Sist: Gitt en ikkesingulær kurve C, definerte vi $\operatorname{div}(\omega) \in \operatorname{Div}(C)$ for $\omega \in \Omega_C$, og lot

$$K_C = \operatorname{div}(\omega) \in \operatorname{Pic}(C),$$

veldefinert siden $\operatorname{div}(\omega_1) \sim \operatorname{div}(\omega_2)$ for $\omega_1, \omega_2 \in \Omega_C$. Definerte genus $g(C) = l(K_C) = \dim \mathcal{L}(K_C)$, hvor

$$\begin{aligned} \mathcal{L}(K_C) &= \{f \in \overline{K}(C) \mid \operatorname{div}(f) + \operatorname{div}(\omega) \geq 0\} \\ &\cong \text{vektorrommet av regulære differensialer} \subset \Omega_C. \end{aligned}$$

Eksempel. $g(\mathbb{P}^1) = 0$, siden $\omega \in \Omega_{\mathbb{P}^1}$ regulær $\Rightarrow \omega = 0$.

Definisjon. En *elliptisk kurve* er et par (E, O), hvor E er en ikkesingulær kurve med $g(E) = 1$, og $O \in C$ er et valgt punkt. Hvis E er definert over K og $O \in E(K)$, så er (E, O) en elliptisk kurve definert over K.

Weierstrass-ligninger. Vi skal se at alle elliptiske kurver kan beskrives som kurver i $E \subset \mathbb{P}^2$ definert av en bestemt type ligning, som kalles Weierstrass-ligningen. Den ser slik ut:

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Punktene i E er løsninger $(x, y) = [x : y : 1]$ av denne ligningen, pluss ett punkt "i uendelig", dvs. med koordinater $[\alpha : \beta : 0]$, nemlig $O = [0 : 1 : 0]$.

Feilaktig formulert oppgave: Vis at ligningen til en tredjegradskurve i $\mathbb{P}^2$ som skjærer linja $\{Z = 0\}$ bare i $[0 : 1 : 0]$ har formen over. **Nei, dette stemmer ikke, f.eks. er $y = x^3$ en tredjegradskurve som skjærer linja i uendelig bare i $[0 : 1 : 0]$.**

Riktig oppgave: Vis at hvis

$$\sum_{j=0}^{3} \left(\sum_{i=0}^{3-j} b_{ij} y^i x^j \right)$$

er ligningen til en kurve i $\mathbb{P}^2$ som skjærer $\{Z = 0\}$ bare i $[0 : 1 : 0]$, så er

$$b_{12} = b_{21} = b_{03} = 0.$$

Anta nå at $\operatorname{char} K \neq 2$: Kan da gjøre variabelskifte $y \mapsto y - \frac{a_1x + a_3}{2}$, og får

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Hvis $\operatorname{char} K \neq 3$, kan vi videre gjøre variabelskiftet $x \mapsto x - \frac{a_2'}{3}$, og får da

$$y^2 = x^3 + a_4''x + a_6'',$$

som vi skriver om til

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

Merknad. Vi kommer heretter til å anta $\operatorname{char} K \notin \{2, 3\}$.

Merknad. Vi kan også faktorisere høyre side i Weierstrass-ligningen og få

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3), \qquad \lambda_i \in \overline{K},$$

hvor $\lambda_1 + \lambda_2 + \lambda_3 = 0$.

Definisjon. Vi kaller et polynom f på formen $f = y^2-(x^3+Ax+B)$ et *Weierstrass-polynom.*

Definisjon. Gitt et Weierstrass-polynom f, er *diskriminanten*

$$\Delta(f) = -16(4A^3 + 27B^2)$$

Lemma. *Vi har $\Delta(f) = 0$ hvis og bare hvis $x^3 + Ax + B$ har en dobbel rot (altså hvis det finnes $i \neq j$ slik at $\lambda_i = \lambda_j$).*

Bevis. $x^3 + Ax + B$ har en dobbel rot i $\overline{K}$ hvis og bare hvis det finnes en x som er løsning av x^3+Ax+B og $3x^2+A$, lett å sjekke dette er hvis og bare hvis $\Delta = 0$. □

Proposisjon. *Kurven $E \in \mathbb{P}^2$ gitt ved et Weierstrass-polynom f er singulær hvis og bare hvis $\Delta(f) = 0$.*

I så fall har E nøyaktig ett singulært punkt, $(\alpha, 0)$, hvor α er en dobbel rot av $x^3 + Ax + B$.

Bevis. Kurven E er singulær i $(\alpha, \beta) \in E$ hvis og bare hvis $\frac{\partial}{\partial x}(f)(\alpha, \beta) = \frac{\partial}{\partial y}(f(\alpha, \beta)) = 0$.

Må da ha $\beta = 0$ og $3\alpha^2 + A\alpha = 0$, som sammen med $\alpha^3 + A\alpha + B = 0$ er ekvivalent med at $x^3 + Ax + B$ har en dobbel rot i $(\alpha, 0)$. Dette betyr at $\Delta = 0$.

