} + \underline{3} = \underline{13} = \underline{1}$$

e anche

$$\underline{10} + \underline{11} = \underline{21} = \underline{9}$$

e anche

$$\underline{24} = \underline{12} = \underline{0}.$$

L'orologio è un gruppo abeliano

In pratica, per ogni due ore $\underline{a}, \underline{b}$ abbiamo che

$$\underline{a} + \underline{b} = \underline{r}$$

dove r è il resto della divisione per 12 del numero $a + b$ (quindi $0 \leq r \leq 11$).

L'orologio è un gruppo abeliano

In pratica, per ogni due ore $\underline{a}, \underline{b}$ abbiamo che

$$\underline{a} + \underline{b} = \underline{r}$$

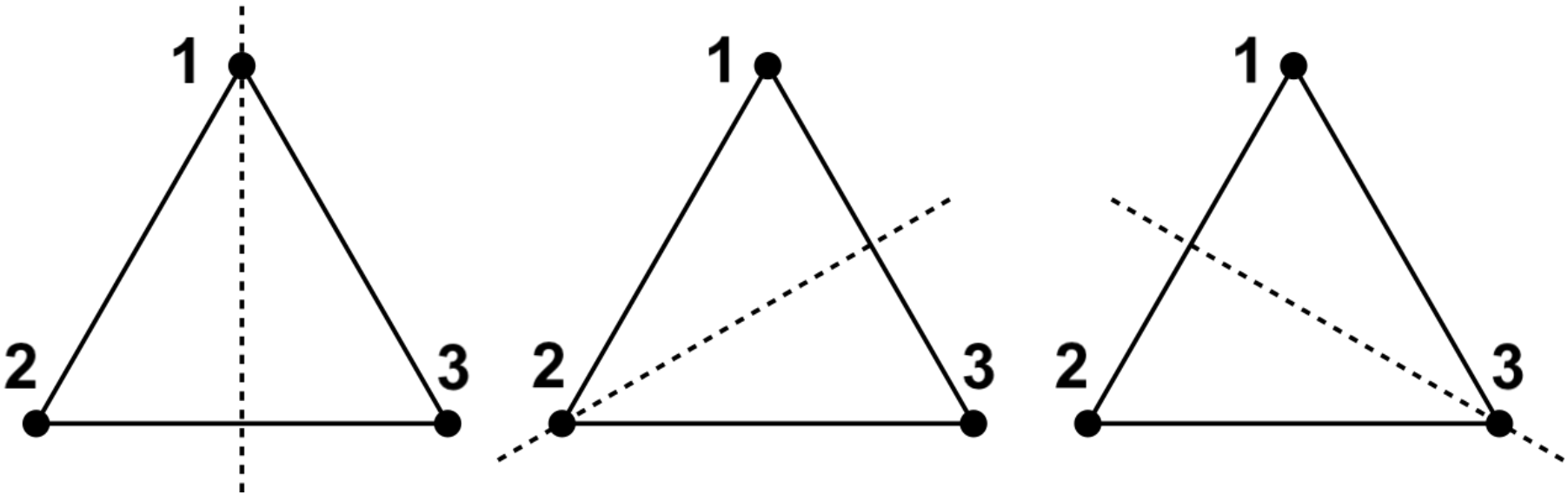
dove r è il resto della divisione per 12 del numero $a + b$ (quindi $0 \leq r \leq 11$).

Il gruppo dell'orologio può essere definito per qualsiasi numero di ore, cioè si può costruire il gruppo

$$(\mathbb{Z}_n, +)$$

delle **classi di resto modulo** n che contiene gli elementi $\{\underline{0}, \underline{1}, \ldots, \underline{n-1}\}$ e nel quale $\underline{n} = \underline{0}$.

Esempio di un gruppo non abeliano



Esempio di un gruppo non abeliano

Il gruppo delle simmetrie del triangolo equilatero si chiama **gruppo simmetrico su tre elementi** $\mathrm{Sym}(3)$ e contiene sei elementi: tre rotazioni (di cui una di 0 gradi) e tre riflessioni.

Esempio di un gruppo non abeliano

Il gruppo delle simmetrie del triangolo equilatero si chiama **gruppo simmetrico su tre elementi** $\mathrm{Sym}(3)$ e contiene sei elementi: tre rotazioni (di cui una di 0 gradi) e tre riflessioni.

Consideriamo la rotazione r di 120^0 antioraria

$$1 \overset{r}{\mapsto} 2$$

$$2 \overset{r}{\mapsto} 3$$

$$3 \overset{r}{\mapsto} 1$$

Esempio di un gruppo non abeliano

Il gruppo delle simmetrie del triangolo equilatero si chiama **gruppo simmetrico su tre elementi** $\mathrm{Sym}(3)$ e contiene sei elementi: tre rotazioni (di cui una di 0 gradi) e tre riflessioni.

Consideriamo la rotazione r di 120^0 antioraria

$$1 \overset{r}{\mapsto} 2$$

$$2 \overset{r}{\mapsto} 3$$

$$3 \overset{r}{\mapsto} 1$$

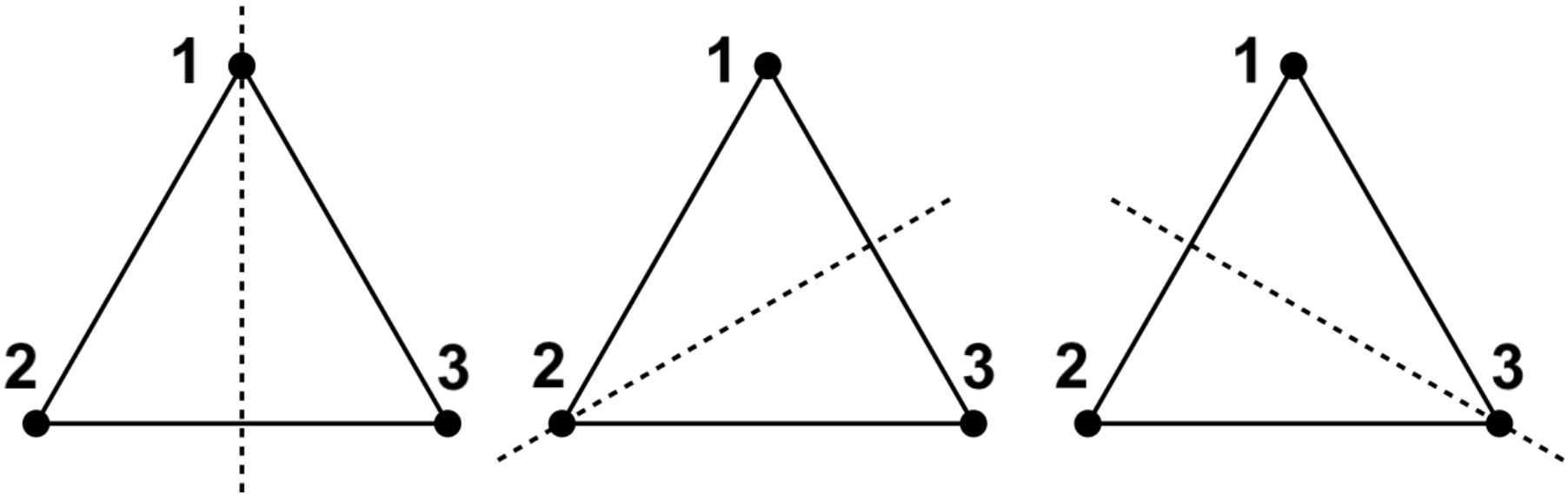
e la riflessione s attorno all'asse verticale

$$1 \overset{s}{\mapsto} 1$$

$$2 \overset{s}{\mapsto} 3$$

$$3 \overset{s}{\mapsto} 2$$

Esempio di un gruppo non abeliano



Esempio di un gruppo non abeliano

Adesso calcoliamo s seguito da r

$$1 \overset{s}{\mapsto} 1 \overset{r}{\mapsto} 2$$
$$2 \overset{s}{\mapsto} 3 \overset{r}{\mapsto} 1$$
$$3 \overset{s}{\mapsto} 2 \overset{r}{\mapsto} 3$$

che è la riflessione attorno all'asse che passa per il vertice 3.

