

Stichworte:

- Definition Punkteaddition $P+Q$ auf $E(k)$ mit 3. Schnittpunkt $P \neq Q$ von $G(P, Q) \cap E(k)$
- \mathcal{O} ist neutrales Element • Invertieren leicht bei Kurve Weierstraßform • explizite Formeln für "+"

2.4.3 Die Gruppenstruktur elliptischer Kurven

Sei $E(k)$ eine elliptische Kurve über einem Körper k . (Da wir auch über Tangenten sprechen möchten, muss die Kurve nicht-singulär sein.)

1.) Satz: (a) Seien $P, Q \in E(k)$, $P \neq Q$, $G = G(P, Q) \subseteq \mathbb{P}^2(k)$ die projektive Gerade, die P und Q verbindet.

Dann hat G noch einen dritten Schnittpunkt mit $E(k)$ gemäß Vielfachheiten gezählt (d.h. ev. P bzw. Q selbst, falls $m(P; G, E(k)) = 2$ bzw. $m(Q; G, E(k)) = 2$).

(b) Sei G die Tangente an $E(k)$ im Punkt $P \in E(k)$.

Dann hat G noch einen dritten Schnittpunkt mit $E(k)$ gemäß Vielfachheiten gezählt (d.h. ev. P selbst, falls $m(P; G, E(k)) = 3$).

2.) Bew.: Als Ergänzung zum Satz von Bezout haben wir Satz 15.) kennengelernt, der im Spezialfall $\deg F_1 = 1, \deg F_2 = 3$ dann $\sum_{P \in C_1 \cap C_2} m(P, C_1, C_2) \in \{0, 1, 3\}$ liefert (s. V10-Bsp. 16.)).

Also gilt auch hier: $\sum_{R \in G \cap E(k)} m(R; G, E(k)) \in \{0, 1, 3\}$.

Zu (a): Ist $G = G(P, Q)$, folgt $2 \leq \#(G \cap E(k)) \leq \sum_{R \in G \cap E(k)} m(R; G, E(k)) \in \{0, 1, 3\}$, das geht nur, wenn die Vielfachensumme = 3 ist,

also ex. ein $R \in G \cap E(k)$

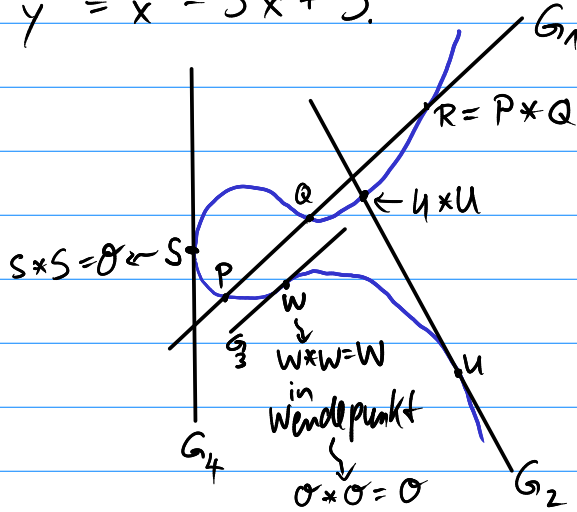
mit $R \notin \{P, Q\}$, falls $m(P; G, E(k)) = 1 = m(Q; G, E(k))$

oder mit $R = P$, falls $m(P; G, E(k)) = 2$

oder mit $R = Q$, falls $m(Q; G, E(k)) = 2$.

Zu (b): Ist G die Tangente an $E(k)$ in $P \in E(k)$, ist $m(P; G, E(k)) \geq 2$ nach V9-Satz 20.). Es folgt wie im Beweis zu (a) wieder, dass die Vielfachensumme = 3 ist, also die Existenz eines $R \in G \cap E(k)$ mit $R \neq P$, falls $m(P; G, E(k)) = 2$ und $R = P$, falls $m(P; G, E(k)) = 3$ gilt. \square

- 3) Bsp.: Betr. die elliptische Kurve $E(k)$ zur (kurzen) Weierstraßgleichung $y^2 = x^3 - 3x + 3$.
(OK, da $4 \cdot (-3)^3 + 27 \cdot 3^2 \neq 0$)



Jede Gerade, die $E(k)$ in zwei Punkten schneidet, schneidet $E(k)$ in einem dritten Punkt, gemäß Vielfachheiten gezählt. Der dritte Schnittpunkt kann auch $O \in \mathbb{P}^1$ sein.

