

Stichworte: • Diskriminantenkriterium:  $C_F$  in W-Form nicht-singulär  $\Leftrightarrow \Delta(C_F(k)) \neq 0$   
• Beweis unterscheidet char  $k=2$ , char  $k=3$ , und sonst • Diskriminante eines Polynoms

## 2.4.2 Das Diskriminantenkriterium

1.) Def.: Sei  $C_F(k)$  die projektive ebene Kurve zum langen Weierstraßpolynom  
$$F(X, Y, Z) = Y^2 Z + a_1 X Y Z + a_3 Y Z^2 - X^3 - a_2 X^2 Z - a_4 X Z^2 - a_6 Z^3.$$

Dann heißt die Zahl

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

$$\text{mit } b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1 a_3, \quad b_6 = a_3^2 + 4a_6$$

$$\text{und } b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

die Diskriminante der Kurve  $C_F(k)$ .

2.) Bem.: Im Fall einer Kurve  $C_F(k)$  in einer kurzen Weierstraßform  
 $f(x, y) = y^2 - x^3 - ax - b$  haben wir  $\Delta(C_F(k)) = -8(2a)^3 - 27 \cdot (4b)^2 = -16(4a^3 + 27b^2)$ ,  
da  $a_1=0, a_3=0, a_2=0, a_4=a, a_6=b \leadsto b_2=0, b_4=2a, b_6=4b, b_8=-a^2$ , vgl.  
Übungsaufgabe 3 Blatt 4.

Wir zeigen das Diskriminantenkriterium:

3.) 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.

4.) Bem.: • Bei diesem Kriterium, wenn  $\Delta \neq 0$ , erhalten wir, dass  $C_F(\bar{k})$   
über dem alg. Abschluss  $\bar{k}$  keine singulären Punkte enthält (insb. auch über  $k$ ,  
aber über  $\bar{k}$  ist eben noch stärker). Deswegen haben wir uns bei unserer Def.  
von "nicht-singulärer Kurve" auf  $\bar{k}$  bezogen, was wegen Satz 3.) also  
mathematisch leichter wird. Für char  $k \neq 2$  kann es aber nicht sein, dass  $C_F$   
über  $k$  keine singulären Punkte hat und über  $\bar{k}$  hingegen schon.

- Das Kriterium ist in der Praxis nützlich, da eine Kurve in Weierstraßform (die vielleicht per Zufallsgenerator für die Koeffizienten erzeugt worden ist), damit leicht auf Nicht-Singularität durch Berechnung der einfachen Formel für  $\Delta$  getestet/überprüft werden kann (so dass eine elliptische Kurve vorliegt).
- Der Beweis unterscheidet wesentlich die Fälle char  $k=2$ , char  $k=3$  und sonst.

5.) Bew.: Die Kurve  $C_f(k)$  ist nicht-singulär genau dann, wenn ihre affine Kurve  $C_f(k)$  mit  $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$  nicht-singulär ist. Wir zeigen den Satz deswegen im Affinen (der einzige nicht-affine Punkt  $O = [0:1:0]$  der Kurve ist immer regulär, vgl. VII, Bem. 5)).

Nun enthält  $C_f(\bar{k})$  einen singulären Punkt genau dann, wenn  $\exists r, s \in \bar{k} : f(r,s) = 0, \frac{\partial f}{\partial x}(r,s) = 0, \frac{\partial f}{\partial y}(r,s) = 0$  gilt  

$$= \underline{a_1s - 3r^2 - 2a_2r - a_4} = \underline{2s + a_1r + a_3}$$

Wir unterscheiden weiter

mehrere Fälle nach dem Wert der Charakteristik von  $k$ :

6.) 1. Fall:  $\text{char } k = 2$  und  $a_1 = 0$ .

↳: Dann ist hier  $b_2 = b_4 = 0, b_6 = a_3^2, \Delta = -2^7 a_3^4 = a_3^4$ .

Weiter gilt  $\frac{\partial f}{\partial y} = a_3$ , so dass, falls ein sing. Pkt. ex., dann  $a_3 = 0$ , also  $\Delta = 0$  folgt.

