Seminar zu Zahlentheorie und kommutativer Algebra: Algebraische Kurven

Prof. Dr. Annette Werner, Dr. Ben Heuer

Wintersemester 2024-25

In diesem Seminar beschäftigen wir uns mit der grundlegenden Theorie ebener algebraischer Kurven und ihrer rationalen Punkte. Ebene algebraische Kurven über $\mathbb{Q}$ sind polynomielle Gleichungen in zwei Variablen x, y mit rationalen Koeffizienten, also z.B.

$$C : ax^4 + bxy + cy^2 = 0$$

für gewisse $a, b, c \in \mathbb{Q}$. Die Frage, welche Lösungen $x, y \in \mathbb{Q}$ solche polynomiellen Gleichungen haben können, beschäftigt die Mathematik seit der Zeit des antiken Griechenlands. Heutzutage sind solche Fragestellungen Gegenstand der arithmetischen Geometrie, die zahlentheoretische Fragestellungen mit geometrischen Mitteln untersucht.

Innerhalb der arithmetischen Geometrie ist die Theorie der algebraischen Kurven ein herausragendes Beispiel dafür, wie algebraische Methoden mit geometrischer Intuition verbunden werden können, um zahlentheoretische Probleme zu lösen. Nicht nur historisch gesehen bildet das Studium algebraischer Kurven daher einen Ausgangspunkt der algebraischen Geometrie. Auch für das heutige Studium algebraischer Geometrie sind "klassische" algebraische Kurven ein ausgezeichnetes Untersuchungsgegenstand, um geometrische Intuition zu entwickeln und die Motivation weiterführender Konzepte zu verstehen. Die arithmetische Geometrie algebraischer Kurven ist bis heute ein zentraler Forschungsgegenstand der modernen Zahlentheorie, inbesondere auf dem Gebiet der elliptischen Kurven, z.B. durch den Beweis von Fermats Letztem Satz durch Wiles und Taylor–Wiles (1994) oder die Birch–Swinnerton-Dyer Vermutung, eines der Millenium-Probleme.

Das Seminar ist daher besonders geeignet für Teilnehmende der Vorlesung zur algebraischen Geometrie und/oder zur Arithmetik elliptischer Kurven, da sich diese Veranstaltungen jeweils gut ergänzen. Der Besuch dieser Vorlesungen ist aber nicht notwendig für die Teilnahme am Seminar.

Wir beginnen in diesem Seminar mit vorbereitenden Betrachtungen zu rationalen Punkten von Kurven über $\mathbb{Q}$: Hierfür studieren wir mit elementaren geometrischen und zahlentheoretischen Methoden Kegelschnitte und einen Spezialfall von Fermats Letztem Satz. Wir motivieren dann das Konzept der projektiven Kurven und besprechen Singularitäten von Kurven. Anhand der Schnitttheorie sehen wir, warum der Übergang von affinen auf projektive Kurven von Vorteil ist. Als Hauptsatz beweisen wir schließlich den Satz von Bézout.

Für das Seminar folgen wir hauptsächlich dem Buch von Silverman–Tate [1], welches als e-Book in der Bibliothek verfügbar ist. Beachten Sie, dass unsere Quellen auf englisch geschrieben sind, der Vortrag soll aber als Tafelvortrag auf Deutsch gehalten werden. Unklarheiten bei der Übersetzung können gegebenenfalls bei der Vorbesprechung geklärt werden.

Kontaktieren Sie bitte Herrn Heuer im Vorfeld rechtzeitig, das heißt mindestens drei bis vier Wochen vor ihrem Vortrag, damit wir eine Vorsprechung vereinbaren können. Hier haben Sie die Möglichkeit, die Ausarbeitung Ihres Vortrags zu besprechen und Fragen zu stellen. Diese Vorbesprechung kann auf zoom erfolgen.

Beachten Sie bitte auch unsere allgemeinen Tipps und Hinweise zur Vorbereitung eines gelungenen Seminarvortrages unter folgendem Link: https://www.uni-frankfurt.de/134848419.pdf.

Wir empfehlen allen Teinehmenden zur Einführung ins Thema die Seiten 1-8 in [1] zu lesen. Die jeweils als Referenzen angegebenen Stellen im Buch beziehen sich nur auf das vorzustellende Material. Selbstverständlich müssen Sie für gewöhnlich auch andere Teile im Buch lesen, um dieses Material verstehen zu können.