I punktet $[0 : 1 : 0]$ kan vi bruke koordinater $[x' : 1 : z']$, altså $z' = Z/Y$, $x' = X/Y$. Den homogene formen til f, nemlig

$$ZY^2 - (X^3 + AXZ^2 + BZ^3)$$

gir da den inhomogene ligningen

$$g = z - (x^3 + Axz^2 + Bz^3).$$

Her er $\frac{\partial}{\partial z} g(0, 0) = 1$, så kurven er ikkesingulær i $[0 : 1 : 0]$. □

Merknad. Hvis $A, B \in \mathbb{R}$, kan vi si noe om mengde $E(\mathbb{R})$ ved hjelp av Δ, denne mengden har to sammenhengskomponenter hvis $\Delta(f) > 0$ og én sammenhengskomponent hvis $\Delta(f) < 0$.

To typer singulariteter. Hvis $\Delta = 0$, hvordan ser singularitetene til C ut?

Vi har to tilfeller:

- $A, B \neq 0$, som er hvis og bare hvis $\lambda_1 = \lambda_2 \neq \lambda_3$.
- $A, B = 0$, som er hvis og bare hvis $\lambda_1 = \lambda_2 = \lambda_3 = 0$.

I det første tilfellet kan gjøre variabelskiftet $x \mapsto x + \lambda_1$, og får

$$y^2 - x^2(x + 3\lambda_1),$$

som er lik

$$(y - (3\lambda_1)^{1/2}x)(y + (3\lambda_1)^{1/2}x) + x^3,$$

som betyr at C har en *node* i $(0, 0)$.

Hvis alle $\lambda_i = 0$, er ligningen $y^2 - x^3$, dette kalles en *cusp.*

EN FLOTT TEGNING.

Merknad. Hvis E er singulær (hvis $\Delta = 0$), så finnes det rasjonale avbildninger $\mathbb{P}^1 \to E$ og $E \to \mathbb{P}^1$ som er inverse til hverandre. Det vil si at slike E er birasjonale til $\mathbb{P}^1$.

Definisjon. Gitt en Weierstrass-ligning $y^2 = x^3 + Ax + B$, så er *j-invarianten* lik

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Eksempel. To eksempler skiller seg ut:

- $A = 0 \rightsquigarrow j = 0$
- $B = 0 \rightsquigarrow j = 1728$ (kurven jeg alltid tegner)

Proposisjon. *La (E_1, O_1) og (E_2, O_2) være elliptiske kurver gitt av Weierstrass-ligninger*

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

og

$$y^2 = x^3 + A'x + B.$$

Da er $E_1 \cong E_2$ over K hvis og bare hvis vi kan transformere ligning 1 til ligning to ved variabelskiftet $x \mapsto u^2 x$, $y \mapsto u^3 y$ for en $u \in K$.

Bevis utsatt litt. $\square$

Med andre ord, $E_1 \cong E_2$ (over K) hvis og bare hvis det finnes en $u \in K$ slik at

$$A = u^4 A', B = u^6 B'.$$

Proposisjon. *Hvis E_1, E_2 er kurver gitt av Weierstrass-ligninger f_1, f_2, så er $E_1 \cong E_2$ hvis og bare hvis $j(f_1) = j(f_2)$.*

Bevis. Hvis E_1 er isomorf med E_2, så sendes f_1 til f_2 under en bestemt transformasjon. Men

$$j = 2^8 3^3 \frac{A^3}{4A^3 + 27B^2}$$

er invariant under $A \mapsto u^4 A$, $B \mapsto u^6 B$, så $j(f_1) = j(f_2)$.

Anta nå at $j(f_1) = j(f_2)$. Det betyr enten at $A_1 = A_2 = 0$, eller at

$$\frac{B_1^2}{A_1^3} = \frac{B_2^2}{A_2^3}.$$

Vi må vise at $E_1 \cong E_2$, som skjer hvis det finnes en $u \in \overline{K}$ slik at $A_1 = u^4 A_2$ og $B_1 = u^6 B_2$.

Tilfelle 1: $A_1 = A_2 = 0$: Ta $u = (B_1/B_2)^{1/6}$.

Tilfelle 2: $B_1 = B_2 = 0$: Ta $u = (A_1/A_2)^{1/4}$.

Tilfelle 3: Ingen A_i, $B_i = 0$: Ta $u = (\frac{B_1 A_2}{A_1 B_2})^{1/2}$, og får

$$u^4 A_2 = \frac{B_1^2 A_2^3}{B_2^2 A_1^2} = \frac{B_1^2 A_1^3}{B_1^2 A_1^2} = A_1,$$

tilsvarende får vi $u^6 B_2 = B_1$. □

Proposisjon. (1) *Hvis E er en Weierstrass-kurve definert over K, så er $j(E) = j(f) \in K$.*

(2) *For ethvert element $j \in K$, så finnes det en elliptisk kurve E definert over K med $j(E) = j$.*

Bevis. (1) er opplagt fra definisjonen av j.

For (2), må vi finne $A, B \in K$ slik at

$$2^6 3^3 \frac{A^3}{4A^3 - 27B^2} = j.$$

Hvis $j = 0$, sett $A = 0$, $B = 1$. Hvis $j = 1728$, sett $B = 0$, $A = 1$. Ellers reduserer ligningen til

$$\frac{B^2}{A^3} = \alpha,$$

med $0 \neq \alpha \in K$, og vi kan sette $B = A = \alpha^{-1}$. □