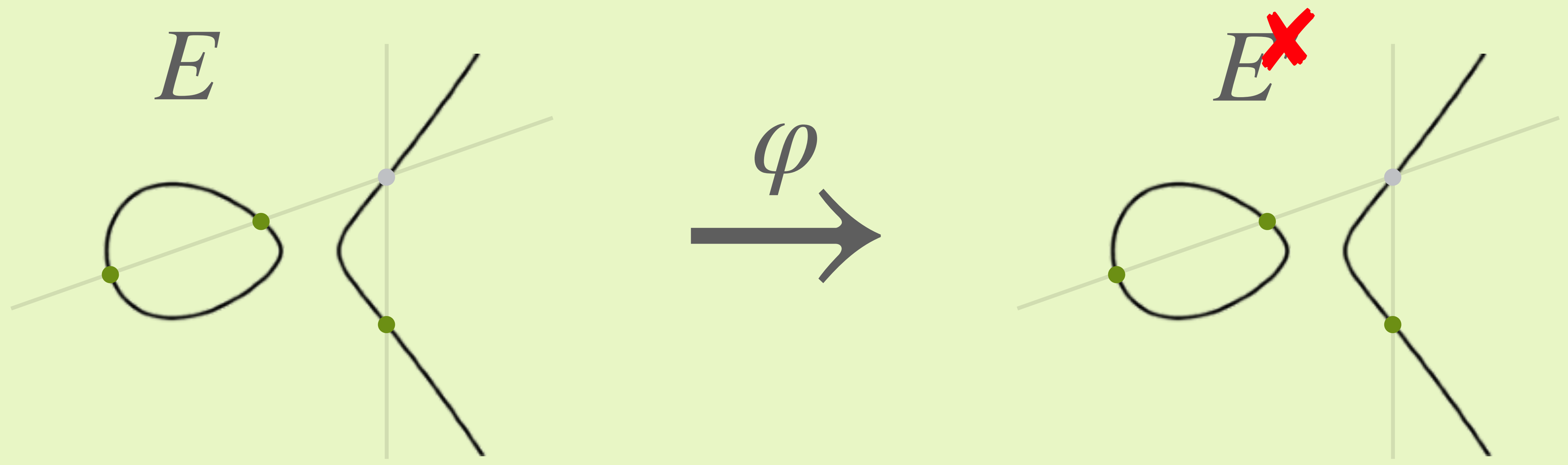
PART 1
SQIsign

endomorphism



~~Isogeny~~ Endomorphism

- "nice" map φ (group homomorphism) between elliptic curves $E \to \cancel{E'}\ E$
- given by rational functions: a point $(x, y) \in E$ is mapped to $(\ f_1(x,y)/f_2(x,y)\ ,\ g_1(x,y)/g_2(x,y)\ )$
- size of $\ker \varphi$ is same as degree of φ!

toy example

$$E : y^2 = x^3 + x \xrightarrow{\ \varphi\ } E : y^2 = x^3 + x$$

$$(x, y) \mapsto \left(\frac{x^4 - 2x^2 + 1}{4(x^3 + x)} , \frac{x^6y + 5x^4y - 5x^2y - y}{8(x^6 + 2x^4 + x^2)} \right) \qquad \text{over } \mathbb{F}_{11}$$

Can check

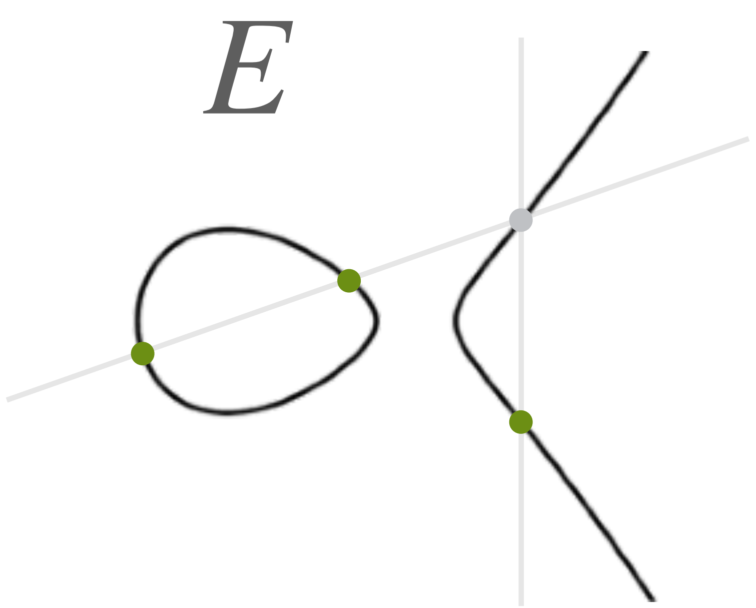
- this is a group homomorphism: $\varphi(\mathcal{O}) = \mathcal{O}$ and $\varphi(P + Q) = \varphi(P) + \varphi(Q)$
- looks difficult… but actually this just the map $[2] : P \mapsto P + P$
- so $[2]$ has kernel $\mathcal{O}, (0,0), (8 + 7i, 0), (3 + 4i, 0)$, degree $[2]$ is 4 = 2^2

second toy example

Frobenius map. $\pi : (x, y) \mapsto (x^q, y^q)$ **always** an endomorphism for E over $\mathbb{F}_q$

PART 1

SQIsign



Given just any E over $\mathbb{F}_{q}$, we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$