Seminar Arithmetik Elliptischer Kurven
Wintersemester 2010/11

Elliptische Kurven lassen sich leicht definieren als Nullstellenmengen von Polynomen vom Grad 3 in zwei Variablen. Einerseits kann man elliptische Kurven über $\mathbb{C}$ aus dem Blickwinkel der klassischen algebraischen oder auch der komplex-analytischen Geometrie studieren. Andererseits kann man sich nach dem Lösungsverhalten der definierenden Polynomgleichung fragen. Die arithmetische Geometrie versucht, beide Blickwinkel zu verfolgen, und die Geometrie der elliptischen Kurve über endlichen Körpern oder Zahlkörpern in Zusammenhang mit den Lösungen der Polynomgleichung zu bringen. Ziel des Seminars soll es sein, verschiedene Aspekte elliptischer Kurven kennenzulernen.

1 Vortragsliste

1. **Elliptische Kurven über $\mathbb{C}$ und elliptische Funktionen**

   18.10. und 25.10.2010

   Definition elliptische Funktion, (Motivation elliptische Integrale), Beispiele für elliptische Funktionen: Weierstrass $\wp$-Funktion, meromorphe Funktionen, Funktionenkörper von elliptischen Kurven (Eisenstein-Reihen, Uniformisierung)

   [Sil09, Kapitel VI], [Ahl66, Kapitel 7]

2. **Definitionen und Beispiele**

   08.11. und 15.11.2010

   Allgemeine Definitionen von Divisoren, Satz von Riemann-Roch, Satz von Hurwitz, immer am Beispiel elliptischer Kurven und ohne Beweise.

   Definition elliptische Kurve, Beispiele, Weierstrass-Normalform für elliptische Kurven (Herleitung aus Riemann-Roch), j-Invariante und Klassifikation

   [Sil09, Kapitel II.3-5, III.1], evtl auch [Har77, Kapitel IV.1,IV.2 und Theorem IV.4.1, Prop. IV. 4.6]

3. **Gruppengesetz**

   22.11.2010

   Konstruktion der Gruppenstruktur auf einer elliptischen Kurve (geometrisch und über Riemann-Roch), z.B. [Sil09, Kapitel III.2]

4. **Isogenien und Endomorphismenring**

   29.11. und 06.12.2010

   Isogenien und Endomorphismen über $\mathbb{C}$ [Sil09, Kapitel VII.4-5]

   Definition Isogenie, duale Isogenie

   Beschreibung Endomorphismenring und Automorphismengruppe von elliptischen Kurven, (ohne Beweis) [Sil09, Kapitel III.9-10]

5. **Tate-Modul und Weil-Paarung**

   13.12.2010

   Torsionspunkte, Struktur der Gruppe der Torsionspunkte, [Sil09, Kapitel III.4 und III.6]

   Tate-Modul, Weil-Paarung

6. **Elliptische Kurven über $\mathbb{F}_q$ und Weil-Vermutung**

   10.01.2011

   Anzahl der rationalen Punkte auf elliptischen Kurven über endlichen Körpern, Hasse-Schranke, Weil-Vermutung, Beweis im Fall elliptischer Kurven

   Literatur z.B. Kapitel III.7-8 und V.1-2 in [Sil09]

7. **Satz von Mordell-Weil**

   17.01.2011 und 24.01.2011

   Beweisskizze des Satzes, z.B. Kapitel VIII [Sil09] oder [Ser97]: schwacher Satz von Mordell-Weil, Abstiegsargument und Höhenfunktionen auf elliptischen Kurven,

   Zur Vereinfachung: nur Spezialfall elliptischer Kurven über $\mathbb{Q}$, Aussagen über elliptische Kurven über lokalen Körpern ohne Beweis

8. **Hasse L-Funktionen**

   31.01.2011

   Definition Hasse L-Funktion für elliptische Kurven, analytische Eigenschaften, insbesondere Funktionalgleichung in einem Beispiel [Kob93, Kapitel II.§5]. Diskussion des Satzes von Weil im Zusammenhang mit Funktionalgleichung, [Kob93, p. 142/143].

9. **Die Vermutung von Birch und Swinnerton-Dyer**

   07.02.2011

   Definition L-Reihe zu elliptischen Kurven, Definition der arithmetischen Invarianten in der Vermutung (Tate-Shafarevich-Gruppe, elliptischer Regulator,...), Formulierung der Vermutung, Vergleich mit Klassenzahlformel.

Literatur

[Ahl66] L.V. Ahlfors. Complex analysis: An introduction of the theory of analytic functions of one complex variable. Second edition, McGraw-Hill 1966.

[Har77] R. Hartshorne. Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, 1977.

[Hus04] D. Husemöller. Elliptic curves. Second edition. Graduate Texts in Mathematics, 111. Springer-Verlag, New York, 2004.

[Kna92] A.W. Knapp. Elliptic curves. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[Kob93] N. Koblitz. Introduction to elliptic curves and modular forms. Second edition. Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1993.

[Kob94] N. Koblitz. A course in number theory and cryptography. Second edition. Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1994.

[Ser97] J.-P. Serre. Lectures on the Mordell-Weil theorem. Third edition. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1997.

[Sil09] J.H. Silverman. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[Sil97] J.H. Silverman. A survey of the arithmetic theory of elliptic curves. In: *Modular forms and Fermat's last theorem*, 17–40, Springer, New York, 1997.

[ST92] J.H. Silverman und J. Tate. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Wer02] A. Werner. Elliptische Kurven in der Kryptographie. Springer, 2002.