Esempio di un gruppo non abeliano

Adesso calcoliamo s seguito da r

$$1 \overset{s}{\mapsto} 1 \overset{r}{\mapsto} 2$$
$$2 \overset{s}{\mapsto} 3 \overset{r}{\mapsto} 1$$
$$3 \overset{s}{\mapsto} 2 \overset{r}{\mapsto} 3$$

che è la riflessione attorno all'asse che passa per il vertice 3.

Se invece calcoliamo r seguito da s

$$1 \overset{r}{\mapsto} 2 \overset{s}{\mapsto} 3$$
$$2 \overset{r}{\mapsto} 3 \overset{s}{\mapsto} 2$$
$$3 \overset{r}{\mapsto} 1 \overset{s}{\mapsto} 1$$

che è la riflessione attorno all'asse che passa per il vertice 2.

Esempio di un gruppo non abeliano

Adesso calcoliamo s seguito da r

$$1 \overset{s}{\mapsto} 1 \overset{r}{\mapsto} 2$$
$$2 \overset{s}{\mapsto} 3 \overset{r}{\mapsto} 1$$
$$3 \overset{s}{\mapsto} 2 \overset{r}{\mapsto} 3$$

che è la riflessione attorno all'asse che passa per il vertice 3.

Se invece calcoliamo r seguito da s

$$1 \overset{r}{\mapsto} 2 \overset{s}{\mapsto} 3$$
$$2 \overset{r}{\mapsto} 3 \overset{s}{\mapsto} 2$$
$$3 \overset{r}{\mapsto} 1 \overset{s}{\mapsto} 1$$

che è la riflessione attorno all'asse che passa per il vertice 2.

Dunque $rs \neq sr$ e quindi $\mathrm{Sym}(3)$ **non** è abeliano.

Tabelle di moltiplicazione

Tabelle di moltiplicazione

Per scrivere un gruppo $(G, *)$ abbiamo bisogno di due ingredienti

Tabelle di moltiplicazione

Per scrivere un gruppo $(G, *)$ abbiamo bisogno di due ingredienti

1. La lista degli elementi $\{a_1, a_2, \ldots\}$ in G ordinata in qualche modo

Tabelle di moltiplicazione

Per scrivere un gruppo $(G, *)$ abbiamo bisogno di due ingredienti

1. La lista degli elementi $\{a_1, a_2, \ldots\}$ in G ordinata in qualche modo
2. Una tabella che abbia righe e colonne etichettate dagli elementi $a_1, a_2, \ldots$

Tabelle di moltiplicazione

Proprietà di questa tabella

Tabelle di moltiplicazione

Proprietà di questa tabella

1. **Sudoku:** Ogni lettera appare una volta sola in ogni riga ed ogni colonna

Tabelle di moltiplicazione

Proprietà di questa tabella

1. **Sudoku:** Ogni lettera appare una volta sola in ogni riga ed ogni colonna

2. **Simmetria diagonale se il gruppo è abeliano:** Se un gruppo è abeliano la tabella è simmetrica rispetto alla diagonale

Esempi di tabelle di moltiplicazione

Trasferiamoci altrove!

ESERCIZIO

SIA $G = \{a, b, c, d\}$ GRUPPO E VOGLIAMO COMPLETARE LA TABELLA

$*$	a	b	c	d
a		d		
b				a
c		$c * b$	c	
d				

$*$	a	b	c	d
a		d		
b				a
c			c	
d				

USIAMO

CHE $c = e$

SAPPIAMO CHE

$$c * c = c = c * e$$

LEGGE DI CANCELLAZIONE $\Longrightarrow$ $c = e$ ELEMENTO NEUTRO

$*$	a	b	c	d
a		d	a	
b			b	a
c	a	b	c	d
d			d	

$*$	a	b	c	d
a		d	a	
b			b	a
c	a	b	c	d
d			d	

DATO CHE $a * b = d$

ALLORA $b * b \neq d$

$\Longrightarrow$ $b * b = c$

$*$	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

DUE $\Longrightarrow$ POSSIBILITÀ

QUESTO È $(\mathbb{Z}_4, +)$

ABELIANI

$*$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	d	d	c

QUESTO È IL GRUPPO DI KLEIN (DEFINITO COSÌ)

Isomorfismi: come distinguere due gruppi

Formalizziamo quanto visto negli esempi precedenti.

Definizione

Diciamo che due gruppi

$$(G, *) = \{e, a, b, c, \ldots\}$$
$$(G', \star) = \{e', a', b', c', \ldots\}$$

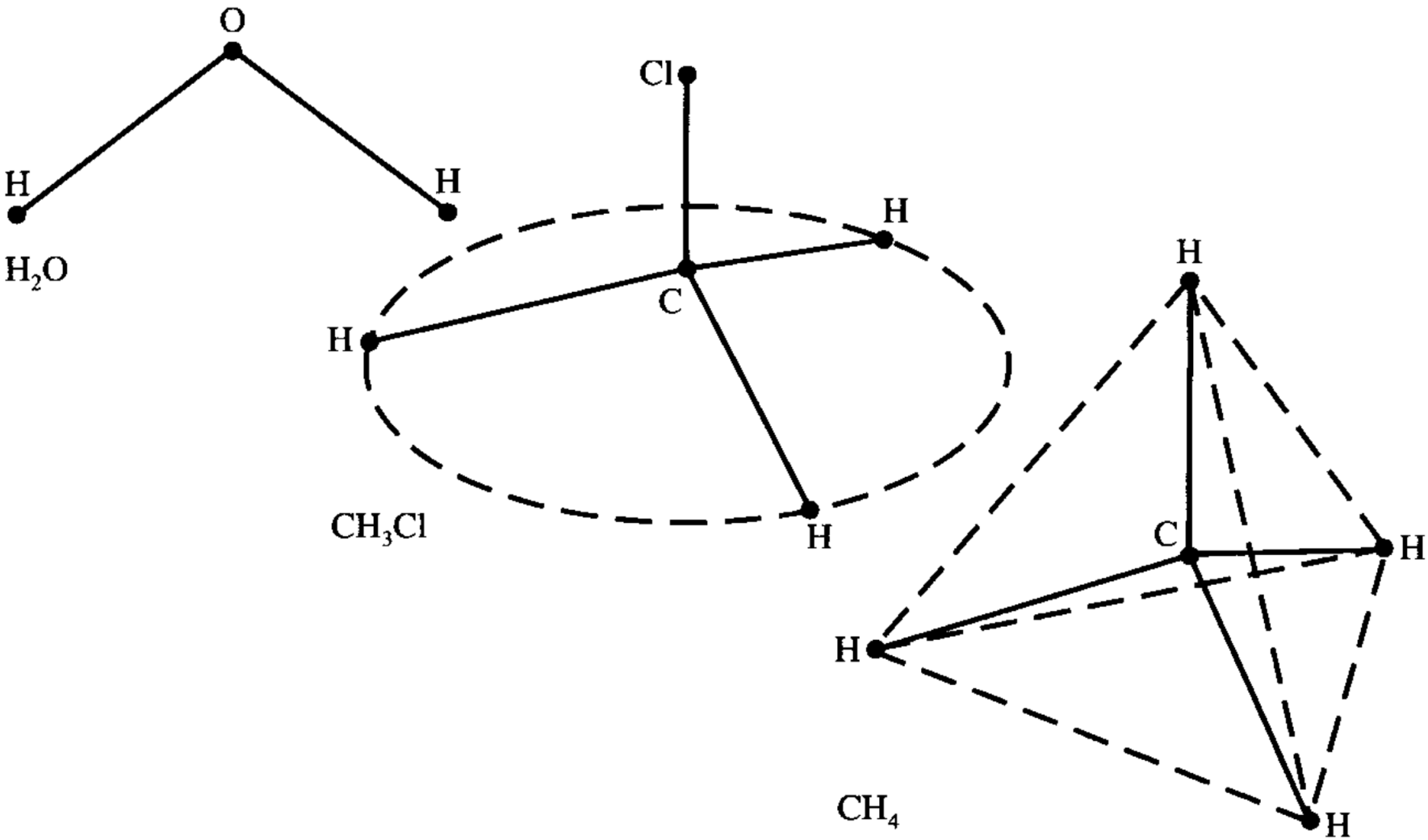
sono **isomorfi** se esiste una **corrispondenza biunivoca** $f : G \to G'$ (cioè per ogni x' di G' esiste un unico x in G tale che $f(x) = x'$) tale che le tabelle di moltiplicazione si corrispondono, cioè se $x * y = z$ nella tabella di G, allora

