Sist.

- Beregnet $\mathrm{Pic}^0(E)$, og viste at $\kappa\colon E \to \mathrm{Pic}^0(E)$ gitt ved
$$\kappa(P) = P - O,$$
er en bijeksjon.
- Siden $\mathrm{Pic}^0(E)$ er abelsk gruppe, blir E via dette abelsk gruppe.
- Ga en geometrisk beskrivelse av gruppeloven: Gitt $P, Q \in E$, er
$$P + Q = R,$$
hvor R er konstruert ved $R' = T(P, Q)$, $R = T(O, R')$.

  Eksempel: Hvis $P = (x, y)$, så er $-P = (x, -y)$.
- Fant formler for $P+Q$, dvs. hvis $P, Q \in E$ med $(x_1, y_1) \in E$ og $Q = (x_2, y_2)$, så er
$$P + Q = (x_3, y_3),$$
med $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = -\lambda x_3 - \nu$, hvor $y = \lambda x + \nu$ er linja gjennom P og Q, $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$.

Proposisjon. *La E være en elliptisk kurve. Det finnes en morfi $-\colon E \to E$ slik at*
$$-(P) = -P \qquad \forall P \in E$$

Bevis. Bruker $x, y \in \overline{K}(E)$, definerer den rasjonale avbildningen
$$- = [x : -y : 1]\colon E \to E.$$
Hvis $P \neq O$, så er x, y regulære, så $-$ er regulær i P, og for $P = (x_0, y_0)$ er $-(P) = (x_0, -y_0) = -P$.

I punktet O bruker vi
$$- = [xy^{-1} : -1 : y^{-1}].$$
Sjekker at xy^{-1} og y^{-1} er regulære og lik 0 i O, så $-(O) = [0 : 1 : 0] = O$. □

Proposisjon. *La $P \in E$. Det finnes en morfi $\tau_P\colon E \to E$ slik at*
$$\tau_P(Q) = P + Q \qquad \forall Q \in E.$$

Bevis. Hvis $P = O$, lar vi $\tau_O = \mathrm{id}_E$.

Ellers, skriv $P = (x_1, y_1)$, la
$$\lambda = \frac{y - y_1}{x - x_1}, \quad \nu = \frac{y_1 x - y x_1}{x - x_1} \in \overline{K}(E).$$

Hvor er λ, ν regulære? For $Q \in E$, er $Q = O$ eller $Q = (x, y)$ for $x, y \in \overline{K}$. Hvis $x \neq x_1$ er da både λ og ν regulære. Altså: λ, μ er regulære i Q i hvert fall hvis $Q \notin \{O, P, -P\}$.

Definer en rasjonal avbildning $\tau_P = [f_0 : f_1 : f_2]\colon E \to E$ ved
$$f_0 = \lambda^2 - x - x_1, \quad f_1 = -\lambda f_0 + \nu, \quad f_2 = 1.$$

Hvis $Q \notin \{O, P, -P\}$, så er f_1, f_2 regulære i Q, så τ_P er regulær i Q. Da er $\tau_P(Q) = Q + P$, ved beregningene fra forrige forelesning:

$$[f_0(Q) : f_1(Q) : 1] = (f_0(Q), f_1(Q)) = P + Q$$

Er τ_P en morfi? Ja, siden E er en ikkesingulær kurve.

I hver av $Q = O, P, -P$ kan vi altså finne en $g \in \overline{K}(E)$ slik at gf_0, gf_1, gf_2 er regulære i Q.

Lar være å sjekke at også for $Q = O, P, -P$ er da

$$\tau_P(Q) = [gf_0(Q) : gf_1(Q) : gf_2(Q)] = Q + P.$$

□

Morfiene $\tau_P \colon E \to E$ for ulike P er slik at for $P, Q \in E$, er

$$\tau_P \circ \tau_Q = \tau_Q \circ \tau_P = \tau_{P+Q}.$$

Spesielt er τ_P for alle P en isomorfi, med invers τ_{-P}, siden $\tau_O = \mathrm{id}_E$.

Proposisjon. *La X være en varietet, og la $\phi, \psi \colon X \to E$ være to morfier. Da finnes en morfi $\phi + \psi \colon X \to E$ slik at*

$$(\phi + \psi)(P) = \phi(P) + \psi(P) \qquad \forall P \in X.$$

Idé til bevis. La $\phi = [f_0' : f_1' : f_2']$, la $\psi = [g_0' : g_1' : g_2']$, med $f_i', g_i' \in \overline{K}(X)$, og anta for enkelhets skyld at $f_2', g_2' \neq 0$. Kan da skrive $\phi = [f_0 : f_1 : 1]$ og $\psi = [g_0 : g_1 : 1]$, med $f_i = f_i'/f_2'$ og $g_i = g_i'/g_2'$.