⇒: Ist  $\Delta = 0$ , folgt  $\frac{\partial f}{\partial y} = 0$ . Nun ex.  $r, s \in \bar{k}$  mit  $r^2 + a_4 = 0, s^2 + a_3s = r^3 + a_2r^2 + a_4r + a_6$ , also ist  $(r,s) \in A^2(\bar{k})$  singulärer Punkt auf  $C_f(\bar{k})$ .

7.) 2. Fall:  $\text{char } k = 2$  und  $a_1 \neq 0$ .

Wir haben in Charakteristik 2, dass gilt:

$$\Delta = -a_4^4 (a_1^2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2) - 2^7 a_3^4 + a_1^3 a_3^3$$

$$= a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 + a_1^4 a_4^2 + a_1^3 a_3^3 + a_3^4$$

↳:

Hat  $C_f(\bar{k})$  einen singulären Pkt., ex.  $r, s \in \bar{k}$  mit  $f(r,s) = 0$ ,

d.h.  $a_1s + r^2 + a_4 = 0$  und  $a_1r + a_3 = 0$ .

Da  $a_1 \neq 0$ , folgt

$$r = \frac{a_3}{a_1}, \quad s = \frac{a_3^2 + a_1^2 a_4}{a_1^3}$$

Durch Einsetzen in  $f(r,s)$  folgt  $0 = f(r,s) = \Delta a_1^{-6}$ , also  $\Delta = 0$ .

$$f(r,s) = s^2 + \frac{a_1 r s + a_3 s}{a_1} + r^3 + a_2 r^2 + a_4 r + a_6 = a_1^{-6} (a_3^4 + a_1^4 a_4^2 + a_1^3 a_3^3 + a_2 a_1^4 a_3^2 + a_4 a_1^5 a_3 + a_6 a_1^6)$$

⇒: Ist  $\Delta = 0$ , def. wir  $r, s$  wie oben,

dann ist  $f(r,s) = \Delta a_1^{-6}$ , also  $f(r,s) = 0$ , womit ein singulärer Punkt konstruiert ist.

8.) 3. Fall: char  $k = 3$ .

Via Rechnen in Charakteristik 3 folgt  $\Delta = -b_2^2 b_8 - 8b_4^3$ .

Betr. die Abb.  $\bar{\phi}: C_F(k) \rightarrow C_{H_1}(k)$  aus V11-Satz 8.) (i)

$$\text{mit } H_1(x, y, z) = y^2 z - x^3 - \frac{1}{4} b_2 x^2 z - \frac{1}{2} b_4 x z^2 - \frac{1}{4} b_6 z^3,$$

die die lange Weierstraßform  $F$  auf die kurze Form  $H_1$  bringt.

Es ist  $\Delta(C_{H_1}(k)) = \Delta(C_F(k))$  durch Nachrechnen, somit genügt es  $\mathcal{Q}$ , das Diskriminantenkriterium für die kurze Form  $H_1$  zu zeigen.

9.) Die Kurve  $C_{H_1}(\bar{k})$  enthält genau dann einen singulären Punkt,

wenn es  $r, s \in \bar{k}$  gibt mit

$$s^2 - r^3 - \frac{1}{4} b_2 r^2 - \frac{1}{2} b_4 r - \frac{1}{4} b_6 = 0, \quad 3r^2 + \frac{1}{2} b_2 r + \frac{1}{2} b_4 = 0, \quad 2s = 0,$$

d.h. falls  $r$  eine doppelte Nst. des Polynoms  $\sigma(x) := x^3 + \frac{1}{4} b_2 x^2 + \frac{1}{2} b_4 x + \frac{1}{4} b_6$

ist, sprich  $\sigma(r) = 0 = \sigma'(r)$  ist.

Über  $\bar{k}$  zerfällt  $\sigma$  in 3 Linearfaktoren:  $\sigma(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ , die  $\alpha_i \in \bar{k}$ .

