Ausarbeitung des Seminarvortrags

Das Gruppengesetz auf elliptischen Kurven: Assoziativität

Seminar Kryptographie, TU Kaiserslautern

Sommersemester 2011

Pablo Luka

Version vom 14. 05. 2011

Inhaltsverzeichnis

1 Projektive ebene Kurven

Vereinbarung 1.1. In der gesamten Ausarbeitung bezeichne K stets einen Körper. Außerdem schreiben wir auch $x_1 = x$, $x_2 = y$ und $x_3 = z$.

1.1 Die projektive Ebene

Motivation 1.2. Um das Verhalten von Schnittpunkten zweier Kurven in der affinen Ebene $\mathbb{A}^2_K := K^2$ zu untersuchen, hätte man gerne, dass sich je zwei Kurven (an mindestens einem Punkt) schneiden.

Definition 1.3. Die *projektive Ebene* $\mathbb{P}^2_K$ *über* K ist die Menge aller Geraden in $\mathbb{A}^3_K := K^3$, die $0 \in \mathbb{A}^3_K$ enthalten. Ist $0 \neq p = (p_0, p_1, p_2) \in \mathbb{A}^3_K$ gegeben, so schreiben wir

$$P = (p_0 : p_1 : p_2) := \{\lambda p \mid \lambda \in K\} \in \mathbb{P}^2_K$$

für die Gerade, die p und 0 enthält. $p_0, p_1, p_2 \in K$ nennt man auch die *homogenen Koordinaten von* P.

Bemerkung 1.4.

(a) Die Abbildung

$$\mathbb{A}^2_K \longrightarrow \mathbb{P}^2_K : (p_0, p_1) \longmapsto (p_0 : p_1 : 1)$$

ist offensichtlich injektiv. Auf diese Weise ist also $\mathbb{A}^2_K$ eine Teilmenge von $\mathbb{P}^2_K$.

(b) Genauer ist die Abbildung

$$\mathbb{P}^2_K \longrightarrow \mathbb{A}^2_K \dot\cup \mathbb{P}^1_K : (p_0 : p_1 : p_2) \longmapsto \begin{cases} (p_0 : p_1 : p_2), & p_2 = 0, \\ \left(\frac{p_0}{p_2}, \frac{p_1}{p_2}\right), & p_2 \neq 0 \end{cases}$$

bijektiv, wobei

$$\mathbb{P}^1_K := \{(p_0 : p_1 : 0) \mid (p_0, p_1) \neq (0, 0)\}$$

Gerade im Unendlichen heißt.

(c) Natürlich sind die homogenen Koordinaten eines Punktes in $\mathbb{P}^2_K$ nur bis auf die Multiplikation mit einem $\lambda \in K \setminus \{0\}$ definiert: zum Beispiel ist $(1 : 2 : 1) = (2 : 4 : 2) \in \mathbb{P}^2_{\mathbb{Q}}$. Ist $F \in K[x, y, z] \setminus \{0\}$ ein homogenes Polynom und $\lambda \in K \setminus \{0\}$, dann ist $F(\lambda x, \lambda y, \lambda z) = \lambda^{\deg f} \cdot F$, und weil K ein Körper ist, ist deshalb für jedes $p \in \mathbb{A}^3_K$ genau dann $F(p) = 0$, wenn $F(\lambda p) = 0$ ist. Damit ist es sinnvoll, $F(p_0 : p_1 : p_2) = 0$ zu schreiben, wenn $F(p_0, p_1, p_2) = 0$ ist.

Definition und Bemerkung 1.5.

(a) Eine *projektive ebene Kurve* ist die projektive Nullstellenmenge

$$V(F) := \left\{ P \in \mathbb{P}^2_K \;\middle|\; F(P) = 0 \right\} \subset \mathbb{P}^2_K$$

eines homogenen Polynoms $F \in K[x, y, z] \setminus K$. Ist K algebraisch abgeschlossen, so unterscheiden sich je zwei quadratfreie homogene Polynome $F, G \in K[x, y, z] \setminus K$ mit $V(F) = V(G)$ nur um eine Einheit, und man nennt dann $\deg V(F) := \deg F$ den *Grad* der Kurve.

