Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 6

Die Gruppenstruktur

Ein wesentliches Charakteristikum einer elliptischen Kurve ist, dass es auf ihr die Struktur einer kommutativen Gruppe gibt, die wir additiv schreiben. Dabei ist der Nullpunkt frei wählbar, man kann jeden K-Punkt als neutrales Element wählen. Dies ist der Grund, warum man bei der Definition einer elliptischen Kurve die Existenz eines K-rationalen Punktes fordert. Allerdings ist die Verknüpfung geometrisch signifikanter, wenn man einen Wendepunkt als Nullpunkt wählt. Meistens arbeitet man mit einer kurzen Weierstraßgleichung und setzt dann den unendlich fernen Punkt $(0,1,0)$ als Nullpunkt $\mathfrak{O}$ an.

Bemerkung 6.1. Die Idee zu dieser Addition ist recht einfach und zeigt, warum hier der Kurvengrad 3 entscheidend ist. Zwei verschiedene Punkte $P,Q \in E \subseteq \mathbb{P}^2$ legen eine projektive Gerade G in der projektiven Ebene fest. Der Durchschnitt $E \cap G$ besteht aus drei Punkten, gezählt mit Multiplizitäten, wobei natürlich P und Q zum Durchschnitt gehören. Wenn die Gerade G weder zu P noch zu Q tangential ist, so gibt es noch einen weiteren Schnittpunkt R. Dieser Punkt ist nun *nicht* die Summe von P und Q. Dies kann nicht sein, da ja die drei Punkte des Schnittes gleichberechtigt sind (dann würde beispielsweise $P+Q+Q = R+Q = P$, also $Q+Q = \mathfrak{O}$ mit dem Nullpunkt $\mathfrak{O}$ für alle Punkte gelten). Stattdessen soll für ein solches kolineares Punktetripel

$$P+Q+R = \mathfrak{O}$$

gelten, also $P+Q = -R$. Wo liegt $-R$? Nach dem gleichen Prinzip gilt

$$-R+R+\mathfrak{O} = \mathfrak{O},$$

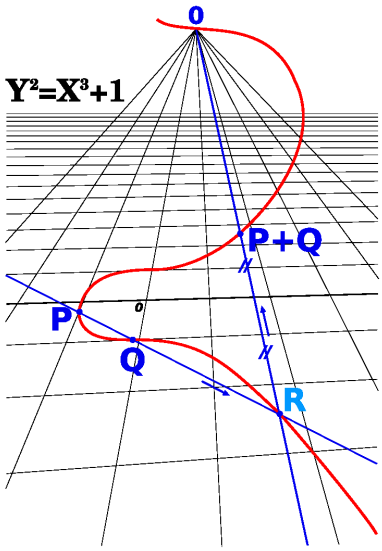
d.h. $-R$ ist der dritte Schnittpunkt der Kurve mit der durch $\mathfrak{O}$ und R festgelegten Geraden. Wenn die Gerade G tangential zu P und wenn R der dritte Schnittpunkt ist, so ist die obige Gleichung als

$$2P+R = \mathfrak{O}$$

zu interpretieren und

$$P+R = -P$$

bzw. $2P = -R$. Für den Nullpunkt ergibt sich aus $2\mathfrak{O} = -R = \mathfrak{O}$, dass $\mathfrak{O}$ eine Wendepunkt sein muss. Von dieser Idee her kann man sich gut vorstellen, dass es eine wohldefinierte Verknüpfung auf einer elliptischen Kurve gibt. Es ist aber keineswegs klar, dass diese durch polynomiale Ausdrücke gegeben ist, dass sie assoziativ ist und dass es sich wirklich um eine Gruppe handelt.



DEFINITION 6.2. Es sei $E = V_+(F) \subseteq \mathbb{P}^2_K$ eine elliptische Kurve über K und sei $\mathfrak{O} \in E$ ein fixierter K- Wendepunkt der Kurve. Zu K-Punkten $P, Q \in E$ sei $\overline{P,Q}$ die projektive Gerade durch P und Q, die bei $P = Q$ als Tangente durch P zu interpretieren ist, und sei $P \star Q$ der neben P und Q dritte Punkt auf der Kurve. Dann nennt man

$$-P := \mathfrak{O} * P$$

das *Negative* zu P und

$$P + Q := -(P * Q) = \mathfrak{O} * (P * Q)$$

die *Summe* der beiden Punkte.