Nun hat ein Polynom  $\sigma$  genau dann eine doppelte Nst.,

$$\text{falls seine Diskriminante } \text{disc}(\sigma) := (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$$

verschwindet, vgl. unten Bem. 14.)

10.) Somit ist im 3. Fall z.z.:  $\Delta = 0 \Leftrightarrow \text{disc}(\sigma) = 0$ .

$$\text{Wegen } \text{disc}(x^3 + mx^2 + vx + w) = m^2 v^2 - 4m^3 w - 4v^3 - 27w^2 + 18m v w,$$

vgl. Kor. 16.),

erhalten wir mit  $m = \frac{b_2}{4}$ ,  $v = \frac{b_4}{2}$ ,  $w = \frac{b_6}{4}$  dann in Charakteristik 3, dass

$$\text{disc}(\sigma) = \frac{1}{64} b_2^2 b_4^2 - \frac{1}{64} b_2^3 b_6 - \frac{1}{2} b_4^3.$$

$$\text{Wegen } 4b_8 = b_2 b_6 - b_4^2$$

$$[\text{z.B. } = (a_1^2 + 4a_2)(a_3^2 + 4a_6) - (2a_4 + a_1 a_3)^2 = \dots = 4b_8]$$

$$= \underline{a_1^2 a_3^2} + 4a_1^2 a_6 + 4a_2 a_3^2 + 4^2 a_2 a_6 - (4a_4^2 + 4a_4 a_1 a_3 + \underline{a_1^2 a_3^2}) = 4b_8 = \text{z.B.}]$$

$$\text{erhalten wir } \text{disc}(\sigma) = \frac{1}{16} (-b_2^2 b_8 - 8b_4^3) = \frac{1}{16} \Delta.$$

Aus dieser Formel folgt die Beh. im 3. Fall.

11.) 4. Fall:  $\text{char } k > 3$ , d.h.  $\text{char } k \geq 5$ , oder  $\text{char } k = 0$ .

Mit der Bijektion  $\Psi \circ \Phi : C_F(k) \rightarrow C_{H_2}(k)$  zum kurzen Weierstraßpolynom

$$H_2(x, y, z) = y^2 z - x^3 + 27c_4 x z^2 + 54c_6 z^3$$

bzw.  $h_2(x, y) = y^2 - x^3 + 27c_4 x + 54c_6$ ,

$$\text{wo } c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2 b_4 - 216b_6,$$

folgt durch Untersuchung der Ableitungen wieder:

$$C_F(k) \text{ nicht-sing.} \Leftrightarrow C_{H_2}(k) \text{ nicht-sing.}$$

Wir berechnen

$$\Delta(C_{H_2}(k)) = 2^6 3^3 (c_4^3 - c_6^2) = \dots = 2^{12} 3^{12} \Delta(C_F(k)),$$

also genügt es, die Beh. für  $C_{H_2}(k)$  zu zeigen.

Wie im 3. Fall:

$$C_{H_2}(\bar{k}) \text{ enthält sing. Pkt.} \Leftrightarrow \underbrace{\sigma(x) = x^3 - 27c_4 x - 54c_6}_{\substack{v \\ w}} \\ \text{hat doppelte Nst.} \Leftrightarrow \text{disc}(\sigma) = 0$$

Wegen der Formel in Kor. 16.) für  $\text{disc}(\sigma)$  folgt mit  $u=0, v=-27c_4, w=-54c_6$ :

$$\text{disc}(\sigma) = 0 \Leftrightarrow 4 \cdot 27^3 c_4^3 - 27 \cdot 54^2 c_6^2 = 0 \Leftrightarrow c_4^3 - c_6^2 = 0.$$

Daraus folgt die Beh. □

Theoretische Ergänzungen zum Begriff "Diskriminante":

12.) Def.: Die Diskriminante eines Polynoms  $\sigma \in k[x], n = \deg \sigma \geq 1$ , ist

$$\text{disc}(\sigma) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) \in \bar{k},$$

falls  $\alpha_1, \dots, \alpha_n \in \bar{k}$  die Nullstellen von  $\sigma$  in  $\bar{k}$  bezeichnen.

