Prof. Dr. H. Brenner **Osnabrück WS 2021/2022**

Elliptische Kurven

Arbeitsblatt 2

Aufgaben

Aufgabe 2.1. Diskutiere den Zusammenhang zwischen ebenen algebraischen Kurven und dem Satz über implizite Funktionen.

Aufgabe 2.2. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a genau dann eine mehrfache Nullstelle von F ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

Aufgabe 2.3. Es sei K ein Körper der positiven Charakteristik $p > 0$. Bestimme die Menge der Polynome $F \in K[T]$ mit formaler Ableitung $F' = 0$.

Aufgabe 2.4. Beweise den Satz von Schwarz für den Polynomring

$$K[X_1, \ldots, X_n]$$

über einem beliebigen Körper K, also die Vertauschbarkeit von formalen partiellen Ableitungen.

Aufgabe 2.5. Es sei K ein Körper und seien $F, G \in K[X_1, \ldots, X_n]$ Polynome. Zeige, dass für die partiellen Ableitungen die Produktregel

$$\partial_i(FG) = F\partial_i(G) + G\partial_i(F)$$

gilt.

Aufgabe 2.6. Es sei K ein Körper und seien $F_1, \ldots, F_m \in K[X_1, \ldots, X_n]$ und $G_1, \ldots, G_k \in K[Y_1, \ldots, Y_m]$ Polynome. Wir setzen

$$H_i = G_i(F_1, \ldots, F_m).$$

Zeige, dass die formalen partiellen Ableitungen die „formale Kettenregel“

$$\begin{pmatrix} \frac{\partial H_1}{\partial X_1} & \cdots & \frac{\partial H_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial H_k}{\partial X_1} & \cdots & \frac{\partial H_k}{\partial X_n} \end{pmatrix} = \begin{pmatrix} \frac{\partial G_1}{\partial Y_1} & \cdots & \frac{\partial G_1}{\partial Y_m} \\ \vdots & \ddots & \vdots \\ \frac{\partial G_k}{\partial Y_1} & \cdots & \frac{\partial G_k}{\partial Y_m} \end{pmatrix} \left(\frac{F_j}{Y_j} \right) \circ \begin{pmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_m}{\partial X_1} & \cdots & \frac{\partial F_m}{\partial X_n} \end{pmatrix}$$

erfüllen, wobei der Ausdruck $\frac{F_j}{Y_j}$ bedeutet, dass die Variablen Y_j durch die Polynome F_j zu ersetzen sind.

AUFGABE 2.7. Es sei K ein Körper der Charakteristik $p \geq 0$. Man charakterisiere die Polynome $F \in K[X,Y]$ mit der Eigenschaft, dass

(1) die erste partielle Ableitung,
(2) die zweite partielle Ableitung,
(3) beide partiellen Ableitungen

0 sind.

Die beiden folgenden Aufgaben beziehen sich auf homogene Polynome. Dieses Konzept werden wir in der dritten Vorlesung erläutern.

AUFGABE 2.8. Es sei $H \in K[X_1, \ldots, X_n]$ ein (in der Standardgraduierung) homogenes Polynom vom Grad e. Zeige die Beziehung

$$eH = X_1 \frac{\partial H}{\partial X_1} + \cdots + X_n \frac{\partial H}{\partial X_n}.$$

AUFGABE 2.9.*

(1) Zeige, dass formales partielles Ableiten auf dem Polynomring

$$K[X_1, \ldots, X_n]$$

bezüglich einer Variablen und Dehomogenisieren bezüglich einer anderen Variablen vertauschbar sind.
(2) Zeige, dass dies nicht für die gleiche Variable stimmt.

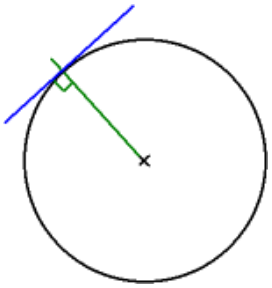
AUFGABE 2.10. Es sei $R \subseteq S$ ein direkter Summand von kommutativen Ringen. Es sei $I \subseteq R$ ein Ideal und $f \in R$. Zeige, dass aus $f \in IS$ die Zugehörigkeit $f \in I$ folgt.

AUFGABE 2.11. Es sei K ein Körper.

a) Zeige, dass der Graph eines Polynoms $F \in K[X]$ eine glatte algebraische Kurve ist.

b) Es seien $F, G \in K[X]$ Polynome ohne gemeinsame Nullstelle. Zeige, dass der Graph der rationalen Funktion F/G ebenfalls eine glatte algebraische Kurve ist.

Aufgabe 2.12. Zeige, dass der Einheitskreis über einem Körper der Charakteristik $\neq 2$ glatt ist und bestimme für jeden Punkt die Gleichung der Tangente.



Aufgabe 2.13. Es sei K ein Körper und $F \in K[X,Y]$ ein nichtkonstantes Polynom mit einfachen Primfaktoren und mit zugehöriger ebener Kurve $C = V(F)$. Zeige, dass C nur endlich viele singuläre Punkte besitzt.