SATZ 6.3. *Es sei $E = V_+(F) \subseteq \mathbb{P}^2_K$ eine elliptische Kurve über einem Körper K und sei $\mathfrak{O} \in E$ ein fixierter K-Wendepunkt der Kurve. Dann bildet die Menge der K-Punkte von E mit der Addition eine kommutative Gruppe mit $\mathfrak{O}$ als neutralem Element.*

Beweis. Die Verknüpfung ist wohldefiniert, da $\star$ auf einer glatten Kurve vom Grad 3 wohldefiniert ist. Die Verknüpfung ist kommutativ, da dies für $\star$ gilt. Es ist

$$P + \mathfrak{O} = \mathfrak{O} \star (\mathfrak{O} \star P).$$

Rechts steht der neben $\mathfrak{O}$ und P dritte Punkt der dadurch definierten Geraden $\overline{\mathfrak{O}, P}$. Dieser Punkt definiert aber mit $\mathfrak{O}$ eben diese Gerade, und daher ist der dritte Punkt darauf neben diesem Punkt und $\mathfrak{O}$ wiederum gleich P. Das bedeutet, dass $\mathfrak{O}$ das neutrale Element ist. Ferner ist

$$P + (-P) = \mathfrak{O} \star (P \star (-P)) = \mathfrak{O} \star (P \star (\mathfrak{O} \star P)) = \mathfrak{O} \star \mathfrak{O} = \mathfrak{O},$$

wobei die letzte Gleichheit darauf beruht, dass $\mathfrak{O}$ ein Wendepunkt ist.

Zum Nachweis der Assoziativität $(P+Q)+R = P+(Q+R)$ betrachten wir die folgenden Geraden mit jeweils drei relevanten Punkten, die auf der elliptischen Kurve liegen.

(1) L_1 durch $P, Q, -(P+Q)$.
(2) L_2 durch $R, P+Q, -((P+Q)+R)$.
(3) L_3 durch $Q+R, \mathfrak{O}, -(Q+R)$.
(4) L_4 durch $Q, R, -(Q+R)$.
(5) L_5 durch $P, Q+R, -(P+(Q+R))$.
(6) L_6 durch $P+Q, \mathfrak{O}, -(P+Q)$.

Es sei

$$D := L_1 \cup L_2 \cup L_3$$

und

$$D' := L_4 \cup L_5 \cup L_6,$$

die selbst kubische Kurven sind, ihr Durchschnitt mit E besteht aus den angeführten neun Punkten, die im Allgemeinen aber mit Multiplizitäten auftreten können. Wir nehmen an, dass alle Punkte verschieden sind, die anderen Situationen erfordern Sonderbetrachtungen, siehe Aufgabe 6.2. Die Schnittpunkte $E \cap D$ sind also

$$\mathfrak{O}, P, Q, R, P+Q, -(P+Q), Q+R, -(Q+R), -((P+Q)+R),$$

die Schnittpunkte $E \cap D'$ sind die gleichen Punkte mit der Ausnahme, dass ganz hinten $-(P+(Q+R))$ steht. Nach Satz Anhang 3.1 folgt in dieser Situation aber (wir können zum algebraischen Abschluss übergehen)

$$-((P+Q)+R) = -(P+(Q+R)).$$

□

Auch wenn $\mathfrak{O}$ kein Wendepunkt der Kurve ist, so kann man ihn dennoch als neutrales Element einer Gruppenaddition nehmen. In diesem Fall muss man die Definition des Negativen folgendermaßen abändern: Es sei $\mathfrak{O}'$ der dritte Schnittpunkt der Tangente an $\mathfrak{O}$ mit der Kurve. Dann ist $-P$ der dritte Schnittpunkt der Gerade durch P und $\mathfrak{O}$.

