Arithmetik elliptischer Kurven

Prof. Dr. Stefan Schröer, Dr. Irene Bouw
Montags, 14–16 Uhr, Seminarraum 25.22.02.81

Das Seminar richtet sich an Studenten ab dem fünften Semester. Es sollen gemeinsam einige Abschnitte aus dem Buch von Silverman und Tate über elliptische Kurven über $\mathbb{Q}$ erarbeitet werden. Dabei wird es um die Sätze von Mordell und Nagell–Lutz über die Gruppe der rationalen Punkte solcher elliptischer Kurven gehen. Vorkenntnisse über algebraische Geometrie oder elliptische Kurven sind hilfreich, aber nicht notwendig.

17.10 (**Irene Bouw**) Vorbesprechung und Einführung.

24.10 (**Irene Bouw**) Ebene algebraische Kurven. Referenz: [4, Appendix A], [2, Kapitel 1].

31.10 (**Denis Skorodumov**) Elliptische Kurven und das Gruppengesetz. Referenz: [4, §I.2–3]. Weierstraß'sche-Normalform. Das Gruppengesetz. Die Duplikationsformel. Beispiele.

7.11 (**Maziar Khosrobeik**) Diophantische Gleichungen. Referenz: [4, §I.1, III.7], [2, Kapitel 1]. Diophantische Gleichungen über $\mathbb{Q}$. Parametrisierung von Kegelschnitten, Beispiele: $x^2 + y^2 = 1$, $y^2 = x^3 + x^2$. Die rationale Punkte einer elliptischen Kurve lassen sich nicht parametrisieren.

14.11 (**Illya Gendler**) Torsionspunkte. Referenz: [4, Kapitel II]. Auszug aus Kapitel II, ohne Beweise, aber mit Beispielen. Beschreiben Sie die 2- und 3-Torsionspunkte einer elliptische Kurve. Formulieren Sie die Sätze von Mordell, Nagel–Lutz und Mazur. Beispiele.

21.11 (**Lisa Bettermann**) Höhen. Referenz: [4, §III.1], [3, §VIII.4]. Definieren Sie die Höhefunktionen H und h. Beweis der Endlichkeitseigenschaft, Lemma 1 und des Abstiegs-Theorem aus [4, §III.1]. Strategie des Beweises des Satzes von Mordell.

28.11 (**Eva Schmerge**) Höheabschätzungen. Referenz: [4, §III.2–3], [3, §VIII.4]. Zeige: falls $P = (x, y) \in C(\mathbb{Q})$, so ist $x = m/e^2$, $y = n/e^3$ mit $m, n, e \in \mathbb{Z}$, $e > 0$ und $\mathrm{ggT}(m, e) = \mathrm{ggT}(n, e) = 1$. Zeige: $|n| \leq KH(P)^{3/2}$, für ein konstante $K = K(a, b, c) > 0$. Beweis von Lemmas 2 und 3.

5.12 (**Konstantinos Georgiades**) Elliptische Kurven über $\mathbb{C}$ und Isogenien. Referenz: [4, §III.4], [1, Anhang zu §V.3]. Beschreibung einer elliptischen Kurve über $\mathbb{C}$ als $C = \mathbb{C}/\Lambda$, wobei $\Lambda \subset \mathbb{C}$ ein Gitter ist. Isogenien. Beweise der Proposition aus [4, §III.4]. Diese Vortrag soll von einem Student gehalten werden, der die Vorlesung *elliptische Kurven und elliptische Funktionen* gehört hat.

12.12 (**Olivia Krajuc**) Beweis des Satzes von Mordell I. Referenz: [4, §III.5]. Ende des Beweises des Satzes von Mordell in dem Fall, dass C einen rationalen 2-Torsionspunkt hat.

19.12 (**Robert Jones**) Beispiele. Referenz: [4, §III.6].

9.1 (**Daniel Appel**) Beweis des Satzes von Mordell II. [3, §VIII.1] Skizzieren Sie den Beweis des schwachen Satzes von Mordell. Dies liefert der Beweis des Satzes von Mordell im allgemeinen Fall. Dieser Vortrag sollte von einen Studenten mit Vorkenntnissen in der Zahlentheorie gehalten werden.

16.1 (**Gregor Golenia**) Der Satz von Siegel. Referenz: [4, §V.1–2]

References

[1] E. Freitag and R. Busam. *Funktionentheorie*. Springer-Lehrbuch. Springer-Verlag, 1993.

[2] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, 1994.

[3] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[4] J. H. Silverman and J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, 1992.