Sist:

- Jobber med $K = \overline{K} = \mathbb{C}$.
- **Gitter** $\Lambda \subset \mathbb{C}$ en *diskret* undergruppe med $\Lambda \cong \mathbb{Z}^2$.
- **Elliptisk funksjon** = meromorf funksjon f på $\mathbb{C}$ slik at
$$f(z+\omega) = f(z) \quad \forall \omega \in \Lambda$$
- Weierstrass $\wp$-funksjon
$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$
$$\wp'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$$
- Viste
$$\wp'(z)^2 = 4\wp(z)^3 + g_2(\Lambda)\wp(z) + g_3(\Lambda) \quad g_2(\Lambda), g_3(\Lambda) \in \mathbb{C}$$

Vi skal se at dette naturlig gir en bijeksjon mellom $\mathbb{C}/\Lambda$ og en elliptisk kurve, men for beviset tar vi først en omvei og ser på divisorer på $\mathbb{C}/\Lambda$.

Divisorgruppa til $\mathbb{C}/\Lambda$

På nøytaktig samme måte som for en algebraisk kurve, kan vi definere divisorgruppa til $\mathbb{C}/\Lambda$:

Definisjon. Gruppa $\mathrm{Div}(\mathbb{C}/\Lambda)$ er gruppa av formelle lineære summer $\sum n_i(w_i)$, hvor $w_i \in \mathbb{C}/\Lambda$.

Vi kan nå gi parallelle definisjoner av alt det vi tidligere har definert ved divisorer på en algebraisk kurve, ved å la elliptiske funksjoner spille rollen til rasjonale funksjoner:

- **Graden** til en divisor $D = \sum n_i(w_i) \in \mathrm{Div}(\mathbb{C}/\Lambda)$ er $\deg(D) = \sum n_i$.
- $\mathrm{Div}^0(\mathbb{C}/\Lambda) = \{D \in \mathrm{Div}(\mathbb{C}/\Lambda) \mid \deg(D) = 0\}$.
- For en $f \in \mathbb{C}(\Lambda)^*$, er
$$\mathrm{div}(f) = \sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) \in \mathrm{Div}^0(\mathbb{C}/\Lambda).$$
- Avbildningen $\mathrm{div}\colon \mathbb{C}(\Lambda)^* \to \mathrm{Div}^0(\mathbb{C}/\Lambda)$ er en homomorfi, og $\mathrm{div}(f) = 0$ hvis og bare hvis f er konstant.
- Picard-gruppa $\mathrm{Pic}(\mathbb{C}/\Lambda) = \mathrm{Div}(\mathbb{C}/\Lambda)/\mathrm{div}(\mathbb{C}(\Lambda)^*)$, og
$$\mathrm{Pic}^0(\mathbb{C}/\Lambda) = \mathrm{Div}^0(\mathbb{C}/\Lambda)/\mathrm{div}(\mathbb{C}(\Lambda)^*).$$

Lemma. *Hvis $w_1, w_2 \in \mathbb{C}/\Lambda$, så er $(w_1) \sim (w_2)$ hvis og bare hvis $w_1 = w_2$.*

Bevis. La $f \in \mathbb{C}(\Lambda)^*$ være slik at $\mathrm{div}(f) = (w_1) - (w_2)$. Da er f en funksjon av orden ≤ 1, altså konstant, så $\mathrm{div}(f) = 0$. □

Noen prinsipale divisorer. For å forstå hvordan $\operatorname{div}(f)$ ser ut for generelle elliptiske f, begynner vi med å studere $\operatorname{div}(f)$ for noen f relatert til $\wp(z)$ og $\wp'(z)$.

La $\omega_1, \omega_2 \in \Lambda$ være en basis for Λ, og la $\omega_3 = \omega_1 + \omega_2$.

