**Picard-gruppa til en elliptisk kurve.** La $(E, O)$ være en elliptisk kurve.

*Spørsmål:* Kan vi beregne (grad 0) Picard-gruppa $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{div}(\overline{K}(E)^*)$?

**Lemma.** *La $P \in E$. Hvis $f \in \mathcal{L}(P)$, så er $f$ konstant.*

*Bevis.* Ved Riemann–Roch er $\dim \mathcal{L}(P) = \deg(P) = 1$, og vi har $1, f \in \mathcal{L}(P)$. Dermed er $f = a \cdot 1$ for en $a \in \overline{K}$. □

**Lemma.** *La $P, Q \in E$ med $P \neq Q$. Da er $P - Q \not\sim 0$.*

*Bevis.* Hvis $P - Q \sim 0$, så finnes en $f \in \overline{K}(E)^*$ slik at $\mathrm{div}(f) = P - Q$. Da er $f \in \mathcal{L}(P - Q) \subseteq \mathcal{L}(P)$, så $f$ er konstant. Altså er $\mathrm{div}(f) = 0$, så $P = Q$. □

**Proposisjon.** *La $D \in \mathrm{Div}^0(E)$. Da finnes et unikt punkt $P \in E$ slik at $D \sim P - O$.*

*Bevis. Det finnes et punkt $P$:* Ved Riemann–Roch er

$$\dim \mathcal{L}(D + O) = \deg(D + O) = 1$$

og dermed finnes $f \in \mathcal{L}(D + O)$. Har

$$\mathrm{div}(f) + D + O \geq 0,$$

altså $\mathrm{div}(f) + D + O = \sum n_i P_i$ med $n_i \geq 0$. Har også

$$\deg(\mathrm{div}(f)) + \deg(D + O) = 0 + 1 = 1,$$

dermed er $\sum n_i = 1$, så $\mathrm{div}(f) + D + O = P$ for et $P \in E$. Dermed er $D \sim P - O$.

*Punktet er unikt:* Hvis $Q - O \sim D$, så er $Q - O \sim P - O$, dermed er $Q \sim P$, dermed er $Q = P$. □

La $\sigma\colon \mathrm{Div}^0(E) \to E$ være avbildingen $\sigma(D) = P$.

**Lemma.** *Avbildningen $\sigma$ er surjektiv.*

*Bevis.* $\sigma(P - O) = P$. □

**Lemma.** *For $D_1, D_2 \in \mathrm{Div}^0(E)$, så er $\sigma(D_1) = \sigma(D_2)$ hvis og bare hvis $D_1 \sim D_2$.*

*Bevis. Hvis:* Opplagt fra definisjonen.

*Bare hvis:* $D_1 - D_2 \sim (\sigma(D_1) - O) - (\sigma(D_2) - O) = 0$. □

**Proposisjon.** *Avbildningen $\sigma\colon \mathrm{Pic}^0(E) \to E$ er en bijeksjon. Inversavbildningen $\sigma^{-1} = \kappa\colon E \to \mathrm{Pic}^0(E)$ er gitt ved*

$$\kappa(P) = P - O.$$

Siden $\mathrm{Pic}^0(E)$ er en abelsk gruppe, blir nå $E$ også en abelsk gruppe:

**Definisjon.** *Gruppestrukteren på en elliptisk kurve* er gitt ved

$$P + Q = \sigma(\kappa(P) + \kappa(Q)).$$

*Merknad.* Hvis $(E, O)$ er definert over $K$, så vil $E(K) \subset E$ danne en undergruppe.

**Geometrisk definisjon av gruppestrukturen.** La nå $(E, O)$ være Weierstrass-kurven gitt ved

$$y^2 = x^3 + Ax + B.$$

Gitt en linje $l \subset \mathbb{P}^2$, så vil $l \cap E$ bestå av 3 punkter (telt med multiplisitet), skriver

$$l \cap E = P_1 + P_2 + P_3$$

**Definisjon.** Gitt to punkter $P, Q \in E$, skriver vi $l(P, Q) \in \mathbb{P}^2$ for linja utspent av $P, Q$ hvis $P \neq Q$, eller for tangentlinja i $P$ hvis $P = Q$. Vi har $l(P, Q) \cap E = P + Q + R$, og skriver $T(P, Q) = R$.[1]

*Eksempel.* $T(O, O) = O$, siden tangentlinja til $O$ er linja i uendelig $l_\infty = \{[\alpha : \beta : 0]\}$, og $l_\infty \cap E = O$.

