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

Elliptische Kurven

Vorlesung 4

Ebene projektive Kurven

DEFINITION 4.1. Eine *projektive ebene Kurve* ist die Nullstellenmenge $C = V_+(F) \subset \mathbb{P}^2_K$ zu einem homogenen nicht-konstanten Polynom

$$F \in K[X,Y,Z].$$

Zu einer ebenen affinen Kurve $V(G) \subset \mathbb{A}^2_K$ (in den Koordinaten X,Y) liegt insgesamt die Situation

$$V = V(G) \subset \mathbb{A}^2_K = D_+(Z) \subset \mathbb{P}^2_K$$

vor. Die affine Kurve ist abgeschlossen in der affinen Ebene, aber nicht in der projektiven Ebene, dort kommen noch einzelne Punkte hinzu. Den (Zariski-topologischen) Abschluss von V in $\mathbb{P}^2_K$ nennt man den *projektiven Abschluss* der Kurve.

KOROLLAR 4.2. *Es sei K ein algebraisch abgeschlossener Körper. Zu einer ebenen affinen Kurve*

$$V = V(G) \subseteq \mathbb{A}^2_K \subseteq \mathbb{P}^2_K$$

mit $G \in K[X,Y]$ wird der Zariski-Abschluss von V in $\mathbb{P}^2_K$ durch $C = V_+(H)$ beschrieben, wobei H die Homogenisierung von G in $K[X,Y,Z]$ bezeichnet.

Beweis. Dies folgt direkt aus Satz 28.8 (Algebraische Kurven (Osnabrück 2017-2018)), da nach Aufgabe 4.13 die Homogenisierung eines Hauptideals das durch die Homogenisierung des Erzeugers erzeugte Hauptideal ist. □

Die vorstehende Aussage gilt nicht ohne die Voraussetzung, dass der Körper algebraisch abgeschlossen ist, siehe Aufgabe 4.8. Wir werden aber generell $V_+(H)$ mit der Homogenisierung H als richtige projektive Version der affinen Kurve ansehen, da dieses Konzept sich bei Körpererweiterungen gut verhält.

BEMERKUNG 4.3. Es sei $G \in K[X,Y]$ mit der Homogenisierung $F \in K[X,Y,Z]$. Man gewinnt G aus F zurück, indem man Z durch 1 ersetzt. G beschreibt dann den Durchschnitt $D_+(Z) \cap V_+(F)$. Die beiden anderen affinen Ausschnitte, also

$$D_+(X) \cap V_+(F) \text{ und } D_+(Y) \cap V_+(F)\,,$$

sind gleichberechtigt und liefern insbesondere affine Umgebungen für die Punkte von $C = V_+(F)$, die nicht in $D_+(Z)$ liegen.

Von der affinen Kurve $V(G)$ aus gesehen sind die Punkte im Unendlichen die Punkte aus $V_+(F) \cap V_+(Z)$. Das ist der Schnitt der projektiven Kurve mit einer projektiven Geraden. Dies ist eine endliche Menge, es sei denn die projektive Gerade ist eine Komponente der Kurve, was aber nicht sein kann, wenn man mit einer affinen Kurve startet (da Z kein Teiler der Homogenisierung ist). Zur Berechnung der unendlich fernen Punkte betrachtet man die homogene Zerlegung

$$G = G_d + \cdots + G_m \text{ mit } m \leq d$$

und die Homogenisierung

$$F = G_d + G_{d-1}Z + \cdots + G_m Z^{d-m}.$$

Zur Berechnung des Durchschnittes mit $V_+(Z)$ muss man $Z = 0$ setzen, so dass man die Nullstellen des homogenen Polynoms $G_d(X,Y)$ (in zwei Variablen) berechnen muss. Der Grad d gibt also sofort eine Schranke, wie viele unendlich ferne Punkte es maximal auf der Kurve geben kann.

