-1-
Ell KK
V11

<u>Stichworte</u>: • Def. elliptische Kurve, lange Weierstraßform
• $\mathcal{O} = [0:1:0]$ liegt auf allen elliptischen Kurven in langer Weierstraßform
• Kurze Weierstraßform für char $k \neq 2$ und für char $k \neq 2$ und $\neq 3$ mit Beweis
• Def. j-Invariante und Diskriminante

---

§2.4 Elliptische Kurven

2.4.1 Definition elliptischer Kurven und vereinfachte Weierstraßgleichungen

Wir geben nun die Definition einer elliptischen Kurve. Sei k ein Körper.

1) <u>Def.</u>: Eine elliptische Kurve $E(k)$ ist eine nichtsinguläre, irreduzible projektive Kurve vom Grad 3, die einen (k-rationalen) Wendepunkt enthält.

2) <u>Bem.</u>: • Es reicht, die Wendepunktbedingung durch $E(k) \cap \mathbb{P}^2(k) \neq \emptyset$ zu ersetzen (ist aber aufwendig zu zeigen, lassen dies deswegen sein.) • Eine Kurve C heißt irreduzibel, wenn sie nicht die Vereinigung zweier Kurven $\neq C$ ist. Z.B. ist $C_F(k)$ mit $F(X,Y,Z) = XY$ reduzibel.

3) <u>Bem.</u>: Durch eine sogenannte birationale Transformation kann angenommen werden, dass der Wendepunkt $\mathcal{O} = [0:1:0]$ ist. Eine Übungsaufgabe zeigt, dass dann die Kurven-gleichung die folgende vereinfachte Form hat:

4) <u>Def.</u>: Eine elliptische Kurve $E_F(k)$ ist eine nicht-singuläre, projektive ebene Kurve $C_F(k) \subseteq \mathbb{P}^2(k)$, wobei F ein homogenes Polynom vom Grad 3 der Form

$$\circledast: F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

ist mit Koeffizienten $a_1, a_2, a_3, a_4, a_6 \in k$. Ist F klar, schreiben wir $E(k)$.

4) <u>Bem.</u>: • Die Monome X^2Y, Y^3, XY^2 brauchen also nicht vorzukommen.
• Die Numerierung der Koeffizienten ist historisch bedingt.
• Die affine Version lautet also:

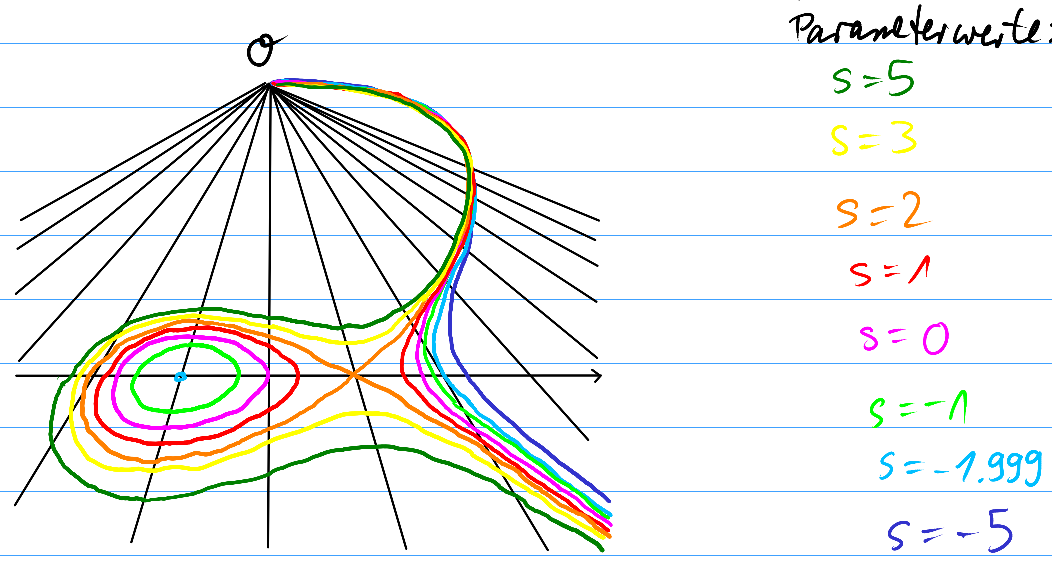
$$\circledast_{\text{affin}}: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Die Form $\circledast$ nennen wir auch die lange Weierstraßform, das Polynom heißt langes Weierstraßpolynom.
• Wir werden sehen, dass man dies auf eine noch einfachere Form bringen kann.