(b) Ist $f \in K[x,y] \setminus K$, dann heißt das (vom Grad $\deg f$) homogene Polynom

$$z^{\deg f} \cdot f\left(\tfrac{x}{z}, \tfrac{y}{z}\right) \in K[x,y,z]$$

die *Homogenisierung von* f *bezüglich* z.

(c) Ist $F \in K[x,y,z]$ ein homogenes Polynom, so heißt $F_{z=1} := F(x,y,1) \in K[x,y]$ die *Dehomogenisierung von* f *bezüglich* z. Analog sind $F_{x=1} \in K[y,z]$ und $F_{y=1} \in K[x,z]$ definiert.

(d) Eine *projektive Gerade* ist eine projektive ebene Kurve, die durch ein *lineares homogenes Polynom* definiert wird, d.h. durch ein homogenes Polynom vom Grad 1. Insbesondere ist also die Gerade im Unendlichen, $\mathbb{P}^1_K = V(z)$, eine projektive Gerade.

(e) Eine *projektive Kubik* ist eine projektive ebene Kurve, die durch ein homogenes Polynom vom Grad 3 definiert wird.

Lemma 1.6. Sind $P, Q \in \mathbb{P}^2_K$ zwei verschiedene Punkte, so gibt es genau eine projektive Gerade, die P und Q enthält.

Beweis. Sei $P = (p_0 : p_1 : p_2)$ und $Q = (q_0 : q_1 : q_2)$. Dann hat die Matrix

$$M := \begin{pmatrix} p_0, p_1, p_2 \\ q_0, q_1, q_2 \end{pmatrix} \in \mathrm{Mat}(2 \times 3, K)$$

den Rang 2, ihr Kern also die Dimension 1. Ist $\ker M = \langle (a,b,c)^t \rangle$, so ist die gesuchte Gerade also die projektive Nullstellenmenge von $ax + by + cz \in K[x,y,z]$, und jede Gerade, die P und Q enthält, wird durch $ax + by + cz$ definiert. □

Bemerkung 1.7. Für $i = 1,2,3$ sei

$$U_i := \left\{ (p_0 : p_1 : p_2) \in \mathbb{P}^2_K \;\middle|\; p_i \neq 0 \right\} = \mathbb{P}^2_K \setminus V(x_i) \subset \mathbb{P}^2_K.$$

Offenbar ist

$$\varphi_i : \mathbb{A}^2_K \longrightarrow U_i : (a,b) \longmapsto \begin{cases} (1 : a : b), & i = 1, \\ (a : 1 : b), & i = 2, \\ (a : b : 1), & i = 3 \end{cases}$$

für alle $i = 1,2,3$ bijektiv.

1.2 Der Satz von Bézout

Definition 1.8. Sei $F \in K[x,y,z] \setminus K$ homogen. Ein Punkt $P \in V(F)$ heißt *Singularität von* $V(F)$, falls

$$\nabla F(P) = \left(\tfrac{\partial F}{\partial x}(P), \tfrac{\partial F}{\partial y}(P), \tfrac{\partial F}{\partial z}(P) \right) = (0,0,0)$$

ist. Ist P keine Singularität von $V(F)$, dann heißt die projektive Gerade

$$V\left(\tfrac{\partial F}{\partial x}(P) \cdot x + \tfrac{\partial F}{\partial y}(P) \cdot y + \tfrac{\partial F}{\partial z}(P) \cdot z \right)$$

die *Tangente von* $V(F)$ *bei* P. Beachte, dass die Definition nicht von der Wahl der homogenen Koordinaten von P abhängt, da die partielle Ableitung eines homogenen Polynoms nach einer Unbestimmten wieder homogen ist. Schließlich heißt $V(F)$ *glatt*, wenn $V(F)$ keine Singularitäten hat.

Definition und Bemerkung 1.9. Sei $P \in \mathbb{P}^2_K$ und $p = (a,b) \in \mathbb{A}^2_K$ mit $\varphi_i(a,b) = P$ für ein $i \in \{1,2,3\}$.

