Supersingular Isogeny Diffie-Hellman

Valeriia Kulynych

Université de Toulon

May 25th, 2018

Outline

Definition

An elliptic curve is a pair (E, O), where E is a curve of genus 1 and $O \in E$.

Composition law is defined as follows: Let $P, Q \in E$, L be the line connecting P and Q (tangent line to E if $P = Q$), and R be the third point of intersection of L with E. Let L' be the line connecting R and O. Then $P \oplus Q$ is the point such that L' intersects E at R, O and $P \oplus Q$.

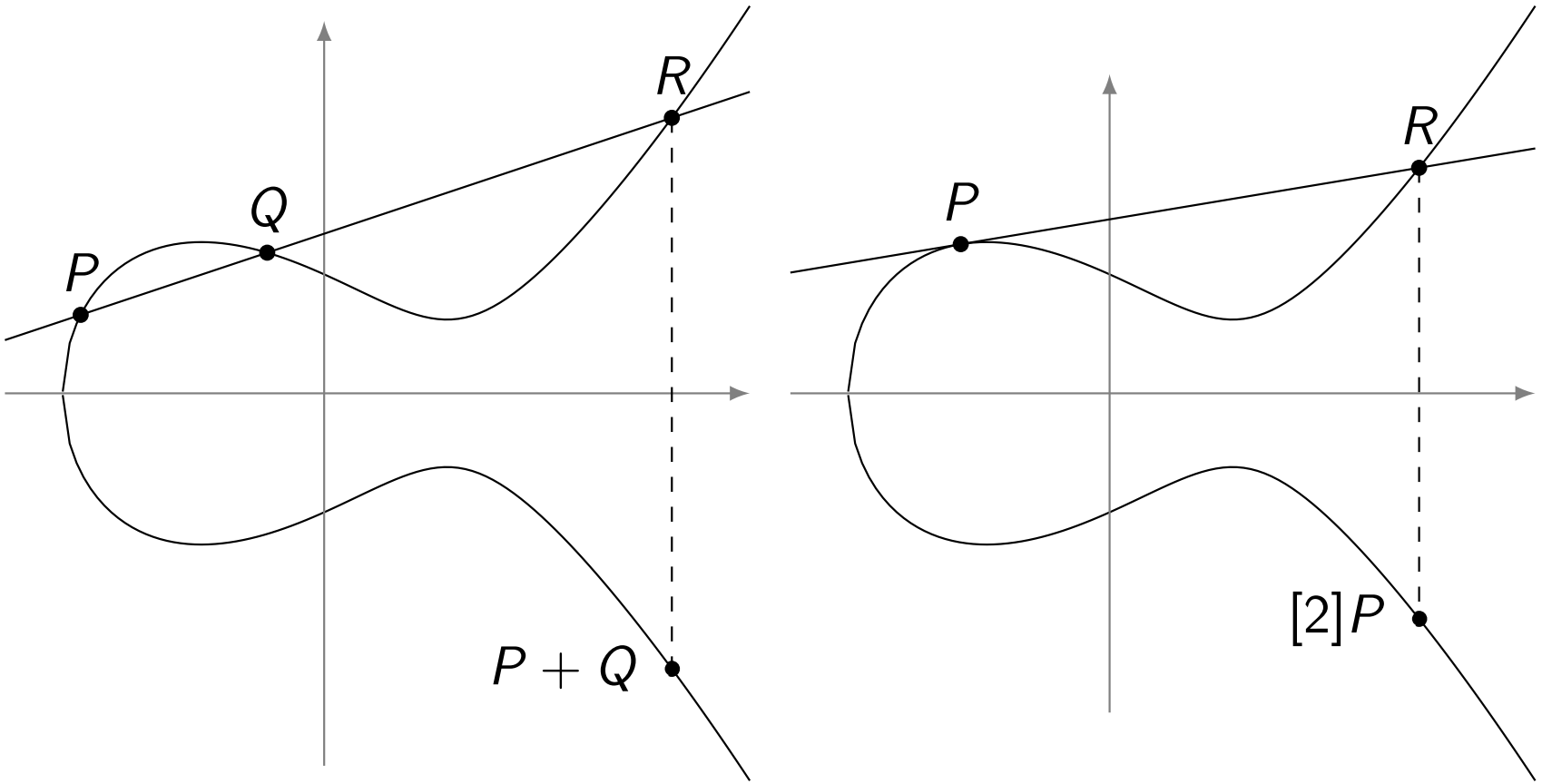

Figure: An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.