Bemerkung 6.4. Zu einer elliptischen Kurve E über K ist nach Satz 6.3 $(E(K), +, \mathfrak{O})$, die Menge der K-rationalen Punkte von E, eine kommutative Gruppe. Zu einer Körpererweiterung $K \subseteq L$ gehört die Gruppe $(E(L), +, \mathfrak{O})$, in der $E(K)$ eine Untergruppe ist. Die Gruppe $E(K)$ kann endlich oder unendlich sein. Für einen endlichen Körper K ist $E(K)$ stets endlich, da ja $\mathbb{P}^2_K$ nur endlich viele K-Punkte besitzt. Für einen algebraisch abgeschlossenen Körper ist $E(K)$ stets unendlich. Für $K = \mathbb{Q}$ oder einen anderen Zahlkörper ist es eine schwierige Frage, ob $E(K)$ endlich oder unendlich ist. Der wichtigste Satz ist hierbei der Satz von Mordell-Weil.

SATZ 6.5. *Es sei E eine elliptische Kurve über einem Körper K mit kurzer Weierstraßgleichung $y^2 = x^3 + ax + b$. Es sei der unendlich ferne Punkt $\mathfrak{O} = (0,1,0)$ als neutrales Element festgelegt. Dann ist die Negation auf E durch*

$$-(x,y) = (x,-y)$$

und die Addition auf E durch die rationalen Ausdrücke

$$(x_1,y_1)+(x_2,y_2) = \left(\alpha^2 - x_1 - x_2,\, -\alpha^3 + \alpha(x_1+x_2) - \beta\right)$$

mit

$$\alpha = \frac{y_2-y_1}{x_2-x_1} = \frac{x_1^2+x_1x_2+x_2^2+a}{y_2+y_1}$$

und

$$\beta = y_1 - \alpha x_1 = \frac{x_2y_1 - x_1y_2}{x_2-x_1}$$

gegeben.

Beweis. Wir bestimmen zuerst das Negative. Zu einem Punkt

$$P = (x,y)$$

ist die Verbindungsgerade mit $\mathfrak{O}$ durch die affine Gleichung

$$X - x = 0$$

bzw. die projektive Geichung $X - xZ = 0$ gegeben. Auf dieser Geraden liegt auch der Punkt $(x,-y)$, der auch auf der elliptischen Kurve liegt, da ja dort y allein quadratisch eingeht. Also ist $-P = (x,-y)$ der dritte Punkt dieser Geraden. Wenn hierbei $y = 0$ ist, so ist

$$-P = P$$

und die eben angeführte Gerade ist tangential an diesen Punkt.

Der Ausdruck α bedeutet die Steigung der Verbindungsgeraden. Wegen

$$\begin{aligned}
\frac{y_2-y_1}{x_2-x_1} &= \frac{(y_2-y_1)(y_2+y_1)}{(x_2-x_1)(y_2+y_1)} \\
&= \frac{y_2^2-y_1^2}{(x_2-x_1)(y_2+y_1)} \\
&= \frac{x_2^3+ax_2+b-x_1^3-ax_1-b}{(x_2-x_1)(y_2+y_1)} \\
&= \frac{(x_2-x_1)(x_2^2+x_1x_2+x_1^2+a)}{(x_2-x_1)(y_2+y_1)} \\
&= \frac{x_2^2+x_1x_2+x_1^2+a}{y_2+y_1}
\end{aligned}$$

stimmen die beiden Ausdrücke für α als Elemente des Funktionenkörpers zum affinen Koordinatenring $K[X,Y]/(Y^2-X^3-aX-b)$ und ebenso als K-wertige Funktionen außerhalb der Polstellen überein. Die Steigung der

Verbindungsgerade besitzt also eine zweifache Darstellung, aus der rechten Darstellung ist klar, dass sie auch bei

$$(x_1, y_1) = (x_2, y_2)$$

bei $y_1 \neq 0$ definiert ist und dass der Zähler in die Ableitung $3x_1^2+a$ übergeht. Bei $x_1 = x_2$ und $y_2 = -y_1$ ist der Ausdruck nicht definiert, dies ist der oben behandelte Fall der Negation, wo ja die Summe $\mathfrak{O}$ ergibt.

