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

Elliptische Kurven

Vorlesung 2

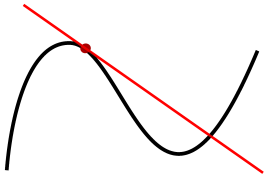
Glatte Kurven

Ein reelles Polynom $F \in \mathbb{R}[X,Y]$ in zwei Variablen kann man als eine differenzierbare Funktion $F\colon \mathbb{R}^2 \to \mathbb{R}$, die algebraische Kurve $v = V(F) \subseteq \mathbb{R}^2$ ist die Faser von F über dem Nullpunkt $0 \in \mathbb{R}$. In dieser Situation ist der Satz über implizite Abbildungen anwendbar. Er besagt für einen Punkt $P = (a,b) \in V = \mathbb{R}^2$, dass unter der Voraussetzung, dass zumindest eine partielle Ableitung $\frac{\partial F}{\partial x}$ oder $\frac{\partial F}{\partial y}$ in P nicht 0 ist, es eine offene Ballumgebung $P \in U(P,\epsilon)$, ein reelles Intervall $]-\delta,\delta[$ und eine stetig differenzierbare Abbildung

$$]-\delta,\delta[\longrightarrow U(P,\epsilon)$$

derart gibt, dass eine Bijektion des Intervalls mit dem Faserausschnitt $V \cap U(P,\epsilon)$ vorliegt. Das bedeutet, dass die Faser V lokal in einem solchen Punkt wie ein differenzierbar gekrümmtes Intervall aussieht, also eine eindimensionale reelle Mannigfaltigkeit in diesen Punktes ist. Wenn beide partiellen Ableitungen in P gleich 0 sind, so kann man diesen Satz nicht anwenden. Für das Studium der algebraischen Kurven ist es wichtig, dass man die Voraussetzung des Satzes, dass zumindest eine partielle Ableitung nicht verschwindet, über einem beliebigen Körper formulieren kann, obwohl es für die Schlussfolgerung des Satzes keine unmittelbare Entsprechung gibt.

Für Polynome kann man das Konzept einer partiellen Ableitung auf jeden Grundkörper formal übertragen, wobei in positiver Charakteristik einige Besonderheiten auftreten, siehe hierzu die Aufgaben.



Definition 2.1. Es sei K ein Körper und $F \in K[X,Y]$ ein von 0 verschiedenes Polynom. Es sei $P \in C = V(F) \subset \mathbb{A}^2_K$ ein Punkt der zugehörigen affinen ebenen Kurve. Dann heißt P ein *glatter Punkt* von C, wenn

$$\frac{\partial F}{\partial X}(P) \neq 0 \text{ oder } \frac{\partial F}{\partial Y}(P) \neq 0$$

gilt. Andernfalls heißt der Punkt *singulär*.

DEFINITION 2.2. Es sei K ein Körper und $F \in K[X,Y]$ ein von 0 verschiedenes Polynom. Man nennt $C = V(F) \subset \mathbb{A}^2_K$ eine *glatte Kurve*, wenn sie in jedem L-Punkt $P \in C_L \subseteq \mathbb{A}^2_L$ glatt ist.

Bei einer glatten Kurve fordert man also, dass nicht nur die K-Punkte, sondern auch die L-Punkte zu einer beliebigen Körpererweiterung $K \subseteq L$ glatt sind. Es genügt, dies für die Punkte des algebraischen Abschlusses $\overline{K}$ zu fordern. Da eine über K definierte Kurve überhaupt keinen K-Punkt besitzen muss, ist eine solche Formulierung nötig, um einen sinnvollen Begriff zu erhalten.

LEMMA 2.3. *Es sei K ein Körper und $F \in K[X,Y]$ ein von 0 verschiedenes Polynom mit der zugehörigen Kurve $C = V(F)$. Dann sind folgende Eigenschaften äquivalent.*

(1) *C ist eine glatte Kurve.*
(2) *Jeder Punkt $P \in C_{\overline{K}} \subseteq \mathbb{A}^2_{\overline{K}}$ ist glatt, wobei $\overline{K}$ einen algebraischen Abschluss von K bezeichnet.*
(3) *Die Polynome $F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}$ erzeugen in $\overline{K}[X,Y]$ das Einheitsideal.*
(4) *Die Polynome $F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}$ erzeugen in $K[X,Y]$ das Einheitsideal.*

