Elliptische Kurven – Sommersemester 2005

KAPITEL I: ELLIPTISCHE KURVEN IM KOMPLEXEN

§1: Voraussetzungen aus der Funktionentheorie

Meromorphe Funktionen, Laurent-Entwicklung, Residuensatz, Maximumprinzip

§2: Doppeltperiodische Funktionen

Holomorphe sind konstant, für meromorphe ist die Residuensumme im Periodenparallelogramm Null, Summe der Nullstellen und Pole einer doppeltperiodischen Funktion im Periodenparallelogramm ist ein Gitterpunkt

§3: Die WEIERSTRASSsche $\wp$-Funktion

Konvergenz, Ableitung, Körper der elliptischen Funktionen zu einem Gitter ist $\mathbb{C}(\wp, \wp')$, LAURENT-Reihe der $\wp$-Funktion, EISENSTEIN-Reihen, Differentialgleichung

§4: Die Gruppenstruktur auf der kubischen Kurve

Einbettung des Torus $\mathbb{C}/\Lambda$ in die projektive Ebene, WEIERSTRASS-Gleichung, Diskriminante, Nichtsingularität der Bildkurve, Kollinearität der Bilder von z_1, z_2 und $z_1 + z_2$ und Additionsformel für die $\wp$-Funktion

§5: Affine und Projektive Varietäten

Affine und projektive Räume, homogene und inhomogene Polynome, reguläre und rationale Abbildungen, Singularitäten, Normalformen für kubische Kurven

§6: Elliptische Modulfunktionen

Ähnlichkeit von Gittern, SL_2-Operation auf der oberen Halbebene, automorphe Formen und ihr Gewicht, Erzeugung durch g_2 und g_3

§7: Die j-Funktion

Bijektivität der Abbildung $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}$, Existenz von Gittern zu kubischen WEIERSTRASS-Gleichungen, jede nichtsinguläre kubische Kurve in $\mathbb{P}^2(\mathbb{C})$ ist ein Torus.

Literatur: Der Stoff von §1 ist in jedem Lehrbuch der Funktionentheorie zu finden.
§§2–4, 6, 7 folgen im wesentlichen LANG, Kapitel 1–3. für §5 kann man Lehrbücher der algebraischen Geometrie konsultieren, z.B. ŠAFAREVIČ, Kap. 1, §§1–4.

SERGE LANG: Elliptic Functions, *Addison Wesley,* 1973

IGOR R. SCHAFAREWITSCH: Grundzüge der algebraischen Geometrie, *Vieweg,* 1972

IGOR R. SHAFAREVICH: Basic Algebraic Geometry, *Springer,* 1971, [2]1974

KAPITEL II: ELLIPTISCHE KURVEN ALS ABELSCHE VARIETÄTEN

§1: LEFSCHETZ-Prinzip und Reduktion modulo p

Allgemeines LEFSCHETZ-Prinzip, Anwendung auf das Assoziativgesetz in char 0, Reduktion und Liftung von Varietäten, Assoziativgesetz für Kurven über endlichen Körpern

§2: Punkte endlicher Ordnung

Die Gruppe $E[m]$ über $\mathbb{C}$, Hinweis auf LUTZ-NAGELL und MAZUR, Punkte der Ordnung zwei = Verzweigungspunkte, Punkte der Ordnung drei = Wendepunkte, Wendepunktkonfiguration, Situation über $\mathbb{R}$, n-Teilungspolynome

§3: Isogenien und Endomorphismen

Koordinatenring, Funktionenkörper, Grad einer Isogenie,

§4: Divisoren

Divisoren, Hauptdivisoren, (lineare) Äquivalenz, Divisorenklassen, JACOBISCHE, Jac($\mathbb{P}^1$) ist trivial, Jac(E) $\cong E$ für elliptische Kurven, die Abbildungen φ^* und φ_* zu $\varphi\colon E_1 \to E_2$, Morphismen, die O festlassen sind Gruppenhomomorphismen

§4a: Anhang: Funktionenkörper einer Veränderlichen

Funktionenkörper, Bewertungen, Bewertungsringe, Satz von RIEMANN-ROCH, Geschlecht eines Funktionenkörpers, Funktionenkörper vom Geschlecht null und eins, Hauptkurve eines Funktionenkörpers, Körpererweiterungen und Morphismen von Kurven, Grad eines Morphismus, Verzweigungsindex und Restklassengrad, $\sum e_i f_i = n$

§5 Morphismen zwischen elliptischen Kurven

Isogenien mit vorgegebenem Kern, Morphismen sind surjektiv oder konstant, im separablen Fall ist der Grad gleich der Ordnung des Kerns

§6 Die WEIL-Paarung

Eigenschaften, Konstruktion, Nachweis der Eigenschaften, Interpretation des Grads eines Morphismus als Determinante einer 2×2-Matrix

§7 Der Satz von HASSE

Punkte in $E(\mathbb{F}_q)$ liegen im Kern von FROBENIUS – Identität, Abschätzung des Grads dieser Abbildung, $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$

Literatur: SILVERMAN, Kap. II, III, V, VI; WASHINGTON, Kap. 2, 3, 4.1+2; zu §4a eventuell auch STICHTENOTH, Kap. I und Abschnitt III.1

JOSEPH H. SILVERMAN: The Arithmetic of Elliptic Curves, *Springer,* 1986

HENNING STICHTENOTH: Algebraic Function Fields and Codes, *Springer,* 1993

LAWRENCE C. WASHINGTON: Elliptic Curves – Number Theory and Cryptography, *Chapman & Hall/CRC,* 2003