

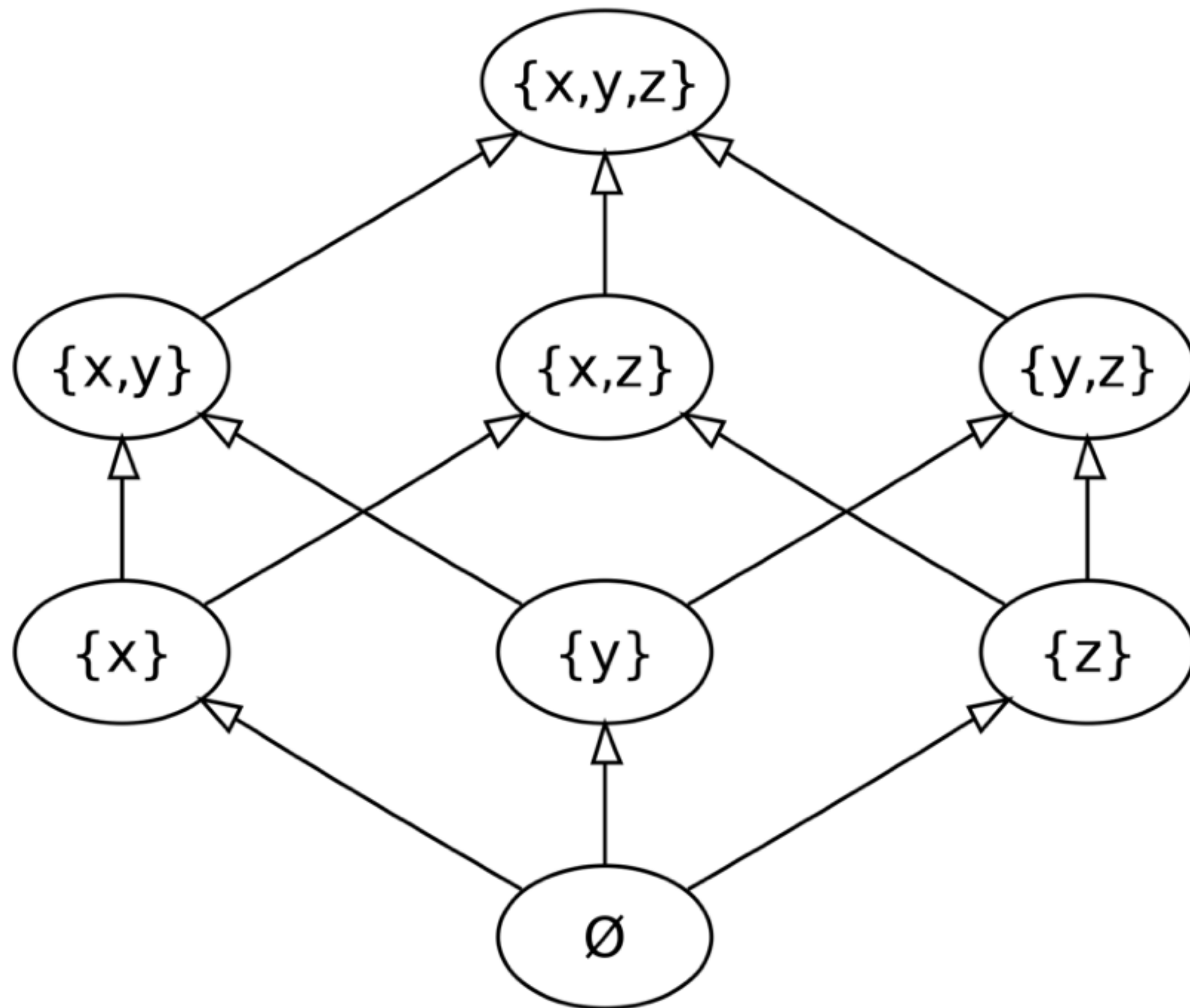
Introduction to Lattice Based Cryptography