$$f(x) \star f(y) = f(z)$$

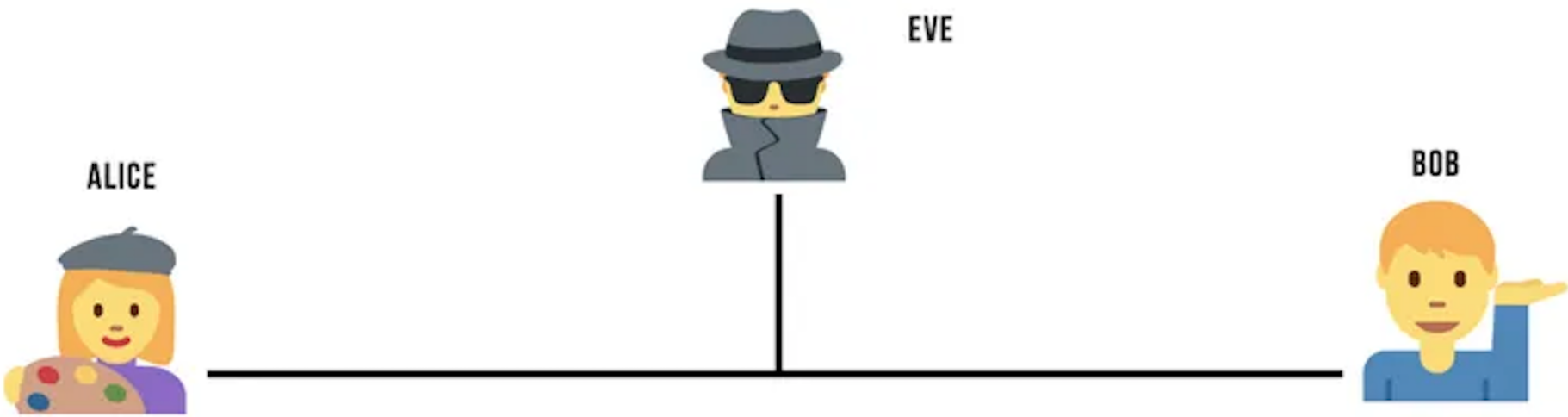
nella tabella di G'.

A cosa servono i gruppi?

Chimica

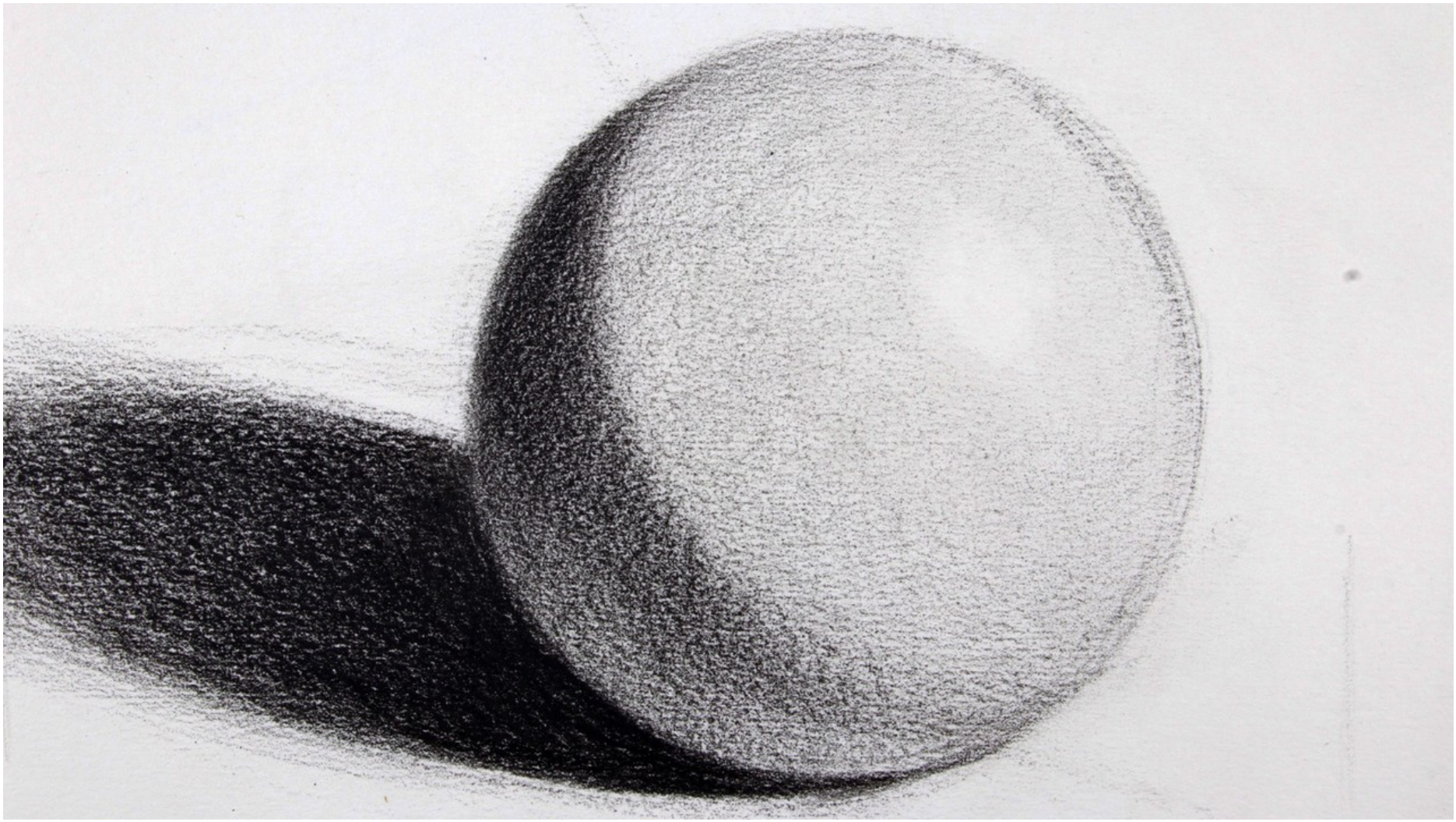


Crittografia



Discriminare le forme degli oggetti

Discriminare le forme degli oggetti



Contare oggetti

Quante configurazioni?