5.) **Bem.:** Welche Punkte liegen auf $E(k)$, die nicht affin sind?
Ist $P = [r:s:0] \in \mathbb{P}^2(k) \setminus \mathbb{A}^2(k)$ ein solcher Punkt, dann ergibt Einsetzen in ⊗ dann $r^3 = 0$, dann muss $s \neq 0$ sein, d.h. $P = [0:s:0] = [0:1:0]$.
Diesen unendlich fernen Punkt, der allen elliptischen Kurven gemeinsam ist, nennen wir $\mathcal{O} := [0:1:0]$ ("Oh").
Dieser Punkt ist nie singulär, da $\frac{\partial F}{\partial z}(0,1,0) = 1 \neq 0$.
Somit genügt es, ein Polynom F der Form ⊗ die Nichtsingularität auf $C_F(k) \cap i(\mathbb{A}^2(k))$, also im Affinen zu testen.

6.) **Bsp.:** Sei $F(X,Y,Z) = Y^2Z - X^3 - XZ$, für dieses gilt $a_1 = a_2 = a_3 = a_6 = 0$.
Dann ist $C_F(\mathbb{F}_p) \cap \mathbb{A}^2(\mathbb{F}_p)$ für $p \geq 3$ nicht-singulär, also eine ell. Kurve.

7.) Veranschaulichung, dass z.B. alle elliptischen Kurven $E_s(\mathbb{R})$ zur Gleichung $y^2 = x^3 - 3x + s$, $s \in \mathbb{R}$, den unendlich fernen Punkt $\mathcal{O} = [0:1:0]$ gemeinsam haben:



Das Bild ist perspektivisch so verzerrt, dass der unendlich ferne Punkt $\mathcal{O} = [0:1:0]$, der für die Richtung der y-Achse steht, am Horizont erscheint. (Das Zittern in den Kurven ist vom Abmalen per Hand.)

Vereinfachte Weierstraßgleichungen:

8) **Satz:** Sei $E_F(k)$ eine elliptische Kurve mit
$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$
(i) Falls char $k \neq 2$, ist die Abb.
$$\Phi : \mathbb{P}^2(k) \to \mathbb{P}^2(k)$$
$$[r:s:t] \mapsto [r : s + \tfrac{a_1}{2}r + \tfrac{a_3}{2}t : t]$$ bijektiv und es ist
$\Phi(E_F(k)) = E_{H_1}(k)$ ebenfalls eine elliptische Kurve
mit $H_1(X,Y,Z) = Y^2Z - X^3 - \frac{1}{4}b_2X^2Z - \frac{1}{2}b_4XZ^2 - \frac{1}{4}b_6Z^3$,
wobei $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$.
(ii) Falls char $k \neq 2$ und char $k \neq 3$, ist die Abb.
$$\Psi : \mathbb{P}^2(k) \to \mathbb{P}^2(k)$$
$$[r:s:t] \mapsto [36r + 3b_2t : 216s : t]$$ bijektiv und es ist
$\Psi(E_{H_1}(k)) = E_{H_2}(k)$ ebenfalls eine elliptische Kurve
mit $H_2(X,Y,Z) = Y^2Z - X^3 + 27c_4XZ^2 + 54c_6Z^3$,
wobei $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

9) **Bem.:** Wir können die lange Weierstraßgleichung im Fall char $k \neq 2$ also stets zur affinen Glg. $y^2 = x^3 + a_2x^2 + a_4x + a_6$ vereinfachen; falls char $k \neq 2$ und char $k \neq 3$ gilt, sogar zu $y^2 = x^3 + a_4x + a_6$.
Wir nennen diese Glg. die Kurze Weierstraßgleichung, das entsprechende Polynom dann das kurze Weierstraßpolynom.

