Elliptic Curves - Summary

Matteo Durante, s2303760, Leiden University

20th May 2019

Definition 1. Let $\mathbb{K}$ be a field.

- The affine n-space over $\mathbb{K}$ is $\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \overline{K}^n$.
- The rational $\mathbb{K}$-points of $\mathbb{A}^n$ are $\mathbb{A}^n(\mathbb{K}) = \mathbb{K}^n$.
- For a set $S \subset \overline{\mathbb{K}}[x_0, \dots, x_n]$ we define $\mathbb{V}(S) = \{P \in \mathbb{A}^n \mid f(P) = 0 \textit{ for all } f \in S\}$. In particular, if $I = (S)$, then $\mathbb{V}(S) = \mathbb{V}(I)$.
- An algebraic variety over $\overline{\mathbb{K}}$ is a set $\mathbb{V}(I)$ for some prime ideal I of $\overline{\mathbb{K}}[x_0, \dots, x_n]$.
- For a set $V \subset \mathbb{A}^n$, let $\mathbb{I}(V) = \{f \in \overline{\mathbb{K}}[x_0, \dots, x_n] \mid f(P) = 0 \textit{ for all } P \in V\}$.

Theorem 2. *There is a 1:1 correspondence between the varieties in $\mathbb{A}^n$ and the prime ideals of $\overline{\mathbb{K}}[x_0, \dots, x_n]$ given by $V \mapsto \mathbb{I}(V),\ I \mapsto \mathbb{V}(I)$.*

Definition 3. The affine coordinate ring of a variety $V \subset \mathbb{A}^n$ is $\overline{\mathbb{K}}[V] = \overline{\mathbb{K}}[x_1, \dots, x_n]/\mathbb{I}(V)$.