Sist.

- Alle isogenier $\phi : E_1 \to E_2$ er gruppehomomorfier.
- Gitt ikkekonstant isogeni ϕ får vi endelig undergruppe $\ker \phi \subset E_1$.

Så på koblingen *isogenier ut av* E_1 med *endelige undergrupper av* E_1. Vi fortsetter å anta at $\operatorname{char} K = 0$.

Proposisjon. *La* $\phi\colon E_1 \to E_2$ *være ikkekonstant isogeni.* $\ker \phi \subset E_1$ *er en endelig abelsk gruppe, og kroppsutvidelsen* $\phi^*\colon \overline{K}(E_2) \to \overline{K}(E_1)$ *er Galois med Galoisgruppe* $\ker \phi$*.*

$$\begin{array}{lll} \ker\phi \subset & E_1 & \overline{K}(E_1) \\ & \downarrow{\scriptstyle \phi} & {\scriptstyle \phi^*}\uparrow \\ & E_2 & \overline{K}(E_2) \end{array}$$

Proposisjon. *Gitt et diagram av isogenier*

$$\begin{array}{ccc} E_1 & \xrightarrow{\ \psi\ } & E_2 \\ & {\scriptstyle \phi}\searrow & \\ & & E_3 \end{array}$$

slik at $\ker \phi \subseteq \ker \psi$*, så finnes en unik* $\lambda\colon E_2 \to E_3$ *slik at* $\lambda \circ \phi = \psi$*.*

$$\begin{array}{ccc} E_1 & \xrightarrow{\ \psi\ } & E_2 \\ & {\scriptstyle \phi}\searrow & \circlearrowleft \ \exists!\,\vdots\,{\scriptstyle \lambda} \\ & & \downarrow \\ & & E_3 \end{array}$$

Teorem. *La* E *være en elliptisk kurve og la* $\Phi \subset E$ *være en endelig undergruppe. Da finnes en unik elliptisk kurve* E' *og en isogeni* $\phi\colon E \to E'$ *slik at* $\Phi = \ker \phi$*.*

$$\begin{array}{lll} \Phi \subset & E_1 & \\ & \exists!\,\vdots\,{\scriptstyle \phi} & \\ & \downarrow & \\ \exists! & E_2 & \ker\phi = \Phi \end{array}$$

Bevis. For hvert punkt $T \in \Phi$ har vi $\tau_T^* \in \operatorname{Aut}(\overline{K}(E)/\overline{K})$, og dette gir en inklusjon $\Phi \subset \operatorname{Aut}(\overline{K}(E)/\overline{K})$. Vi ser på

$$\overline{K}(E)^\Phi = \{f \in \overline{K}(E) \mid \tau_T^*(f) = f, \forall T \in \Phi\} \subset \overline{K}(E)$$

Et resultat fra Galois-teori sier at kroppsutvidelsen $\overline{K}(E)/\overline{K}(E)^\Phi$ er Galois med $\operatorname{Aut}(\overline{K}(E)/\overline{K}(E)^\Phi) = \Phi$.

Spesielt er utvidelsen $\overline{K}(E)/\overline{K}(E)^\Phi$ endelig. Dermed er

$$\operatorname{tr.deg.}(\overline{K}(E)^\Phi/\overline{K}) = \operatorname{tr.deg.}(\overline{K}(E)/K) = 1,$$

så det finnes en unik ikkesingulær kurve E' med $\overline{K}(E') \cong \overline{K}(E)^\Phi$, og en morfi $\phi\colon E \to E'$ slik at $\phi^*\colon \overline{K}(E') \to \overline{K}(E)^\Phi$ identifiserer $\overline{K}(E')$ med $\overline{K}(E)^\Phi$.

Kan sjekke at genus til E' er 1, vi gjør ikke det.

Lar vi $O' = \phi(O) \in E'$, så blir (E', O') en elliptisk kurve, ϕ en isogeni. Vet da ved resultatet over at

$$\mathrm{Aut}(\overline{K}(E)/\phi^*\overline{K}(E')) = \ker\phi,$$

så

$$\Phi = \mathrm{Aut}(\overline{K}(E)/\overline{K}(E)^\Phi) = \mathrm{Aut}(\overline{K}(E)/\phi^*(\overline{K}(E')) = \ker\phi.$$

□

Eksempel. La E_1 være en gitt elliptisk kurve. Hvis $\phi\colon E_1 \to E_2$ er en isogeni av grad 2, hvordan kan E_2 og ϕ se ut? Resultatet over sier at $\phi\colon E_1 \to E_2$ er entydig bestemt av $\ker\phi$.

Hvis $\deg\phi = 2$, så er $|\ker\phi| = 2$, så $\ker\phi \cong \mathbb{Z}/2\mathbb{Z}$. Det betyr at $\ker\phi = \{O, P\}$, hvor $2P = O$, og altså er

$$P \in \{P_1, P_2, P_3\},$$

hvor $P_i = (\alpha_i, 0)$ og α_i er røttene av $x^3 + Ax + B$.

Uformelt oppsummert finnes det tre ulike isogenier ut av E_1 med grad 2, en for hvert 2-torsjonspunkt (unntatt O).

Den duale isogenien.

Teorem (+ Definisjon)**.** *La $\phi\colon E_1 \to E_2$ være en ikkekonstant isogeni. Da finnes en unik isogeni $\hat{\phi}\colon E_2 \to E_1$ slik at*

$$\hat{\phi} \circ \phi = [\deg\phi] \in \mathrm{End}\, E_1.$$

Vi kaller $\hat{\phi}$ den duale isogenien til ϕ (og setter $\widehat{[0]} = [0]$).