10) **Bem.:** Auch im Fall char $k = 2$ lässt sich die lange Weierstraßgleichung vereinfachen, das ist nicht schwer, wenn $a_1 \neq 0$, aber auch für $a_1 = 0$ möglich. Wir behandeln dies hier nicht näher.

11) **Bew.:** Zu (i): Φ macht als Abb. nur Sinn, wenn 2 invertierbar in k ist, d.h. falls char $k \neq 2$ ist. Φ ist dann bijektiv, da Φ die Umkehrabb. $\Phi^{-1}([r:s:t]) = [r : s - \frac{a_1}{2}r - \frac{a_3}{2}t : t]$ hat.
(Klar: $\Phi^{-1}(\Phi([r:s:t])) = \Phi^{-1}([r : s + \frac{a_1}{2}r + \frac{a_3}{2}t : t]) = [r:s:t]$ ✓)

• Weiter bezeichnen wir mit Φ, Φ^{-1} auch die zugehörigen (affinen) Abbildungen $\Phi, \Phi^{-1}: k^3 \to k^3$, $\Phi(r,s,t) = (r, s + \frac{a_1}{2} r + \frac{a_3}{2} t, t)$
bzw. $\Phi^{-1}(r,s,t) = (r, s - \frac{a_1}{2} r - \frac{a_3}{2} t, t)$.

Nun können wir nachrechnen, dass $H_1(X,Y,Z) = F(X, Y - \frac{a_1}{2}X - \frac{a_3}{2}Z, Z)$:

[r.S. $= (Y - \frac{a_1}{2}X - \frac{a_3}{2}Z)^2 Z + a_1 X(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z)Z + a_3(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z)Z^2$

$- X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$

$= Z \cdot \left[Y^2 - 2Y\left(\frac{a_1}{2}X + \frac{a_3}{2}Z\right) + \left(\frac{a_1^2}{4}X^2 + 2\cdot\frac{a_1a_3}{4}XZ + \frac{a_3^2}{4}Z^2\right)\right]$

$+ a_1XYZ - \frac{a_1^2}{2}X^2Z - \frac{a_1a_3}{2}XZ^2 + a_3YZ^2 - \frac{a_1a_3}{2}XZ^2 - \frac{a_3^2}{2}Z^3$

$- X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$

$= Y^2Z - X^3 + \left(-\frac{a_1^2}{4} - a_2\right)X^2Z + \left(-\frac{a_1a_3}{2} - a_4\right)XZ^2 + \left(-\frac{a_3^2}{4} - a_6\right)Z^3$

$=: Y^2Z - X^3 - \frac{1}{4}b_2X^2Z - \frac{1}{2}b_4XZ^2 - \frac{1}{4}b_6Z^3 =$ l.S.

mit den im Satz angegebenen Zahlen b_2, b_4, b_6.]

• Es folgt $H_1(r,s,t) = F(\Phi^{-1}(r,s,t))$, also gilt: $F(r,s,t) = 0 \iff H_1(\Phi(r,s,t)) = 0$, so dass $\Phi(E_F(k)) = C_{H_1}(k)$ folgt. Es bleibt z.z., daß $C_{H_1}(k)$ nicht-singulär ist: Mit der Kettenregel (vgl. V7_Satz 4.)) rechnen wir nach:

$\frac{\partial H_1}{\partial X}(r,s,t) = \frac{\partial F}{\partial X}(\Phi^{-1}(r,s,t)) - \frac{a_1}{2}\frac{\partial F}{\partial Y}(\Phi^{-1}(r,s,t))$, $\frac{\partial H_1}{\partial Y}(r,s,t) = \frac{\partial F}{\partial Y}(\Phi^{-1}(r,s,t))$,

$\frac{\partial H_1}{\partial Z}(r,s,t) = -\frac{a_3}{2}\frac{\partial F}{\partial Y}\Phi^{-1}(r,s,t) + \frac{\partial F}{\partial Z}(\Phi^{-1}(r,s,t))$.