**Definisjon.** *Komposisjonsloven av punkter på $E$* er operasjonen $\oplus \colon E \times E \to E$ gitt som følger.

Gitt $(P, Q) \in E$, la $R = T(P, Q)$. La $R' = T(O, R)$. Vi setter $P \oplus Q = R'$.

**Proposisjon.** *For komposisjonsloven gjelder*

*a) Hvis $T(P, Q) = R$, så er $(P \oplus Q) \oplus R = O$.*

*b) For alle $P \in E$, så er $O \oplus P = P$.*

*c) For alle $P = (x, y) \in E$, så $P' = (x, -y) \in E$ slik at $P \oplus P' = O$.*

*Bevis.* TEGN OG FORKLAR □

Hvis vi visste at $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$, så ville $\oplus$ definert en gruppestruktur på $E$. Vi kan gjøre mer enn det:

**Proposisjon.** *Den geometriske addisjonen $\oplus$ stemmer overens med Picard-gruppe-addisjonen definert tidligere.*

Først et lemma.

**Lemma.** *Hvis $l$ er en linje i $\mathbb{P}^2$, slik at*

$$l \cap E = P_1 + P_2 + P_3,$$

*så er $P_1 + P_2 + P_3 \sim 3O \in \mathrm{Div}^0(E)$.*

*Bevis.* La $F = aX + bY + cZ$ være ligningen til $l$, og la $f = F/Z$. Da er $f \in \overline{K}(E)$, og $\mathrm{div}(f) = P_1 + P_2 + P_3 - 3O$. Dermed er

$$P_1 + P_2 + P_3 \sim 3O.$$

□

[1] Forelesers notasjon.

*Bevis for proposisjon.* La $P, Q \in E$, la $R = T(P, Q)$, og $R' = T(O, R) = P \oplus Q$. Har (1) $P + Q + R \sim 3O$ og (2) $R + R' + O \sim 3O$. Lignin (1) gir

$$(P - O) + (Q - O) \sim O - R,$$

og (2) gir $O - R \sim R' - O$, altså

$$(P - O) + (Q - O) \sim R' - O = P \oplus Q - O.$$

□

0.1. **Formler for $P + Q$.** Skriver nå $P + Q$ i stedet for $P \oplus Q$.

La $E$ være gitt ved Weierstrass-polynom $f = y^2 - (x^3 + Ax + B)$.

*Spørsmål:* Gitt $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$, kan vi beregne $P_1 + P_2 = (x_3, y_3)$?

*Eksempel.* Hvis $x_1 = x_2$, og $y_1 = -y_2$, så er $T(P_1, P_2) = O$, og vi har $P_1 + P_2 = O$.

Anta $x_1 \neq x_2$. Sett $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, og $\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$, da er

$$y = \lambda x + \nu$$

ligningen til linja $l(P_1, P_2)$ gjennom $P_1$, $P_2$.

**Lemma.** *Hvis $x_1 \neq x_2$, så er*

$$x_3 = \lambda^2 - x_1 - x_2$$

*og*

$$y_3 = -\lambda x_3 - \nu.$$

*Bevis.* Finner først $T(P_1, P_2) = (x_3', y_3')$, siden $(x_3, y_3) = (x_3', -y_3')$. Beregner snittpunktene $l(P_1, P_2) \cap E$. Setter inn

$$y = \lambda x + \nu.$$

i $(x^3 + Ax + B) - y^2$, og får

$$x^3 - \lambda^2 x^2 + (A - 2\lambda)x + B - \nu^2 = (x - x_1)(x - x_2)(x - x_3').$$

Dette gir

$$x_3' = \lambda^2 - x_1 - x_2, \qquad y_3' = \lambda x_3 + \nu$$

som gir $y_3 = -\lambda x_3 - \nu$. □