Beispiel 4.4. Wir betrachten den Standardkegel

$$V(X^2 + Y^2 - Z^2) \subset \mathbb{A}^3_K.$$

Da dies durch eine homogene Gleichung gegeben ist, kann man diesen Kegel auch sofort als eine ebene projektive Kurve (vom Grad zwei)

$$V_+(X^2 + Y^2 - Z^2) \subset \mathbb{P}^2_K$$

auffassen. Die Schnitte des Kegels mit einer beliebigen Ebene $E \subset \mathbb{A}^3_K$ nennt man Kegelschnitte. Diese bekommen nun eine neue Interpretation. Eine Ebene E, auf der nicht der Nullpunkt liegt, kann man in natürlicher Weise identifizieren mit einer offenen affinen Ebene $D_+(L) \subseteq \mathbb{P}^2_K$ (wobei L eine homogene Linearform ist, die den Untervektorraum zu E beschreibt). Die Schnitte mit dem Kegel sind dann verschiedene affine Ausschnitte aus der ebenen projektiven Kurve $V_+(X^2 + Y^2 - Z^2)$. Insbesondere sind also Kreis, Hyperbel und Parabel solche affinen Ausschnitte.

Die Schnitte mit einer Ebenen durch den Nullpunkt sind hingegen projektiv verstanden die endlichen Teilmengen $V_+(X^2 + Y^2 - Z^2) \cap V_+(L)$.

Definition 4.5. Es sei K ein Körper und $d \geq 1$. Dann heißt die ebene projektive Kurve

$$V(X^d + Y^d + Z^d) \subseteq \mathbb{P}^2_K$$

die *Fermat-Kurve* vom Grad d.

Für $d = 1$ handelt es sich einfach um eine projektive Gerade.

Glattheit von projektiven Kurven

Ein Punkt $P \in C = V_+(F) \subseteq \mathbb{P}^2_K$ einer ebenen projektiven Kurve liegt stets auch in einer affin-algebraischen Umgebung. Wegen $P = (a,b,c) \neq (0,0,0)$ ist zumindest eine Koordinate $\neq 0$, bei $c \neq 0$ liegt der Punkt auf

$$V_+(F) \cap D_+(X) = V(\tilde{F}) \subseteq \mathbb{A}^2_K,$$

wobei $\tilde{F}$ hier die Dehomogenisierung von F bezüglich der dritten Variablen bezeichnet. In dieser Situation kann man den Punkt P auf Glattheit im Sinne der Definition 2.1 untersuchen. Es stellt sich heraus, dass es dabei nicht darauf ankommt, in welcher affinen Umgebung man die Glattheit überprüft, siehe Aufgabe 4.18.

Definition 4.6. Es sei K ein Körper. Eine ebene projektive Kurve $C = V_+(F) \subset \mathbb{P}^2_K$ zu einem homogenen Polynom $F \in K[X,Y,Z]$ heißt *glatt*, wenn sie in jedem L-Punkt $P \in C_L \subseteq \mathbb{P}^2_L$ glatt ist.

Lemma 4.7. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik $p \geq 0$ und sei $C = V_+(X^d + Y^d + Z^d) \subset \mathbb{P}^2_K$ die Fermat-Kurve vom Grad d. Die Charakteristik sei kein Teiler von d. Dann ist C eine glatte Kurve.*

Beweis. Da Glattheit eine lokale Eigenschaft ist, können wir mit einem beliebigen affinen Ausschnitt argumentieren. Da die Situation symmetrisch ist, können wir uns auf das affine Teilstück

$$V(X^d + Y^d + 1) \subset \mathbb{A}^2_K$$

beschränken. Die partiellen Ableitungen sind dX^{d-1} und dY^{d-1}. Aufgrund der Voraussetzung über die Charakteristik ist $d \neq 0$, so dass beide Ableitungen nur bei $x = y = 0$ verschwinden. Dieser Punkt gehört aber nicht zur Kurve. □