Beweis. Von (1) nach (2) ist klar, da die Glattheit ja eine Anforderung an jede Körpererweiterung ist. Sei (2) erfüllt. Angenommen, das Ideal $(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})$ sei nicht das Einheitsideal. Dann gibt es nach Lemma 11.3 (Kommutative Algebra) ein maximales Ideal $\mathfrak{m}$ in $\overline{K}[X,Y]$ mit

$$(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) \subseteq \mathfrak{m}.$$

Da $\overline{K}$ algebraisch abgeschlossen ist, ist nach Satz 10.10 (Algebraische Kurven (Osnabrück 2017-2018)) das Ideal $\mathfrak{m}$ ein Punktideal, also von der Form $\mathfrak{m} = (X-a, Y-b)$ mit $a, b \in \overline{K}$. Die Inklusionsbedingung

$$(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) \subseteq (X-a, Y-b)$$

bedeutet

$$F(a,b) = \frac{\partial F}{\partial X}(a,b) = \frac{\partial F}{\partial Y}(a,b) = 0$$

und somit ist $P = (a,b)$ ein nichtglatter Punkt von $C_{\overline{K}}$, im Widerspruch zu (2). Von (3) nach (4) gilt für jedes Ideal (siehe Aufgabe 2.10). Von (4) nach (1). Sei $K \subseteq L$ eine beliebige Körpererweiterung. Dann ist erst recht das Ideal $(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})$ in $L[X,Y]$ das Einheitsideal. Für einen Punkt

$$P = (a,b) \in \mathbb{A}^2_L$$

können dann nicht F und die partiellen Ableitungen simultan verschwinden, es liegt also ein glatter Punkt vor. □

Bemerkung 2.4. Für einen glatten Punkt $P = (a, b) \in C = V(F)$ einer ebenen algebraischen Kurve nennt man die durch die Gleichung

$$\frac{\partial F}{\partial X}(P)(X-a) + \frac{\partial F}{\partial Y}(P)(Y-b) = 0$$

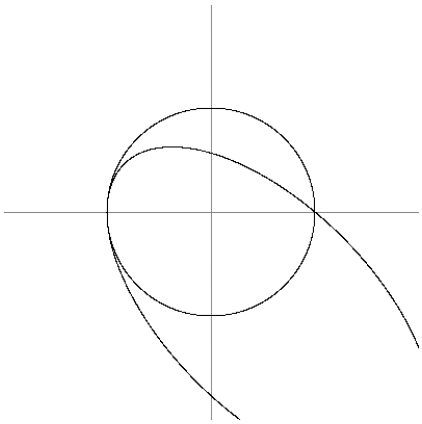
gegebene Gerade die *Tangente* im Punkt P an die Kurve. Bei $P = (0,0) \in C$ kann man die Glattheit und die Tangente einfach ablesen. Man zerlegt F in die homogenen Komponenten

$$F = F_0 + F_1 + F_2 + \cdots + F_d.$$

Dabei ist der konstante Term $F_0 = 0$, da der Nullpunkt ein Punkt der Kurve ist, und der lineare Term ist $F_1 = uX + vY$. Hierbei ist

$$\frac{\partial F}{\partial X}(P) = u \text{ und } \frac{\partial F}{\partial Y}(P) = v$$

(da die höheren homogenen Komponenten von F keinen Beitrag zu den partiellen Ableitungen im Nullpunkt leisten), es liegt genau dann ein glatter Punkt vor, wenn $F_1 \neq 0$ und die Bedingung $uX + vY = 0$ beschreibt die Tangente.



Bei einer algebraischen Kurve sind die Schnittpunkte von irreduziblen Komponenten niemals glatt.

Die folgende Ausssage zeigt, dass ein Kreuzungspunkt zweier irreduzibler Komponenten niemals glatt sein kann.

Lemma 2.5. *Es sei $C = V(F)$ eine ebene algebraische Kurve und $F = F_1 \cdots F_n$ die Zerlegung in verschiedene Primfaktoren. Es sei $P \in C$ ein glatter Punkt der Kurve. Dann liegt P auf nur einer Komponente $C_i = V(F_i)$ der Kurve.*

Beweis. Siehe Aufgabe 2.14. □

Lemma 2.6. *Es sei K ein Körper, sei $G \in K[X]$ ein Polynom, das in verschiedene Linearfaktoren zerfalle. Es sei $d \in \mathbb{N}_+$ kein Vielfaches der*

Charakteristik von K. Dann ist die durch die Gleichung $Y^d = G$ gegebene algebraische Kurve glatt.

