Sist.

- Definerte *isogeni*, morfi $\phi\colon E_1 \to E_2$ slik at $\phi(O_1) = O_2$.
- *Gruppen* av slike er $\mathrm{Hom}(E_1, E_2)$ med
$$(\phi + \psi)(P) = \phi(P) + \psi(P) \qquad \phi, \psi \in \mathrm{Hom}(E_1, E_2), P \in E_1$$
- Skriver $\mathrm{End}(E) = \mathrm{Hom}(E, E)$, så på $[m] \in \mathrm{End}(E)$, gitt på punkter ved
$$[m](P) = mP.$$
- Viste at hvis $0 \neq m \in \mathbb{Z}$, så er $[m] \neq [0]$.

Proposisjon. *Gruppen* $\mathrm{Hom}(E_1, E_2)$ *er torsjonsfri, dvs. hvis* $0 \neq \phi \in \mathrm{Hom}(E_1, E_2)$ *og* $n \geq 1$, *så er* $n\phi \neq 0$.

Bevis. Har $n\phi = [n] \circ \phi$, hvor $[n] \in \mathrm{End}(E_2)$, siden for alle $P \in E_1$ er
$$(n\phi)(P) = n(\phi(P)) = ([n] \circ \phi)(P).$$
Siden $[n], \phi \neq 0$, er både $[n]$ og ϕ surjektive, så $[n] \circ \phi$ er surjektiv og altså ulik $[0]$. $\square$

Teorem. *La* $\phi \in \mathrm{Hom}(E_1, E_2)$. *Da definerer* ϕ *en gruppehomomorfi, det vil si at for alle* $P, Q \in E_1$ *har vi*
$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Husk følgende generelle konstruksjon:

Definisjon. Gitt en morfi av ikkesingulære kurver $\phi\colon C_1 \to C_2$, er *pushforward langs* ϕ homomorfien $\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ gitt ved
$$\phi_*(\sum_{i=1}^{r} n_i P) = \sum_{i=1}^{r} n_i \phi(P).$$

Proposisjon. *Hvis* $D_1 \sim D_2 \in \mathrm{Div}(C_1)$, *så er* $\phi_*(D_1) \sim \phi_*(D_2)$.

Korollar. *Homomorfien* $\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ *induserer en homomorfi* $\phi_*\colon \mathrm{Pic}(C_1) \to \mathrm{Pic}(C_2)$.

Bevis for Teorem. La $P, Q \in E_1$ og $R = P + Q$. Har da (per def. av $+$)
$$R - O_1 \sim (P - O_1) + (Q - O_1) = P + Q - 2O_1 \in \mathrm{Div}(E_1)$$
Dermed er
$$\phi(R) - O_2 = \phi_*(R - O_1) \sim \phi_*(P + Q - 2O_1) = \phi(P) + \phi(Q) - 2O_2,$$
som betyr at $\phi(R) = \phi(P) + \phi(Q)$. $\square$

Korollar. *Hvis* $\phi \in \mathrm{Hom}(E_1, E_2)$, *så er* $\phi(E_1[k]) \subset E_2[k]$ *for alle* $k \geq 1$.

Bevis. Hvis $P \in E_1$ med $kP = O_1$, så er $k\phi(P) = \phi(kP) = \phi(O_1) = O_2$. $\square$

Teorem. *For en elliptisk kurve E, så er* $\mathrm{End}(E)$ *en (muligens ikke-kommutativ) ring, med sum som tidligere definert, og produkt gitt ved $\phi\psi = \phi \circ \psi$.*

I denne ringen er $\phi\psi \neq 0$ hvis ϕ og $\psi \neq 0$.

Bevis. Vet at $\mathrm{End}(E)$ med $+$ er abelsk gruppe.

Må sjekke

(1) $(\phi\psi)\chi = \phi(\psi\chi)$: Opplagt.

(2) $\exists$ multiplikativ enhet: Ta $[1]$, opplagt at $[1]\psi = \psi = \psi[1]$.

(3) a) $\phi(\psi + \chi) = \phi\psi + \phi\chi$ og b) $(\psi + \chi)\phi = \psi\phi + \chi\phi$.

For *a*), har

$$\phi(\psi + \chi)(P) = \phi(\psi(P) + \chi(P)) = \phi(\psi(P)) + \phi(\chi(P)) = (\phi\psi + \phi\chi)(P),$$

merk at vi bruker at ϕ er en homomorfi. *b*) er tilsvarende, men enklere.

Hvis $\phi, \psi \neq 0$, så er ϕ, ψ surjektive, som betyr at $\phi\psi$ er surjektiv og ulik 0. □

Eksempel. For alle E, gir $n \mapsto [n] \in \mathrm{End}(E)$ en ringinklusjon $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$.

Kan vises at hvis $\mathrm{char}\, K = 0$, så er $\mathrm{End}(E) = \mathbb{Z}$ for "de fleste" E. Hvis $\mathrm{End}(E) \neq \mathbb{Z}$, sies E å *ha kompleks multiplikasjon.*

Eksempel. La E være gitt ved $y^2 = x^3 - x$. Definer en morfi $[i]\colon E \to E$ ved

$$[i] = [-x : iy : 1].$$

Da har vi $[i]^2 = [x : -y : 1] = [-1]$, så $[i] \in \mathrm{End}(E) \setminus \mathbb{Z}$, og vi får en inklusjon $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(E)$.

