$\varphi : E \to E'$

Definition 2. The *kernel* $\ker \varphi$ are the points $P \in E$ that are mapped to infinity $\mathcal{O}' \in E'$. For all isogenies we will care about, the degree $\deg \varphi$ is equal to the size of $\ker \varphi$.

$$\ker \varphi := \{ \ P \in E \ \mid \ \varphi(P) = \mathcal{O}' \ \}.$$

The kernel is *cyclic* if every point in $\ker \varphi$ is a multiple of some *generator* $K \in \ker \varphi$. Then, for $n = \deg \varphi$,

$$\ker \varphi = \{ \ K, \ [2]K, \ [3]K, \ \ldots, \ [n]K \ \}$$

$$\varphi : E \to E'$$

Definition 2. The *kernel* $\ker \varphi$ are the points $P \in E$ that are mapped to infinity $\mathcal{O}' \in E'$. For all isogenies we will care about, the degree $\deg \varphi$ is equal to the size of $\ker \varphi$.

$$\ker \varphi := \{\ P \in E \ \mid\ \varphi(P) = \mathcal{O}'\ \}.$$

The kernel is *cyclic* if every point in $\ker \varphi$ is a multiple of some *generator* $K \in \ker \varphi$. Then, for $n = \deg \varphi$,

$$\ker \varphi = \{\ K,\ [2]K,\ [3]K,\ \ldots,\ [n]K\ \}$$

Theorem 1. If the kernel $\ker \varphi$ is cyclic, with generator $K = (x_K, y_K) \in E(\mathbb{F}_q)$, then it's easy to compute a smooth degree φ: We can compute E' and $\varphi(P)$ for $P \in E(\mathbb{F}_q)$.

KU LEUVEN