Beweis. Die Voraussetzungen ändern sich nicht, wenn wir zu einer Körpererweiterung übergehen, wir können also direkt einen Punkt $(x, y) \in V(Y^d - G) \subseteq K^2$ betrachten und müssen zeigen, dass er glatt ist. Nehmen wir also an, dass er nicht glatt ist. Die partiellen Ableitungen sind G' und dY^{d-1}. Wegen $d \neq 0$ in K folgt (bei $d \geq 2$, bei $d = 1$ ist diese partielle Ableitung konstant $\neq 0$) $y = 0$. Aus der Kurvengleichung folgt $G(x) = 0$ und aus der ersten partiellen Ableitung folgt $G'(x) = 0$. Doch dann ist x eine mehrfache Nullstelle von G, was nach Voraussetzung ausgeschlossen ist. □

Für uns wird insbesondere der Fall $Y^2 = G(X)$ mit einem Polynom G vom Grad 3 ohne mehrfache Nullstelle entscheidend sein.

Wir bestimmen für einige kubische Kurven, die nicht glatt sind, die singulären Punkte.

Beispiel 2.7. Wir betrachten die durch das Polynom $V(Y^2 - X^3)$ gegebene Neilsche Parabel über einem Körper der Charakteristik $\neq 2, 3$. Die partiellen Ableitungen sind

$$\frac{\partial F}{\partial X} = -3X^2 \text{ und } \frac{\partial F}{\partial Y} = 2Y\,.$$

Wenn man diese $= 0$ setzt, so folgt direkt, dass $(0, 0)$ der einzige singuläre Punkt der Kurve ist und diese ansonsten glatt ist.

Beispiel 2.8. Wir betrachten die durch das Polynom $V(Y^2 - X^3 - 3X^2)$ gegebene *Tschirnhausen Kubik* über einem Körper der Charakteristik $\neq 2, 3$. Die partiellen Ableitungen sind

$$\frac{\partial F}{\partial X} = -3X^2 - 6X \text{ und } \frac{\partial F}{\partial Y} = 2Y\,.$$

Wenn man diese (zusammen mit der Kurvengleichung selbst) $= 0$ setzt, so folgt $Y = 0$ und somit auch

$$X^2(X + 3) \;=\; 0 \;=\; X(X + 2).$$

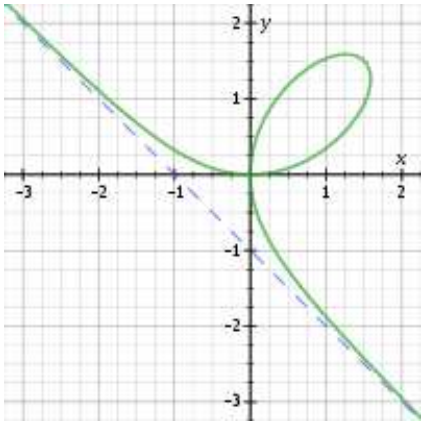
Somit ist der Nullpunkt $(0, 0)$ der einzige singuläre Punkt der Kurve, die ansonsten glatt ist.

Beispiel 2.9. Das *Kartesische Blatt* wird durch die Gleichung $F = X^3 + Y^3 - 3XY = 0$ beschrieben, der Grundkörper habe nicht die Charakteristik. Die partiellen Ableitungen sind

$$\frac{\partial F}{\partial X} = 3X^2 - 3Y \text{ und } \frac{\partial F}{\partial Y} = 3Y^2 - 3X\,.$$

Rene Descartes (1596-1650)

Wenn man diese (zusammen mit der Kurvengleichung selbst) $= 0$ setzt, so folgt $Y = X^2$ und $X = Y^2$, also auch $Y = Y^4$ (ebenso für X). Dann ist $Y = X = 0$, und somit liegt im Nullpunkt eine Singularität vor, oder X und Y sind beide eine dritte Einheitswurzel (und zwar sind beide 1 oder es sind die beiden anderen dritten Einheitswurzeln). An diesen anderen Verschwindungsstellen der beiden partiellen Ableitungen hat aber F den Wert -1, diese sind also keine Punkte der Kurve. Der Nullpunkt ist also der einzige nichtglatte Punkt der Kurve.



