Sist: Definerte *elliptisk kurve* = et par (E, O) av ikkesingulær kurve E med genus 1, og et punkt $O \in E$. Hvis E er definert over K og $O \in E(K)$, så sier vi at (E, O) er definert over K.

Påstod at alle elliptiske kurver kan defineres av et *Weierstrass-polynom* f, dvs. $E = V_f \subset \mathbb{P}^2$ med

$$f = y^2 - (x^3 + Ax + B) \qquad A, B \in \overline{K}.$$

Vi bruker $\operatorname{char} K \neq 2, 3$, i det generelle tilfellet ser Weierstrass-polynomet mer komplisert ut.

Punkter i E er $(x, y) = [x : y : 1]$, hvor x, y er løsninger av $f(x, y) = 0$, pluss $O = [0 : 1 : 0]$.

Definerte *diskriminanten* $\Delta(f) = -16(4A^3 + 27B^2)$, og j-invarianten $j(f) = -1728\frac{(4A)^3}{\Delta}$. Viste at $E_1 = V_{f_1}$ og $E_2 = V_{f_2}$ er isomorfe (over $\overline{K}$) hvis og bare hvis $j(f_1) = j(f_2)$.

Definisjon. Hvis E er en elliptisk kurve, så er

$$j(E) = j(f)$$

hvor f er et Weierstrass-polynom for E.

Legendre-formen. Kan faktorisere høyre side av Weierstrass-ligningen over $\overline{K}$ og få

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$$

Proposisjon. *(1) For en elliptisk kurve E, finnes en $\lambda \in \overline{K}$ slik at $E = E_\lambda$, hvor E_λ er kurven definert ved Weierstrass-ligningen i Legendre-form*

$$E_\lambda : y^2 = x(x - 1)(x - \lambda).$$

(2) Vi har

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

Bevis. (1): La E være gitt av Weierstrass-ligningen

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3).$$

Variabelskiftet $x \mapsto x + \lambda_1$ gir ligningen formen

$$y^2 = x(x - \lambda_2')(x - \lambda_3').$$

Variabelskiftet $x \mapsto u^2 x$, $y \mapsto u^3 y$, med $u = (\lambda_2')^{1/2}$, gir ligningen formen

$$u^6 y^2 = u^2 x(u^2 x - \lambda_2')(u^2 x - \lambda_3'),$$

som ved å dele på u^6 gir

$$y^2 = x(x - 1)(x - \lambda_3'').$$

(2): Ligningen

$$y^2 = x(x - 1)(x - \lambda) = x^3 - (1 + \lambda)x^2 - \lambda x$$

blir etter variabelskiftet $x \mapsto x + \frac{1+\lambda}{3}$ til $y^2 = x^3 + Ax + B$, med A og B eksplisitte funksjoner av λ. Sett inn i $j(E) = -1728\frac{(4A^3)}{\Delta}$ og regn ut. $\square$

Fra en elliptisk kurve til en Weierstrass-ligning. Vi skal nå vise at abstrakte elliptiske kurver svarer til kurver definert av Weierstrass-ligninger.

Husk fra tidligere: For $D \in \mathrm{Div}(C)$, så er

$$\mathcal{L}(D) = \{f \in \overline{K}(C) \mid \mathrm{div} f + D \geq 0\}, \quad l(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

Spesielt, hvis $P \in C$ og $n \geq 0$, er

$$\mathcal{L}(nP) = \{f \in \overline{K}(C) \mid f \text{ har pol av orden } \leq n \text{ i } P, \text{ regulær ellers}\}.$$

Teorem (Riemann–Roch for en genus 1 kurve)**.** *Hvis C er en ikkesingulær kurve av genus 1 og $D \in \mathrm{Div}(C)$ er en divisor med $\deg D > 0$, så er*

$$l(D) = \deg D$$

Teorem. *La (E, O) være en elliptisk kurve.*

(a) *Det finnes $x, y \in \overline{K}(E)$, slik at*

$$\phi \colon E \to \mathbb{P}^2, \quad \phi = [x : y : 1]$$

gir en isomorfi fra E til en Weierstrass-kurve

$$C \subset \mathbb{P}^2 \colon y^2 = x^3 + Ax + B,$$

slik at $\phi(O) = [0 : 1 : 0]$.

Vi kaller x, y for Weierstrass-koordinater for E.

(b) *To ulike Weierstrass-koordinater x, y og x', y' for E er relatert ved $x = u^2 x', y = u^3 y'$ for en $u \in \overline{K}$.*

(c) *Hvis en Weierstrass-kurve C som over er ikkesingulær, så er den en elliptisk kurve.*

Merknad. Hvis (E, O) er definert over K, så kan x, y velges slik at $A, B \in K$, og i punkt 2 er da $u \in K$.

