Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K18: Das Diskriminantenkriterium

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

---

18.1. Einleitung: Wir zeigen das Diskriminantenkriterium für elliptische Kurven.

18.2. 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 $C_F(k)$.

18.3. 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:

18.4. 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.

18.5. **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 $a_1=0$, $a_3=0$, $a_2=0$, $a_4=a$, $a_6=b$ $\rightsquigarrow$ $b_2=0$, $b_4=2a$, $b_6=4b$, $b_8=-a^2$.

In (ü) - Aufgabe 1, Blatt 10, wurde gezeigt: $g(x)=x^3+ax+b$ hat genau dann eine mehrfache Nullstelle, wenn $4a^3+27b^2=0$ ist (sofern $\mathrm{char}\,k \neq 2,3$). In diesem Fall, mit $g(x)=(x-u)^2(x-v)$, gibt es singuläre Punkte: $\frac{\partial f}{\partial y} = 2y$, $\frac{\partial f}{\partial x} = -\frac{\partial g}{\partial x} = -2(x-u)(x-v) - (x-u)^2$, so dass $(u,0)$ bzw. $[u:0:1]$ einen singulären Punkt ergibt.

Wir zeigen das Diskriminanten Kriterium:

18.6. **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.

18.7. **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 18.6 also mathematisch leichter wird. Für $\mathrm{char}\,k \neq 2$ 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 Δ getestet/überprüft werden kann (so dass eine elliptische Kurve vorliegt).

- Der Beweis unterscheidet wesentlich die Fälle $\mathrm{char}\,k = 2$, $\mathrm{char}\,k = 3$ und sonst.

18.8. **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. Bem. 17.7.).

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

$\frac{\partial f}{\partial x}(r,s) = a_1s - 3r^2 - 2a_2r - a_4$, $\frac{\partial f}{\partial y}(r,s) = 2s + a_1r + a_3$

Wir unterscheiden weiter mehrere Fälle nach dem Wert der Charakteristik von k:

18.9. **1. Fall: $\mathrm{char}\, k = 2$ und $a_1 = 0$.**

„$\Leftarrow$": Dann ist hier $b_2 = b_4 = 0$, $b_6 = a_3^2$, $\Delta = -27a_3^4 = a_3^4$.
Weiter gilt $\frac{\partial f}{\partial y} = a_3$, so dass, falls ein sing. Pkt. ex., dann $a_3 = 0$, also $\Delta = 0$ folgt.

„$\Rightarrow$": 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 $(r,s) \in \mathbb{A}^2(\bar{k})$ singulärer Punkt auf $C_f(\bar{k})$.

18.10. **2. Fall: $\mathrm{char}\, k = 2$ und $a_1 \neq 0$.**

Wir haben in Charakteristik 2, dass gilt:

$$\Delta = -a_4^4(a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2) - 27a_3^4 + a_1^3a_3^3$$
$$= a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_1^3a_3^3 + a_3^4.$$

„$\Rightarrow$":
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

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

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

$f(r,s) = s^2 + \underbrace{a_1rs + a_3s}_{=0} + r^3 + a_2^2r^2 + a_4r + a_6 = a_1^{-6}(a_3^4 + a_1^4a_4^2 + a_1^3a_3^3 + a_2a_1^4a_3^2 + a_4a_1^5a_3 + a_6a_1^6)$

„⇒": 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.

18.11. 3. Fall: $\mathrm{char}\, k = 3$.
Via Rechnen in Charakteristik 3 folgt $\Delta = -b_2^2 b_8 - 8 b_4^3$.
Betr. die AGG. $\bar{\phi} : C_F(k) \to C_{H_1}(k)$ aus Satz 17.11.(i)
mit $H_1(X,Y,Z) = Y^2Z - X^3 - \frac{1}{4} b_2 X^2 Z - \frac{1}{2} b_4 X Z^2 - \frac{1}{4} b_6 Z^3$,
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 o.E., das Diskriminantenkriterium für die kurze Form H_1 zu zeigen.

18.12. Die Kurve $C_{H_1}(\bar{k})$ enthält genau dann einen singulären Punkt, wenn es $r, s \in \bar{k}$ gibt mit
$s^2 - r^3 - \frac{1}{4} b_2 r^2 - \frac{1}{2} b_4 r - \frac{1}{4} b_6 = 0$, $3r^2 + \frac{1}{2} b_2 r + \frac{1}{2} b_4 = 0$, $2s = 0$,
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 σ in 3 Linearfaktoren: $\sigma(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$, die $\alpha_i \in \bar{k}$.
Nun hat ein Polynom σ genau dann eine doppelte Nst.,
falls seine Diskriminante $\mathrm{disc}(\sigma) := (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$
verschwindet, vgl. unten Bem. 18.17.