(a) Die Menge

$$\mathcal{O}_{\mathbb{P}^2_K,P} := \mathcal{O}_{\mathbb{A}^2_K,p} := \left\{ \frac{f}{g} \;\middle|\; f,g \in K[x,y],\ g(p) \neq 0 \right\} \subset K(x,y)$$

ist sogar ein Ring (nämlich der lokale Ring $K[x,y]_{\langle x-a,y-b\rangle}$), und heißt der *lokale Ring von* $\mathbb{A}^2_K$ *bei* p bzw. der *lokale Ring von* $\mathbb{P}^2_K$ *bei* P. Man kann zeigen, dass diese Definition nicht von der Wahl von p abhängt.

(b) Seien $F, G \in K[x,y,z] \setminus K$ zwei homogene Polynome. Dann heißt

$$I_P(V(F),V(G)) := \dim_K \left(\mathcal{O}_{\mathbb{P}^2_K,P} / \langle F_{x_i=1}, G_{x_i=1} \rangle \right) \in \mathbb{N} \cup \{\infty\}$$

die *Schnittzahl von* $V(F)$ *und* $V(G)$ *bei* P. Man kann zeigen, dass

$$I_P(V(F),V(G)) < \infty \iff \operatorname{ggt}(F,G) = 1$$

und

$$I_P(V(F),V(G)) > 0 \iff P \in V(F) \cap V(G)$$

gilt. Es gibt auch eine Möglichkeit, die Schnittzahl bei P über die Resultante von $F_{z=1}, G_{z=1} \in K[x,y] = K[x][y]$ zu bestimmen. Diese liegt in $K[x] \subset K[[x]]$, und die Schnittzahl bei P ist dann die Ordnung der Resultante, wenn man vorher P durch eine Koordinatentransformation aus $\mathrm{GL}(3,K)$ auf $(0:0:1)$ abbildet.

(c) Ist $F \in K[x,y,z] \setminus K$ homogen, dann heißt

$$\operatorname{mult}_{(0:0:1)} V(F) := \operatorname{ord} F_{z=1}$$

die *Multiplizität von* $V(F)$ *bei* $(0:0:1)$. Die Multiplizität $\operatorname{mult}_P V(F)$ von $V(F)$ bei P erhält man, wenn man P durch eine Koordinatentransformation aus $\mathrm{GL}(3,K)$ auf $(0:0:1)$ abbildet, und dann dort die Multiplizität von $V(F)$ berechnet. P heißt *einfach auf* $V(F)$, wenn $\operatorname{mult}_P V(F) = 1$ ist.

Proposition 1.10. Sei K algebraisch abgeschlossen und seien $F, G \in K[x,y,z] \setminus K$ homogen mit $\operatorname{ggt}(F,G) = 1$. Dann gilt

$$I_P(V(F),V(G)) \geq \operatorname{mult}_P V(F) \cdot \operatorname{mult}_P V(G)$$

für alle $P \in \mathbb{P}^2_K$. Dabei gilt die Gleichheit genau dann, wenn $V(F)$ und $V(G)$ keine gemeinsame Tangente besitzen.

Beweis. Die Aussage wird hier nicht bewiesen. □

Theorem 1.11 (Satz von Bézout)**.** Sei K algebraisch abgeschlossen und seien $F, G \in K[x,y,z] \setminus K$ zwei homogene Polynome mit $\operatorname{ggt}(F,G) = 1$. Dann gilt

$$\sum_{P \in V(F) \cap V(G)} I_P(V(F),V(G)) = \deg(F) \cdot \deg(G).$$

Insbesondere ist $V(F) \cap V(G) \neq \emptyset$.

Beweis. Die Aussage wird hier nicht bewiesen. □

Beispiel 1.12. Sei K algebraisch abgeschlossen und seien $F, G \in K[x,y,z]$ homogen vom Grad 1 mit $\operatorname{ggt}(F,G) = 1$. Dann sind $V(F)$ und $V(G)$ zwei verschiedene projektive Geraden, und nach dem Satz von Bézout schneiden sie sich in genau einem Punkt.