Contare oggetti

Se X è insieme, una corrispondenza biunivoca $X \to X$ si chiama **permutazione**.

Contare oggetti

Se X è insieme, una corrispondenza biunivoca $X \to X$ si chiama **permutazione**.

Definizione

Se G è un gruppo di permutazioni di un insieme X, possiamo definire due concetti

Contare oggetti

Se X è insieme, una corrispondenza biunivoca $X \to X$ si chiama **permutazione**.

Definizione

Se G è un gruppo di permutazioni di un insieme X, possiamo definire due concetti

1. L'**orbita** $\mathcal{O}_x$ di un elemento x è l'insieme di tutti i possibili elementi della forma $g(x)$ al variare di g in G.

Contare oggetti

Se X è insieme, una corrispondenza biunivoca $X \to X$ si chiama **permutazione**.

Definizione

Se G è un gruppo di permutazioni di un insieme X, possiamo definire due concetti

1. L'**orbita** $\mathcal{O}_x$ di un elemento x è l'insieme di tutti i possibili elementi della forma $g(x)$ al variare di g in G.
2. L'**insieme dei punti fissi** $\mathrm{Fix}(g)$ **di un** g in G è l'insieme degli elementi x di X tali che $g(x) = x$

Contare oggetti

Esempio

1. Se X è un quadrato con vertici $\{1, 2, 3, 4\}$ in senso antiorario e t è la riflessione che scambia $1 \longleftrightarrow 2$ e $3 \longleftrightarrow 4$, allora il gruppo $G = \{\mathrm{id}, t\}$ ha due orbite

$$\mathcal{O}_1 = \{1, 2\}$$
$$\mathcal{O}_3 = \{3, 4\}$$

e osserviamo che $\mathrm{Fix}(t)$ è vuoto.

2. Se X è triangolo equilatero ed s è la riflessione di X che passa per il vertice 1 (vista prima), allora $\mathrm{Fix}(s) = \{1\}$.

Contare oggetti

Sia X un qualsiasi insieme. Denotiamo con $|X|$ la cardinalità dell'insieme X, cioè il numero di oggetti contenuti in X (che possono essere infiniti).

Formula (Burnside)

Sia G un gruppo di permutazioni di X e supponiamo che G e X siano finiti.

Se N è il numero di tutte le orbite $\mathcal{O}_x$ possibili distinte, abbiamo che

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Contare oggetti

Esercizio

Quante sono le collane con tre perle di due colori (blu e verde) che siano distinte tra loro, a meno di simmetrie del triangolo?

Contare oggetti

Esercizio

Quante sono le collane con tre perle di due colori (blu e verde) che siano distinte tra loro, a meno di simmetrie del triangolo?

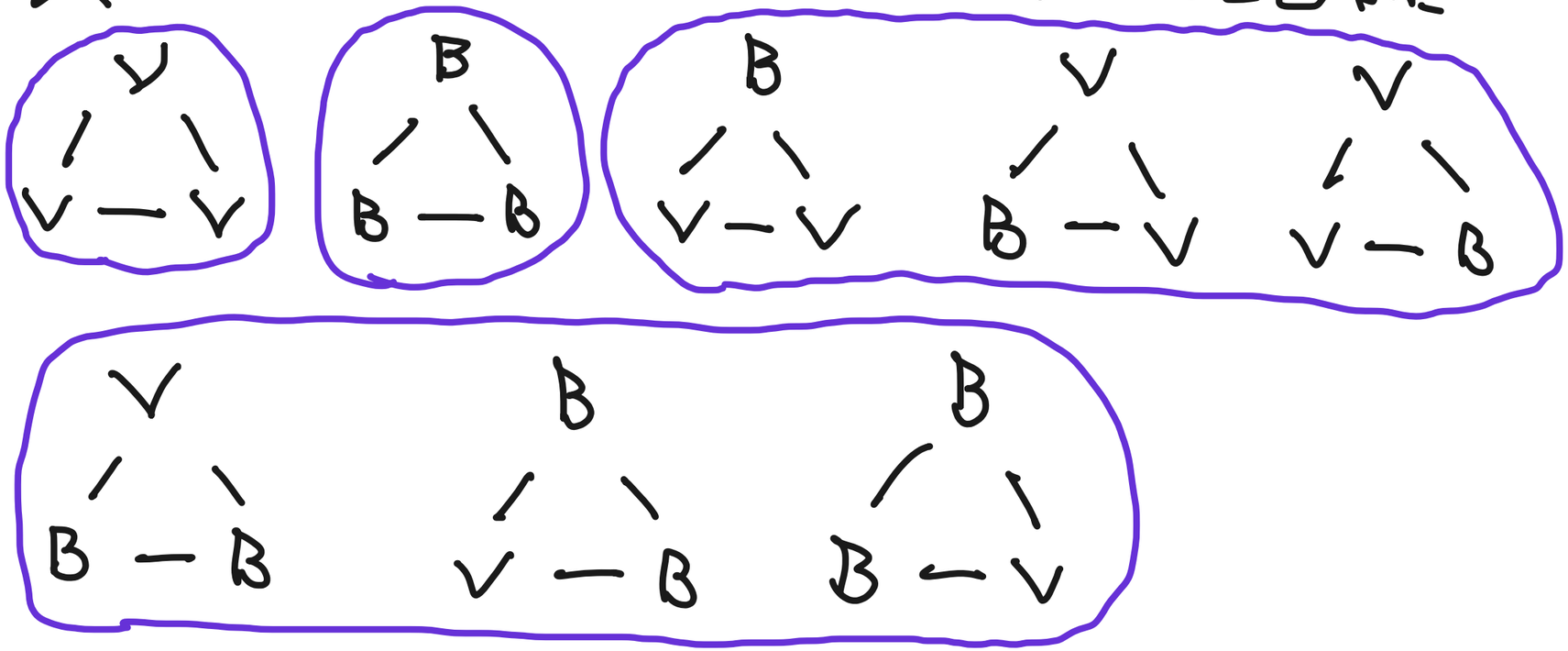
Trasferiamoci altrove!

ESERCIZIO

QUANTE CONFIGURAZIONI DI COLLANE CON TRE PERLE BLU E VERDI CI SONO ???

