Fachbereich Mathematik und Statistik
Dr. Michele Serra
Prof. Dr. Salma Kuhlmann
SS 2023

# Introduction to Elliptic Curves

## Exercise Sheet 6
## Isogenies

Let $K$ be a field with $\operatorname{char} K \neq 2, 3$. Let $E_1 : Y^2 = f_1(X)$ and $E_2 : Y^2 = f_2(X)$ be elliptic curves defined over $K$ in short Weierstraß form, where $f_i(X) = X^3 + a_i X + b_i$, for $i = 1, 2$.

**Exercise 20** (Optional – it just consists of adapting the case of endomorphisms) **(2 points)**
Let $\varphi\colon E_1 \to E_2$ be an isogeny. Show that there exist polynomials $u, v, s, t \in K[X]$ such that $\gcd(u, v) = \gcd(s, t) = 1$ and, for all $(x : y : 1) \in E(\bar{K})$ we have

$$\varphi(x : y : 1) = (u(x)t(x) : s(x)v(x)y : v(x)t(x)) \,. \tag{1}$$

We call this the *canonical* or *standard* form of $\varphi$. We can also use the affine representation

$$\varphi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y\right)$$

notice that, $v$ or $t$ might vanish at some points – you will characterise these in Exercise 22(a).

Let $\varphi\colon E_1 \to E_2$ be an isogeny and let its canonical form be given by (1). Show that:

**Exercise 21** **(2+2 points)**

(a) $v^3 \mid t^2$ and $t^2 \mid v^3 f_1$ .

(b) $v(X)$ and $t(X)$ have the same roots in $\bar{K}$.

**Exercise 22** **(6+1 points)**

(a) For a point $O \neq P = (x, y) \in E(K)$ we have $P \in \ker(\varphi) \iff v(x) = 0$

(b) $\ker(\varphi)$ is a finite subgroup of $E(\bar{K})$.

*Please hand in your solutions by* ***Wednesday, 12 July 2023, 13:30h*** *in the* ***"envelope-postbox" by F409*** *or per e-mail.*