Vortrag 1: Rationale Punkte von Kegelschnitten

Referenz: [1, §1.1, S.9-14]

In diesem Vortrag sehen wir ein erstes Beispiel dafür, wie Geometrie und Zahlentheorie miteinander verbunden werden können, um rationale Lösungen von Gleichungen zu finden: Besprechen Sie zunächst kurz die Theorie der rationalen Punkte linearer Gleichungen, also Gleichungen der Form

$$ax + by + c = 0$$

für Koeffizienten $a, b, c \in \mathbb{Q}$ und Variablen x, y.

Erklären Sie dann die Parameterdarstellung rationaler Punkte von Kegelschnitten, das heißt Gleichungen der Form

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

für $a, b, c, d, e, f \in \mathbb{Q}$. Beweisen Sie als Anwendung die Parameterdarstellung von Lösungen der pythagoräischen Gleichung

$$x^2 + y^2 = z^2.$$

Falls die Zeit dies zulässt, zeigen Sie noch, dass $x^2 + y^2 = 3$ keine rationalen Lösungen hat (S.14).

Vortrag 2: Fermat's Letzter Satz für $n = 4$ und unendlichen Abstieg

Referenz: [3, §2-3] Führen Sie die Fermat-Gleichung

$$x^n + y^n = z^n.$$

ein und formulieren Sie "Fermat's Letzten Satz".

Führen Sie dann die Beweismethode des "unendlichen Abstiegs" ein, indem Sie zunächst den Beweis erklären, dass $X^2 = d$ für $d \in \mathbb{Z}$ keine Lösungen in $\mathbb{Q}$ hat falls es keine Lösung in $\mathbb{Z}$ hat. Beweisen Sie dann durch "unendlichen Abstieg" dass

$$x^4 + y^4 = z^2$$

keine nicht-trivialen Lösungen in $\mathbb{Q}$ hat (Theorem 3.1). Folgern Sie, dass die kubische Gleichung

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

nur die triviale Lösung $x = y = 0$ in $\mathbb{Q}$ hat (Corollary 3.8).

Vortrag 3: Ebene projektive Kurven

Referenz: [1, Appendix A.1-A.2, S. 220-226, 228-231]

Motivieren Sie anhand der Fermat-Gleichung die algebraische Definition der projektiven Ebene $\mathbb{P}^2$. Besprechen Sie dann die geometrische Definition von $\mathbb{P}^2$ und erklären Sie die Äquivalenz zur algebraischen Definition.

Führen Sie dann ebene affine algebraische Kurven ein. Erklären Sie die Definition homogener Gleichungen und die Definition ebener projektiver algebraischer Kurven. Besprechen Sie Homogenisierung und Dehomogenisierung von Gleichungen.

Definieren Sie den Grad und führen Sie die Begriffe “Geraden” (engl. “line” für Kurven von Grad 1), “Kegelschnitte” (engl. “conics” für Kurven von Grad 2), “Kubiken” (engl. “cubics” für Kurven von Grad 3) ein.

Definieren Sie rationale Kurven und rationale Punkte (S.229). Besprechen Sie schließlich noch Tangenten und singuläre Punkte inklusive Beispielen (S.230-231). Besprechen Sie auch die homogene Version in Exercise A.5 (S.255) wenn die Zeit dies zulässt.

Vortrag 4: Geraden und projektive Koordinatentransformationen

Referenz: [1, §A.2, S.231-232, 254-256] Erinnern Sie an die Definition von Geraden im $\mathbb{P}^2$ als Kurven von Grad 1, d.h. Gleichungen der Form

$$\alpha X + \beta Y + \gamma Z = 0.$$

Beweisen Sie die folgenden Aussagen (Exercise A.1 auf S.254):

1. Für zwei Punkte $P_1 \neq P_2$ in $\mathbb{P}^2$ gibt es genau eine Gerade die durch P_1 und P_2 geht.
2. Zwei beliebige verschiedene Geraden treffen sich in genau einem Punkt in $\mathbb{P}^2$.

Erklären Sie dann wie invertierbare Matrizen in $M_3(k)$ projektive Koordinatentransformationen $\phi : \mathbb{P}^2 \to \mathbb{P}^2$ definieren (§A.2, S.231-232). Zeigen Sie, nun die folgenden Lemmata (aus Exercise A.10-11 auf S.256)

3. ϕ schickt Kurven von Grad d in $\mathbb{P}^2$ auf Kurven von Grad d. Insbesondere schickt ϕ Geraden auf Geraden (Exercise A.10).
4. Seien $P_1 = [x_1, y_1, z_1]$, $P_2 = [y_1, y_2, y_3]$, $P_2 = [z_1, z_2, z_3] \in \mathbb{P}^2$. Dann gibt es eine Gerade die durch alle drei Punkte geht genau dann wenn die folgende Matrix nicht invertierbar ist:

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}$$

   Gibt es keine solche Gerade, so gibt es eine Koordinatentransformation, welche

$$P_1 \mapsto [1, 0, 0], \quad P_2 \mapsto [0, 1, 0], \quad P_3 \mapsto [0, 0, 1]$$

   abbildet (A.11.a).
5. Für jede Gerade $L \subseteq \mathbb{P}^2$ und jeden Punkt P der nicht auf L gibt, gibt es eine Koordinatentransformation, die P auf $[0, 0, 1]$ schickt und L auf die Gerade

$$\mathbb{P}^2 \setminus \mathbb{A}^2 = \{[x, y, 0] | x, y \in k\} = \{[x, y, z] | 0 \cdot x + 0 \cdot y + 1 \cdot z = 0\},$$

   welche “Gerade im unendlichen” genannt wird (A.11.(d)). Hinweis: Verwenden sie 1 und 4.

Vortrag 5: Schnitte von Kurven

Referenz: [1, Appendix A.3, S. 233-242]

Zeigen Sie direkt aus der Definition, dass sich zwei verschiedene Geraden in $\mathbb{P}^2$ in genau einem Punkt schneiden.

Besprechen Sie ausführlich die Beispiele für Schnitte projektiver Kurven auf S.233-237. Legen Sie dabei besonderen Fokus darauf, anhand der Grafiken auf S.235 die jeweiligen algebraischen Phänomene mit der geometrischen Intution in Einklang zu bringen

Nutzen Sie das Beispiel unten auf Seite 236 um die Begriffe Irreduzibilität, irreduzible Komponenten und gemeinsame Komponenten von Kurven zu motivieren.

Falls die Zeit dies zulässt, besprechen Sie noch weitere Beispiele aus Exercise A.12 (S.257).

Vortrag 6: Schnittzahlen

Referenz: [1, Appendix A.3, S.245-251] [4, §4.2]

Definieren Sie den lokalen Ring $\mathcal{O}_P$ eines Punktes $P \in \mathbb{A}^2(k)$ und beweisen Sie die grundlegenden Eigenschaften von $\mathcal{O}_P$ aus Aufgabe A.15 (S.257). Definieren Sie die Schnittzahl (Multiplizität eines Schnittpunktes) wie auf S.245-246.

Erklären Sie zweitens, wie man die Definition der Schnittzahl auf Punkte in $\mathbb{P}^2(k)$ ausdehnt, indem man homogene Koordinaten einführt (S. 248) und zeigen Sie die Kompatibilität mit der affinen Definition (5.1) und (5.2) auf S. 249. Zeigen Sie schließlich, dass die Schnittzahl invariant unter projektiver Koordinatentransformation ist (5.3).

Definieren Sie transversale Schnitte und zeigen Sie, dass sich zwei Kurven C und C' im Punkt P transversal schneiden, genau dann wenn $I(C, C', P) = 1$ [1, (6.1)-(6.5) auf S.250-251] (siehe auch §4.2 in [4]).

Vortrag 7: Der Satz von Bézout I: Endlichkeit der Schnittmenge

Referenz: [1, Appendix A.5, 237, S.242-244, 249]

Sei k ein algebraisch abgeschlossener Körper. Formulieren Sie den Satz von Bézout (S.237) und geben Sie zunächst ein Übersicht über den Beweis indem Sie Schritte (1)-(4) auf S.242-243 nennen.

Zeigen Sie als erstes Lemma für den Beweis zunächst (5.4) auf S.249: Für jede endliche Menge S in $\mathbb{P}^2(k)$ gibt es eine Gerade in $\mathbb{P}^2$, die S nicht schneidet.

Seien nun C_1 und C_2 projektive Kurven ohne gemeinsame Komponenten. Es seien d_1, d_2 die Grade von C_1 und C_2 und f_1, $f_2 \in k[X, Y]$ die dehomogenisierten Gleichungen. Sei $C_1 \cap C_2 \cap \mathbb{A}^2$ die Menge der Schnittpunkte von C_1 und C_2 in $\mathbb{A}^2(k)$. Zeigen Sie:

$$\#(C_1 \cap C_2 \cap \mathbb{A}^2) \leq \dim_k(k[X, Y]/(f_1, f_2)),$$

indem Sie (1.1)-(1.2) beweisen. Zeigen Sie zweitens, dass

$$\dim_k(k[X, Y]/(f_1, f_2)) \leq d_1 d_2,$$

indem Sie (1.3)-(1.6) beweisen.