Korollar 1.13. Ist K beliebig und sind $F, G \in K[x,y,z] \setminus K$ zwei homogene Polynome mit $\operatorname{ggt}(F,G) = 1$, dann gilt

$$|V(F) \cap V(G)| \leq \sum_{P \in V(F) \cap V(G)} I_P(V(F), V(G)) \leq \deg(F) \cdot \deg(G).$$

Beweis. Dies folgt unmittelbar aus dem Satz von Bézout, denn ist $\overline{K}$ der algebraische Abschluss von K, so sind $V(F)$ und $V(G)$ in $\mathbb{P}^2_K$ Teilmengen von $V(F)$ und $V(G)$ in $\mathbb{P}^2_{\overline{K}}$. Also ist jeder Schnittpunkt der beiden Kurven in $\mathbb{P}^2_K$ auch ein Schnittpunkt der Kurven in $\mathbb{P}^2_{\overline{K}}$. □

Korollar 1.14. Sei K algebraisch abgeschlossen. Sind $F, G \in K[x,y,z] \setminus K$ zwei homogene Polynome mit $\operatorname{ggt}(F,G) = 1$, dann gilt

$$\sum_{P \in V(F) \cap V(G)} \operatorname{mult}_P V(F) \cdot \operatorname{mult}_P V(G) \leq \deg(F) \cdot \deg(G).$$

Beweis. Dies folgt unmittelbar aus Proposition 1.10 und dem Satz von Bézout. □

Korollar 1.15. Sind $V(F)$ und $V(G)$ zwei projektive ebene Kurven mit $|V(F) \cap V(G)| > \deg(F) \cdot \deg(G)$, so muss $\operatorname{ggt}(F,G) \neq 1$ gelten.

Korollar 1.16. Sind $V(F)$ und $V(G)$ zwei projektive ebene Kurven mit $|V(F) \cap V(G)| = \deg(F) \cdot \deg(G)$, dann sind alle $P \in V(F) \cap V(G)$ einfach auf $V(F)$ und auf $V(G)$.

Spezialfall 1.17. Ist K algebraisch abgeschlossen, $L \subset \mathbb{P}^2_K$ eine projektive Gerade und $C \subset \mathbb{P}^2_K$ eine projektive Kubik, dann ist

$$\sum_{P \in L \cap C} I_P(L, C) = 1 \cdot 3 = 3.$$

1.3 Der Noethersche Fundamentalsatz

Theorem 1.18 (Max Noethers Fundamentalsatz, AF+BG-Theorem)**.** Sei K algebraisch abgeschlossen und seien $F, G, H \in K[x,y,z] \setminus K$ homogen mit $\operatorname{ggt}(F,G) = 1$. Es gibt genau dann homogene $A, B \in K[x,y,z]$ mit

$$\deg A = \deg H - \deg F, \quad \deg B = \deg H - \deg G \quad \text{und} \quad H = AF + BG,$$

wenn

$$H_{x_i=1} \in \langle F_{x_i=1}, G_{x_i=1} \rangle \trianglelefteq \mathcal{O}_{\mathbb{P}^2_K, P} \quad \text{für alle } P \in V(F) \cap V(G),\ i \in \{1,2,3\} \quad \text{mit } \varphi_i^{-1}\{P\} \neq \emptyset$$

gilt.

Beweis. Die Aussage wird hier nicht bewiesen. □

Definition und Bemerkung 1.19. Sei K algebraisch abgeschlossen.

