

Elliptische Kurven

PROGRAMM DES SEMINARS IM WS 2005/2006

27.10.05: VARIETÄTEN

- affine und projektive Varietäten; rationale Punkte und Definitionskörper; reguläre Funktionen; Körper der rationalen Funktionen; Morphismen; projektiver Abschluss; Dimension; Glattheit
- [S] I; [H] I.1 - I.5; [M] I.1 - I.5; sehr erhellend ist [M] I.7 zur Dimensionstheorie

03.11.05: KURVEN (I)

- Ordnung einer Funktion in einem Punkt einer Kurve; Polstellen; Fortsetzungsprinzip für projektive Kurven; Beziehung zwischen Kurven und Funktionenkörpern vom Transzendenzgrad 1; Verzweigung; Frobeniusabbildung
- [S] II.1 - II.2; [H] I.6; ein kurzer Abstecher zur Normalisierung wäre ganz schön, vgl. [M] III.8, insbes. Th.8.

10.11.05: KURVEN (II)

- Divisoren und Divisorenklassengruppe; Differentialformen auf Kurven und die kanonische Divisorenklasse; Aussage des Satzes von Riemann-Roch; Hurwitz-Formel
- [S] II.3 - II.5; für "vernünftige" Definition von Differentialformen vgl. [H] II.8 und - vor allem - [M] III.4 (beides zusammen mit [E] II.16!); für cohomologische Interpretation und Beweis des Riemann-Roch vgl. [H] IV.1; eine gute Referenz für einen nicht-cohomologischen Beweis ist [Se]

17.11.05: ELLIPTISCHE KURVEN: GRUPPENGESETZ UND WEIERSTRASSGLEICHUNGEN

- Diskriminante, j -Invariante und invariantes Differential einer Weierstraßgleichung; Gruppengesetz auf einer glatten Weierstraßkurve; der singuläre Fall; abstrakte Definition einer elliptischen Kurve; die Weierstraß-Form einer solchen und das Gruppengesetz (mittels Riemann-Roch!)
- [S] III.1 - III.3; dieses Material ist auch gut in den ersten Abschnitten von [H] IV.4 dargestellt; dort findet man auch die Interpretation des Gruppengesetzes, daß eine elliptische Kurve ihre eigene Jacobi-Varietät ist

24.11.05: ISOGENIEN

- Isogenien; Bsp.: Multiplikationsabbildungen $[m]$, Frobenii; Beziehung zur Galoistheorie der Funktionenkörper; Quotient elliptischer Kurven durch eine endliche Untergruppe; Konstruktion und Eigenschaften der dualen Isogenie (hierzu Einschub über das invariante Differential)
- [S] III.4 - III.6

01.12.05: TATEMODUL; ENDOMORPHISMEN ELLIPTISCHER KURVEN

- Definition und grundlegende Eigenschaften des Tatemoduls; kurze(!) Diskussion der Weil-Paarung; Klassifikationssätze für Endomorphismenring und Automorphismengruppe einer elliptischen Kurve
- [S] III.7 - III.10

08.12.05: FORMALE GRUPPEN

- allg. Definition, formale Gruppen über lokalen Ringen vs. Gruppenstrukturen, Differentiale auf formalen Gruppen, *log* und *exp*, formale Gruppe einer elliptischen Kurve
- [S] IV.1 - IV.6

15.12.05: ELLIPTISCHE KURVEN ÜBER ENDLICHEN KÖRPERN

- Anzahlformel der rationalen Punkte über einem endlichen Körper; Weil-Vermutung für elliptische Kurven; nach Belieben kurze Diskussion der Hasse-Invariante (Supersingularität)
- [S] VI, vor allem VI.1 und VI.2

12.01.06: ELLIPTISCHE KURVEN ÜBER LOKALEN KÖRPERN

- minimale Weierstraßgleichungen; Reduktion (gut und schlecht); Punkte endlicher Ordnung
- [S] VII, vor allem VII.1 - VII.4

19.01.06: DAS MORDELL-WEIL-THEOREM

- Aussage von Mordell-Weil; Formulierung und Beweis des schwachen Mordell-Weil-Theorems (hier sollte man anstelle von Proposition 1.6 auf den Satz von Minkowski verweisen, wie in Remark 1.7 beschrieben); Axiomatik von Höhenfunktionen; Skizze der Vorgehensweise für elliptische Kurven über \mathbb{Q}
- [S] VIII.1, VIII.3 - VIII.4

26.01.06: HÖHENFUNKTIONEN AUF ELLIPTISCHEN KURVEN

- allgem. Konstruktion der Höhenfunktionen auf elliptischen Kurven und Fertigstellung des Beweises von Mordell-Weil
- [S] VIII.5 - VIII.6

Literatur:

[E] Eisenbud, D. *Commutative Algebra*

[H] Hartshorne, R. *Algebraic Geometry*

[M] Mumford, D. *The Red Book of Varieties and Schemes*

[S] Silverman, J. H. *The Arithmetic of Elliptic Curves*

[Se] Serre, J.-P. *Groupes Algébriques et Corps de Classes*