Aufgabe 3.12

Vor.: Sei E/K eine elliptische Kurve und $m \geq 2$ eine ganze Zahl, teilerfremd zu $\mathrm{char}(K)$, falls $\mathrm{char}(K) > 0$.

Beh.: Die kanonische Abbildung

$$\alpha : \mathrm{Aut}(E) \longrightarrow \mathrm{Aut}(E[m])$$

ist für $m \geq 3$ injektiv und für $m = 2$ ist $\ker(\alpha) = \{[1], [-1]\}$.

Bew.: Für alle Isogenien Ψ bezeichne $\widehat{\Psi}$ die duale Isogenie zu Ψ.
Dann erhält man: $[\deg([n] - [l]\Psi)] \overset{(III.6.2a)}{=} ([n] - [l]\Psi)(\widehat{[n] - [l]\Psi}) \overset{(III.6.2b,c)}{=} ([n] - [l]\Psi)(\widehat{[n]} - \widehat{[l]}\widehat{\Psi} \overset{(III.6.2d)}{=} ([n] - [l]\Psi)([n] - [l]\widehat{\Psi}) = [n^2] - [nl]\widehat{\Psi} - [ln]\Psi + [l^2\deg(\Psi)] = [n^2] - [ln](\Psi + \widehat{\Psi}) + [l^2\deg(f)]$
Sei $\mathrm{trace}(\Psi) \in \mathbb{Z}$ definiert durch $[\mathrm{trace}(\Psi)] := \Psi + \widehat{\Psi}$. Dies ist wohldefiniert, da obige Gleichung mit $l = -1, n = 1$ liefert: $[\deg([1]+\Psi)] = [1]+[\deg(\Psi)]+(\Psi+\widehat{\Psi})$, d.h. $\Psi + \widehat{\Psi} = [\deg([1] + \Psi) - 1 - \deg(\Psi)]$.
Obige Gleichung kann man daher auch schreiben als

$$[\deg([n] - [l]\Psi)] = [n^2 - ln\mathrm{trace}(\Psi) + l^2\deg(\Psi)] \tag{1}$$

Dann gilt

$$(\mathrm{trace}(\Psi))^2 \leq 4\deg(\Psi) \tag{2}$$

denn:
$(2) \Leftrightarrow X^2 - \mathrm{trace}(\Psi)X + \deg(\Psi) \geq 0 \qquad \forall X \in \mathbb{R}$
$\Leftrightarrow X^2 - \mathrm{trace}(\Psi)X + \deg(\Psi) \geq 0 \qquad \forall X \in \mathbb{Q}$
$\Leftrightarrow n^2 - \mathrm{trace}(\Psi)nl + \deg(\Psi)l^2 \geq 0 \qquad \forall n, l \in \mathbb{Z}$
$\overset{(1)}{\Leftrightarrow} \deg([n] - [l]\Psi) \geq 0 \qquad \forall n, l \in \mathbb{Z}$ (Gilt wegen der Def. des Grades immer.)

Sei $\phi \in \mathrm{Aut}(E)$, sodass ϕ auf $E[m]$ die Identität induziert, d.h. $\phi \in \ker(\alpha)$. Also induziert $\phi + [-1]$ auf $E[m]$ die Nullabbildung. Da wegen der Voraussetzung an m (III.5.4) liefert, dass $[m]$ separabel ist und offensichtlich $\ker([m]) = E[m] \subseteq \ker(\phi - 1)$ gilt, folgt mit (III.4.11)

$$\phi + [-1] = g \circ [m]$$

für ein $g \in \mathrm{End}(E)$. Also ist $\phi = [1] + g \circ [m]$.
Dann gelten:

$$[\mathrm{trace}(\phi)] \overset{Def.}{=} [1] + g[m] + (\widehat{[1] + g[m]}) \overset{(III.6.2b,c)}{=} [1] + g[m] + \underbrace{\widehat{[1]}}_{=[1]} + \widehat{g}\,\underbrace{\widehat{[m]}}_{=[m]} = \overset{(III.6.2d)}{=} [2] + (g + \widehat{g})[m] = [2 + \mathrm{trace}(g)m] \tag{3}$$

$$[\deg(\phi)] = [\deg([1] + g[m])] \overset{(1)}{=} [1 + \mathrm{trace}(g)m + \deg(g)m^2] \tag{4}$$

Außerdem ist deg(ϕ)=1, da ϕ ein Automorphismus ist.
$\overset{(2)}{\Rightarrow}$ |trace(Φ)| $\leq 2 \overset{(3)}{\Rightarrow}$ |$m$trace(g)| ≤ 4
Und da (4) $\Rightarrow m\text{trace}(g) = -m^2\deg(g)$, folgt $|m^2\deg(g)| \leq 4$.
Im Fall $m \geq 3$ ergibt dies $|\deg(g)| < 1$. Da $\deg(g) \in \mathbb{N}_0$, muss also $\deg(g) = 0$, d.h. $g = [0]$ sein und damit $\phi = [1]$, d.h. $\ker(\alpha) = \{[1]\}$.
Im Fall $m = 2$ muss entweder $g = [0]$ gelten, woraus $\phi = [1]$ folgt, oder $\deg(g) = 1$, woraus mit (4) folgt $\text{trace}(g) = -2$, woraus wiederum mit (3) folgt $\text{trace}(\phi) = 2 + m\text{trace}(g) = -2$. Somit ist $\deg((\phi + [1])^2) = (\deg(\phi + [1]))^2 = (1 + \deg(\phi) + \text{trace}(\phi))^2 = 0 \Rightarrow (\phi + [1])^2 = 0$ Da End(E) nullteilerfrei ist (vgl. III.4.2c), ist also $\phi + [1] = [0]$, d.h. $\phi = [-1]$. Da offensichtlich $[-1]$ die Identität auf $E[m]$ induziert, ist $\ker(\alpha) = \{[1], [-1]\}$. $\square$