Seminar Elliptische Kurven
Wintersemester 2017/18

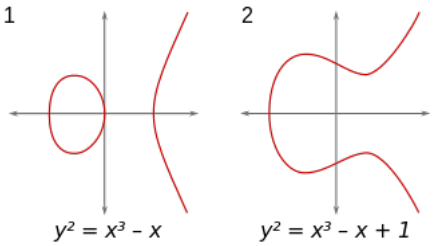
Inhalt

Eine elliptische Kurve E über einem Körper K ist die Lösungsmenge in K^2 einer Gleichung der Form

$$E: y^2 = x^3 + ax + b$$

(mit $4a^3 + 27b^2 \neq 0$) zusammen mit einem „unendlich fernen Punkt“ ∞. In der Sprechweise der algebraischen Geometrie handelt es sich um eine glatte projektive Kurve über K.

Das Aussehen und die Eigenschaften elliptischer Kurven hängen dabei stark vom Körper K ab. Typische Beispiele elliptischer Kurven über $\mathbb{R}$ sind rechts abgebildet. Über $\mathbb{C}$ ist es dagegen sinnvoll, sich eine elliptische Kurve als Torus vorzustellen. Sucht man dagegen nach Lösungen über $\mathbb{Q}$, kann es passieren, dass die Kurve nur endlich viele rationale Punkte hat.



Auf einer elliptischen Kurve E kann man eine Addition definieren, die E zu einer abelschen Gruppe macht. Der Satz von Mordell-Weil besagt, dass die Gruppe $E(\mathbb{Q})$ der rationalen Punkte von E endlich erzeugt ist.

Elliptische Kurven spielen eine fundamentale Rollen bei vielen Resultaten und Problemstellungen der Zahlentheorie. Ein Beispiel ist Andrew Wiles' Beweis von Fermats letztem Satz, der darauf basiert, dass jede elliptische Kurve über $\mathbb{Q}$ „modular“ ist. Eine weitere berühmte Vermutung stammt von Birch und Swinnerton-Dyer und besagt, dass der Rang des freien Anteils einer elliptischen Kurve über $\mathbb{Q}$ gleich der Verschwindungsordnung einer zu E assoziierten L-Funktion $L(E, s)$ bei $s = 1$ ist.

Auch in unserem Alltag spielen elliptische Kurven eine große Rolle. Die neuen Personalausweise in Deutschland nutzen zur Authentifizierung Verschlüsselungsalgorithmen, die auf der Theorie der elliptischen Kurven basieren.

Im Seminar wollen wir uns die Grundlagen der Theorie der elliptischen Kurven über $\mathbb{Q}$ und $\mathbb{C}$ erarbeiten. Dabei werden wir uns am Buch von J. S. Milne orientieren. Das Buch ist unter folgender URL erhältlich: `http://www.jmilne.org/math/Books/ectext5.pdf`

Vorraussetzungen und Kontakt

Das Seminar richtet sich vorrangig an Studierende im Master Mathematik oder Technomathematik. Bei Interesse gibt es aber auch Vorträge, die für Bachelorstudierende dieser Studiengänge geeignet sind. Vorausgesetzt werden gute Kenntnisse der Grundvorlesungen, insbesondere der Funktionentheorie und der Algebra. Vorkenntnisse aus der algebraischen Geometrie sind hilfreich, aber nicht zwingend notwendig.

Das Seminar findet Montags, 9-11h in Raum E 2 304 statt. Am ersten Termin (9. Oktober 2017) findet eine Vorbesprechung statt. Interessenten werden gebeten, sich bereits vorab per Email zu melden. Der erste Vortrag ist am 30. Oktober. Jeweils eine Woche vor den jeweiligen Vorträgen findet eine Vorbesprechung mit der Dozentin statt. Es wird erwartet, dass Sie dazu

eine handschriftliche Ausarbeitung Ihres Vortrags vorbereiten.
Dr. Claudia Alfes-Neumann, alfes@math.uni-paderborn.de