La $\lambda = \frac{g_1 - f_1}{g_0 - f_0}$, $\nu = \frac{f_1 g_0 - f_0 g_1}{g_0 - f_0} \in \overline{K}(X)$, og definer

$$\phi + \psi = [h_0 : h_1 : 1] \colon X \to E$$

med

$$h_0 = \lambda^2 - g_0 - f_0, \quad h_1 = -\lambda h_1 - \nu.$$

Hvis h_0, h_1 er regulære i $P \in X$, så er

$$(\phi + \psi)(P) = [h_0(P) : h_1(P) : 1] = \phi(P) + \psi(P).$$

Vanskelig: Kan vise at $\phi + \psi$ er regulær overalt og $(\phi + \psi)(P)$ holder for alle $P \in X$. □

Isogenier.

Definisjon. La (E_1, O_1), (E_2, O_2) være to elliptiske kurver, og la $\phi \colon E_1 \to E_2$ være en morfi. Hvis $\phi(O_1) = O_2$ så er ϕ en *isogeni*.

Lemma. *Hvis $\phi \colon E_1 \to E_2$ er en morfi, så er $\tau_{-\phi(O_1)} \circ \phi$ en isogeni.*

Bevis. $\tau_{-\phi(O_1)} \circ \phi(O_1) = \tau_{-\phi(O_1)}(\phi(O_1)) = -\phi(O_1) + \phi(O_1) = O_2$. □

Definisjon. Gitt E_1, E_2, skriver vi $\mathrm{Hom}(E_1, E_2)$ for mengden av isogenier.

Vet at en morfi av kurver $\phi\colon E_1 \to E_2$ er enten konstant eller surjektiv. Har den spesielle isogenien

$$[0]\colon E_1 \to E_2$$

gitt ved

$$[0](P) = O_2 \quad \forall P \in E_1,$$

og alle andre isogenier ϕ er surjektive. Slike ϕ er bestemt av kroppinklusjonen

$$\phi^*\colon \overline{K}(E_2) \hookrightarrow \overline{K}(E_1).$$

Proposisjon. *Gitt $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, ligger $\phi + \psi$ i $\mathrm{Hom}(E_1, E_2)$. Med denne operasjonen blir $\mathrm{Hom}(E_1, E_2)$ en abelsk gruppe.*

Bevis. Må sjekke (1) assosiativitet, (2) $\exists$ enhetselement, (3) $\exists$ inverser.

(1): Rett fram.

(2): $[0]$ er et enhetselement.

(3): Gitt $\phi \in \mathrm{Hom}(E_1, E_2)$, så er $- \circ \phi \in \mathrm{Hom}(E_1, E_2)$ en invers til ϕ, med $-\colon E_2 \to E_2$. □

Definisjon. Skriver $\mathrm{End}(E) = \mathrm{Hom}(E, E)$.

Eksempel. For $m > 0$, definer $[m] = \mathrm{id}_E + \cdots + \mathrm{id}_E \in \mathrm{End}(E)$. For $m < 0$, definer $[m] = -[-m]$.

Konkret er $[m](P) = mP \in E$ for alle P og alle $m \in \mathbb{Z}$.

Har $[m_1] + [m_2] = [m_1 + m_2]$ og $[m_1] \circ [m_2] = [m_1 m_2]$.

Definisjon. Gitt en $m \in \mathbb{Z}$, er gruppa av *m-torsjonspunkter* i E gitt ved

$$E[m] = \{P \in E \mid mP = O\} \subset E.$$

Lemma. *La E være Weierstrass-kruven gitt ved $y^2 - (x^3 + Ax + B)$. Hvis $P \in E$, så er $2P = O$ hvis og bare hvis enten $P = O$ eller $P = (x_0, 0)$, hvor x_0 er rot av $x^3 + Ax + B$.*

Bevis. Hvis $P = O$, så er $2P = O$. Hvis $P \neq O$, så er $P = (x, y)$ og $-P = (x, -y)$. Har $2P = O \Leftrightarrow P = -P \Leftrightarrow y = 0 \Rightarrow x_0^3 + Ax_0 + B = 0$. □

Proposisjon. *For alle $m \in \mathbb{Z}$, så er $[m] \neq [0] \in \mathrm{End}(E)$.*

Bevis. Har $[m] \neq [0] \Leftrightarrow [m]$ er ikke surjektiv. Dermed, hvis $[m_1], [m_2] \neq [0]$, så er $[m_1 m_2] = [m_1] \circ [m_2] \neq 0$, siden komposisjonen av surjektive morfier er surjektiv.

Ved lemmaet over finnes Q slik at $2Q \neq O$, så $[2] \neq [0]$. Dermed er $[2]$ surjektiv, så for alle $n \geq 1$ er

$$[2^n] = [2] \circ \cdots \circ [2],$$

også surjektiv.

Hvis m er odde og $P \in E[2]$, så skriver vi $m = 2k + 1$ og får

$$[m](P) = mP = 2kP + P = O + P = P,$$

altså er $[m] \neq [0]$.

For $0 \neq m \in \mathbb{Z}$ kan vi skrive $m = 2^n k$ med k odde. Siden $[2^n]]$ og $[k]$ er surjektive, så er $[m] = [2^n][k]$ surjektiv, og altså er $[m] \neq [0]$. $\square$