SOLUZIONE

X = CONFIGURAZIONI DI COLLANE



$G = Sym(3)$

$|G| = 6$

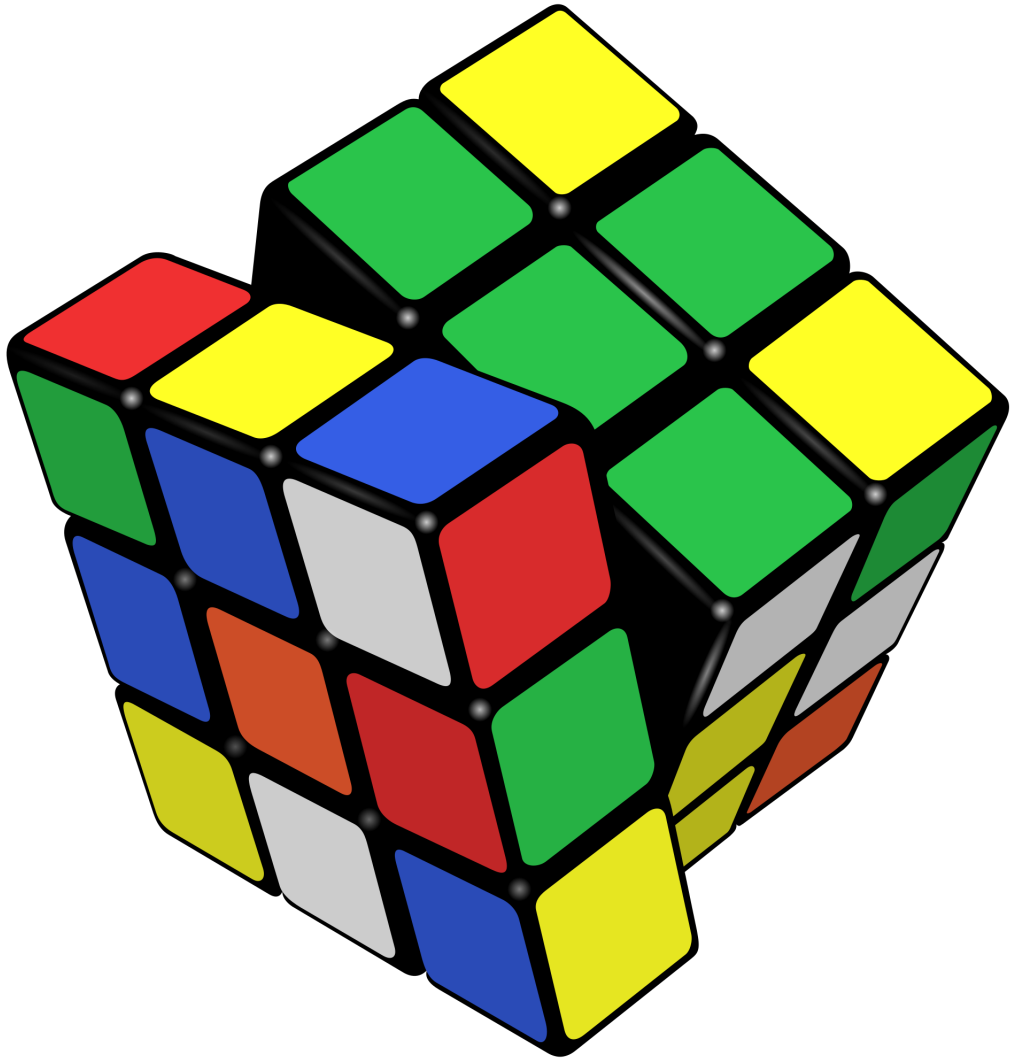
g	$Fix(g)$
e	8
r, r^2	2
s	4
rs	4
r^2s	4

$$N = \frac{1}{6}\left(8 \cdot 1 + 2 \cdot 2 + 4 \cdot 3\right) = 4$$

$|G| = |Sym(3)|$

Il cubo di Rubik

Il cubo di Rubik



Il cubo di Rubik

Come nell'esercizio sulle collane, studiamo l'insieme X di tutte le possibili configurazioni del cubo di Rubik che si ottengono a partire da quella iniziale (in cui ogni faccia ha un solo colore) e applicandoci le trasformazioni contenute nel gruppo G di Rubik

Il cubo di Rubik

Come nell'esercizio sulle collane, studiamo l'insieme X di tutte le possibili configurazioni del cubo di Rubik che si ottengono a partire da quella iniziale (in cui ogni faccia ha un solo colore) e applicandoci le trasformazioni contenute nel gruppo G di Rubik

... Sì, ma cos'è il gruppo di Rubik G?

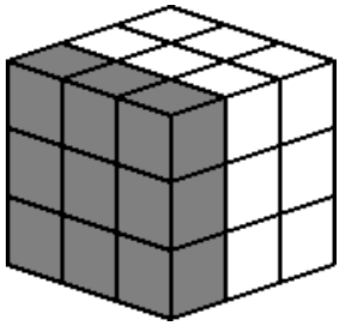
Il cubo di Rubik

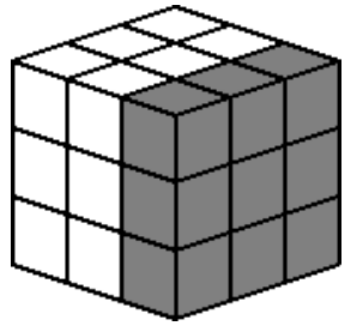
Come nell'esercizio sulle collane, studiamo l'insieme X di tutte le possibili configurazioni del cubo di Rubik che si ottengono a partire da quella iniziale (in cui ogni faccia ha un solo colore) e applicandoci le trasformazioni contenute nel gruppo G di Rubik

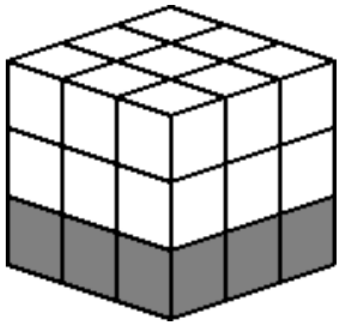
... Sì, ma cos'è il gruppo di Rubik G?

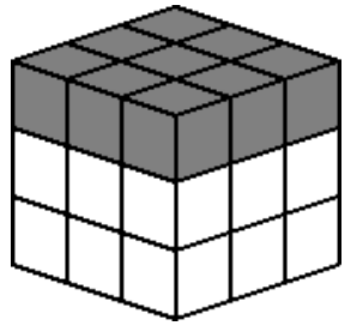
Il cubo di Rubik si può manipolare con rotazioni orarie delle singole facce di 90^0.

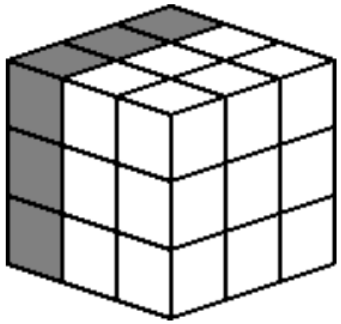
Il cubo di Rubik

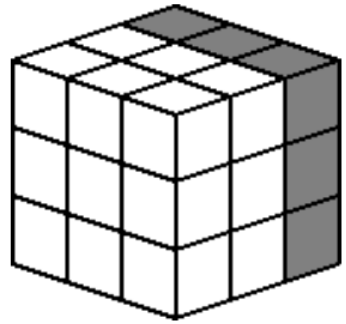
Front F 

Right R 

Down D 

Up U 

Left L 

Back B 

Il cubo di Rubik

Immaginiamo di avere un cubo davanti a noi e diamo nomi alle sue facce

1. U denota la faccia di sopra
2. F denota la faccia di fronte a noi
3. L denota la faccia a sinistra.
4. R denota la faccia a destra
5. B denota la faccia dietro.
6. D denota la faccia di sotto.

Le rotazioni avvengono in modo orario immaginando che l'osservatore guardi quella faccia.

Infine denotiamo con le lettere $\{U, F, L, R, B, D\}$ anche le rotazioni orarie di 90^0 delle facce di cui sopra

Ad esempio, ULF significa che ruotiamo la faccia di sopra di 90^0, poi quella di sinistra, poi quella di fronte. L'inverso di questo elemento sarà $F^{-1}L^{-1}U^{-1}$.

Il cubo di Rubik

Il **gruppo del cubo di Rubik** G è il gruppo che contiene qualsiasi parola fatta dalle lettere $\{U, F, L, R, B, D\}$ e dai loro inversi. Le lettere $\{U, F, L, R, B, D\}$ sono dette **generatori di** G.

Quindi $U^2F^{-1}L^{30}B^{-2}RBRFL$ è un elemento del nostro gruppo G.

Il numero di elementi del gruppo è enorme

$$|G| = 2^{27}3^{14}5^3 7^2 11 = 43.252.003.274.489.856.000$$

Il cubo di Rubik: efficienza della risoluzione

Vale il seguente straordinario risultato.

Il cubo di Rubik: efficienza della risoluzione

Vale il seguente straordinario risultato.

Teorema

1. Data una qualsiasi configurazione, bastano al più 20 mosse (cioè 20 dei generatori $\{U, F, L, R, B, D\}$ e i loro inversi) per tornare a quella iniziale.