(a) Ein *Nullzyklus in* $\mathbb{P}^2_K$ ist eine formale Summe $\sum_{P \in \mathbb{P}^2_K} n_P P$, wobei die n_P ganze Zahlen sind und fast alle n_P verschwinden. Die Menge aller Nullzyklen in $\mathbb{P}^2_K$ ist eine abelsche Gruppe. Der *Grad* eines Nullzyklus' $\sum_{P \in \mathbb{P}^2_K} n_P P$ ist $\sum_{P \in \mathbb{P}^2_K} n_P$.
Man sagt, der Nullzyklus $N_1 = \sum_{P \in \mathbb{P}^2_K} n_P P$ ist *größer* als ein Nullzyklus $N_2 = \sum_{P \in \mathbb{P}^2_K} m_P P$ (und schreibt dann $N_1 \geq N_2$), wenn $n_P \geq m_P$ für alle P gilt.
Schließlich heißt ein Nullzyklus $\sum_{P \in \mathbb{P}^2_K} n_P P$ *positiv*, wenn alle n_P nicht-negativ sind, d.h. wenn er größer als der triviale Nullzyklus ist.

(b) Seien $F, G \in K[x,y,z]$ homogen mit $\operatorname{ggt}(F,G) = 1$. Dann heißt der positive Nullzyklus

$$V(F) \bullet V(G) := \sum_{P \in \mathbb{P}^2_K} I_P(V(F), V(G))P$$

der *Schnittzyklus von* $V(F)$ *und* $V(G)$. Ist K algebraisch abgeschlossen, so hat dieser Schnittzyklus offenbar den Grad $\deg(F) \cdot \deg(G)$ nach dem Satz von Bézout.
Offensichtlich gilt $V(F) \bullet V(G) = V(G) \bullet V(F)$.

(c) Für homogene $F, G, H \in K[x,y,z] \setminus K$ mit $\operatorname{ggt}(F,G) = \operatorname{ggt}(F,H) = 1$ gilt

$$V(F) \bullet V(G \cdot H) = V(F) \bullet V(G) + V(F) \bullet V(H),$$

und ist zusätzlich $A \in K[x,y,z]$ homogen mit $\deg A = \deg G - \deg F$, dann gilt außerdem

$$V(F) \bullet V(G + A \cdot F) = V(F) \bullet V(G).$$

Proposition 1.20. Sei K algebraisch abgeschlossen, seien $F, G, H \in K[x,y,z] \setminus K$ homogen und sei $P \in V(F) \cap V(H) \subset \mathbb{P}^2_K$. Wenn

$$\operatorname{mult}_P V(F) = 1 \quad \text{und} \quad I_P(V(H), V(F)) \geq I_P(V(G), V(F))$$

gilt, dann ist

$$H_{x_i=1} \in \langle F_{x_i=1}, G_{x_i=1} \rangle \trianglelefteq \mathcal{O}_{\mathbb{P}^2_K, P} \quad \text{für alle} \quad P \in V(F) \cap V(G),\ i \in \{1,2,3\} \quad \text{mit} \quad \varphi_i^{-1}\{P\} \neq \emptyset.$$

Beweis. Die Aussage wird hier nicht bewiesen. □

Korollar 1.21. Sei K algebraisch abgeschlossen und seien $F, G, H \in K[x,y,z] \setminus K$ homogen mit $\operatorname{ggt}(F,G) = 1$. Sind alle Schnittpunkte von $V(F)$ und $V(G)$ einfach auf $V(F)$, und gilt außerdem

$$V(H) \bullet V(F) \geq V(G) \bullet V(F),$$

dann gibt es ein homogenes $B \in K[x,y,z] \setminus K$ mit $\deg B = \deg H - \deg G$ und

$$V(B) \bullet V(F) = V(H) \bullet V(F) - V(G) \bullet V(F).$$

Beweis. Da die Voraussetzungen von Proposition 1.20 erfüllt sind, gibt es nach dem Noetherschen Fundamentalsatz homogene $A, B \in K[x,y,z]$ mit

$$\deg A = \deg H - \deg F, \quad \deg B = \deg H - \deg G \quad \text{und} \quad H = AF + BG,$$

und es folgt

$$V(H) \bullet V(F) = V(AF + BG) \bullet V(F) = V(BG) \bullet V(F) = V(B) \bullet V(F) + V(G) \bullet V(F).$$

□

Proposition 1.22. Sei K algebraisch abgeschlossen und seien C, C' und C'' projektive Kubiken. Sei außerdem $C' \bullet C = \sum_{i=1}^{9} P_i$ für (nicht notwendig verschiedene) $P_1, \ldots, P_9 \in \mathbb{P}^2_K$, die auf C einfach sind, und sei $Q \in \mathbb{P}^2_K$ mit $C'' \bullet C = \sum_{i=1}^{8} P_i + Q$. Dann ist $Q = P_9$.