• Ist $P = [r:s:t] \in C_{H_1}(\bar{k})$, dann ist $\Phi^{-1}(P) = \Phi^{-1}([r:s:t])$ als Punkt der Kurve $C_F(\bar{k})$ nicht-singulär, da F elliptische Kurve ist. Die drei Ableitungen von F in $\Phi^{-1}(P)$ sind also nicht alle $=0$, also sind auch die drei Ableitungen von H_1 in (r,s,t) nicht alle $=0$. Also ist P auf $C_{H_1}(\bar{k})$ nicht-singulär.

Zu (ii): Ψ hat die Inverse $[r:s:t] \mapsto [\frac{1}{36}r - \frac{b_2}{12}t : \frac{1}{216}s : t]$,
da wegen char $k \neq 2, \neq 3$ die Zahlen $\frac{1}{36}, \frac{1}{12}, \frac{1}{216} = \frac{1}{2^3 3^3}$ in k existieren,
und leicht zu bestätigen ist, dass $\Psi(\Psi^{-1}([r:s:t])) = [r:s:t]$ gilt.

Durch geduldiges Nachrechnen zeigt man $H_2(X,Y,Z) = 2^6 3^6 H_1(\frac{1}{36}X - \frac{b_2}{12}Z, \frac{1}{216}Y, Z)$.
Daraus folgt: $H_1(r,s,t) = 0 \iff H_2(\Psi(r,s,t)) = 0$, d.h. $\Psi(E_{H_1}(k)) = C_{H_2}(k)$.
Wieder mit der Kettenregel kann auch die Nicht-Singularität von $C_{H_2}(k)$ gezeigt werden. □

Wir definieren zwei wichtige Kennzahlen projektiver Kurven wie folgt.

12) __Def.:__ Sei $C_F(k)$ die projektive ebene Kurve zum langen Weierstraßpolynom

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

- Dann heißt die Zahl

$$\Delta = \Delta(C_F(k)) = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

mit $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$

und $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_6^2 - a_4^2$

die Diskriminante der Kurve $C_F(k)$.

- Die Zahl

$$j = j(C_F(k)) := \frac{(b_2^2 - 24b_4)^3}{\Delta} = \frac{c_4^3}{\Delta}$$ heißt die j-Invariante der Kurve $C_F(k)$.

13) __Bem.:__ • Die j-Invariante legt die Isomorphieklasse der elliptischen Kurve über $\bar{k}$ fest: Zwei elliptische Kurven sind isomorph über $\bar{k}$ genau dann wenn sie dieselbe j-Invariante besitzen. [Ohne Bew.]

- j ist unabh. von der Wahl der speziellen Kurvengleichung.

14) __Bem.:__ Die Diskriminante einer Kurve $C_F(k)$ ist ein nützliches Hilfsmittel um zu testen, ob eine Kurve, die durch eine lange Weierstraßgleichung gegeben ist, nicht-singulär (und damit elliptisch) ist:

15) __Satz:__ Sei die Kurve $C_F(k)$ gegeben durch das lange Weierstraßpolynom F.

Dann ist $C_F(k)$ nicht-singulär genau dann, wenn $\Delta(C_F(k)) \neq 0$ ist.

Mit der angegebenen Formel für Δ ist dies auch rechnerisch leicht zu testen – wichtig, um elliptische Kurven für die Anwendungen zu konstruieren.

Dieses Diskriminantenkriterium zeigen wir in Vorlesung V12.