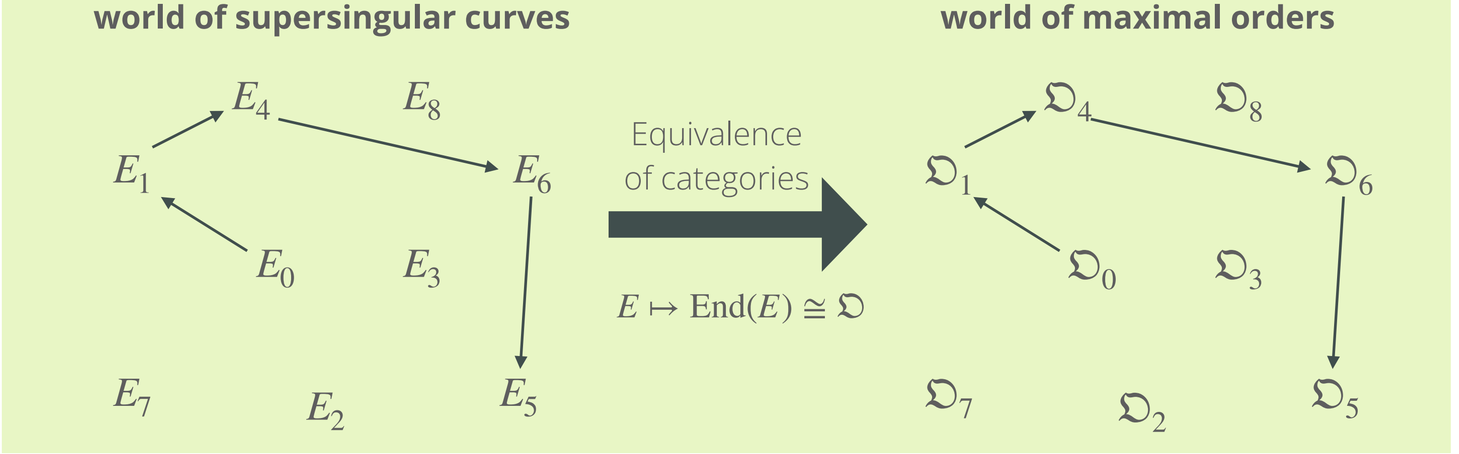
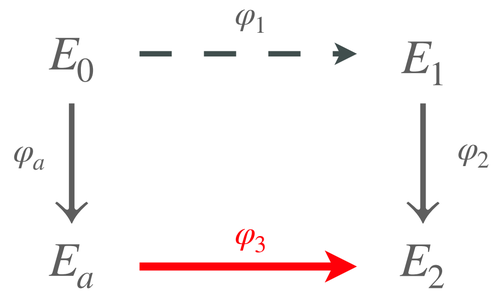
PART 1

SQIsign

Deuring correspondence



computing the signature

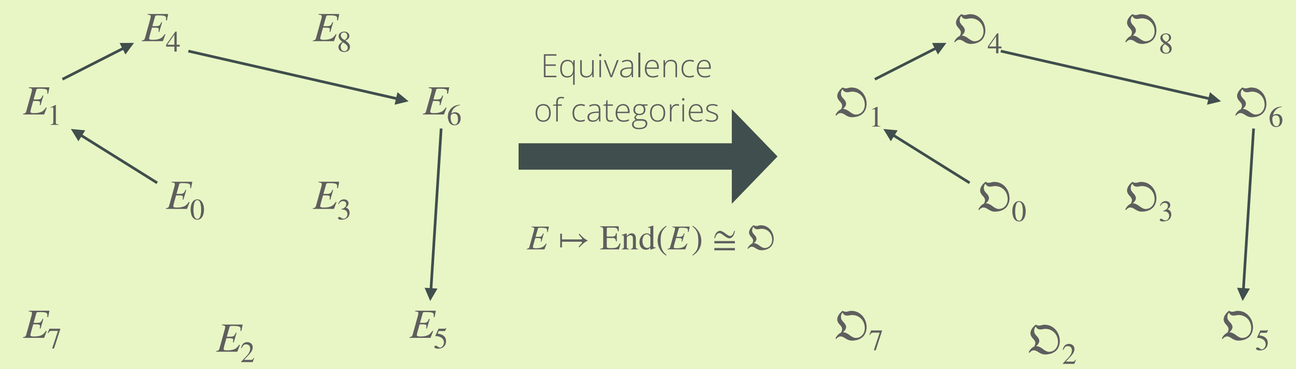


Fact: Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

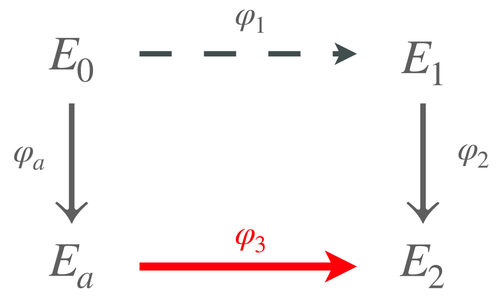
PART 1

SQIsign

Deuring correspondence



computing the signature



Fact: Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

curve-order dictionary

supersingular curves	quaternion orders
curve E (up to Galois conjugacy)	maximal order $\mathfrak{O}$ (up to isomorphism)