Vortrag 8: Der Satz von Bézout II: Dimension des Koordinatenrings

Referenz: [1, Appendix A.5, S.244-249]

Folgern Sie zunächst aus dem letzten Vortrag: Die Schnittmenge $C_1 \cap C_2$ ist endlich, (5.5) auf S.249. Folgern Sie mithilfe von (5.4) aus dem letzten Vortrag, dass wir durch eine Koordinatentransformation annehmen können, dass C_1 und C_2 keinen Schnittpunkt in $\mathbb{P}^2 \setminus \mathbb{A}^2$ haben (sich also "nicht im unendlichen treffen"). Zeigen Sie, dass in diesem Fall

$$\dim_k(k[X, Y]/(f_1, f_2)) = d_1 d_2$$

indem Sie (2.1)-(2.4) auf S.244-245 beweisen.

Zeigen Sie nun die Endlichkeitseigenschaften (3.1)-(3.3) auf S.246.

Vortrag 9: Der Satz von Bézout III: Der Beweis

Referenz: [1, Appendix A.5, S.246-248]

Dieser Vortrag beschließt den Beweis des Satzes von Bézout. Hierfür ist noch zu zeigen, dass

$$\sum_{P \in \mathbb{A}^2(k)} I(C_1 \cap C_2, P) = \dim(k[X, Y]/(f_1, f_2)).$$

Zeigen Sie zunächst die Ungleichung $\leq$ indem Sie (3.4)-(3.6) auf S.246-247 beweisen.

Zeigen Sie dann (4.1)-(4.5) um die Ungleichung $\geq$ zu beweisen (S.248).

Falls die Zeit dies zulässt, können Sie abschließend noch den Satz von Cayley-Bacharach und den Satz von Pascal erwähnen (S.240 unten).

Vortrag 10: Das Gruppengesetz der Lösungen kubischer Gleichungen

Referenz: [1, §I.2, S.15-21] [2, §III.2].

Sei K ein beliebiger Körper. Definieren Sie elliptische Kurven als nicht-singuläre kubische projektive Kurven C in $\mathbb{P}^2$ mit einem gegebenen Punkt $\mathcal{O} \in C(K)$. Nutzen Sie den Satz von Bézout um die Verknüpfung

$$* : C(K) \times C(K) \to C(K), \quad P, Q \mapsto P * Q$$

zu definieren. Erklären Sie dann, wie man $*$ und $\mathcal{O}$ benutzt, um das Gruppengesetz

$$+ : C(K) \times C(K) \to C(K)$$

zu definieren. Zeigen Sie, dass $\mathcal{O}$ eine neutrales Element ist, und dass $+$ kommutativ ist. Skizzieren Sie dann den Beweis der Assoziativität. Geben Sie hierfür die Aussage des kubischen Satzes von Cayley–Bacharach Theorem (S.240 unten) wieder, und erklären sie die Beweisskizze auf S.16-17.

Wenn die Zeit dies zulässt, können Sie noch skizzieren, wie die projektiven Transformationen aus Vortrag 4 es ermöglichen, jede elliptische Kurve in Weierstraß-Normalform zu bringen (siehe auch [1, S. 22-23]).

Vortrag 11: Ausblick

Zum Abschluss geben in diesem Vortrag die Dozenten einen Überblick über weiterführende Themen zu Kurven, insbesondere Faltings' Satz (Mordellvermutung), sowie einen Ausblick auf aktuelle Forschungsthemen rund um elliptische Kurven. Zu den möglichen Themen gehören L-Funktionen, die Vermutung von Birch-Swinnerton Dyer, Modularität, Fermats Letzter Satz, die Vermutung des beschränkten Rangs, Elliptic Curve Cryptography, ...

References

[1] Joseph H Silverman and John T Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992. Einsehbar hier[1]: `https://ubffm.hds.hebis.de/Record/HEB465037895`

[2] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[3] Keith Conrad. Proofs by descent, 2007. Einsehbar hier: `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/descent.pdf`.

[4] Klaus Hulek. *Elementare algebraische Geometrie: grundlegende Begriffe und Techniken mit zahlreichen Beispielen und Anwendungen.* Springer-Verlag, 2012.

[1] Bitte beachten Sie: Es gibt auch neuere Auflage (2015) dieses Buches. Diese können Sie ebenfalls verwenden falls Sie darauf Zugriff haben, beachten Sie dann allerdings die veränderten Seitenzahlen. Wir richten uns in diesem Programm nach der Auflage, die in der Bibliothek als e-Book frei verfügbar ist.