XXVIth ISM Graduate Symposium

Félix Larose-Gervais, May 2024

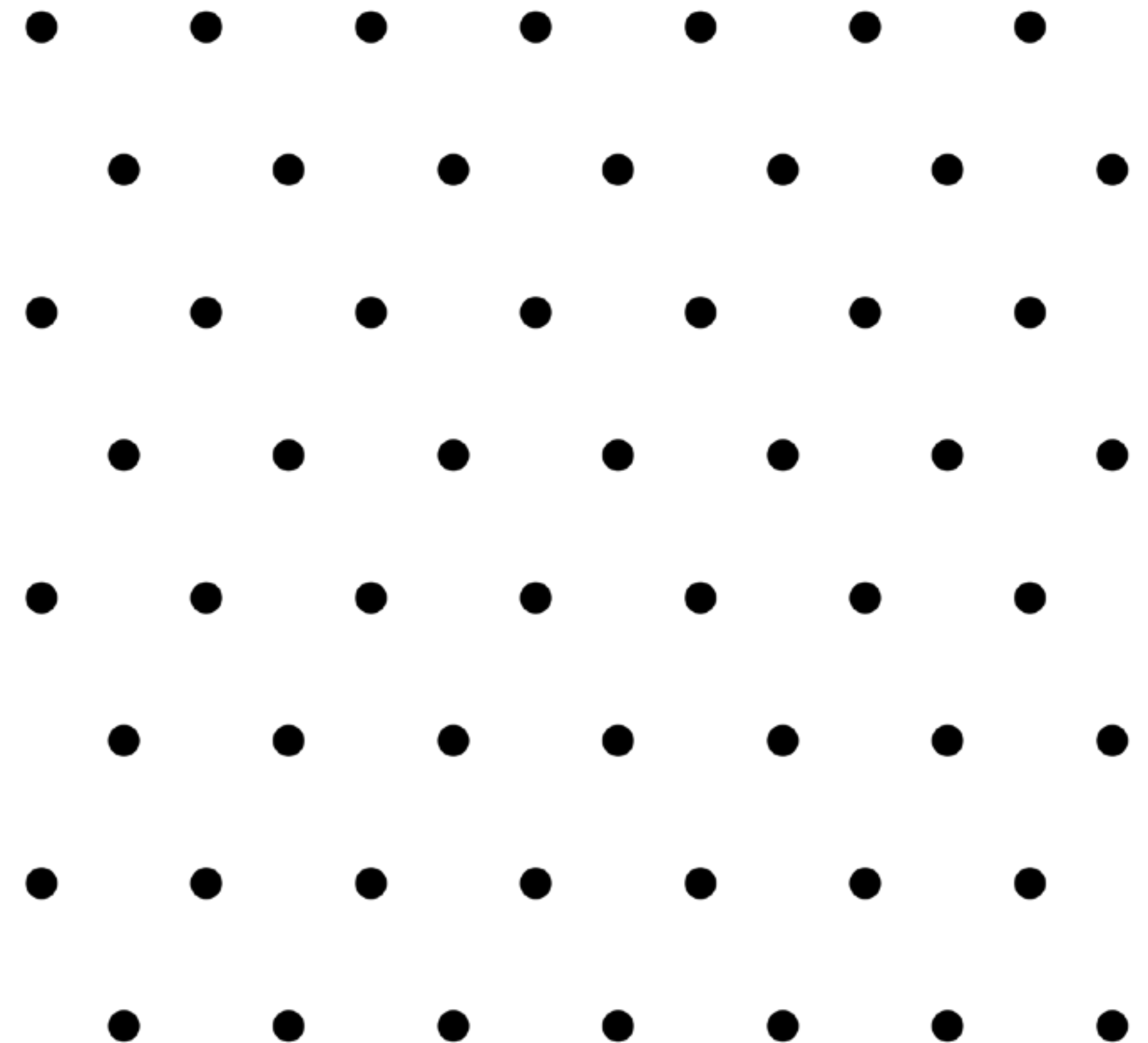
Lattice?

Treillis ❌



[https://en.wikipedia.org/wiki/Lattice_\(order\)](https://en.wikipedia.org/wiki/Lattice_(order))

Réseaux ✅



[https://en.wikipedia.org/wiki/Lattice_\(group\)](https://en.wikipedia.org/wiki/Lattice_(group))