Aufgabe 2.14. Beweise Lemma 2.5.

Aufgabe 2.15.*

Betrachte die beiden reellen Kurven

$$V(X^5 - X^3 + 2XY + 7Y^2 - 9)$$

im Punkt $(1,1)$ und

$$V(X^4 + Y^4 - 3X^2Y^2 + 5X + 7Y)$$

im Nullpunkt. Sind diese beiden Kurven lokal in den angegebenen Punkten zueinander diffeomorph?

Aufgabe 2.16.*

Bestimme die singulären Punkte der ebenen algebraischen Kurve

$$V\left(-2X^3 + 3X^2Y - Y + \frac{2}{3}\sqrt{\frac{1}{3}}\right) \subset \mathbb{A}^2_{\mathbb{C}}\,.$$

Einige der nächsten Aufgaben verwenden die beiden folgenden Definitionen.

Es sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X,Y]$ ein von 0 verschiedenes Polynom. Es sei $P \in C = V(F) \subset \mathbb{A}^2_K$ ein Punkt der

zugehörigen affinen ebenen Kurve, der (nach einer linearen Variablentransformation) der Nullpunkt sei. Es sei

$$F = F_d + F_{d-1} + \cdots + F_m$$

die homogene Zerlegung von F mit $F_d \neq 0$ und $F_m \neq 0$, $d \geq m$. Dann heißt m die *Multiplizität* der Kurve im Punkt P.

Es sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X,Y]$ ein von 0 verschiedenes Polynom. Es sei $P \in C = V(F) \subset \mathbb{A}^2_K$ ein Punkt der zugehörigen affinen ebenen Kurve, der (nach einer linearen Variablentransformation) der Nullpunkt sei. Es sei

$$F = F_d + F_{d-1} + \cdots + F_m$$

die homogene Zerlegung von F mit $F_d \neq 0$ und $F_m \neq 0$, $d \geq m$. Es sei $F_m = G_1 \cdots G_m$ die Zerlegung in lineare Faktoren. Dann nennt man jede Gerade $V(G_i)$, $i = 1, \ldots, m$, eine *Tangente* an C im Punkt P.

Glattheit ist äquivalent zu Multiplizität 1, eine große Multiplizität ist also ein Maß für eine Singularität. In diesem Fall gibt es mehrere Tangenten.

Aufgabe 2.17. Es sei $H(X) \in K[X]$, sei $F = Y - H$ und $C = V(F) \subseteq \mathbb{A}^2_K$ der Graph von H, aufgefasst als ebene algebraische Kurve. Es sei

$$P = (a,b) = (a, H(a))$$

ein Punkt des Graphen.

(1) Zeige, dass die Multiplizität von C in P gleich 1 ist.
(2) Zeige, dass die Tangente in P an C mit der üblichen Tangente an einen Graphen im Punkt a übereinstimmt.

Aufgabe 2.18. Betrachte die durch $y = 2x^4 + 3x^2 - x + 1$ gegebene Kurve mit dem Punkt $P = (1,5)$. Finde eine Koordinatentransformation derart, dass P zum Punkt $(0,0)$ wird und die Tangente an P zur x-Achse.

Aufgabe 2.19. Bestimme für die Kurve $V(X^3 + Y^3 - 3XY + 1)$ die singulären Punkte über $\mathbb{R}$ und über $\mathbb{C}$. Man gebe jeweils die Multiplizität und die Tangenten an.

Aufgabe 2.20. Es sei K ein algebraisch abgeschlossener Körper und seien $G, H \in K[X,Y]$ Polynome mit $G(P) = H(P) = 0$ für einen bestimmten Punkt $P \in \mathbb{A}^2_K$. Es sei $F = GH$. Zeige, dass jede Tangente von G in P und jede Tangente von H in P auch eine Tangente von F in P ist.

AUFGABE 2.21. Es sei K ein algebraisch abgeschlossener Körper. Betrachte die Kurve

$$C = V(x^3 + 5x^2y - 6xy^2 - x^2 - xy + 4y^2).$$

(1) Bestimme die Tangenten im Nullpunkt.
(2) Zeige, dass $P = (1, 2)$ ein Punkt der Kurve ist, und berechne die Tangente(n) von C in P über die Ableitung.
(3) Führe eine Variablentransformation durch derart, dass P in den neuen Variablen der Nullpunkt ist, und bestimme die Tangente(n) in P aus der transformierten Kurvengleichung.

AUFGABE 2.22. Bestimme für die algebraische Kurve

$$C = V\big(9y^4 + 10x^2y^2 + x^4 - 12y^3 - 12x^2y + 4y^2\big)$$

die Singularitäten sowie deren Multiplizitäten und Tangenten.

AUFGABE 2.23. Sei R ein kommutativer Ring. Zeige, dass R genau dann ein lokaler Ring ist, wenn $a + b$ nur dann eine Einheit ist, wenn a oder b eine Einheit ist.

AUFGABE 2.24. Sei R ein kommutativer Ring. Zeige die Äquivalenz folgender Aussagen.