18.13. Somit ist im 3. Fall z.z.: $\Delta = 0 \Leftrightarrow \operatorname{disc}(G) = 0$.

Wegen $\operatorname{disc}(x^3 + ux^2 + vx + w) = u^2v^2 - 4u^3w - 4v^3 - 27w^2 + 18uvw$,
vgl. Kor. 18.19,
erhalten wir mit $u = \frac{b_2}{4}$, $v = \frac{b_4}{2}$, $w = \frac{b_6}{4}$ dann in Charakteristik 3, dass
$$\operatorname{disc}(G) = \frac{1}{64} b_2^2 b_4^2 - \frac{1}{64} b_2^3 b_6 - \frac{1}{2} b_4^3.$$
Wegen $4b_8 = b_2 b_6 - b_4^2$
$$[\text{r.S.} = (a_1^2 + 4a_2)(a_3^2 + 4a_6) - (2a_4 + a_1 a_3)^2 = \ldots = 4b_8 \checkmark]$$
$$= a_1^2 a_3^2 + 4a_1^2 a_6 + 4a_2 a_3^2 + 4^2 a_2 a_6 - (4a_4^2 + 4a_4 a_1 a_3 + a_2^2 a_3^2) = 4b_8 = \text{l.S.}$$

erhalten wir $\operatorname{disc}(G) = \frac{1}{16}(-b_2^2 b_8 - 8b_4^3) = \frac{1}{16}\Delta$.
Aus dieser Formel folgt die Beh. im 3. Fall.

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

Mit der Bijektion $\Psi \circ \Phi : C_F(k) \to C_{H_2}(k)$ zum kurzen Weierstraßpolynom
$$H_2(X,Y,Z) = Y^2Z - X^3 + 27c_4 X Z^2 + 54 c_6 Z^3$$
bzw. $h_2(x,y) = y^2 - x^3 + 27c_4 x + 54c_6$,
wo $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$,
folgt durch Untersuchung der Ableitungen wieder:
$C_F(k)$ nicht-sing. $\Leftrightarrow$ $C_{H_2}(k)$ nicht-sing.
Wir berechnen
$$\Delta(C_{H_2}(k)) = 2^6 3^9 (c_4^3 - c_6^2) = \ldots = 2^{12} 3^{12} \Delta(C_F(k)),$$
also genügt es, die Beh. für $C_{H_2}(k)$ zu zeigen.
Wie im 3. Fall:
$C_{H_2}(\bar{k})$ enthält sing. Pkt. $\Leftrightarrow$ $G(x) = x^3 - \underbrace{27c_4}_{v} x - \underbrace{54c_6}_{w}$
hat doppelte Nst. $\Leftrightarrow \operatorname{disc}(G) = 0$

Wegen der Formel in Kor. 18.19 für $\operatorname{disc}(\sigma)$ folgt mit $u=0$, $v=-27c_4$, $w=-54c_6$:

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

Daraus folgt die Beh. □

Anhang:
Theoretische Ergänzungen zum Begriff "Diskriminante":

18.15 **Def.:** Die Diskriminante eines Polynoms $\sigma \in k[X]$, $n := \deg \sigma \geq 1$, ist

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

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

18.16. **Bem.:** Man vgl. dies mit der Diskriminante p^2-4q eines quadratischen Polynoms $\sigma(X) = X^2+pX+q \in k[X]$, wir haben $\alpha_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4}-q} = -\frac{p}{2} \pm \frac{1}{2}\sqrt{\underbrace{p^2-4q}_{\operatorname{disc}(\sigma)}}$

also genau $(\alpha_1-\alpha_2)^2 = \operatorname{disc}(\sigma)$.

Ist dies $=0$, ist $\alpha_1=\alpha_2$ eine doppelte Nullstelle von σ.

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

18.18. **Bem.:** • Ist $\sigma \in k[X]$, $n=\deg\sigma \geq 1$, ein normiertes Polynom, kann die Beziehung

$$\operatorname{disc}(\sigma) = (-1)^{n(n-1)/2} \operatorname{Res}(\sigma, \sigma')$$

mit der in Def. 16.7. behandelten Resultante gezeigt werden.

• Aus dieser wichtigen Formel folgt wegen unser Definition für die Resultante, dass stets $\operatorname{disc}(\sigma) \in k$ gilt.

18.19. **Kor.:** Es gilt $\operatorname{disc}(x^3+ux^2+vx+w) = u^2v^2 - 4wu^3 - 4v^3 - 27w^2 + 18uvw$.

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

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

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

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

$$= -w\big(2u(2u\cdot 2u - 3v) - v\cdot 6u\big) + 3w\big(u(2u\cdot 2u - 3v) + 3(3w - 2uv)\big)$$
$$+ v\big(v(2u\cdot 2u - 3v) - v(u\cdot 2u - v)\big) + 3v\big(v(3v - 2u^2) - wu + vu^2 - v^2\big)$$

$$= -w\cdot 8u^3 + 6uvw + 6uvw + 12wu^3 - 9uvw + 27w^2 - 18uvw$$
$$+ v^2\cdot 4u^2 - 3v^3 - 2v^2u^2 + v^3 + 9v^3 - 6v^2u^2 - 3uvw + 3u^2v^2 - 3v^3$$
$$= 4wu^3 - u^2v^2 + 27w^2 + 4v^3 - 18uvw \quad \checkmark$$

Jetzt: $(-1)^{3\cdot(3-1)/2} = -1$ beachten. □