Lemma 4.8. *Es sei K ein Körper, sei $G \in K[X,Z]$ ein homogenes Polynom vom Grad $d+1$, das in (homogen) verschiedene homogene Linearfaktoren der Form $\alpha_i X + \beta_i Z$ mit $\alpha_i \neq 0$ zerfalle. Es sei $d \in \mathbb{N}_+$ kein Vielfaches der Charakteristik von K. Dann ist die durch die Gleichung $Y^d Z = G(X,Z)$ gegebene projektive Kurve glatt.*

Beweis. Auf der offenen Menge $D_+(Z)$ erhält man die in Lemma 2.6 beschriebene Situation, diese Punkte sind also glatt. Auf dem Komplement $V_+(Z)$ wird die Gleichung zu

$$0 = G(X,0) = \alpha X^{d+1}$$

mit einem Vorfaktor $\alpha \neq 0$, woraus $X = 0$ folgt. Es gibt also nur noch den weiteren Punkt P mit den Koordinaten $(0,1,0)$. Eine affine Umgebung dieses Punktes ist $D_+(Y)$, die affine Version der Gleichung auf diesem Teilstück ist $Z = G(X,Z)$. Die partielle Ableitung nach Z ist $1 + \sum \gamma_{ij} X^i Z^j$ mit $i+j = d$.

Im Nullpunkt, der dem Punkt P entspricht, ist dies gleich 1, daher ist dies auch ein glatter Punkt. □

DEFINITION 4.9. Eine glatte ebene projektive Kurve $V_+(F) \subseteq \mathbb{P}^2_K$ mit $F \in K[X,Y,Z]$ homogen vom Grad 3, die zumindest einen K-rationalen Punkt besitzt, heißt *elliptische Kurve* über K.

Über einem algebraisch abgeschlossenen Körper ist die Bedingung über die Existenz eines rationalen Punktes stets erfüllt. Diese Bedingung ist im Allgemeinen nötig, um sicherzustellen, dass die Menge der K-Punkte eine Gruppe bilden - es gibt ja keine leere Gruppe. Eine elliptische Kurve ist also insbesondere projektiv. Wegen der Beziehung zwischen affinen und projektiven Kurven über den projektiven Abschluss bzw. die Homogenisierung kann man aber wiederum häufig die affine Situation betrachten und eine Variable sparen. In der nächsten Vorlesung werden wir überlegen, auf welche Gestalt man eine elliptische Kurve durch eine Variablentransformation bringen kann und wie die affine Version davon aussieht. Es wird sich (bei Charakteristik $\neq 2,3$) ergeben, dass die affine Version von der Gestalt (kurze Weierstraßform) $Y^2 = X^3 + aX + b$ ist, mit Koeffizienten $a, b \in K$, die sicherstellen, dass das kubische Polynom rechts keine mehrfache Nullstelle besitzt. Wenn wir im Folgenden von der durch $Y^2 = X^3 + aX + b$ gegebenen elliptischen Kurve sprechen, so meinen wir in Wahrheit die durch die homogene Gleichung $Y^2Z = X^3 + aXZ^2 + bZ^3$ gegebene elliptische Kurve. Der einzige Punkt darauf, der nicht auf dem affinen Ausschnitt liegt, ist $(0,1,0)$, und dieser sichert die Existenz eines K-rationalen Punktes.

BEISPIEL 4.10. Es sei $n \in \mathbb{N}_+$. Wir betrachten die Gleichung

$$Y^2 = X^3 - n^2X = X(X-n)(X+n)$$

über einem Körper K, wobei die Charakteristik p kein Teiler von $2n$ sei. Dann liegt eine glatte kubische Kurve vor. Die partiellen Ableitungen sind $3X^2 - n^2$ und $2Y$. Ein singulärer Punkt könnte allenfalls in $y = 0$ und somit bei $x = 0, n, -n$ vorliegen, doch ist da $3x^2 - n^2 \neq 0$.

