Projective Space and Elliptic Curves

[Koblitz]: I.3

Let K be a field.

- **Affine Space.** The affine n-space over K is the set

$$\mathbb{A}^n(K) := \{(x_1, x_2, \ldots, x_n) : x_i \in K\}.$$

- **Projective Space.** The projective n-space over K is the set

$$\mathbb{P}^n(K) := \{P = (x_0, x_1, x_2, \ldots, x_n) : x_i \in K, P \neq (0, \ldots, 0)\}/\sim,$$

where $(x_0, x_1, x_2, \ldots, x_n) \sim (y_0, y_1, y_2, \ldots, y_n)$ if and only if

$$(x_0, x_1, x_2, \ldots, x_n) = \lambda(y_0, y_1, y_2, \ldots, y_n), \text{ for some } \lambda \in K^\times.$$

An equivalence class is denoted by $[x_0, x_1, x_2, \ldots, x_n]$, and the individual $x_0, \ldots, x_n$ are called homogeneous coordinates for the corresponding point.

Plane Curves

- **Affine plane curves.** Let $f(x, y) \in K[x, y]$ be a non-constant polynomial without repeated factors in $\overline{K}$. The equation $f(x, y) = 0$ gives an affine curve C. Denote

$$C(F) = \{(x, y) \in F^2 : f(x, y) = 0\}$$

  the set of F-rational points on C for a given extension field F of K.
- **Projective plane curves.** Let $\tilde{f}(X, Y, Z) \in K[X, Y, Z]$ be a non-constant homogeneous polynomial without repeated factors in $\overline{K}$. The equation $\tilde{f}(X, Y, Z) = 0$ gives a projective plane curve C. Denote

$$C(F) = \{[X, Y, Z] \in \mathbb{P}^2(F) : \tilde{f}(X, Y, Z) = 0\}$$

  the set of F-rational points on C for the extension field F of K.

Some equivalent definitions. Let K be a field. An elliptic curve over K can be defined as

- a nonsingular projective curve E of genus 1 together with a base point $O \in E(K)$.
- a nonsingular projective plane curve over K of the form

$$E: \; Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

  $a_i \in K$. (Here $\mathcal{O} = [0, 1, 0]$ is the base point.)

Remark. Such equation is the so-called Weierstrass equation.

- We can write the Weierstrass equation for our elliptic curve using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$:

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K.$$

- If $\mathrm{char}(K) \neq 2, 3$, we can simplify the equation as

$$E:\ y^2 = x^3 + ax + b,\ a, b \in K,$$

by using suitable linear substitutions.