Lemma. *Vi har*

$$\operatorname{div}(\wp'(z)) = \left(\frac{\omega_1}{2}\right) + \left(\frac{\omega_2}{2}\right) + \left(\frac{\omega_3}{2}\right) - 3(0).$$

Bevis. Siden $\wp'(z)$ er en odde elliptisk funksjon, og

$$-\frac{\omega_i}{2} = \frac{\omega_i}{2} \pmod{\Lambda},$$

har vi at

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right),$$

så

$$\wp'\left(\frac{\omega_i}{2}\right) = 0.$$

Siden $\wp'$ har orden 3, så har $\wp'$ maksimalt 3 distinkte nullpunkter i $\mathbb{C}/\Lambda$. Siden $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2}$ er distinkte, har vi altså at nullpunktene til $\wp'$ er nøyaktig disse tre. □

Lemma. *La $w \in (\mathbb{C}/\Lambda) \setminus \{0\}$, og la $f(z) = \wp(z) - \wp(w)$. Da er*

$$\operatorname{div}(f(z)) = (w) + (-w) - 2(0)$$

Bevis. Ordenen til f er 2, så f har to nullpunkter talt med multiplisitet. Vi har alltid $f(w) = 0$. To caser

(1) $w = \frac{\omega_i}{2}$ for en $i \in \{1, 2, 3\}$: Da er $f'(w) = \wp'(w) = 0$, så dermed er w et dobbelt nullpunkt.

(2) $w \neq \frac{\omega_i}{2}$ for noen i: Da er $w \neq -w$, så $f(-w) = f(w) = 0$ og $-w$ er det andre nullpunktet til f.

□

Lemma. *For $w_1, w_2 \in (\mathbb{C}/\Lambda) \setminus \{0\}$, så finnes en elliptisk funksjon g slik at*

$$\operatorname{div}(g) = (w_1 + w_2) + (w_1 - w_2) - 2(w_1).$$

Bevis. Sett $g(z) = f(z - w_1)$ med f som i forrige lemma. □

Proposisjon. *Homomorfien $\operatorname{Div}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$ gitt ved*

$$\sum n_i(w_i) \mapsto \sum n_i w_i$$

er surjektiv, med kjerne $\operatorname{div}(\mathbb{C}(\Lambda)^*)$, dvs. at vi har en gruppeisomorfi

$$\operatorname{Pic}^0(\mathbb{C}/\Lambda) \cong \mathbb{C}/\Lambda.$$

Bevis. Det vanskelige punktet er å vise

$$\sum n_i(w_i) \sim 0 \Leftrightarrow \sum n_i w_i = 0.$$

Gitt en divisor $D = \sum n_i(w_i)$, kan vi bruke den generelle relasjonen[1]

$$(z_1 + z_2) + (z_1 - z_2) \sim 2(z_1)$$

til å vise at $D \sim (\sum n_i w_i) - (0)$, som er lik 0 hvis og bare hvis $\sum n_i w_i = 0$. □

Mer konkret betyr dette at alle $D \in \mathrm{Pic}^0(\mathbb{C}/\Lambda)$ kan representeres som

$$D = (z) - (0)$$

for en $z \in \mathbb{C}/\Lambda$, og $(z_1) - (0) + (z_2) - (0) = (z_1 + z_2) - (0)$.

Proposisjon. *(1) Kurven E_Λ definert av $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ er elliptisk.*

(2) Avbildningen $\phi\colon \mathbb{C}/\Lambda \to E_\Lambda$ definert av

$$\phi(z) = [\wp(z) : \wp'(z) : 1]$$

er en bijeksjon.

(3) Avbildningen bevarer gruppestrukturene.

(4) $E_\Lambda[n] \cong \mathbb{Z}/n \oplus \mathbb{Z}/n$.

(5) Gitt en elliptisk kurve E, finnes det en $\Lambda \subset \mathbb{C}$ slik at $E \cong E_\Lambda$.

(6) Avbildningen ϕ gir en bijeksjon mellom elliptiske funksjoner på $\mathbb{C}/\Lambda$ og rasjonale funksjoner på E_Λ.