Bevis. Vi har isogenier

$$\begin{array}{ccc} E_1 & \xrightarrow{\ \phi\ } & E_2 \\ & \searrow^{[\deg\phi]} & \\ & & E_1 \end{array}$$

Vi vet at $|\ker\phi| = \deg\phi$. For alle $P \in \ker\phi$ har vi da $(\deg\phi)P = 0$, så dermed har vi $P \in \ker[\deg\phi]$. $\ker\phi \subseteq \ker[\deg\phi]$. Altså finnes en unik $\hat{\phi}\colon E_2 \to E_1$ slik at $\hat{\phi} \circ \phi = [\deg\phi]$.

$$\begin{array}{ccc} E_1 & \xrightarrow{\ \phi\ } & E_2 \\ & \searrow^{[\deg\phi]} \ \circlearrowright & \downarrow{\scriptstyle \hat{\phi}} \\ & & E_1 \end{array}$$

□

Fra definisjonen kan vi også gi en konkret beskrivelse av $\hat{\phi}$:

Proposisjon. *La $\phi\colon E_1 \to E_2$ være ikkekonstant isogeni, og la $Q \in E_2$ med $P \in E_1$ slik at $\phi(P) = Q$. Da er*

$$\hat{\phi}(Q) = (\deg\phi)P \in E_1.$$

Bevis. $\hat{\phi}(Q) = \hat{\phi}(\phi(P)) = (\hat{\phi} \circ \phi)(P) = [\deg \phi](P) = (\deg \phi)P.$ □

Proposisjon. *La $\phi\colon E_1 \to E_2$ være en isogeni.*

a) $\hat{\phi} \circ \phi = [\deg \phi] \in \mathrm{End}(E_1)$ og $\phi \circ \hat{\phi} = [\deg \phi] \in \mathrm{End}(E_2)$.

b) Hvis $\psi\colon E_2 \to E_3$ er en isogeni, så er

$$\widehat{(\psi \circ \phi)} = \hat{\phi} \circ \hat{\psi}.$$

Bevis. a) $\hat{\phi} \circ \phi = [m]$ per def. Får da

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi,$$

så siden ϕ er ikkekonstant er $[m] = \phi \circ \hat{\phi}$.

b) Må sjekke at

$$(\hat{\phi} \circ \hat{\psi}) \circ \psi \circ \phi = [\deg(\psi \circ \phi)].$$

Har

$$\begin{aligned}(\hat{\phi} \circ \hat{\psi}) \circ \psi \circ \phi = \hat{\phi} \circ [\deg \psi] \circ \phi = [\deg \psi] \circ \hat{\phi} \circ \phi = [\deg \psi] \circ [\deg \phi] \\ = [(\deg \psi)(\deg \phi)] = [\deg \psi \circ \phi]\end{aligned}$$

□

Proposisjon (Vanskelig, vises ikke)**.** *Hvis $\psi\colon E_1 \to E_2$ er en isogeni, så er*

$$\widehat{(\psi + \phi)} = \hat{\psi} + \hat{\phi}.$$

Proposisjon. *For alle $m \in \mathbb{Z}$, så er $\widehat{[m]} = [m]$ og $\deg[m] = m^2$.*

Bevis. Har at $\widehat{[0]} = [0]$ og $\widehat{[\pm 1]} = [\pm 1]$. Gitt at $\widehat{[m]} = [m]$, så er

$$\widehat{[m+1]} = \widehat{[m] + [1]} = [m] + [1] = [m+1],$$

og tilsvarende for $[m-1]$, så ved induksjon får vi et bevis.

For påstanden om graden vet vi nå at

$$[\deg[m]] = \widehat{[m]} \circ [m] = [m][m] = [m^2].$$

□

Korollar. *For alle $m \in \mathbb{Z}$ er $E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.*

Bevis. Se først på $m = p$ for et primtall p. Siden $E[p] = p^2$, er enten

$$E[p] = \mathbb{Z}/p \oplus \mathbb{Z}/p \text{ eller } E[p] = \mathbb{Z}/p^2$$

Men siden $px = 0$ for alle $x \in E[p]$, må det første tilfellet være det riktige.

For en generell m har vi, for alle divisorer d av m, at $E[d] \subset E[m]$ med

$$E[d] = \{x \in E[m] \mid dx = 0\}.$$

Oppgave: Fullfør beviset ved å vise: Hvis G er en abelsk gruppe med $|G| = m^2$ og for alle divisorer d av m, så er $|\{x \in G \mid dx = 0\}| = d^2$, så må $G = \mathbb{Z}/m \oplus \mathbb{Z}/m$. Bruk at G kan skrives entydig som

$$G = \oplus_{i=1}^{r} \mathbb{Z}/({p_i}^{e_i})$$

og finn begrensninger på hva p_i og e_i kan være. □

Proposisjon. *a)* $\deg \hat{\phi} = \deg \phi$.

b) ϕ er den duale isogenien til $\hat{\phi}$, altså: $\hat{\hat{\phi}} = \phi$.

Bevis. a) Siden $\hat{\phi} \circ \phi = [\deg \phi]$, så er

$$\deg(\hat{\phi}) \deg(\phi) = \deg([\deg \phi]) = (\deg \phi)^2,$$

som gir $\deg(\hat{\phi}) = \deg \phi$.

b) Vi har vist at $\phi \circ \hat{\phi} = [\deg \phi] = [\deg \hat{\phi}]$, som betyr at ϕ er den duale isogenien til $\hat{\phi}$.

□