Gemäß der Definition der Addition müssen wir zu den beiden Punkten (x_1, y_1) und (x_2, y_2) die zugehörige Verbindungsgerade (bzw. Tangente im identischen Fall) und den dritten Schnittpunkt mit der Kurve bestimmen. Seien die Punkte zunächst verschieden. Die verbindende Gerade ist dann

$$(y_2 - y_1)X - (x_2 - x_1)Y - x_1y_2 + x_2y_1 = 0$$

(einfach die beiden Punkte einsetzen). Da die Punkte verschieden sind, sind sie in mindestens einer Koordinaten verschieden und somit liegt in der Tat eine Gerade vor. Wenn $x_1 = x_2$ ist, so ist

$$y_1 = -y_2,$$

und die verbindende Gerade wird wie oben zu

$$X - x_1 = 0$$

mit $\mathfrak{O}$ als drittem Schnittpunkt. In diesem Fall ist

$$P + Q + \mathfrak{O} = \mathfrak{O}.$$

Sei nun $x_1 \neq x_2$. Wir schreiben die Geradengleichung als

$$Y = \alpha X + \beta$$

mit

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1}$$

und

$$\beta = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}.$$

Hier tritt also die erste Beschreibung für α auf.

Wir betrachten nun den Fall $(x_1, y_1) = (x_2, y_2)$ mit $y_1 \neq 0$. Die Tangente in einem Punkt (x_1, y_1) ist durch die lineare Gleichung

$$(3x_1^2 + a)(x - x_1) - 2y_1(y - y_1) = 0$$

gegeben. Diese Gerade hat mit der Kurve in (x_1, y_1) einen doppelten Schnittpunkt und es muss noch einen weiteren Schnittpunkt geben. Wenn man die Gleichung nach y auflöst, so erhält man

$$\begin{aligned} y &= \frac{(3x_1^2 + a)x - 3x_1^3 - ax_1 + 2y_1^2}{2y_1} \\ &= \frac{3x_1^2 + a}{2y_1}x + \frac{-3x_1^3 - ax_1 + 2y_1^2}{2y_1} \\ &= \alpha x + \beta, \end{aligned}$$

hier tritt für α die zweite Beschreibung auf.

Ein Punkt auf der Geraden hat die Form $(x, \alpha x + \beta)$. Die Bedingung, dass er auf der Kurve liegt, wird zu

$$(\alpha x + \beta)^2 \;=\; \alpha^2 x^2 + 2\alpha\beta x + \beta^2 \;=\; x^3 + ax + b$$

bzw. zu

$$x^3 - (\alpha x + \beta)^2 + ax + b \;=\; 0.$$

Von dieser Gleichung in der einen Variablen x kennen wir aber schon die Lösungen x_1 und x_2, die auch gleich sein können. Deshalb gilt

$$x^3 - (\alpha x + \beta)^2 + ax + b \;=\; (x - x_1)(x - x_2)(x - x_3)$$

mit einer dritten, noch nicht bekannten Lösung x_3. Der Koeffizient zu x^2 führt auf

$$\alpha^2 \;=\; x_1 + x_2 + x_3$$

und damit

$$x_3 \;=\; \alpha^2 - x_1 - x_2$$

und

$$\begin{aligned} y_3 &= -\alpha x_3 - \beta \\ &= -\alpha^3 + \alpha(x_1 + x_2) - \beta. \end{aligned}$$