Il cubo di Rubik: efficienza della risoluzione

Vale il seguente straordinario risultato.

Teorema

1. Data una qualsiasi configurazione, bastano al più 20 mosse (cioè 20 dei generatori $\{U, F, L, R, B, D\}$ e i loro inversi) per tornare a quella iniziale.

2. Esiste una configurazione particolare per cui non bastano meno di 20 mosse per riportarla a quella iniziale.

Il cubo di Rubik: efficienza della risoluzione

Vale il seguente straordinario risultato.

Teorema

1. Data una qualsiasi configurazione, bastano al più 20 mosse (cioè 20 dei generatori $\{U, F, L, R, B, D\}$ e i loro inversi) per tornare a quella iniziale.

2. Esiste una configurazione particolare per cui non bastano meno di 20 mosse per riportarla a quella iniziale.

Dunque 20 è davvero il numero necessario per riportare una qualsiasi configurazione a quella iniziale!

... Ma quanto tempo ci può volere?

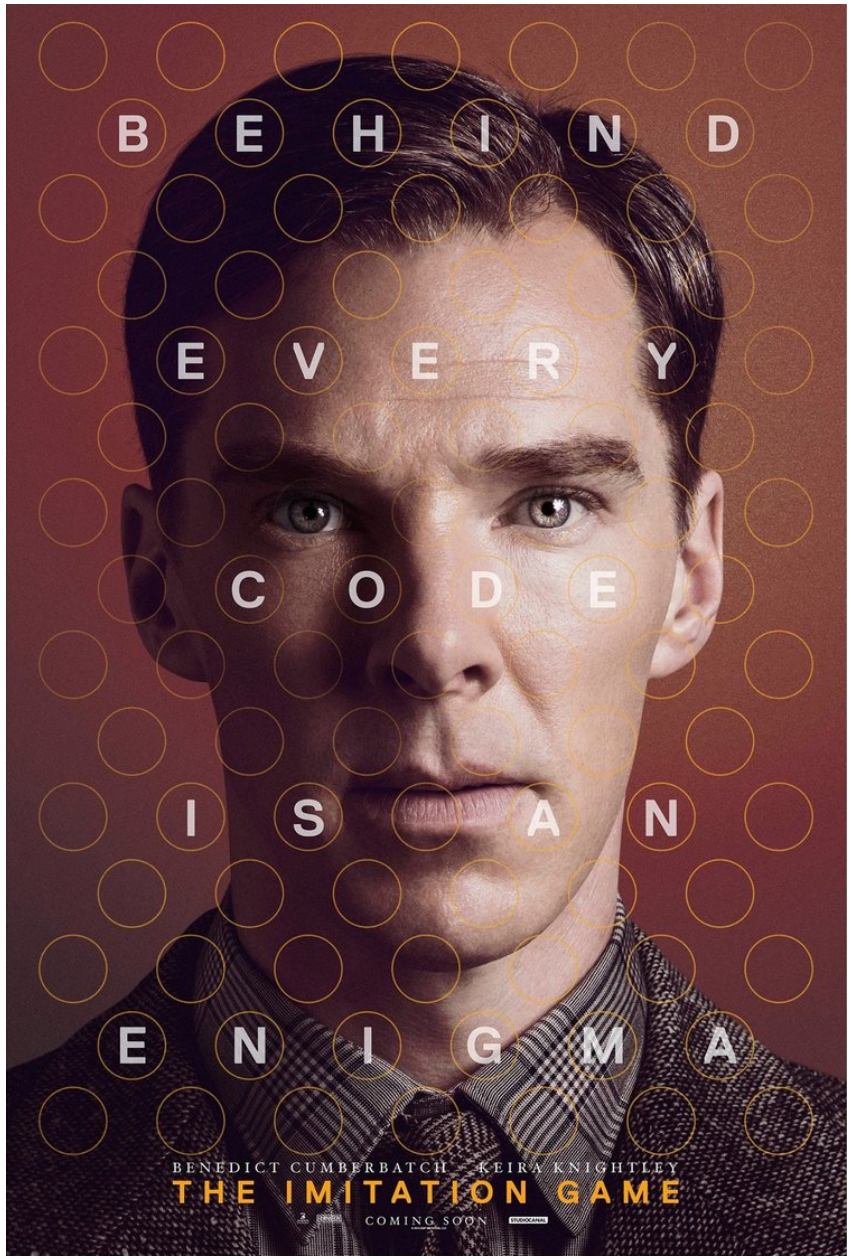
Chi capisce a fondo i cubi di Rubik: gli speedcuber!

Carolina Guidetti è una speedcuber italiana ed è quindi in grado di capire il numero di generatori necessario per tornare alla posizione iniziale molto in fretta

https://www.youtube.com/c/carolinaunarealtaalcubo

Crittografia

Cos'è la crittografia?



Cos'è la crittografia?

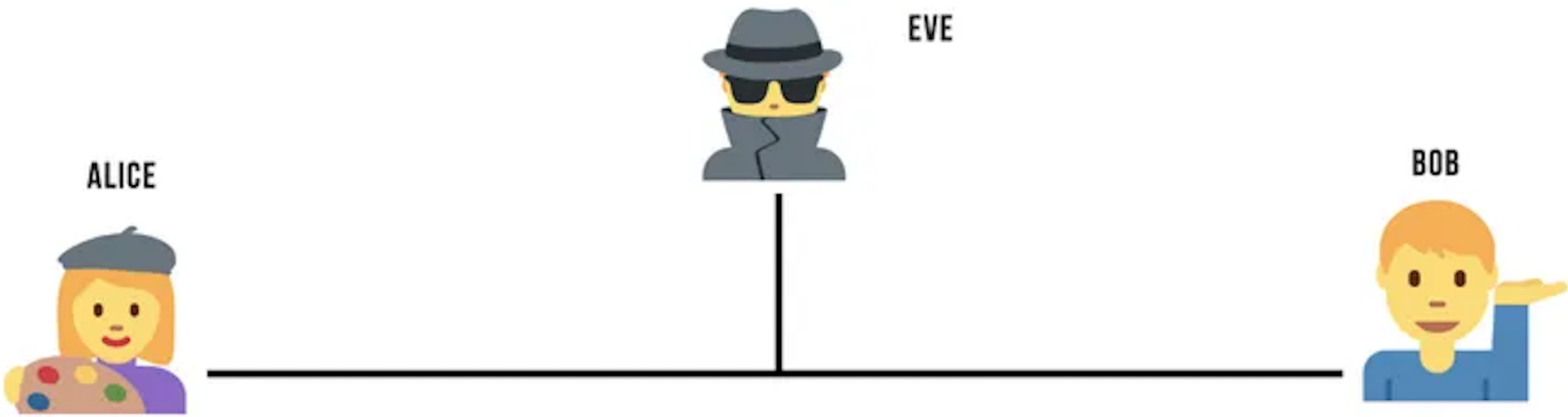
Cos'è la crittografia?

Cos'è la crittografia?

Cos'è la crittografia?

Siamo più precisi

Protagonisti di uno scambio di messaggi in crittografia



Abbiamo due parti (Alice e Bob) che devono scambiarsi un messaggio e Eve che ascolta tutte le loro comunicazioni.

Protocollo più famoso: la sostituzione di Cesare

Ogni lettera se ne sostituisce un'altra che abbiamo concordato.

$$A \longleftrightarrow D, \quad B \longleftrightarrow E, \quad C \longleftrightarrow F, \quad D \longleftrightarrow G, \ldots$$

Ciao come stai? $\longleftrightarrow$ Fndr frph vzdn?