Wir möchten auf $E(k)$ eine Verknüpfung "+" erklären, also eine Punktaddition $P+Q$, bei der wiederum ein Punkt auf der elliptischen Kurve herauskommt. Den dritten Schnittpunkt, den die Gerade $G(P, Q)$ durch zwei Punkte P und Q auf $E(k)$ mit $E(k)$ hat (amt Satz 1.), bezeichnen wir mit $P * Q$.

- 4) Def.: Für $P, Q \in E(k)$, $P \neq Q$, definieren wir also

$$\underline{P * Q} := \begin{cases} R \in (G(P, Q) \cap E(k)) \setminus \{P, Q\}, & \text{falls } m(P; G, E(k)) = 1 = m(Q; G, E(k)), \\ P, & \text{falls } m(P; G, E(k)) = 2, \\ Q, & \text{falls } m(Q; G, E(k)) = 2, \end{cases}$$

sowie $\underline{P * P} := \begin{cases} R \in (T_P(E(k)) \cap E(k)) \setminus \{P\}, & \text{falls } m(P; T_P(E(k)), E(k)) = 2, \\ P, & \text{falls } m(P; T_P(E(k)), E(k)) = 3 \quad (\text{d.h. falls } P \text{ Wendepunkt}). \end{cases}$

- 5) Bem.: • Der unendlich ferne Punkt $O \in E(k)$ erfüllt $O * O = O$, da er ein Wendepunkt ist. • Weiter ist offensichtlich $P * Q = Q * P$ aufgrund der Def.

• Es gilt: $R = P * Q \Rightarrow P = Q * R \Rightarrow Q = R * P$, d.h. $P * (P * Q) = Q$ \square
für alle $P, Q \in E(k)$.

• Es gilt: $P * Q = P * R \Leftrightarrow Q = R$, denn \Leftarrow "v.a." \Rightarrow : Vor. $\Rightarrow P * (P * Q) = P * (P * R) \stackrel{\square}{=} Q = R$.

6.) Bem.: Man beachte, dass für $P = [a : 0 : 1] \in \mathbb{P}^2(k) \cap i(A^2(k))$ die Gerade $G(P, \mathcal{O}) = G(c, a, -a) = \{[x : y : z] \in \mathbb{P}^2(k); x - az = 0\}$

im Affinen eine Parallele zur y-Achse darstellt (Glg. $x = a$).

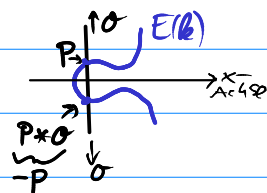
Für eine elliptische Kurve, die durch eine kurze Weierstraßform gegeben und (für $\text{char } k \neq 2$) symmetrisch zur x-Achse ist, wird typischerweise $P * \mathcal{O} \neq P$ sein.

Wegen $(\mathcal{O} * \mathcal{O}) * P = \mathcal{O} * P$ einerseits, da $\mathcal{O} * \mathcal{O} = \mathcal{O}$,

und $\mathcal{O} * (\mathcal{O} * P) = P$ andererseits, wegen \boxtimes ,

Kann die Verknüpfung $*$ also nicht assoziativ sein.

Stattdessen setzen wir unsere Verknüpfung $+$ wie folgt:



7.) Def.: Für $P, Q \in E(k)$ definieren wir

$$P + Q := \mathcal{O} * (P * Q).$$

Ist $E(k)$ in kurzer Weierstraßform und (für $\text{char } k \neq 2$) symmetrisch zur x-Achse, erhält man $P + Q$, indem man den 3. Schnittpunkt $P * Q$ von $G(P, Q)$ mit $E(k)$ dann noch an der x-Achse spiegelt, d.h. das Negative des y-Wertes nimmt.

8.) Bem.: • Es gilt: $\mathcal{O} + P = P$, d.h. \mathcal{O} ist neutrales Element von $+$, weil $\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P) = P$ nach \boxtimes gilt.

$$\begin{aligned} \bullet \text{ Es gilt: } -P &= \mathcal{O} * P, \text{ da } P + (\mathcal{O} * P) = \mathcal{O} * (P * (\mathcal{O} * P)) \\ &= (P * (\mathcal{O} * P)) * \mathcal{O} = (P * (P * \mathcal{O})) * \mathcal{O} \stackrel{\boxtimes}{=} \mathcal{O} * \mathcal{O} = \mathcal{O}. \end{aligned}$$

Es ist nicht auf Anhieb zu sehen, dass hier mit $+$ eine elliptische Kurve $E(k)$ zu einer Gruppe $(E(k), +)$ wird, sprich ob das Assoziativgesetz gilt.

