

# Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

$$\mathcal{R} = \mathbb{Z}_q[X]/(X^N + 1)$$

$$\Phi_M(X) = X^N + 1$$

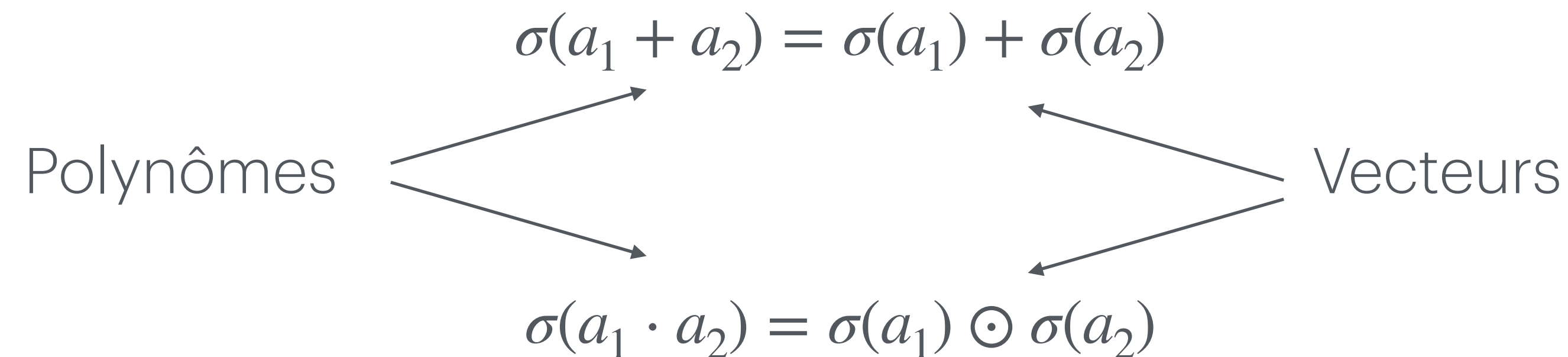
$$M = 2N$$

- Un polynôme  $a(x) \in \mathbb{C}[X]/\Phi_M(X)$  peut être plongé dans  $\mathbb{C}^N$

$$\sigma : \mathbb{C}[X]/\Phi_M(X) \rightarrow \mathbb{C}^N$$

$$a(x) \mapsto^\sigma \left( a(\zeta_M^k) \right)_{k \in \mathbb{Z}_M^\times}$$

- Avec  $\zeta_M^k$  les  $N$  puissances impaires des racines  $M$ -ième de l'unité



# Racines de l'unité

$$\sqrt[2]{1} = \{\zeta_2^0, \zeta_2^1\}$$
$$= \{\pm 1\}$$

$$\zeta_n^k = e^{\frac{2i\pi k}{n}}$$

$$\zeta_2^1 = e^{\frac{2i\pi}{2}}$$

$$= e^{i\pi}$$

$$= -1$$