Protocollo più famoso: la sostituzione di Cesare

Ogni lettera se ne sostituisce un'altra che abbiamo concordato.

$$A \longleftrightarrow D, \quad B \longleftrightarrow E, \quad C \longleftrightarrow F, \quad D \longleftrightarrow G, \ldots$$

$$\text{Ciao come stai?} \longleftrightarrow \text{Fndr frph vzdn?}$$

In questo esempio, abbiamo assegnato ad ogni n-esima lettera la $(n+3)$-esima lettera e ragioniamo nelle **classi di resto modulo 21** cioè nel gruppo $(\mathbb{Z}_{21}, +)$ visto prima nell'orologio.

Si ha $V \longleftrightarrow B$ poiché V è la 20-esima lettera e quindi va nella lettera $\underline{20} + \underline{3} \equiv \underline{2}$.

Protocollo più famoso: la sostituzione di Cesare

Ogni lettera se ne sostituisce un'altra che abbiamo concordato.

$$A \longleftrightarrow D, \quad B \longleftrightarrow E, \quad C \longleftrightarrow F, \quad D \longleftrightarrow G, \ldots$$

$$\text{Ciao come stai?} \longleftrightarrow \text{Fndr frph vzdn?}$$

In questo esempio, abbiamo assegnato ad ogni n-esima lettera la $(n+3)$-esima lettera e ragioniamo nelle **classi di resto modulo 21** cioè nel gruppo $(\mathbb{Z}_{21}, +)$ visto prima nell'orologio.

Si ha $V \longleftrightarrow B$ poiché V è la 20-esima lettera e quindi va nella lettera $\underline{20} + \underline{3} \equiv \underline{2}$.

Osservazione. Questo è il più famoso, ma **non** l'unico modo di cifrare un messaggio! Ad esempio, possiamo fare una qualsiasi sostituzione dove assegniamo ad una lettera dell'alfabeto una ed una sola altra lettera, cioè usiamo una permutazione dell'alfabeto.

Analisi di frequenza

Se Eve legge un messaggio cifrato, si può chiedere a cosa corrisponda ogni lettera.

In italiano ci sono lettere e **digrammi** più frequenti.

Analisi di frequenza

Se Eve legge un messaggio cifrato, si può chiedere a cosa corrisponda ogni lettera.

In italiano ci sono lettere e **digrammi** più frequenti.

Ad esempio, la lettere più frequenti in italiano sono la E, A, I, O, N (in quest'ordine), i digrammi sono ER, ES, ON, RE, EL, EN, DE, DI, SI, TI, LA, AL.

Analisi di frequenza

Se Eve legge un messaggio cifrato, si può chiedere a cosa corrisponda ogni lettera.

In italiano ci sono lettere e **digrammi** più frequenti.

Ad esempio, la lettere più frequenti in italiano sono la E, A, I, O, N (in quest'ordine), i digrammi sono ER, ES, ON, RE, EL, EN, DE, DI, SI, TI, LA, AL.

Eve può leggere un messaggio cifrato e chiedersi quali siano i digrammi e poi iniziare a tradurre un messaggio, così come il fatto che quasi tutte le parole italiane terminano in vocali.

Analisi di frequenza

Se Eve legge un messaggio cifrato, si può chiedere a cosa corrisponda ogni lettera.

In italiano ci sono lettere e **digrammi** più frequenti.

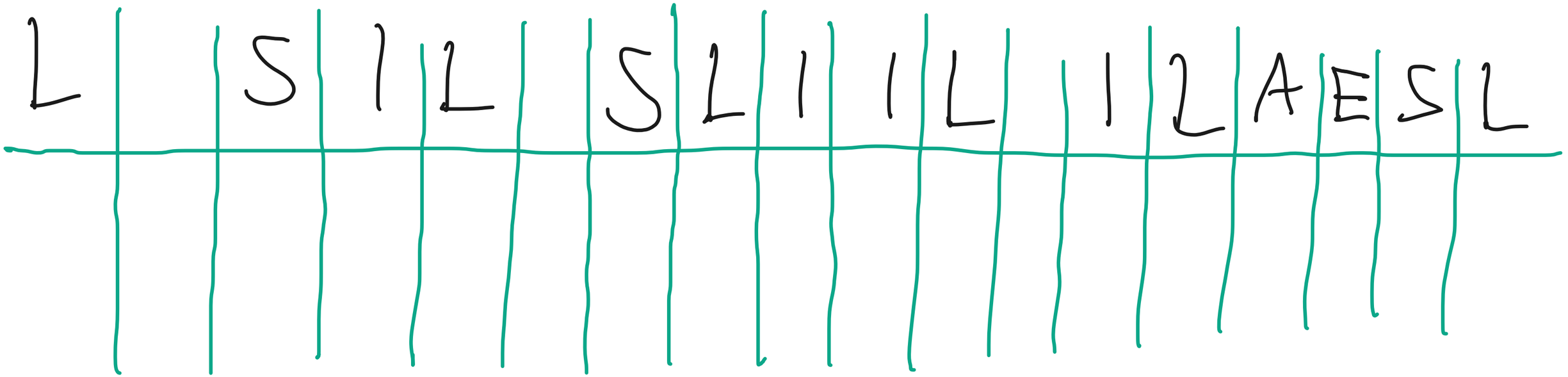
Ad esempio, la lettere più frequenti in italiano sono la E, A, I, O, N (in quest'ordine), i digrammi sono ER, ES, ON, RE, EL, EN, DE, DI, SI, TI, LA, AL.

Eve può leggere un messaggio cifrato e chiedersi quali siano i digrammi e poi iniziare a tradurre un messaggio, così come il fatto che quasi tutte le parole italiane terminano in vocali.

Trasferiamoci altrove!

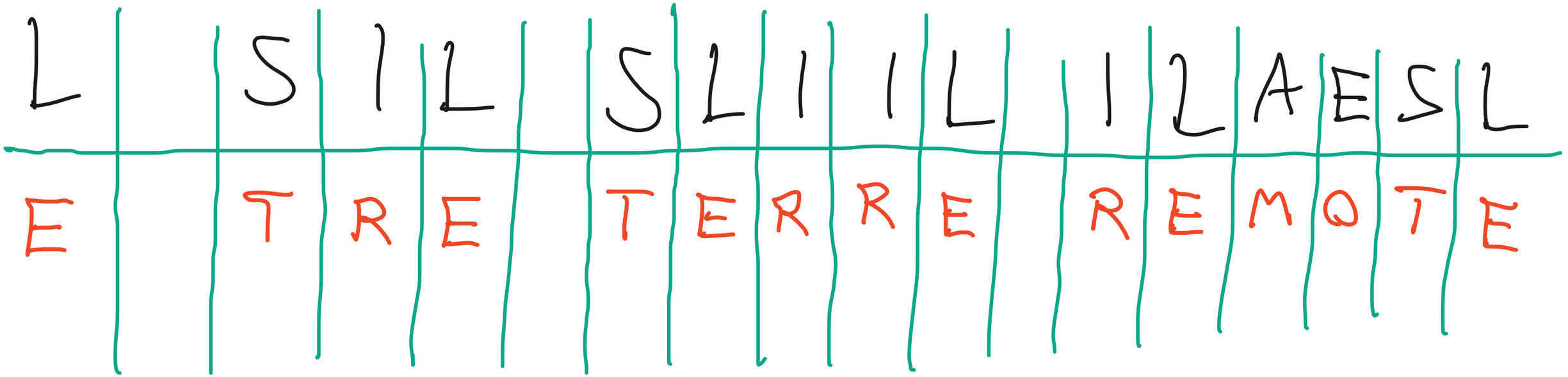
ESERCIZIO

DECODIFICHIAMO QUESTO MESSAGGIO STUDIANDO LETTERE E DIGRAMMI



ESERCIZIO

DECODIFICHIAMO QUESTO MESSAGGIO STUDIANDO LETTERE E DIGRAMMI



Crittografia a chiave pubblica

Scegliere una chiave segreta a partire da una pubblica

Alice e Bob scelgono alcuni dati X che rendono pubblici.