Kongruente Zahlen

Wir betrachten eine erste Beispielklasse von elliptischen Kurven, die mit einem zahlentheoretischen Problem in Zusammenhang steht.

BEISPIEL 4.11. Wir betrachten die Gleichung

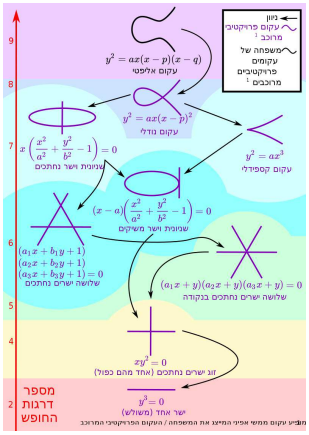
$$Y^2 = X^3 - 25X = X(X-5)(X+5)$$

über $\mathbb{Q}$, vergleiche Beispiel 4.10. Es gibt unmittelbar die drei rationalen Punkte $(0,0)$, $(5,0)$, $(-5,0)$. Wir behaupten, dass auch der rationale Punkt

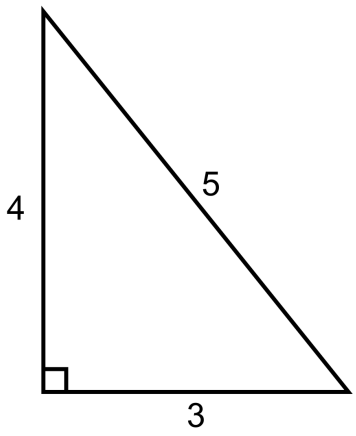
$$\left(\frac{1681}{144}, \frac{62279}{1728}\right)$$

auf der Kurve liegt. Dies beruht auf $\frac{1681}{144} = \frac{41^2}{12^2}$, $\frac{1681}{144} - 5 = \frac{1681}{144} - \frac{720}{144} = \frac{961}{144} = \frac{31^2}{12^2}$ und $\frac{1681}{144} + 5 = \frac{1681}{144} + \frac{720}{144} = \frac{2401}{144} = \frac{49^2}{12^2}$ und auf

$$\frac{62279}{1728} = \frac{31 \cdot 41 \cdot 49}{12^3}.$$



Der rationale Punkt im vorstehenden Beispiel wurde mit Hilfe des Lemmas Lemma 4.13 weiter unten gefunden.



Die Seitenlängen und der Flächeninhalt dieses rechtwinkligen Dreiecks sind ganzzahlig.

Definition 4.12. Eine natürliche Zahl $n \geq 1$ heißt *kongruent*, wenn sie als Flächeninhalt eines rechtwinkligen Dreiecks auftritt, dessen Seitenlängen allesamt rationale Zahlen sind.

Die folgende Tabelle zeigt die kongruenten Zahlen echt unterhalb von 20 zusammen mit einer Realisierung als Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seiten. Die Eigenschaften $n = ab/2$ und $a^2 + b^2 = c^2$ kann man direkt überprüfen. Es ist aber keineswegs klar, wie man die geforderten rechtwinkligen Dreiecke findet, und wie man zeigen kann, dass eine Zahl n nicht kongruent ist. Die nicht aufgeführten Zahlen echt unterhalb 20 sind nicht kongruent.

	Kathete a	Kathete b	Hypotenuse c
5	$\frac{3}{2}$	$\frac{20}{3}$	$\frac{41}{6}$
6	3	4	5
7	$\frac{35}{12}$	$\frac{24}{5}$	$\frac{337}{60}$
13	$\frac{780}{323}$	$\frac{323}{30}$	$\frac{106921}{9690}$
14	$\frac{8}{3}$	$\frac{63}{6}$	$\frac{65}{6}$
15	4	$\frac{15}{2}$	$\frac{17}{2}$