□

Beispiel 6.6. Wir möchten auf der durch

$$y^2 \;=\; x^3 + 1$$

gegebenen elliptischen Kurve die beiden Punkte $(0, 1)$ und $(2, 3)$ addieren. Gemäß Satz 6.5 ist $\alpha = \frac{3-1}{2-0} = 1$ und damit

$$(0, 1) + (2, 3) \;=\; (1 - 0 - 2, -1 + 2 - 1) \;=\; (-1, 0).$$

Korollar 6.7. *Es sei E eine elliptische Kurve über einem Körper K mit kurzer Weierstraßgleichung $y^2 = x^3 + ax + b$. Dann ist die Verdoppelung eines Punktes (x, y) mit $y \neq 0$ durch die rationalen Ausdrücke*

$$\begin{aligned} & 2(x, y) \\ = \;& \big(\alpha^2 - 2x,\, -\alpha^3 + 3x\alpha - y\big) \\ = \;& \left(\frac{9x^4 + 6ax^2 + a^2}{4(x^3 + ax + b)} - 2x,\, \left(-\frac{(3x^2 + a)^3}{8(x^3 + ax + b)^2} + \frac{3x(3x^2 + a)}{2(x^3 + ax + b)} - 1\right)y\right) \\ = \;& \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)},\, \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8(x^3 + ax + b)^2}y\right) \end{aligned}$$

mit

$$\alpha \;=\; \frac{3x^2 + a}{2y}$$

gegeben.

Beweis. Dies folgt aus Satz 6.5, wobei man für α wegen $x_1 = x_2 = x$ den zweiten Ausdruck verwenden muss. Für die letzte Darstellung siehe Aufgabe 6.13. □

KOROLLAR 6.8. *Es sei E eine elliptische Kurve über einem Körper K mit kurzer Weierstraßgleichung $y^2 = x^3 + ax + b$. Es sei*

$$f_2 = \frac{9x^4 + 6ax^2 + a^2}{4(x^3 + ax + b)} - 2x,$$

$$q_2 = -\frac{(3x^2 + a)^3}{8(x^3 + ax + b)^2} + \frac{3x(3x^2 + a)}{2(x^3 + ax + b)} - 1$$

und wir definieren rekursiv

$$f_{m+1} = \frac{(q_m - 1)^2(x^3 + ax + b)}{(f_m - x)^2} - x - f_m$$

und

$$q_{m+1} = -\frac{(q_m - 1)^3(x^3 + ax + b)}{(f_m - x)^3} + \frac{(q_m - 1)}{f_m - x}(2x + f_m) - 1,$$

wobei es sich um rationale Funktionen in der einen Variablen x handelt. Dann wird die m-te Vervielfachung eines Punktes (x, y) auf E durch die rationalen Ausdrücke

$$m(x, y) = (f_m,\, q_m y)$$

beschrieben.

Beweis. Für $m = 2$ handelt es sich um Korollar 6.7. Wir führen Induktion nach $m \geq 3$. Nach Satz 6.5 mit $(x_1,\, y_1) = (x,\, y)$, $(x_2,\, y_2) = (f_m,\, q_m y)$ und $\alpha = \frac{q_m y - y}{f_m - x} = \frac{(q_m - 1)y}{f_m - x}$ gilt

$$\begin{aligned}
& (m+1)(x,y) \\
= \;& (x,y) + m(x,y) \\
= \;& (x,y) + (f_m,\, q_m y) \\
= \;& \left(\left(\frac{(q_m - 1)y}{f_m - x} \right)^2 - x - f_m,\, -\left(\frac{(q_m - 1)y}{f_m - x} \right)^3 + \frac{(q_m - 1)y}{f_m - x}(x + f_m) + \frac{(q_m - 1)y}{f_m - x} x - y \right) \\
= \;& \left(\frac{(q_m - 1)^2(x^3 + ax + b)}{(f_m - x)^2} - x - f_m,\, -\frac{(q_m - 1)^3 y^3}{(f_m - x)^3} + \frac{(q_m - 1)y}{f_m - x}(2x + f_m) - y \right) \\
= \;& \left(f_{m+1},\, \left(-\frac{(q_m - 1)^3(x^3 + ax + b)}{(f_m - x)^3} + \frac{(q_m - 1)}{f_m - x}(2x + f_m) - 1 \right) y \right) \\
= \;& (f_{m+1},\, q_{m+1} y)\,.
\end{aligned}$$

□

Abbildungsverzeichnis