Partendo da X, scelgono un numero segreto K con cui "spostare" ogni messaggio.

Per mandare il messaggio M, Alice manda $Z = M + K$ a Bob.

Bob recupera il messaggio di Alice calcolando $Z - K = M$.

Problema

Scegliere un K che sia difficile per Eve scoprire a partire da X e Z?

Il protocollo di Diffie-Hellman

Alice e Bob

1. Alice e Bob scelgono e **rendono pubblico** un numero primo p
2. Alice e Bob scelgono e **rendono pubblico** un g di $\mathbb{Z}_p$ **primitivo**, cioè tale che $\{\underline{1}, g, g^2, g^3, \ldots, g^{p-2}\} = \{\underline{1}, \underline{2}, \ldots, \ldots, \underline{p-1}\} = \mathbb{Z}_p \setminus \{\underline{0}\}$
3. Alice sceglie **segretamente** un $1 \leq m \leq p-2$ e manda g^m (modulo p) a Bob
4. Bob sceglie **segretamente** un $1 \leq n \leq p-2$ e manda g^n (modulo p) ad Alice
5. Alice e Bob trovano la chiave segreta $K := (g^m)^n = (g^n)^m = g^{mn}$ (modulo p)

Il protocollo di Diffie-Hellman

Alice e Bob

1. Alice e Bob scelgono e **rendono pubblico** un numero primo p
2. Alice e Bob scelgono e **rendono pubblico** un g di $\mathbb{Z}_p$ **primitivo**, cioè tale che $\{\underline{1}, g, g^2, g^3, \ldots, g^{p-2}\} = \{\underline{1}, \underline{2}, \ldots, \ldots, \underline{p-1}\} = \mathbb{Z}_p \setminus \{\underline{0}\}$
3. Alice sceglie **segretamente** un $1 \leq m \leq p-2$ e manda g^m (modulo p) a Bob
4. Bob sceglie **segretamente** un $1 \leq n \leq p-2$ e manda g^n (modulo p) ad Alice
5. Alice e Bob trovano la chiave segreta $K := (g^m)^n = (g^n)^m = g^{mn}$ (modulo p)

Eve

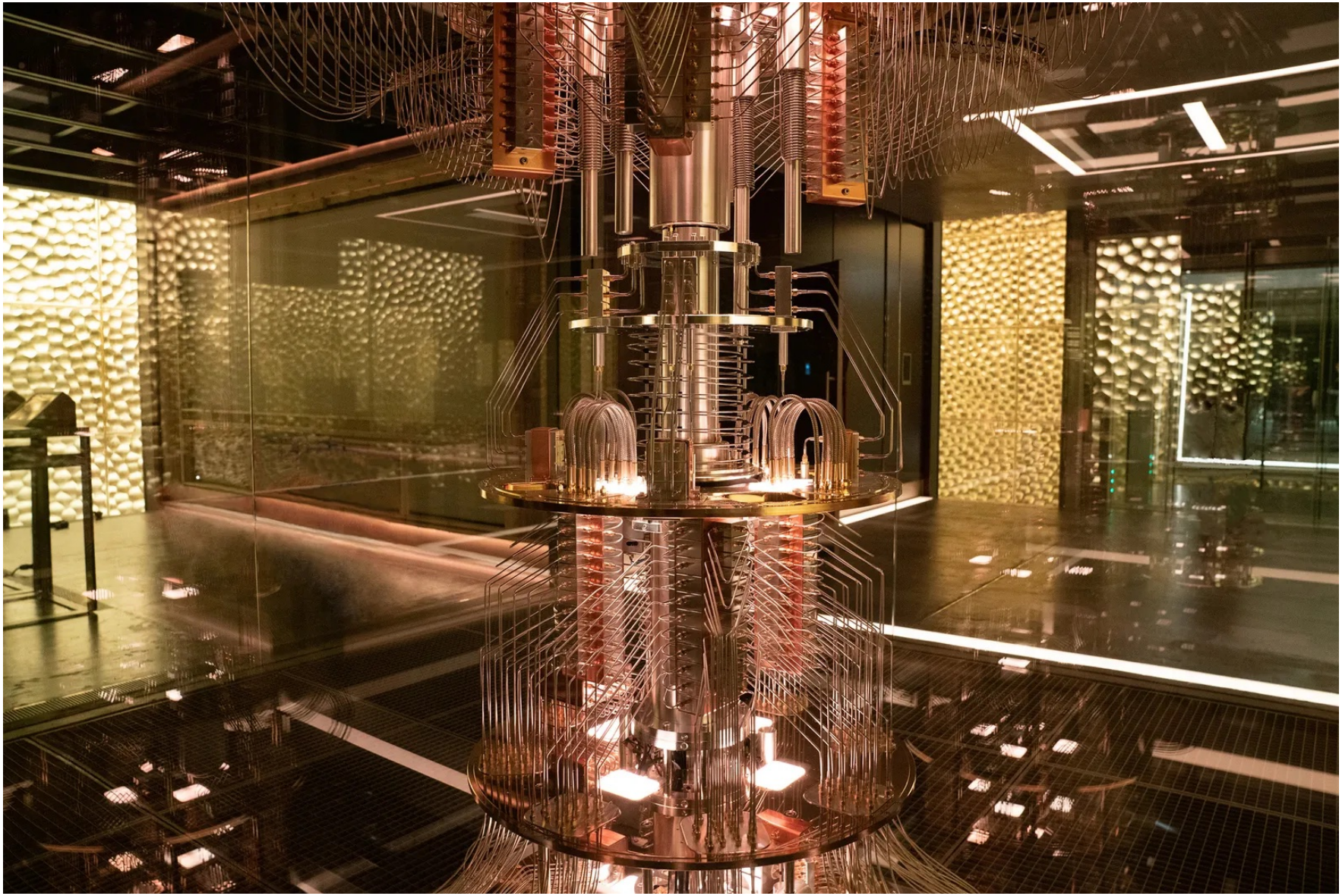
- Eve possiede $p, g, g^m \pmod p, g^n \pmod p$ e risolve il **problema del logaritmo discreto**, cioè dato $h = g^m$, deve calcolare "$m = \log_g(h)$".

Il protocollo di Diffie-Hellman

$$964274047248418797145090983157$$
$$197980855078966882276492572788$$
$$532954904112655338439361306213$$
$$898569516593744267391754033306$$
$$465125919199692703323878557833$$
$$023573312685002670662846477592$$
$$597659826113460619815244721311$$

Crittografia quantistica

Computer quantistici... Ancora non ci siamo, ma...



Maggiori informazioni

1. Su Simmetrie e Gruppi

   http://web.math.unifi.it/users/casolo/dispense/algebra1_19.pdf

   http://web.math.unifi.it/users/casolo/dispense/algebra2_2019.pdf

2. Sulla formula di Burnside

   https://en.wikipedia.org/wiki/Burnside%27s_lemma

3. Sul cubo di Rubik

   http://math.fon.rs/files/DanielsProject58.pdf

   https://web.mit.edu/sp.268/www/rubik.pdf

   https://people.math.harvard.edu/~jjchen/docs/Group%20Theory%20and%20the%20Rubik%27s%20Cube.pdf

4. Su Crittografia

   https://amslaurea.unibo.it/id/eprint/1254/

Grazie della vostra attenzione!