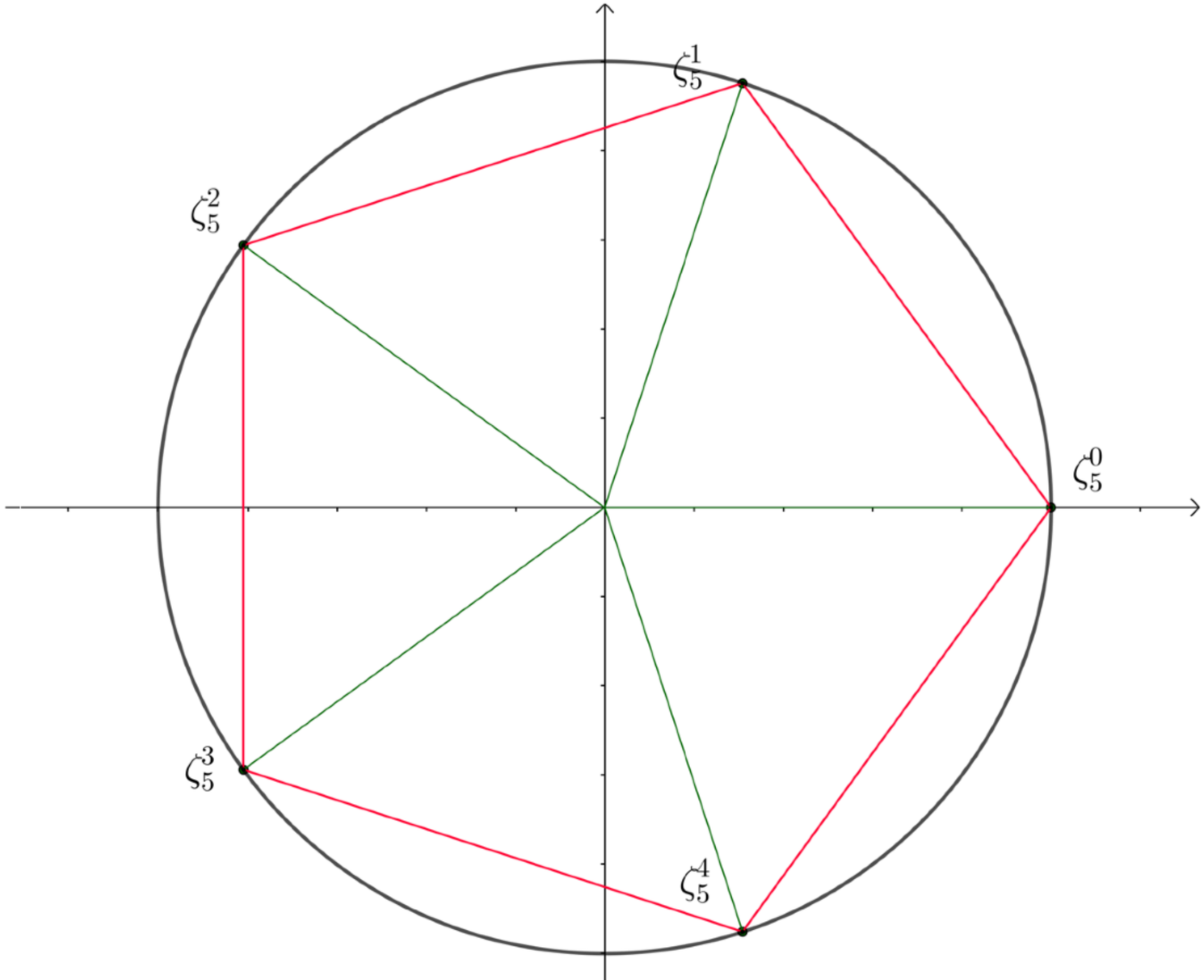
Racines de l'unité

$$\sqrt[5]{1} = \{\zeta_5^k \mid k \in \mathbb{Z}_5\}$$

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

$$\zeta_5^1 = e^{\frac{2i\pi}{5}}$$



Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

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

- On note $\pi : \mathbb{C}^N \to \mathbb{C}^{N/2}$ telle que $\pi(a_1, \ldots a_N) = (a_1, \ldots, a_{N/2})$
- Puisque nos coefficients sont entiers $\forall j \in \mathbb{Z}_M^\times : \zeta_M^j = \overline{\zeta^{-j}_M}$
- Par ex pour $a(x) \in \mathbb{Z}_q[X]/\Phi_8(X)$
- On a 4 coefficients $\Phi_8(X) = X^4 + 1$
- Et $\sigma(a) = (a(\zeta_8^1), a(\zeta_8^3), a(\zeta_8^5), a(\zeta_8^7)) = (z_1, z_2, \overline{z_2}, \overline{z_1})$
- $\pi(\sigma(a)) = (z_1, z_2)$