Beweis. Seien $F, G \in K[x,y,z] \setminus K$ homogen mit $V(F) = C$ und $V(G) = C'$. Da $V(F) \cap V(G)$ endlich ist, muss $\operatorname{ggt}(F,G) = 1$ gelten.
Angenommen, P_9 und Q sind verschieden. Dann gibt es eine projektive Gerade L mit $P_9 \in L$ und $Q \notin L$. Nach dem Spezialfall 1.17 des Satzes von Bézout gibt es dann Punkte $R, S \in \mathbb{P}^2_K$ mit $L \bullet C = P_9 + R + S$.

Offenbar definiert das Produkt H der Polynome, die L und C'' definieren, eine projektive Kurve $V(H)$ vom Grad 4. Es folgt

$$V(H) \bullet C = L \bullet C + C'' \bullet C = P_9 + S + R + \sum_{i=1}^{8} P_i + Q = C' \bullet C + Q + R + S,$$

also gilt insbesondere

$$V(H) \bullet V(F) \geq V(G) \bullet V(F).$$

Nach Korollar 1.21 gibt es ein homogenes $B \in K[x, y, z] \setminus K$ vom Grad $\deg B = \deg H - \deg G = 4 - 3 = 1$ mit

$$V(B) \bullet V(F) = V(H) \bullet V(F) - V(G) \bullet V(F) = C' \bullet C + Q + R + S - C' \bullet C = Q + R + S.$$

Also ist $V(B)$ eine Gerade, die Q, R und S enthält. Insbesondere ist $R, S \in L \cap V(B)$, und nach Lemma 1.6 muss deshalb $L = V(B)$ und damit $Q \in L$ gelten. Also gibt es keine solche Gerade L, d.h. es ist $Q = P_9$. □

2 Elliptische Kurven

2.1 Grundlagen

Definition 2.1. Seien $a_1, \ldots, a_6 \in K$. Die Gleichung

$$E^* : \quad y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

heißt die *homogene Weierstraß-Gleichung bezüglich* $a_1, \ldots, a_6$. Dabei handelt es sich um die Homogenisierung der *affinen Weierstraß-Gleichung*

$$E : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

bezüglich $a_1, \ldots, a_6$. Die Nullstellenmenge von

$$F^* := y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3)$$

bezeichnet man mit $E(K) := V(F^*) \subset \mathbb{P}^2_K$.

Beispiel 2.2. Für $a_1 = a_2 = a_3 = 0$, $a_4 = 2$ und $a_6 = -1$ gilt

$$E(\mathbb{F}_5) = \{(0,2), (0,3), (2,1), (2,4), (4,1), (4,4)\}.$$

Definition und Bemerkung 2.3. Die projektive Kubik $E(K) \subset \mathbb{P}^2_K$ heißt *elliptische Kurve*, falls $E(K)$ glatt ist.

Bemerkung 2.4. Sei $E(K)$ eine elliptische Kurve und sei

$$F^* = y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3)$$

mit $a_1, \ldots, a_6 \in K$.

(a) Die partiellen Ableitungen von F^* sind

$$\begin{aligned} \tfrac{\partial F^*}{\partial x} &= a_1yz - 3x^2 - 2a_2xz - a_4z^2, \\ \tfrac{\partial F^*}{\partial y} &= 2yz + a_1xz + a_3z^2, \\ \tfrac{\partial F^*}{\partial z} &= y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2. \end{aligned}$$

(b) Offensichtlich ist $\mathbb{P}^1_K \cap E(K) = \{(0:1:0)\}$, und wegen $\nabla F^*(0:1:0) = (0,0,1)$ ist die Tangente L an $E(K)$ bei $(0:1:0)$ die Gerade $\mathbb{P}^1_K = V(z)$ im Unendlichen. Insbesondere ist $(0:1:0)$ in L enthalten.
Außerdem kann man zeigen, dass $I_{(0:1:0)}(L, E(K)) = 3$ gilt. (Der algebraische Grund hierfür ist die dritte Potenz bei $F^*(x,y,0) = -x^3$.)
Wegen $\frac{\partial F^*}{\partial z}(0,1,0) = 1 \neq 0$ ist $(0:1:0)$ keine Singularität.

