Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K17: Weierstraßform elliptischer Kurven

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

17.1. Einleitung: Wir definieren elliptische Kurven und zeigen unter bestimmten Voraussetzungen vereinfachte Weierstraßgleichungen für sie. Weiter bringen wir die Definition der j-Invarianten und der Diskriminanten.

Wir geben nun die erste, sehr allgemeine Definition einer elliptischen Kurve. Sei k ein Körper.

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

17.3. Bem.: • Es reicht, die Wendepunktbedingung durch $E(k) \cap \mathbb{P}^2(k) \neq \emptyset$ zu ersetzen (ist aber aufwendig zu zeigen). • 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.

17.4. Bem.: Durch eine sogenannte birationale Transformation kann angenommen werden, dass der Wendepunkt $\mathcal{O} := [0:1:0]$ ist. Es ist möglich zu zeigen, dass dann die Kurven-Gleichung die folgende vereinfachte Form hat:
(Bew. ist in der Literatur selten zu finden; oftmals wird mit Def. 17.5 begonnen.)

17.5 **Def.:** 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 $E(k)$.

17.6. **Bem.:** • Die Monome X^2Y, Y^3, XY^2 brauchen also nicht vorzukommen.

• Die Numerierung der Koeffizienten ist historisch bedingt.

• Die affine Version lautet also:

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

Die Form $\circledast$ nennen wir auch die lange Weierstraßform, das Polynom heißt langes Weierstraßpolynom.

• Wir werden sehen, dass man dies oft auf eine noch einfachere Form bringen kann (A6 17.10.)

17.7. **Bem.:** • Welche Punkte liegen auf $E(k)$, die nicht affin sind?

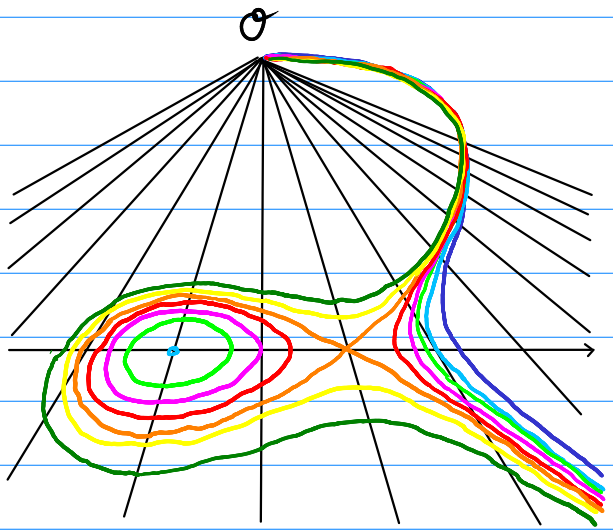
Ist $P = [s:s:0] \in \mathbb{P}^2(k) \setminus \mathbb{A}^2(k)$ ein solcher Punkt, dann ergibt Einsetzen in $\circledast$ dann $s^3 = 0$, dann muss $s \neq 0$ sein, d.h. $P = [0:s:0] = [0:1:0]$.

• 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 $\circledast$ die Nichtsingularität auf $C_F(k) \cap i(\mathbb{A}^2(k))$, also im Affinen zu testen.

17.8. **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.

17.9. **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 $O = [0:1:0]$ gemeinsam haben:



Parameterwerte:
$s = 5$
$s = 3$
$s = 2$
$s = 1$
$s = 0$
$s = -1$
$s = -1.999$
$s = -5$

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

17.10. **Vereinfachte Weierstraßgleichungen:** Der nächste Satz zeigt, dass wir die lange Weierstraßform ⊛ unter bestimmten Voraussetzungen an char k zu einer kurzen Form vereinfachen können.

17.11. **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 $\mathrm{char}\, k \neq 2$, ist die AGG.
$$\Phi : \mathbb{P}^2(k) \to \mathbb{P}^2(k)$$
$$[r:s:t] \mapsto [r : s + \tfrac{a_1}{2}r + \tfrac{a_3}{2}t : t]$$ bijektiv und es ist
$\Phi(E_F(k)) = E_{H_1}(k)$ ebenfalls eine elliptische Kurve
mit $H_1(X,Y,Z) = Y^2Z - X^3 - \tfrac{1}{4}b_2X^2Z - \tfrac{1}{2}b_4XZ^2 - \tfrac{1}{4}b_6Z^3$,
wobei $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$.

