

# Définitions

## Homomorphisme

- Un **homomorphisme** entre deux structures  $(A, \bullet : A \times A \rightarrow A)$  et  $(B, \star : B \times B \rightarrow B)$  est une application  $f : A \rightarrow B$  telle que  $\forall a_1, a_2 \in A$  on a

$$f(a_1 \bullet a_2) = f(a_1) \star f(a_2)$$

- Par exemple  $f(x) = e^x$  est un homomorphisme  $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \times)$  puisque  $\forall x, y \in \mathbb{R}$

$$e^{x+y} = e^x \times e^y$$

# Définitions

## Chiffrement homomorphe

- Un schéma est homomorphe si sa fonction de chiffrement est un homomorphisme