(c) Allgemeiner kann man zeigen, dass alle Punkte $P \in E(K)$ in ihrer Tangente L an $E(K)$ enthalten sind mit $I_P(L, E(K)) \geq 2$.

2.2 Das Gruppengesetz auf elliptischen Kurven

Definition 2.5. Sei K algebraisch abgeschlossen, sei $E(K)$ eine elliptische Kurve und seien $P, Q \in E(K)$ gegeben.

(a) Wir setzen $O := (0 : 1 : 0)$.

(b) Ist $P \neq Q$, dann sei L die projektive Gerade, die P und Q verbindet. Sonst sei L die Tangente an $E(K)$ bei $P = Q$. In jedem Fall gibt es nach dem Spezialfall 1.17 des Satzes von Bézout und nach Bemerkung 2.4(c) einen eindeutigen Punkt $R \in E(K)$ mit $L \bullet E(K) = P + Q + R$. Wir schreiben $P * Q := R$.

(c) Außerdem sei $P + Q := (P * Q) * O$.

Theorem 2.6. Sei K algebraisch abgeschlossen und seien $P, Q, R \in E(K)$.

(a) Die Verknüpfungen $*$ und $+$ sind kommutativ, es ist $(P * Q) * P = Q$ und $O * O = O$.

(b) Ist $L \subset \mathbb{P}^2_K$ eine beliebige Gerade mit $E(K) \cap L = \{P, Q, R\}$, dann ist $(P + Q) + R = 0$.

(c) Es ist $P + O = P$, und $P + Q = O$ genau dann, wenn $P * Q = O$ ist.

(d) Es ist $(P + Q) + R = P + (Q + R)$.

Insbesondere ist $(E(K), +)$ eine abelsche Gruppe mit neutralem Element O, und es ist $-P = P * O$.

Beweis.

(a) Die Kommutativität von $*$ und $+$ folgt direkt aus ihrer Konstruktion. Nach der Definition von $*$ gilt außerdem $(P * Q) * P = Q$, und $O * O = O$ gilt nach Bemerkung 2.4(b).

(b) Wegen $P * Q = R$ und unter der Benutzung von (a) ist

$$(P + Q) + R = (((P * Q) * O) * R) * O = ((R * O) * R) * O = O * O = O.$$

(c) Es ist

$$P + O = (P * O) * O = (O * P) * O = P,$$

und außerdem gilt

$$P + Q = O \iff (P * Q) * O = O \iff ((P * Q) * O) * O = O * O = O$$
$$\iff (P * Q) + O = O \iff P * Q = O * O = O.$$

(d) Seien $L_1, M_1, L_2, M_2, L_3, M_3$ projektive Geraden und $S', S, T', U', U, T'' \in E(K)$ definiert durch

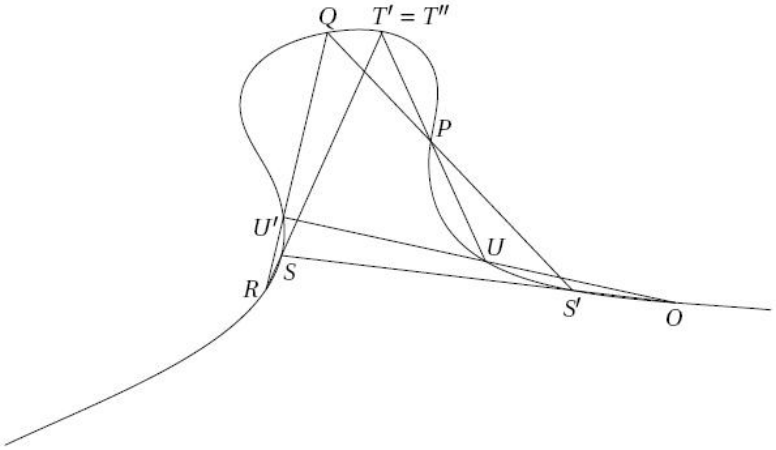
$$\begin{aligned}
L_1 \bullet E(K) &= P + Q + S', \\
M_1 \bullet E(K) &= O + S' + S, \\
L_2 \bullet E(K) &= S + R + T', \\
M_2 \bullet E(K) &= Q + R + U', \\
L_3 \bullet E(K) &= O + U' + U, \\
M_3 \bullet E(K) &= P + U + T'',
\end{aligned}$$