(1) R hat genau ein maximales Ideal
(2) Die Menge der Nichteinheiten $R \setminus R^\times$ bildet ein Ideal in R.

AUFGABE 2.25. Es sei R ein lokaler Ring mit Restekörper K. Zeige, dass R und K genau dann die gleiche Charakteristik haben, wenn R einen Körper enthält.

AUFGABE 2.26.*

Es sei R ein lokaler Ring und $\mathfrak{a}$ ein Ideal von R. Zeige, dass

$$R^\times \longrightarrow (R/\mathfrak{a})^\times$$

surjektiv ist.

AUFGABE 2.27. Bestimme die Unterringe der rationalen Zahlen $\mathbb{Q}$, die lokal sind.

AUFGABE 2.28. Es sei K ein algebraisch abgeschlossener Körper und $R = K[X_1, \ldots, X_n]$. Zeige, dass sämtliche Lokalisierungen von R an maximalen Idealen zueinander isomorph sind.

Aufgabe 2.29. Es sei K ein Körper und betrachte das Achsenkreuz

$$V = V(XY) \subseteq \mathbb{A}^2_K.$$

Bestimme für jeden Punkt $P \in V$, ob der lokale Ring an P ein Integritätsbereich ist oder nicht.

Aufgabe 2.30. Wir betrachten die Neilsche Parabel

$$C = V(X^2 - Y^3) \subseteq \mathbb{A}^2_K$$

über einem algebraisch abgeschlossenen Körper K. Zeige, dass sämtliche Lokalisierungen von C an Punkten $P \neq (0,0)$ zueinander isomorph sind, aber nicht zur Lokalisierung im Nullpunkt.

Aufgabe 2.31. Es sei R die Lokalisierung im Nullpunkt der Kurve

$$C = V(Y^2 - X^2 - X^3) \subseteq \mathbb{A}^2_K$$

und es sei S die Lokalisierung des Achsenkreuzes im Nullpunkt. Sind diese beiden lokalen Ringe isomorph?

Aufgabe 2.32. Sei R ein kommutativer Ring und sei $\mathfrak{m}$ ein maximales Ideal mit Lokalisierung $R_{\mathfrak{m}}$. Es sei $\mathfrak{a}$ ein Ideal, dass unter der Lokalisierungsabbildung zum Kern gehört. Zeige, dass dann $R_{\mathfrak{m}}$ auch eine Lokalisierung von $R/\mathfrak{a}$ ist.

Aufgabe 2.33. Es sei K ein Körper und R eine endlich erzeugte K-Algebra. Es sei $S = R_{\mathfrak{m}}$ die Lokalisierung von R an einem maximalen Ideal $\mathfrak{m}$. Zeige, dass der Restekörper von S endlich über K ist.

Aufgabe 2.34.*

Sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal. Dann ist der Restklassenring $S = R/\mathfrak{p}$ ein Integritätsbereich mit Quotientenkörper $Q = Q(S)$ und $R_{\mathfrak{p}}$ ist ein lokaler Ring mit dem maximalen Ideal $\mathfrak{p}R_{\mathfrak{p}}$. Zeige, dass eine natürliche Isomorphie

$$Q(S) \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$$

vorliegt.

Zu einem Element $f \in R$, $f \neq 0$, in einem diskreten Bewertungsring mit Primelement p heißt die Zahl $n \in \mathbb{N}$ mit der Eigenschaft $f = up^n$, wobei u eine Einheit bezeichnet, die *Ordnung* von f. Sie wird mit $\operatorname{ord}(f)$ bezeichnet.

AUFGABE 2.35. Es sei K ein Körper der Charakteristik 0 und sei $f \in K[X]$, $f \neq 0$, und $a \in K$. Zeige, dass die folgenden „Ordnungen“ von f an der Stelle a übereinstimmen.

(1) Die Verschwindungsordnung von f an der Stelle a, also die maximale Ordnung einer formalen Ableitung mit $f^{(k)}(a) = 0$.
(2) Der Exponent des Linearfaktors $X - a$ in der Zerlegung von f.
(3) Die Ordnung von f an der Lokalisierung $K[X]_{(X-a)}$ von $K[X]$ am maximalen Ideal $(X - a)$.

AUFGABE 2.36. Es sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Zeige, dass die Ordnung

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \operatorname{ord}(f),$$

folgende Eigenschaften besitzt.

(1) $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
(2) $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$.
(3) Es ist $f \in \mathfrak{m}$ genau dann, wenn $\operatorname{ord}(f) \geq 1$ ist.
(4) Es ist $f \in R^\times$ genau dann, wenn $\operatorname{ord}(f) = 0$ ist.

AUFGABE 2.37. Es sei R ein diskreter Bewertungsring. Definiere zu einem Element $q \in Q(R)$, $q \neq 0$, die Ordnung

$$\operatorname{ord}(q) \in \mathbb{Z}.$$

Dabei soll die Definition mit der Ordnung für Elemente aus R übereinstimmen und einen Gruppenhomomorphismus $Q(R) \setminus \{0\} \to \mathbb{Z}$ definieren. Was ist der Kern dieses Homomorphismus?

Abbildungsverzeichnis