Bevis. Må sjekke at $f = 4x^3 - g_2x - g_3$ har 3 distinkte røtter. Siden $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, så har vi

$$\wp'(z) = 0 \Rightarrow \wp(z) \text{ er rot i } f.$$

Vi har vist at $\wp'(\frac{\omega_i}{2}) = 0$ for $i = 1, 2, 3$, og at

$$\wp(z) - \wp(\frac{\omega_i}{2})$$

har dobbelt nullpunkt i $\frac{\omega_i}{2}$. Dermed er $\{\wp(\frac{\omega_i}{2})\}_{i=1,2,3}$ tre distinkte røtter av f.

2) Bildet er opplagt inneholdt i E_Λ.

Vi viser først at ϕ er surjektiv. La $(x, y) \in E$, og se på funksjonen $\wp(z) - x$. Denne er elliptisk og ikkekonstant, så det finnes en z slik at $\wp(z) - x = 0$.

---

[1] Gitt $a, b, c \in \mathbb{C}$, får vi

$$(a) + (b) \sim 2(\frac{a+b}{2})$$
$$(c) + (a+b-c) \sim 2(\frac{a+b}{2})$$
$$\Downarrow$$
$$(a) + (b) - (c) \sim (a+b-c).$$

Med denne relasjonen kan man ved induksjon på n vise at en divisor på formen $\sum_{i=1}^n (z_i) - \sum_{i=1}^n (w_i)$ er rasjonalt ekvivalent til $(\sum_{i=1}^n z_i - \sum_{i=1}^n w_i) - (0)$.

Vi har dermed at $\wp(z) = x$, som siden $(\wp(z), \wp'(z)), (x, y) \in E$ betyr at $\wp'(z) = \pm y$. Hvis $\wp'(z) = -y$, har vi at

$$\phi(-z) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)) = (x, y).$$

For injektivitet: La $w_1, w_2 \in \mathbb{C}/\Lambda \setminus \{0\}$ slik at $\phi(w_1) = \phi(w_2)$. Vi har vist at

$$\operatorname{div}(\wp(z) - \wp(w_1)) = (w_1) + (-w_1) - 2(0),$$

så

$$\wp(w_2) - \wp(w_1) = 0 \Rightarrow w_2 = \pm w_1.$$

Hvis $w_2 = -w_1$, så er $\wp'(w_2) = -\wp'(w_1)$. Da må $\wp'(w_2) = \wp'(w_1) = 0$, som betyr at $w_1, w_2 \in \{\omega_1/2, \omega_2/2, \frac{\omega_3}{2}\}$. Men da er $w_2 = -w_1 = w_1$.

3) Siden ϕ er en bijeksjon, holder det å vise at ϕ^{-1} er en gruppehomomorfi. La $P_1, P_2 \in E$, og la $P_3 = P_1 + P_2$.

Da finnes en $f \in \mathbb{C}(E_\Lambda)$ slik at

$$\operatorname{div}(f) = (P_1 - O) + (P_2 - O) - (P_3 - O) = P_1 + P_2 - P_3 - O.$$

Siden $f \circ \phi$ er en rasjonal funksjon av $\wp, \wp'$, så er den en elliptisk funksjon. Man kan vise at for alle $z \in \mathbb{C}/\Lambda$, så er

$$\operatorname{ord}_z(f \circ \phi) = \operatorname{ord}_{\phi(z)}(f),$$

og dermed er

$$\operatorname{div}(f \circ \phi) = \phi^{-1}(P_1) + \phi^{-1}(P_2) - \phi^{-1}(P_3) - (0),$$

som betyr at $\phi^{-1}(P_3) = \phi^{-1}(P_1) + \phi^{-1}(P_2)$.

4) Beregn gruppen av n-torsjonspunkter i $\mathbb{C}/\Lambda$.

5) Vanskelig, vi viser ikke dette.

6) Hvis $f \in \mathbb{C}(E)$, så er $f \circ \phi$ et rasjonalt uttrykk i $\wp(z), \wp'(z)$, og dermed elliptisk. Vi har påstått (uten bevis) at enhver elliptisk funksjon g er en rasjonal funksjon i $\wp(z)$ og $\wp'(z)$, så dermed er $g \circ \phi^{-1}$ en rasjonal funksjon i x, y på E_Λ. □