Lokale Ringe

Wie in der ersten Vorlesung erwähnt, nennt man $K[X,Y]/(F)$ den Koordinatenring zur Kurve $V(F)$. Zu einem K-Punkt $P = (a,b) \in C = V(F) \subset \mathbb{A}^2_K$ der Kurve gehört das maximalen Ideal $\mathfrak{m} = (X-a, Y-b)$ in $K[X,Y]$

und entsprechend das maximale Ideal in $K[X,Y]/(F)$, das im Allgemeinen wieder mit $\mathfrak{m}$ bezeichnet wird. Das Komplement von $\mathfrak{m}$ besteht aus allen Funktionen, die im Punkt nicht den Wert 0 besitzen. Es handelt sich um ein multiplikatives System, ist also abgeschlossenen unter der Multiplikation und beinhaltet die (konstante Funktion) 1. Zu einem solchen multiplikativen System $S \subseteq R$ in einem kommutativen Ring R kann man die *Nenneraufnahme* R_S konstruieren, dessen Elemente man als $\frac{r}{s}$, $r \in R$, $s \in S$ schreibt und worin die Elemente aus S zu Einheiten werden. Bei einem maximalen Ideal $\mathfrak{m}$ wird die Nenneraufname an $R \setminus \mathfrak{m}$ als $R_{\mathfrak{m}}$ (als Abkürzung für $R_{R\setminus\mathfrak{m}}$) bezeichnet. Mit dieser Konstruktion lässt sich der *lokale Ring* der Kurve im Punkt P beschreiben, und zwar in doppeler Weise als

$$K[X,Y]_{(X-a,Y-b)}/(F) \cong (K[X,Y]/(F))_{\mathfrak{m}}$$

(dabei ist $\mathfrak{m}$ das maximale Ideal aufgefasst im Restklassenring). Dieser Ring beschreibt die wesentlichen algebraischen Eigenschaften des Punktes auf der Kurve. Zunächst handelt es sich um einen lokalen Ring im Sinne der folgenden Definition.

Definition 2.10. Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Im glatten Kurvenfall erfüllt der lokale Ring weitere starke Eigenschaften.

Definition 2.11. Ein *diskreter Bewertungsring* R ist ein Hauptidealbereich mit der Eigenschaft, dass es bis auf Assoziiertheit genau ein Primelement in R gibt.

Satz 2.12. *Es sei K ein Körper, $F \in K[X,Y]$ ein Polynom $\neq 0$ ohne mehrfache Faktoren und sei $P \in C = V(F)$ ein glatter Punkt der Kurve. Es sei R der lokale Ring der Kurve im Punkt P. Dann ist R ein diskreter Bewertungsring.*

Beweis. Zunächst ist R ein noetherscher lokaler Ring, der aufgrund von Lemma 2.5 ein Integritätsbereich ist. Daher sind die einzigen Primideale das Nullideal und das maximale Ideal $\mathfrak{m}_P$. Wir werden zeigen, dass das maximale Ideal ein Hauptideal ist.

Wir können annehmen, dass P der Nullpunkt ist, und schreiben F als

$$F = F_d + \cdots + F_1$$

mit $F_1 \neq 0$. Da P glatt ist, liegt eine solche Gestalt vor. Durch eine Variablentransformation können wir erreichen, dass $F_1 = Y$ ist. Wir können in F die isoliert stehenden Potenzen von X (die Monome, wo kein Y vorkommt) zusammenfassen und bei den anderen Y ausklammern. Dann lässt sich die Gleichung $F = 0$ als

$$Y(1+G) = XH(X)$$

schreiben, wobei $G \in (X,Y)$ ist. Es ist $1+G$ eine Einheit in $K[X,Y]_{(X,Y)}$ und erst recht im lokalen Ring $R = K[X,Y]_{(X,Y)}/(F)$ der Kurve im Nullpunkt. Daher gilt in R die Beziehung

$$Y = \frac{H}{1+G}X.$$

Also wird das maximale Ideal im lokalen Ring R von X allein erzeugt, so dass nach Satz 21.8 (Algebraische Kurven (Osnabrück 2017-2018)) ein diskreter Bewertungring vorliegt. □

Von dieser Aussage gilt auch die Umkehrung, siehe Satz 23.7 (Algebraische Kurven (Osnabrück 2017-2018)).

Wenn der Koordinatenring $R = K[X,Y]/(F)$ ein Integritätsbereich ist, was genau dann der Fall ist, wenn F ein irreduzibles Polynom ist, so kann man den Quotientenkörper davon bilden, der die Nenneraufnahme an allen Elementen $\neq 0$ ist. Der entstehende Körper heißt der *Funktionenkörper* der Kurve. Für jeden Punkt der Kurve ist der Funktionenkörper gleich dem Quotientenkörper des lokalen Ringes in diesem Punkt.

Abbildungsverzeichnis