Ankündigung zum Seminar

Einführung in die Theorie der elliptischen Kurven

Wintersemester 2012/2013

Prof. Dr. K. Wingberg
K. Hübner

Inhalt

Eine *elliptische Kurve* ist die Nullstellenmenge einer kubischen Gleichung der Form

$$E : y^2 = x^3 + Ax + B$$

in der projektiven Ebene. In der Sprache der algebraischen Geometrie sind dies gerade die eindimensionalen projektiven Varietäten vom Geschlecht 1. Neben dem Studium der geometrischen Eigenschaften solcher Kurven ist vor allem die Frage nach *rationalen Punkten* von Interesse, d.h. nach Punkten (x, y) auf E mit rationalen Zahlen $x, y \in \mathbb{Q}$. Während beispielsweise die Frage nach Lösungen von (homogenen) quadratischen Gleichungen (Geschlecht 0) durch den Satz von Hasse-Minkowski eine elegante und effektive Lösung erfährt, stellt dies für Gleichungen der Ordnung 3 eine weitaus größere Herausforderung dar. Für die Anzahl der Punkte einer elliptischen Kurve über endlichen Körpern liefert der *Satz von Hasse-Weil* eine effektive Schranke. Die *Weil-Vermutungen*, welche in ihrer allgemeinen Form erst 1974 durch Pierre Deligne bewiesen wurden, lassen sich für elliptische Funktionen elementar herleiten.

Eine wichtige Eigenschaft einer elliptischen Kurve E über einem Körper K ist die folgende: Man kann auf der Menge der K-rationalen Punkte $E(K)$ eine Verknüpfung derart definieren, dass $E(K)$ zu einer abelschen Gruppe wird, d.h. elliptische Kurven sind *abelsche Varietäten.* Der *Satz von Mordell-Weil* besagt nun, dass für jeden Zahlkörper K die Gruppe $E(K)$ stets endlich erzeugt ist. Nach der berühmten *Birch-Swinnerton-Dyer-Vermutung* ist der Rang einer elliptischen Kurve dabei durch das Nullstellenverhalten ihrer L-Funktion gegeben. Die große Bedeutung der Theorie der elliptischen Kurven für die Zahlentheorie zeigt nicht zuletzt auch der Beweis des Fermatschen Satzes durch Andrew Wiles. Dieser folgt aus der Richtigkeit der *Taniyama-Shimura-Vermutung*, welche eine Verbinung zwischen elliptischen Kurven und Modulformen herstellt.

In diesem Seminar werden wir zunächst die benötigten Grundlagen aus der algebraischen Geometrie bereitstellen und uns dabei insbesondere der Theorie algebraischer Kurven zuwenden. Danach werden wir die Gruppenstruktur einführen und die Geometrie elliptischer Kurven näher untersuchen. Nach dem Studium elliptischer Kurven über endlichen Körpern wenden wir uns dem Beweis des Satzes von Mordell-Weil zu.

Zielgruppe

Studierende der Mathematik (Bachelor/Master und Lehramt)

Voraussetzungen

Algebra I (Für einen Teil der Vorträge sind Vorkenntnisse aus der Vorlesung Algebraische Zahlentheorie I hilfreich, die benötigten Resultate können jedoch mit der Bereitschaft zum eigenständigen Nachlesen auch im Rahmen der Seminarvorbereitung erarbeitet werden.)

Zeit und Ort

Donnerstag, 14 Uhr ct
HS 5 (INF 288)

Vorbesprechung und Anmeldung

Die Vorbesprechung findet an folgendem Termin statt:

Donnerstag, 26. Juli, 16.00 Uhr
HS 4 (INF 288)

Eine Anmeldung ist zudem ab sofort bei Katharina Hübner (Zimmer 007) und per E-Mail (khuebner@mathi.uni-heidelberg.de) möglich. Die Vortragsliste findet sich auch online unter www.mathi.uni-heidelberg.de/∼gaertner/curves

Kontakt: khuebner@mathi.uni-heidelberg.de