Vortragsliste

Einführung in die Theorie der elliptischen Kurven

Wintersemester 2012/2013

Prof. Dr. K. Wingberg
K. Hübner

---

1 Geometrie elliptischer Kurven

Vortrag 1. Algebraische Varietäten (18.10.12)
Affine und projektive Varietäten; Dimension; rationale Punkte; Glattheit; Morphismen von Varietäten
Literatur: [Si] I.1-I.3

Vortrag 2. Kurven (25.10.12)
Ordnung einer Funktion in einem Punkt einer Kurve; Polstellen; Funktionenkörper einer Kurve; Verzweigung; Frobeniusabbildung
Literatur: [Si] II.1-II.2

Vortrag 3. Der Satz von Riemann-Roch (08.11.12)
Divisoren; Differentialformen und die kanonische Divisorenklasse; Aussage des Satzes von Riemann-Roch; Hurwitz-Formel
Literatur: [Si] II.3-II.5, [Ha] V.1-V.2

Vortrag 4. Gruppengesetz und Weierstraß-Gleichungen (15.11.12)
Weierstraß-Gleichungen; Diskriminante; j-Invariante; Gruppengesetz; geometrische Interpretation
Literatur: [Si] III.1-III.2, [ST] I.3-I.4

Vortrag 5. Elliptische Kurven (22.11.12)
Definition von elliptischen Kurven als Kurven vom Geschlecht 1; Weierstraß-Gleichung einer elliptischen Kurven mittels Riemann-Roch; der Additionsmorphismus; kurzer Ausflug zur Theorie von Jacobi-Varietäten (ohne Beweise); [Ha], Th. IV.4.11 als weitere Interpretation des Gruppengesetzes
Literatur: [Si], III.3, [Ha], IV

Vortrag 6. Isogenien (29.11.12)
Isogenien; Multiplikation mit ganzen Zahlen; komplexe Multiplikation; Frobenius-Abbildungen; Zusammenhang mit der Galoistheorie der Funktionenkörper; Quotient einer elliptischen Kurve mit einer endlichen Untergruppe; kurzer Einschub über das invariante Differential; Konstruktion und Eigenschaften der dualen Isogenie
Literatur: [Si], III.4-6

Vortrag 7. Tate-Modul und Weil-Paarung (06.12.12)
Definition und Eigenschaften des Tate-Moduls einer elliptischen Kurve; Darstellung von Isogenien mittels Homomorphismen der Tate-Moduln; Weil-Paarung; kurzer Überblick (ggf. ohne Beweise) über die Strukturaussagen zum Endomorphismenring und zur Automorphismengruppe
Literatur: [Si], III.7-10

2 Elliptische Kurven über endlichen Körpern

Vortrag 8. Elliptische Funktionen über endlichen Körpern (13.12.12)
Beweis des Satzes von Hasse-Weil über rationale Punkte auf elliptischen Kurven über endlichen Körpern; Zeta-Funktionen von Varietäten über endlichen Körpern; Formulierung der Weil-Vermutungen; Beweis für elliptische Kurven
Literatur: [Si], V.1-2

3 Elliptische Kurven über Zahlkörpern

Vortrag 9. Das schwache Mordell-Weil-Theorem (20.12.12)
Formulierung von Mordell-Weil; Beweis des schwachen Mordell-Weil-Theorems (hierbei kann der Beweis von Prop. 1.6 durch die Bemerkung 1.7 ersetzt werden); abstrakte Höhenfunktionen und die Abstiegsmethode; Skizze des Beweises von Mordell-Weil über $\mathbb{Q}$
Literatur: [Si] VIII.1, VIII.3-4

Vortrag 10. Die Höhenfunktion im projektiven Raum (10.01.13)
Definition der Höhe eines Punktes in $\mathbb{P}^N$; Eigenschaften der Höhenfunktion (Verhalten der Höhe unter Körpererweiterungen, Morphismen und Galoiskonjugation); Endlichkeit der Menge der Punkte von beschränkter Höhe
Literatur: [Si], VIII.5

Vortrag 11. Der Satz von Mordell-Weil (17.01.13)
Höhenfunktion auf elliptischen Kurven; Beweis des Satzes von Mordell-Weil; wenn die Zeit reicht: Torsionspunkte auf elliptischen Kurven; Satz von Nagell-Lutz
Literatur: [Si], VIII.6-7

Vortrag 12. Der Rang einer elliptischen Kurve (24.01.13)
Rang einer elliptischen Kurve; numerische Berechenbarkeit; Beispiele; L-Reihe einer elliptischen Kurve, kurzer Überblick zur Birch-Swinnerton-Dyer-Vermutung
Literatur: [ST], IV.1, [Si] Anhang C.16

Bemerkungen zur Literatur: Der erste Teil des Seminars orientiert sich im Wesentlichen an [Si]. Zum Verständnis der Zusammenhänge aus der algebraischen Geometrie ist jedoch auch ein Blick in [Ha] oder ein entsprechendes Lehrbuch der algebraischen Geometrie zu empfehlen. Als ergänzende Literatur zu elliptischen Kurven seien an dieser Stelle noch [Hu] sowie das Vorlesungsskript [Le] angeführt. Das Buch [ST] gibt einen Beweis des Satzes von Mordell-Weil für $K = \mathbb{Q}$ und kann ebenfalls als ergänzende Literatur herangezogen werden. In den Vorträgen 9-11 werden gelegentlich Resultate aus der algebraischen Zahlentheorie verwendet, die sich bei Bedarf in der gängigen Literatur (etwa [Ne], [La]) nachlesen lassen.

Literatur

[Ha] Robin Hartshorne. *Algebraic Geometry.* Springer, 1977.

[Hu] Dale Husemöller. *Elliptic Curves.* Springer, 1987.

[La] Serge Lang. *Algebraic Number Theory, 2nd ed.* Springer, 1994.

[Le] Franz Lemmermeyer. *Elliptische Kurven I.* Vorlesungsskript.

[Ne] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[Si] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[ST] Joseph H. Silverman, John Tate. *Rational Points on Elliptic Curves.* Springer, 1992.