LEMMA 4.13. *Es seien a, b, c rationale Zahlen, die die Seiten eines rechtwinkligen Dreiecks bilden, also*

$$a^2 + b^2 = c^2$$

erfüllen und derart, dass der Flächeninhalt

$$\frac{ab}{2} = n$$

eine natürliche Zahl n ist. Dann ist $\left(\frac{c^2}{4}, \frac{(b^2-a^2)c}{8}\right)$ ein rationaler Punkt der elliptischen Kurve

$$y^2 = x^3 - n^2 x.$$

Beweis. Es ist einerseits

$$\begin{aligned} y^2 &= \frac{(b^2-a^2)^2c^2}{64} \\ &= \frac{(b^2-a^2)^2(a^2+b^2)}{64} \\ &= \frac{a^6 - a^4b^2 - a^2b^4 + b^6}{64} \end{aligned}$$

und andererseits ebenso

$$\begin{aligned} x(x-n)(x+n) &= x^3 - n^2x \\ &= \left(\frac{c^2}{4}\right)^3 - n^2\left(\frac{c^2}{4}\right) \\ &= \frac{(a^2+b^2)^3}{64} - \frac{a^2b^2}{4} \cdot \left(\frac{a^2+b^2}{4}\right) \\ &= \frac{a^6 + 3a^4b^2 + 3a^2b^4 + b^6}{64} - \frac{a^4b^2 + a^2b^4}{16} \\ &= \frac{a^6 - a^4b^2 - a^2b^4 + b^6}{64}. \end{aligned}$$

□

Eine gewisse Umkehrung ist die folgende Aussage.

LEMMA 4.14. *Es sei $n \in \mathbb{N}_+$ und sei E die durch $y^2 = x^3 - n^2x$ gegebene elliptische Kurve über $\mathbb{Q}$. Es gebe einen rationalen Punkt $P = (x, y) \in E(\mathbb{Q})$ mit der Eigenschaft, dass x ein Quadrat (in $\mathbb{Q}$) ist und der Nenner von x in gekürzter Darstellung gerade ist. Dann ist n eine kongruente Zahl.*

Beweis. Es sei $x = u^2$ mit $u \in \mathbb{Q}_+$. Mit $v = y/u$ gilt

$$v^2 + n^2 = \frac{y^2}{u^2} + n^2 = \frac{x^3 - n^2x}{x} + n^2 = x^2 - n^2 + n^2 = x^2.$$

Es liegt also ein rechtwinkliges Dreieck mit den rationalen Seitenlängen v, n und x vor. Es sei r der Nenner von u in gekürzter Darstellung, dieser ist gerade nach Voraussetzung. Wir multiplizieren die rationalen Zahlen (v, n, x) mit r^2. Dabei ist mit r^2x auch r^2v ganzzahlig und so entsteht ein primitives pythagoreisches Tripel, wobei r^2n gerade ist. Nach Satz 10.6 (Zahlentheorie (Osnabrück 2016-2017)) gibt es daher natürliche Zahlen $s > t > 0$ mit

$$r^2v = s^2 - t^2,\ r^2n = 2st,\ r^2x = s^2 + t^2\,.$$

Wir betrachten nun das Dreieck mit den Seitenlängen $\frac{2s}{r}$, $\frac{2t}{r}$, $2u$. Wegen

$$\left(\frac{2s}{r}\right)^2 + \left(\frac{2t}{r}\right)^2 = \frac{4s^2 + 4t^2}{r^2} = \frac{4r^2x}{r^2} = 4x = (2u)^2$$

liegt ein rechtwinkliges Dreieck vor und wegen

$$\frac{1}{2} \cdot \frac{2s}{r} \cdot \frac{2t}{r} = \frac{2st}{r^2} = \frac{r^2n}{r^2} = n$$

ist sein Flächeninhalt gleich n. Somit ist n eine kongruente Zahl. □

Die Beziehung zwischen kongruenten Zahlen und elliptischen Kurven werden wir in Satz 25.10 weiter vertiefen.

Abbildungsverzeichnis