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

Elliptische Kurven

Arbeitsblatt 1

Aufgaben

Aufgabe 1.1. Bestimme im Polynomring $\mathbb{Z}/(3)[X]$ alle irreduziblen Polynome vom Grad 4.

Aufgabe 1.2. Multipliziere in $\mathbb{Z}[x,y,z]$ die beiden Polynome

$$x^5 + 3x^2y^2 - xyz^3 \text{ und } 2x^3yz + z^2 + 5xy^2z - x^2y\,.$$

Aufgabe 1.3. Multipliziere in $\mathbb{Z}/(5)[x,y]$ die beiden Polynome

$$x^4 + 2x^2y^2 - xy^3 + 2y^3 \text{ und } x^4y + 4x^2y + 3xy^2 - x^2y^2 + 2y^2\,.$$

Aufgabe 1.4. Sei R ein Integritätsbereich. Zeige, dass dann auch der Polynomring $R[X]$ integer ist.

Aufgabe 1.5.*

Es sei R ein Integritätsbereich und $R[X]$ der Polynomring über R. Zeige, dass die Einheiten von $R[X]$ genau die Einheiten von R sind.

Aufgabe 1.6. Skizziere im $\mathbb{R}^2$ die Lösungsmenge der folgenden Gleichungen.

(1) $x^2 - y^2 - 1 = 0$,
(2) $x^2 + xy + y^2 = 0$,
(3) $x^2 + y^2 + 1 = 0$,
(4) $x^2 + y^2 = 0$,
(5) $x^2 + y^3 = 0$,
(6) $x^3 - y^5 = 0$,
(7) $x^2 - x^3 = 0$,
(8) $x^3 + y^3 = 1$,
(9) $x^4 + y^4 = 1$,
(10) $-5 + 3x + 4x^2 + x^3 - y^2 = 1$.

Aufgabe 1.7. Berechne den Durchschnitt der Kurven aus Aufgabe 1.6 mit den folgenden Geraden.

(1) $x = 0$,
(2) $y = 0$,
(3) $x = 1$,
(4) $y = -2$,
(5) $x = y$,
(6) $x = -y$,
(7) $2x - 3y + 4 = 0$.

AUFGABE 1.8.*

(1) Finde eine ganzzahlige Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ für die Gleichung
$$x^2 - y^3 + 2 = 0.$$
(2) Zeige, dass
$$\left(\frac{383}{1000}, \frac{129}{100}\right)$$
eine Lösung für die Gleichung
$$x^2 - y^3 + 2 = 0$$
ist.

AUFGABE 1.9.*

Finde auf der ebenen algebraischen Kurve
$$V(X^3 - Y^3 + 4X^2 - 2XY + Y + 3) \subset \mathbb{C}^2$$
einen Punkt.

AUFGABE 1.10. Es sei K ein Körper. Das Bild der durch
$$K \longrightarrow K^2,\, t \longmapsto \left(t^2,\, t^3\right),$$
definierten Kurve heißt *Neilsche Parabel*. Zeige, dass ein Punkt
$$(x, y) \in K^2$$
genau dann zu diesem Bild gehört, wenn er die Gleichung $x^3 = y^2$ erfüllt.

AUFGABE 1.11. Es sei $C \subseteq \mathbb{R}^2$ das Bild unter der polynomialen Abbildung
$$\mathbb{R} \longrightarrow \mathbb{R}^2,\, t \longmapsto \left(t^3 - 1,\, t^2 - 1\right).$$
Bestimme ein Polynom $F \neq 0$ in zwei Variablen derart, dass C auf dem Nullstellengebilde zu F liegt.

AUFGABE 1.12. Wir betrachten die Kurve

$$\mathbb{R} \longrightarrow \mathbb{R}^2,\ t \longmapsto (t^2-1, t^3-t).$$

a) Zeige, dass die Bildpunkte (x, y) der Kurve die Gleichung

$$y^2 = x^2 + x^3$$

erfüllen.

b) Zeige, dass jeder Punkt $(x, y) \in \mathbb{R}^2$ mit $y^2 = x^2 + x^3$ zum Bild der Kurve gehört.

c) Zeige, dass es genau zwei Punkte t_1 und t_2 mit identischem Bildpunkt gibt, und dass ansonsten die Abbildung injektiv ist.

AUFGABE 1.13. Betrachte Gleichungen der Form

$$y^2 = G(x) \text{ mit } G(x) = x^3 + ax^2 + bx + c$$

über $\mathbb{R}$. Skizziere die verschiedenen Lösungsmengen für die Koeffizienten $a, b, c \in \{1, -1, 0\}$.

AUFGABE 1.14. Sei $K = \mathbb{Z}/(7)$. Bestimme alle Punkte in $K^2 = K \times K$, die auf der Kurve liegen, die durch die Gleichung

$$X^2Y + 2Y^3 + 3Y^2 = 0$$

gegeben ist. Wie viele Lösungen gibt es?

AUFGABE 1.15. Bestimme alle Lösungen der Kreisgleichung

$$x^2 + y^2 = 1$$

für die Körper $K = \mathbb{Z}/(2)$, $\mathbb{Z}/(5)$ und $\mathbb{Z}/(11)$.