(ii) Falls $\mathrm{char}\, k \neq 2$ und $\mathrm{char}\, k \neq 3$, ist die AGG.
$$\Psi : \mathbb{P}^2(k) \to \mathbb{P}^2(k)$$
$$[r:s:t] \mapsto [36r + 3b_2t : 216s : t]$$ 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 $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

17.12. **Bem.:** Wir können die lange Weierstraßgleichung im Fall $\mathrm{char}\, k \neq 2$ also stets zur affinen Glg. $y^2 = x^3 + a_2x^2 + a_4x + a_6$ vereinfachen; falls $\mathrm{char}\, k \neq 2$ und $\mathrm{char}\, k \neq 3$ 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.

17.13. **Bem.:** Auch im Fall $\mathrm{char}\, k = 2$ 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.

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

- Weiter bezeichnen wir mit $\underline{\Phi}$, $\underline{\Phi}^{-1}$ auch die zugehörigen (affinen) Abbildungen $\underline{\Phi}, \underline{\Phi}^{-1}: k^3 \to k^3$, $\underline{\Phi}(r,s,t) = (r, s + \frac{a_1}{2} r + \frac{a_3}{2} t, t)$
bzw. $\underline{\Phi}^{-1}(r,s,t) = (r, s - \frac{a_1}{2} r - \frac{a_3}{2} t, t)$.
Nun können wir nachrechnen, dass $H_1(X,Y,Z) = F(X, Y - \frac{a_1}{2} X - \frac{a_3}{2} Z, Z)$:

$$\begin{aligned}
\lceil r.g. &= (Y - \tfrac{a_1}{2} X - \tfrac{a_3}{2} Z)^2 Z + a_1 X (Y - \tfrac{a_1}{2} X - \tfrac{a_3}{2} Z) Z + a_3 (Y - \tfrac{a_1}{2} X - \tfrac{a_3}{2} Z) Z^2 \\
&\quad - X^3 - a_2 X^2 Z - a_4 X Z^2 - a_6 Z^3 \\
&= Z \cdot \Big[Y^2 - 2Y(\tfrac{a_1}{2} X + \tfrac{a_3}{2} Z) + (\tfrac{a_1^2}{4} X^2 + 2 \cdot \tfrac{a_1 a_3}{4} XZ + \tfrac{a_3^2}{4} Z^2) \Big] \\
&\quad + a_1 XYZ - \tfrac{a_1^2}{2} X^2 Z - \tfrac{a_1 a_3}{2} XZ^2 + a_3 YZ^2 - \tfrac{a_1 a_3}{2} XZ^2 - \tfrac{a_3^2}{2} Z^3 \\
&\quad - X^3 - a_2 X^2 Z - a_4 XZ^2 - a_6 Z^3 \\
&= Y^2 Z - X^3 + (-\tfrac{a_1^2}{4} - a_2) X^2 Z + (-\tfrac{a_1 a_3}{2} - a_4) XZ^2 + (-\tfrac{a_3^2}{4} - a_6) Z^3 \\
&=: Y^2 Z - X^3 - \tfrac{1}{4} b_2 X^2 Z - \tfrac{1}{2} b_4 XZ^2 - \tfrac{1}{4} b_6 Z^3 = l.g.
\end{aligned}$$

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

- Es folgt $H_1(r,s,t) = F(\underline{\Phi}^{-1}(r,s,t))$, also gilt: $F(r,s,t) = 0 \Leftrightarrow H_1(\underline{\Phi}(r,s,t)) = 0$, so dass $\underline{\Phi}(E_F(k)) = C_{H_1}(k)$ folgt. Es bleibt z.z., daß $C_{H_1}(k)$ nicht-singulär ist: Mit der Kettenregel (vgl. Satz K13.5) rechnen wir nach:

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

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

- Ist $P = [r:s:t] \in C_{H_1}(\bar{k})$, dann ist $\Phi^{-1}(P) = \Psi^{-1}([r:s:t])$ 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 $[r:s:t] \mapsto \left[\frac{1}{36} r - \frac{b_2}{12} t : \frac{1}{216} s : t\right]$,
da wegen $\mathrm{char}\, k \neq 2, \neq 3$ 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 $H_2(X,Y,Z) = 2^6 3^6 H_1\left(\frac{1}{36} X - \frac{b_2}{12} Z, \frac{1}{216} Y, Z\right)$.
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 $C_{H_2}(a)$ gezeigt werden. □

Wir definieren zwei wichtige Kennzahlen projektiver Kurven wie folgt.

17.15. **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

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

mit $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$
und $b_8 = a_1^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$
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** $C_F(k)$.

17.16. **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.