Isogenier og endelige undergrupper. Antar i denne delen (for enkelhets skyld) at $\mathrm{char}\, K = 0$. Poenget med dette er følgende resultat fra for litt siden.

Proposisjon. *Anta at $\mathrm{char}\, K = 0$, og la $\phi\colon C_1 \to C_2$ være en morfi av ikkesingulære kurver. For $Q \in C_2$, så er $|\phi^{-1}(Q)| = \deg \phi$ unntatt i endelig mange punkter.*

Teorem. *La $\phi\colon E_1 \to E_2$ være en ikkekonstant isogeni. For alle $Q \in E_2$, så er $|\phi^{-1}(Q)| = \deg \phi$.*

Bevis. Homomorfien ϕ er surjektiv. Hvis vi velger $P \in \phi^{-1}(Q)$, så har vi en bijeksjon $\phi^{-1}(O) \leftrightarrow \phi^{-1}(Q)$ gitt ved

$$R \in \phi^{-1}(O_2) \leftrightarrow R + P \in \phi^{-1}(Q).$$

Dermed er $|\phi^{-1}(Q)| = |\phi^{-1}(O_2)|$ for alle Q. Siden det finnes en Q slik at $|\phi^{-1}(Q)| = \deg \phi$, så gjelder dette for alle Q. □

Eksempel. Kan nå beregne $\deg[2] = |\ker[2]| = |E[2]|$. Har $P \in E[2] \Leftrightarrow 2P = O$, som er hvis og bare hvis $P = O$ eller $P = (\alpha, 0)$ med $\alpha^3 + A\alpha + B = 0$. Dermed er $|E[2]| = 4$.

Vi ønsker nå å vise noen resultater som oppsummert sier omtrent at det å spesifisere en isogeni $\phi\colon E_1 \to E_2$ er det samme som å spesifisere en endelig undergruppe $(\ker\phi)$ av E_1.

Teorem. *La $\phi\colon E_1 \to E_2$ være en ikkekonstant isogeni. Da er*

$$\ker\phi \to \operatorname{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2)))$$

gitt ved

$$T \mapsto \tau_T^*\colon \overline{K}(E_1) \to \overline{K}(E_1).$$

en isomorfi av grupper.

Bevis. Sjekker først at $\tau_T^* \in \operatorname{Aut}(\overline{K}(E_1), \phi^*\overline{K}(E_2))$. La $T \in \ker\phi$. Da er $\phi\circ\tau_T = \phi$, siden

$$\phi(\tau_T(P)) = \phi(P+T) = \phi(P) + \phi(T) = \phi(P).$$

Hvis $f \in \overline{K}(E_2)$, så er

$$\tau_T^* \circ \phi^*(f) = f\circ\phi\circ\tau_T = f\circ\phi = \phi^*(f),$$

så $\tau_T^* \in \operatorname{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$.

Har

$$\tau_{T_1}^*\tau_{T_2}^* = (\tau_{T_1}\circ\tau_{T_2})^* = \tau_{T_1+T_2}^*$$

så $T \mapsto \tau_T$ er en gruppehomomorfi.

Siden $|\ker\phi| = \deg\phi \geq |\operatorname{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2)))|$, så holder det å vise at avbildningen $T \mapsto \tau_T^*$ er injektiv. Men hvis $\tau_T^* = \mathrm{id}_{\overline{K}(E_1)}$, så må $\tau_T = \mathrm{id}_{E_1}$, som betyr at $T = O_1$. Altså er avbildningen injektiv. □

Teorem. *La $\phi\colon E_1 \to E_2$ være en ikkekonstant isogeni. Da er kroppsutvidelsen $\phi^*(\overline{K}(E_2)) \subset \overline{K}(E_1)$ en Galois-utvidelse.*

Bevis. Vi har

$$[\overline{K}(E_1) : \phi^*(\overline{K}(E_2))] = \deg\phi = |\ker\phi| = |\operatorname{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))|,$$

som betyr at ϕ^* er Galois. □

Teorem. *La $\phi\colon E_1 \to E_2$ og $\psi\colon E_1 \to E_3$ være ikkekonstante isogenier. Hvis* $\ker\phi \subset \ker\phi$*, så finnes en unik isogeni $\lambda\colon E_2 \to E_3$ slik at $\lambda\circ\phi = \psi$.*

Bevis. Har at $\overline{K}(E_1)$ er en Galois-utvidelse av $\phi^*(\overline{K}(E_2))$ og av $\psi^*(\overline{K}(E_3))$.

Dermed er $\phi^*(\overline{K}(E_2)) = \overline{K}(E_1)^{\ker\phi}$ og $\psi^*(\overline{K}(E_3)) = \overline{K}(E_1)^{\ker\psi}$. Siden $\ker\phi \subset \ker\psi$ har vi da

$$\psi^*(\overline{K}(E_3)) \subseteq \phi^*(\overline{K}(E_2)) \subseteq \overline{K}(E_1),$$

så det finnes en unik $\chi\colon \overline{K}(E_3) \to \overline{K}(E_2)$ slik at $\phi^*\circ\lambda^* = \psi^*$. Vi lar $\lambda\colon E_2 \to E_3$ være bestemt av at $\lambda^* = \chi$. □