9.) Lemma: Liegen drei Punkte $P, Q, R \in E(k)$ einer elliptischen Kurve auf einer projektiven Geraden G , so gilt $(P + Q) + R = \mathcal{O}$, und umgekehrt.

Dabei müssen P, Q, R nicht notwendig verschieden sein.

Bew.: Da $R = P * Q$ nach Vor., folgt $\underbrace{\mathcal{O} * R}_{-R} = \mathcal{O} * \underbrace{(P * Q)}_{P+Q}$, also $-R = P + Q$ bzw. $R + (P + Q) = \mathcal{O}$.

Umgekehrt gilt das ebenso. □

10.) Satz (von Poincaré, 1901): Sei k bel. Körper und $E(k)$ elliptische Kurve.

Die Verknüpfung $+: (P, Q) \mapsto P+Q$ macht $E(k)$ zu einer abelschen Gruppe $(E(k), +)$ mit neutralem Element \mathcal{O} , d.h. (i) $P+\mathcal{O}=P$ für alle $P \in E(k)$,

(ii) $\forall P \in E(k) \exists Q \in E(k): P+Q=\mathcal{O} \sim -P := Q$

(iii) $P+Q=Q+P$ für alle $P, Q \in E(k)$

(iv) $(P+Q)+R=P+(Q+R)$ für alle $P, Q, R \in E(k)$.

Bem.: Schwierig zu beweisen ist die Assoziativität in (iv).

Wir behandeln diese im Vorlesungsteil V14.

Bw. von (i)-(iii): Zu (i): s.o. Bem. 8.) ✓

zu (ii): Sei $P \in E(k)$, setze $Q := \mathcal{O} * P$, s.o. Bem. 8.) ✓

Zu (iii): Klar aufgrund der Def. von $P+Q$. ✓ □

11.) Bem.: • Anstelle \mathcal{O} könnte man prinzipiell jeden Punkt $Q \in E(k)$ zum neutralen Element von $+$ "machen", indem man $U \boxplus V := U+V-Q$ setzt: dann ist $U \boxplus Q = U+Q-Q=U$, $U \boxplus (-U+2Q) = U-U+2Q-Q=Q$, und $(U \boxplus V) \boxplus W = U+V+W-2Q = U \boxplus (V \boxplus W)$.

Die Eigenschaft von Lemma 9.) gilt immer noch, wenn für Q ein Wendepunkt genommen wird. Nun kann eine elliptische Kurve bis zu 9 Wendepunkten haben, vgl. (ii) Aufgabe 4a) - Blatt 5.

• Die Wahl des W.P. $\mathcal{O} := [0:1:0]$ als neutralem Element von $E(k)$ hat den Vorteil, dass die explizite Formel für $+$ rechnerisch einfacher wird, weil dann die Gleichung von $E(k)$ in einfacher (langer oder kurzer) Weierstraßform vorliegt.

Diese explizite Formel wird in Satz 13.) / Satz 14.) angegeben.

• Invertieren, d.h. Berechnen von $-P = P * \mathcal{O}$, ist dann, bei kurzer Weierstraßform in char $k \neq 2$, besonders leicht:

Man spiegelt P an der x -Achse und erhält $-P$, d.h. ist

$P = [a:b:c]$, gilt $-P = [a:-b:c]$. Schnittpunkte von $E(k)$

mit der x -Achse sind dann selbstinvers, d.h. $P = [a:0:c] \in E(k) \Rightarrow P = -P$.

12.) Bsp.: Betr. $E(\mathbb{R})$ mit der Glg. $y^2 = x^3 + 17$ bzw. $y^2 z = x^3 + 17 z^3$.

Dann liegen $P = [-1:4:1]$ und $Q = [-2:3:1]$ auf der Kurve.

Ihre Verbindungsgerade ist $G(P, Q) = \{[x:y:z] \in \mathbb{P}^2(\mathbb{R}); x - y + 5z = 0\}$.