Lemma. *Hvis C er en ikkesingulær kurve, $D_1, D_2 \in \mathrm{Div}(C)$, $f_1 \in \mathcal{L}(D_1)$ og $f_2 \in \mathcal{L}(D_2)$, så er $f_1 f_2 \in \mathcal{L}(D_1 + D_2)$.*

Bevis.

$$\begin{aligned} \mathrm{div}(f_1 f_2) + D_1 + D_2 = \mathrm{div}(f_1) + \mathrm{div}(f_2) + D_1 + D_2 \geq 0 \\ (\mathrm{div}(f_1) + D_1) + (\mathrm{div}(f_2) + D_2) \geq 0. \end{aligned}$$

□

Bevis. Vi studerer vektorrommene $\mathcal{L}(nO)$ for $n \geq 0$, disse danner en kjede

$$\overline{K} = \mathcal{L}(0O) \subseteq \mathcal{L}(O) \subseteq \mathcal{L}(2O) \subseteq \cdots$$

For $n \geq 1$, har vi $\dim \mathcal{L}(nO) = \deg(nO) = n$. Vi beskriver basiser for de første rommene

$$\mathcal{L}(0) = \langle 1 \rangle, \text{ siden } l(0) = 1$$
$$\mathcal{L}(O) = \langle 1 \rangle, \text{ siden } l(O) = 1$$
$$\mathcal{L}(2O) = \langle 1, x \rangle, \text{ siden } l(2O) = 2, \text{ velger en vilkårlig } x$$

Siden $x \in \mathcal{L}(2O) \setminus \mathcal{L}(O)$, er $\operatorname{ord}_O(x) = -2$. Videre

$$\mathcal{L}(3O) = \langle 1, x, y \rangle, \text{ siden } l(3O) = 3, \text{ velger vilkårlig } y.$$

Siden $y \in \mathcal{L}(3O) \setminus \mathcal{L}(2O)$, er $\operatorname{ord}_O(y) = -3$.

Vi har $\operatorname{ord}_O(x^a y^b) = 2a + 3b$, så $x^a y^b \in \mathcal{L}((2a+3b)O) \setminus \mathcal{L}((2a+3b-1)O)$. Følger at

$$\mathcal{L}(4O) = \langle 1, x, y, x^2 \rangle$$
$$\mathcal{L}(5O) = \langle 1, x, y, x^2, xy \rangle$$

I $\mathcal{L}(6O)$ har vi de 7 elementene $1, x, y, x^2, xy, y^2, x^3$, så vi får en lineær relasjon mellom disse. Mer presist har vi $y^2, x^3 \in \mathcal{L}(6O) \setminus \mathcal{L}(5O)$, så vi kan finne $a, b \neq 0$, slik at $ay^2 + bx^3 \in \mathcal{L}(5O)$.

La oss omdefinere $x \mapsto -\frac{a}{b}x$, $y \mapsto \frac{a}{b}y$, får da $y^2 - x^3 \in \mathcal{L}(5O)$. Dette betyr at

$$y^2 - x^3 = cxy + dx^2 + ey + fx + g,$$

som vi sist gang viste at vi kan transformere til

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

ved å gjøre noen variabelskifter.

Da har vi vist at $\phi \colon E \to \mathbb{P}^2$ har bilde i kurven

$$C : y^2 = x^3 + Ax + B,$$

Vi må nå vise (1) at $\phi \colon E \to C$ har grad 1, og (2) at C er ikkesingulær.

For (1): ϕ er opplagt ikke konstant, så den er surjektiv. La $Q_1 = (x_0, y_0) \in C$, med $y_0 \neq 0$. Da er $Q_2 = (x_0, -y_0) \in C$, og $(x_0, \alpha) \in C$ hvis og bare hvis $\alpha = \pm y_0$. Et punkt $P \in E$ er slik at $\phi(P) \in \{Q_1, Q_2\}$, hvis og bare hvis $(x - x_0)(P) = 0$.

Men $x - x_0 \in \overline{K}(E)$ har en dobbel pol i O, og er ellers regulær, så den har maks to nullpunkter. Dermed er $|\phi^{-1}(\{Q_1, Q_2\})| \leq 2 \Rightarrow |\phi^{-1}(Q_1)| = |\phi^{-1}(Q_2)| = 1$.

For (1), holder det å sjekke at for $(x_0, y_0) \in C$, så er $\phi^{-1}(x_0, y_0)$ ett eneste punkt. Funksjonen $x - x_0 \in \overline{K}(E)$ har en pol av orden 2 i O, og er ellers veldefinert, så den må ha nullpunkt i to punkter på E eller ett dobbelt punkt. Hvis $x_0^3 + Ax_0 + B \neq 0$, så finnes to punkter i C, altså $(x_0, \pm y_0)$.

For (2), hvis C er singulær, så finnes en rasjonal avbildning $\psi \colon C \to \mathbb{P}^1$ av grad 1. Dermed er $\psi \circ \phi \colon E \to \mathbb{P}^1$ en rasjonal avbildning av grad 1. Men da er E isomorf med $\mathbb{P}^1$, som motsier at E har genus 1.

(b): Variabelskiftet: Vi har at $\{1, x\}$ og $\{1, x'\}$ er to basiser for $\mathcal{L}(2O)$, altså er $x = u_1 x' + r$. Videre har vi at $\{1, x, y\}$ og $\{1, x', y'\}$ er to basiser for $\mathcal{L}(3O)$, altså er $y = u_2 y' + s_2 x' + t$.

Siden vi har $y^2 = x^3 + Ax + B$ skal transformeres til $(y')^2 = (x')^3 + A'x' + B'$, så må relasjonene over forenkles til $x = u^2 x'$ og $y = u^3 y'$.

(c): Hvis C er Weierstrass-kurve. La $\omega = \frac{dx}{y} \in \Omega_C$, da er $\operatorname{div}(\omega) = 0$, så $\mathcal{L}(\omega) = \mathcal{L}(0) = \overline{K}$. $\square$