13.) Bem.: Man vgl. dies mit der Diskriminante  $p^2 - 4q$  eines quadratischen Polynoms  $\sigma(x) = x^2 + px + q \in k[x]$ , wir haben  $\alpha_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} = -\frac{p}{2} \pm \frac{1}{2} \sqrt{p^2 - 4q}$   
also genau  $(\alpha_1 - \alpha_2)^2 = \text{disc}(\sigma)$ .  
Ist dies = 0, ist  $\alpha_1 = \alpha_2$  eine doppelte Nullstelle von  $\sigma$ .

14.) Bem.:  $\text{disc}(\sigma)$  verschwindet genau dann, wenn  $\sigma$  über  $\bar{k}$  eine doppelte Nullstelle hat.  
Dies folgt unmittelbar aus der Def. von  $\sigma$ .

15.) Bem.: Ist  $\sigma \in k[x]$ ,  $n = \deg \sigma \geq 1$ , ein normiertes Polynom, kann die Beziehung  $\text{disc}(\sigma) = (-1)^{n(n-1)/2} \text{Res}(\sigma, \sigma')$  mit der aus V10-Def. 5.) behandelten Resultante gezeigt werden.  
• Aus dieser wichtigen Formel folgt wegen unserer Definition für die Resultante, dass stets  $\text{disc}(\sigma) \in k$  gilt.

16.) Kor.: Es gilt  $\text{disc}(x^3 + mx^2 + vx + w) = m^2v^2 - 4mw^3 - 4v^3 - 27w^2 + 18mvw$ .

Bew.: Wir haben  $M(\sigma, \sigma') = \begin{bmatrix} w & 0 & 0 & 0 & 0 \\ v & w & 2m & v & 0 \\ m & v & 3 & 2m & v \\ 1 & m & 0 & 3 & 2m \\ 0 & 1 & 0 & 0 & 3 \end{bmatrix}$   $\sigma'(x) = 3x^2 + 2mx + v$

$$\Rightarrow \text{Res}(\sigma) = \det M(\sigma, \sigma') = w \det \begin{bmatrix} w & 2m & v & 0 \\ v & 3 & 2m & v \\ m & 0 & 3 & 2m \\ 1 & 0 & 0 & 3 \end{bmatrix} + v \det \begin{bmatrix} v & w & v & 0 \\ m & v & 2m & v \\ 1 & m & 3 & 2m \\ 0 & 1 & 0 & 3 \end{bmatrix}$$

$$= -w \det \begin{bmatrix} 2m & v & 0 \\ 3 & 2m & v \\ 0 & 3 & 2m \end{bmatrix} + w \cdot 3 \det \begin{bmatrix} w & 2m & v \\ v & 3 & 2m \\ m & 0 & 3 \end{bmatrix}$$

$$+ v \det \begin{bmatrix} v & v & 0 \\ m & 2m & v \\ 1 & 3 & 2m \end{bmatrix} + v \cdot 3 \det \begin{bmatrix} v & w & v \\ m & v & 2m \\ 1 & m & 3 \end{bmatrix}$$

$$= -w (2m(2m \cdot 2m - 3v) - v \cdot 6m) + 3w (m(2m \cdot 2m - 3v) + 3(3w - 2mv))$$

$$+ v (v(2m \cdot 2m - 3v) - v(m \cdot 2m - v)) + 3v (v(3v - 2m^2) - wm + vm^2 - v^2)$$

$$= -w \cdot 8m^3 + 6mwv + 6mvw + 12wm^3 - 9mvw + 27w^2 - 18mvw$$

$$+ v^2 \cdot 4m^2 - 3v^3 - 2v^2m^2 + v^3 + 9v^3 - 6v^2m^2 - 3mvw + 3m^2v^2 - 3v^3$$

$$= 4mw^3 - m^2v^2 + 27w^2 + 4v^3 - 18mvw \quad \checkmark \quad \text{Jetzt: } (-1)^{3 \cdot (3-1)/2} = -1 \text{ beachten. } \square$$