Um $P+Q$ zu berechnen, bestimmen wir den dritten Schnittpunkt $P*Q$ von $G(P, Q)$ und $E(\mathbb{R})$ wie folgt: Setze $y = x+5$ ein und erhalte $(x+5)^2 = x^3 + 17$

⇐ $x^3 - x^2 - 10x - 8 = 0$. Da $x = -1, x = -2$ Nst. der l. G. sind, führt Polynomdiv. durch $(x+1)(x+2)$ zu $x^3 - x^2 - 10x - 8 = (x+1)(x+2)(x-4)$. Der Punkt $P*Q$ hat also x-Koordinate 4, da er auf G liegt, folgt: $P*Q = [4:9:1]$, es folgt $P+Q = [4:-9:1]$.

Ist $E(k)$ gegeben durch das lange Weierstraßpolynom

$$F(X, Y, Z) = Y^2 Z + a_1 X Y Z + a_3 Y Z^2 - X^3 - a_2 X^2 Z - a_4 X Z^2 - a_6 Z^3$$

bzw. $f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$, so möchten wir die Addition "+" für die Krypto-Anwendungen in einer expliziten Formel beschreiben:

13.) Satz: Sei $E(k)$ gegeben durch das lange Weierstraßpolynom F . Dann gilt:

(a) $P = (m, v) \in E(k) \cap A^2(k) \Rightarrow -P = (m, -v - a_1 m - a_3)$

(b) $P = (m, v), Q = (r, s) \in E(k) \cap A^2(k)$

• ist $m = r$ und $v + s + a_1 m + a_3 = 0$, gilt $P + Q = O$,

• sonst ist

$$P + Q = \left(\underbrace{\lambda^2 + a_1 \lambda - a_2 - m - r}_{=: X}, -(\lambda + a_1) X - m - a_3 \right),$$

wobei $\lambda = \frac{s-v}{r-m}, \mu = \frac{vr-sm}{r-m}$ falls $r \neq m$,

und $\lambda = \frac{3m^2 + 2a_2 m + a_4 - a_1 v}{2v + a_1 m + a_3}, \mu = \frac{-m^3 + a_4 m + 2a_6 - a_3 v}{2v + a_1 m + a_3}$ falls $r = m$.

Bew.: wäre langweiliges Nachrechnen. □

Wir geben den Beweis für die Formel bei Kurzer Weierstraßform, wo er leicht zu machen ist:

14.) Satz: Ist $E(k)$ geg. durch $f(x,y) = y^2 - x^3 - ax - b$, so gilt:

(a) Für $P = (m, v) \in E(k)$ gilt $-P = (m, -v)$

(b) Für $P = (m, v), Q = (r, s)$ mit $P \neq -Q$ ist

$$\text{ist } P+Q = (\underbrace{\lambda^2 - m - r}_{=: x}, \lambda(m-x) - v),$$

$$\text{wobei } \lambda = \begin{cases} \frac{s-v}{r-m}, & \text{falls } P \neq Q, \\ \frac{3m^2+a}{2v}, & \text{falls } P = Q. \end{cases}$$

Bem.: Der zweite Fall in b) mit $P = Q$ ist die "Punkteverdopplung" $P+P = 2P$.

Bew.: (a) ✓, (b): • Sei $P \neq -Q, P \neq Q$.

$$\text{Haben } g(P,Q) = \left\{ (m+t, v + \overset{\lambda}{\frac{s-v}{r-m}} t); t \in \mathbb{R} \right\},$$

$$\text{sowie } f(m+t, v+\lambda t) = (v+\lambda t)^2 - (m+t)^3 - a(m+t) - b$$

mit den Nullstellen $t=0, t=r-m$. Eine weitere Nullstelle ist $t=x-m$.

Die Nullstellensumme $0 + r-m + x-m = r+x-2m$ ergibt den Koeffizienten vor t^2 des Polynoms, nämlich $\lambda^2 - 3m$, es folgt $x = \lambda^2 - m - r$,

die y-Koordinate des Punkts auf $g(P,Q)$ ist dann $v + \lambda(x-m)$, für $P+Q$ dann das Negative.

• Ist $Q = P, P \neq -P$ (d.h. $v \neq 0$), nimmt man die Tangente an $E(k)$ in Punkt P ,

$$\text{also } t_p(E(k)) = \left\{ (x,y); (-3m^2-a)x + 2vy + v^2 - 2am - 3b = 0 \right\},$$

$$= \left\{ (m+t, v + \lambda t); t \in \mathbb{R} \right\} \text{ mit Steigung } \lambda := \frac{3m^2+a}{2v}.$$

Der Rest der Rechnung geht wie oben, es folgt $x = \lambda^2$ (dam $= r$) und der angegebene y-Wert für $P+P$. □