Seminar:
Rationale Punkte auf Elliptischen Kurven

Prof. Dr. Otmar Venjakob, Max Witzelsperger

Wintersemester 2022/23

Zu den grundlegenden Gegenständen der Zahlentheorie gehören sogenannte *diophantische Gleichungen*; darunter versteht man polynomiale Gleichungen mit ganzzahligen oder rationalen Koeffizienten. Ein berühmtes diophantisches Problem ist Fermats Behauptung, dass die Gleichung

$$X^n + Y^n = Z^n, \quad \text{mit } n \geq 3$$

keine nicht-triviale Lösung in $\mathbb{Z}^3$ besitzt. Diese Vermutung, aufgestellt im Jahr 1637, konnte erst 1994 durch Andrew Wiles vollständig bewiesen werden.
Für die Behandlung diophantischer Probleme hat sich der geometrische Blickwinkel als essentiell erwiesen: Betrachtet man z.B. eine Gleichung in zwei Variablen, also von der Form

$$F(X, Y) = 0, \quad \text{mit } F \in \mathbb{Q}[X, Y],$$

so lässt sich die Menge C aller *reellen* Lösungen $(x, y) \in \mathbb{R}^2$ der Gleichung als Kurve in der Ebene $\mathbb{R}^2$ zeichnen. Eine solche Menge $C \subseteq \mathbb{R}^2$ heißt eine *ebene algebraische Kurve*. Wir definieren die Teilmengen $C(\mathbb{Q}) := \mathbb{Q}^2 \cap C$ bzw. $C(\mathbb{Z}) := \mathbb{Z}^2 \cap C$ aller *rationalen* bzw. aller *ganzzahligen Punkte* auf C.
Das diophantische Problem besteht nun darin festzustellen, ob diese Mengen nicht-leer sind (Existenz rationaler Punkte), und falls ja, sie möglichst genau zu beschreiben. (kann man z.B. aus einer gegebenen rationalen Lösung weitere konstruieren?)

In diesem Seminar beschäftigen wir uns mit solchen Fragestellungen für ebene Kurven über $\mathbb{Q}$. Einen Schwerpunkt bilden dabei die *elliptischen Kurven*. Das sind Kurven E, welche durch Gleichungen der Form

$$Y^2 = f(X), \quad \text{mit } f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$$

gegeben sind, wobei f keine mehrfachen Nullstellen besitze. Diese haben wichtige Anwendungen in verschiedenen Bereichen der Mathematik, etwa in Wiles' Beweis der Fermat-Vermutung, oder auch bei kryptographischen Verfahren.
Wir werden sehen, dass $E(\mathbb{Q})$ die Struktur einer abelschen Gruppe trägt, deren Verknüpfung durch gewisse geometrische Operationen gegeben ist. Weiter werden wir das *Theorem von Mordell-Weil* kennen lernen, welches besagt, dass die Gruppe $E(\mathbb{Q})$ stets endlich erzeugt ist. Insbesondere gibt es also eine endliche Teilmenge in $E(\mathbb{Q})$, aus der sich alle weiteren rationalen Punkte konstruieren lassen.
Mögliche ergänzende Themen sind komplexe Punkte auf elliptischen Kurven, p-adische Zahlen, Kurven über endlichen Körpern, sowie weitere diophantische Probleme.

Zielgruppe: Bachelor-Studierende der Mathematik ab dem 3. Semester.

Vorbesprechung: Mittwoch, den 27.7.22 um 13:00 Uhr s.t. im SR 9.

Kontakt:
Max Witzelsperger
INF 205, Raum 4.231
Email: mwitzelsperger@mathi.uni-heidelberg.de