AUFGABE 1.16.*

Finde eine Gerade $G \subseteq \mathbb{A}^2_{\mathbb{C}}$, die die Kurve

$$C = V(X^3 + Y^3 + 1) \subseteq \mathbb{A}^2_{\mathbb{C}}$$

in genau einem Punkt schneidet.

AUFGABE 1.17.*

Zeige, dass die Neilsche Parabel

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

jede Gerade durch den Punkt $P = (1, 1) \in C$ in mindestens einem weiteren Punkt trifft.

Aufgabe 1.18.*

Begründe analytisch, dass es einen reellen Schnittpunkt des Einheitskreises $V(x^2+y^2-1)$ mit der Neilschen Parabel $V(y^2-x^3)$ gibt und bestimme numerisch die reelle x-Koordinate eines solchen Schnittpunktes mit einem Fehler $\leq 0,1$.

Aufgabe 1.19. Es sei K ein Körper und es sei

$$K \longrightarrow K^2,\, t \longmapsto (P(t),Q(t)),$$

eine durch zwei Polynome $P(t),Q(t) \in K[t]$ gegebene Abbildung. Es sei B das Bild dieser Abbildung und es sei $G \subseteq K^2$ eine Gerade. Zeige, dass $B \subseteq G$ ist oder dass der Durchschnitt $B \cap G$ endlich ist.

Aufgabe 1.20.*

Sei K ein Körper. Zeige, dass die beiden folgenden Eigenschaften äquivalent sind:

(1) K ist algebraisch abgeschlossen.
(2) Jedes nicht-konstante Polynom $F \in K[X]$ zerfällt in Linearfaktoren.

Aufgabe 1.21. Sei K ein algebraisch abgeschlossener Körper. Bestimme in $K[X]$ die irreduziblen Polynome.

Aufgabe 1.22. Sei K ein algebraisch abgeschlossener Körper. Zeige, dass K nicht endlich sein kann.

Aufgabe 1.23. Es sei $C \subseteq \mathbb{C}^2$ das Bild unter der polynomialen Abbildung

$$\mathbb{C} \longrightarrow \mathbb{C}^2,\, t \longmapsto \left(t^3-t^2+4t+3,\, -t^2+5t-1\right).$$

Bestimme ein Polynom $F \neq 0$ in zwei Variablen derart, dass C auf dem Nullstellengebilde zu F liegt.

Aufgabe 1.24. Wir betrachten die Abbildung

$$f\colon\, \mathbb{R} \longrightarrow S^1 \subseteq \mathbb{R}^2,$$

die einem Punkt $t \in \mathbb{R}$ den eindeutigen Schnittpunkt $\neq (0,-1)$ der durch die beiden Punkte $(t,1)$ und $(0,-1)$ gegebenen Geraden G_t mit dem Einheitskreis

$$S^1 \,=\, \left\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=1\right\}$$

zuordnet. Zeige, dass diese Abbildung wohldefiniert ist und bestimme die funktionalen Ausdrücke, die diese Abbildung beschreiben. Zeige, dass f differenzierbar ist. Ist f injektiv, ist f surjektiv?

AUFGABE 1.25. Wir betrachten die beiden algebraischen Kurven

$$V(x^2+y^2-2) \text{ und } V(x^2+2y^2-1)$$

über dem Körper $\mathbb{Z}/(7)$. Zeige, dass der Durchschnitt leer ist, und finde einen Erweiterungskörper $K \supseteq \mathbb{Z}/(7)$, über dem der Durchschnitt nicht leer ist. Berechne alle Punkte im Durchschnitt über K und über jedem anderen Erweiterungskörper. Man beschreibe auch den Koordinatenring des Durchschnitts.

AUFGABE 1.26.*

Es sei K ein Körper, $K[X_1,\ldots,X_n]$ der Polynomring in n Variablen und sei $\mathbb{A}^n_K$ der zugehörige affine Raum. Zeige die folgenden Eigenschaften.

(1) Es ist $V(0) = \mathbb{A}^n_K$, d.h. der ganze affine Raum ist eine affin-algebraische Menge.
(2) Es ist $V(1) = \emptyset$, d.h. die leere Menge ist eine affin-algebraische Menge.
(3) Es seien $V_1,\ldots,V_k$ affin-algebraische Mengen mit $V_i = V(\mathfrak{a}_i)$. Dann gilt
$$V_1 \cup V_2 \cup \ldots \cup V_k = V(\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_k).$$
Insbesondere ist die Vereinigung von endlich vielen affin-algebraischen Mengen wieder eine affin-algebraische Menge.
(4) Es seien V_i, $i \in I$, affin-algebraische Mengen mit $V_i = V(\mathfrak{a}_i)$. Dann gilt
$$\bigcap_{i\in I} V_i = V\left(\sum_{i\in I} \mathfrak{a}_i\right).$$
Insbesondere ist der Durchschnitt von beliebig vielen affin-algebraischen Mengen wieder eine affin-algebraische Menge.

Abbildungsverzeichnis