also wie in der folgenden Abbildung (siehe [F2008], Proposition 5.6). Multipliziert man die linearen homogenen Polynome, die L_1, L_2 und L_3 definieren, so erhält man eine projektive Kubik C'. Analog erhält man eine Kubik C'' aus M_1, M_2 und M_3, und offenbar gilt

$$\begin{aligned}
C' \bullet E(K) &= O + P + Q + R + S + S' + U + U' + T', \\
C'' \bullet E(K) &= O + P + Q + R + S + S' + U + U' + T''.
\end{aligned}$$

Beachte, dass $O, P, Q, R, S, S', U, U', T'$ nicht notwendig verschieden, und deshalb einfach auf $E(K)$ sind. Aus Proposition 1.22 folgt deshalb $T' = T''$, und damit schließlich

$$(P + Q) + R = (((P * Q) * O) * R) * O = ((S' * O) * R) * O = (S * R) * O = T' * O$$
$$= T'' * O = (P * U) * O = (P * (U' * O)) * O = (P * ((U * R) * O)) * O = P + (Q + R).$$



□

Bemerkung 2.7. Sei $\overline{K}$ der algebraische Abschluss von K und $f \in K[x]$ ein Polynom vom Grad $d \geq 1$. Sind $a_1, \ldots, a_d \in \overline{K}$ die Nullstellen von f und gilt $a_1, \ldots, a_{d-1} \in K$, so ist wegen

$$a_d = x - \frac{f}{LC(f) \cdot (x - a_1) \cdots (x - a_{d-1})} \in K[x]$$

auch $a_d \in K$.

Proposition 2.8. Ist $\overline{K}$ der algebraische Abschluss von K, so ist $E(K)$ eine Untergruppe von $E\left(\overline{K}\right)$.

Beweis. Offenbar reicht es für $P, Q \in E(K)$ zu zeigen, dass auch $P * Q \in E(K)$ gilt. Ohne Einschränkung sei $O \notin \{P, Q, P * Q\}$. Ist $F \in K[x, y]$ das inhomogene $E(K)$ definierende Polynom und $L = V(ax + by + cz)$ die Gerade, die man zur Berechnung von $P * O$ verwendet, so sind die homogenen y-Koordinaten von P, Q und $P * Q$ Nullstellen des Polynoms $F\left(-\frac{b}{a}y - \frac{c}{a}, y\right) \in K[y]$ vom Grad 3. Nach Bemerkung 2.7 folgt, dass $P * Q \in E(K)$ ist. □

Literaturverzeichnis

[B2011] Mohamed Barakat: *Cryptography*. Vorlesungsskript, 2010/2011.
http://www.mathematik.uni-kl.de/~barakat/Lehre/WS10/Cryptography/lecture_notes/Cryptography.pdf

[F2008] William Fulton: *Algebraic Curves*. 2008.
http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[M2010] Thomas Markwig: *Computational Algebraic Geometry*. Vorlesungsskript, 2010.
http://www.mathematik.uni-kl.de/~keilen/download/LectureNotes/compalggeom.pdf

[M2009] Thomas Markwig: *Theorie und Visualisierung algebraischer Kurven und Flächen*. Vortragsausarbeitung, 2009.
http://www.mathematik.uni-kl.de/~keilen/download/Lehre/EMWS08/fortbildung.pdf

Index