

Seminar über elliptische Kurven

Dienstags 14-16h, Seminarraum 0.003

Vorbesprechung: Donnerstag 18.7.2013, 15h, Raum N 0.003

ERSTER TEIL: KOMPLEXE THEORIE

Der erste Teil des Seminars behandelt die Theorie von 1-dimensionalen komplexen Tori. Eine gute Übersicht über das Thema liefert der Abschnitt über elliptische Funktionen im Buch von Hartshorne [Har, p. 326 ff.]. Insbesondere ist dieser Abschnitt (im Gegensatz zur dort benutzten Referenz [HC]) in moderner Sprache formuliert.

1) Komplexe Mannigfaltigkeiten und komplexe Liegruppen

Definition einer komplexen Mannigfaltigkeit [Huy, 2.1], [FG, IV, 1]. Abbildungen zwischen komplexen Mannigfaltigkeiten. Produkte. Holomorphe Funktionen. Globale holomorphe Funktionen auf kompakten komplexen Mannigfaltigkeiten sind konstant [Huy, Prop. 2.1.5] (wir brauchen eigentlich nur den Fall einer 1-dimensionalen Mannigfaltigkeit).

Beispiele, insbesondere projektiver Raum und Hyperflächen, siehe z.B. [Huy, p.56, 57]. Quotienten nach Gruppenoperationen [Huy, Prop. 2.1.13] (wir brauchen nur den Fall einer diskreten Gruppe).

Tangentenraum einer komplexen Mannigfaltigkeit [FG, p.164 ff.], siehe auch [Huy, Def, 2.2.14].

Definition einer komplexen Liegruppe [FG, IV,2. p.171 f.], siehe auch [God] (Vorsicht: Im Buch von Godement werden sowohl reelle als auch komplexe Liegruppen behandelt, wir interessieren uns aber nur für den komplexen Fall). Beispiel komplexer Torus.

Liealgebra einer Liegruppe [God, 5.7]. Einparameter-Untergruppen und Exponentialabbildung [God, 6.1]. Elementare Eigenschaften und Regularität [God, 6.2, 6.3 Thm. 3].

2) Eindimensionale komplexe Tori

Definition einer elliptischen Kurve als eindimensionale kompakte komplexe Liegruppe [Mum, 1] (wir interessieren uns nur für den eindimensionalen Fall). Elliptische Kurven sind kommutativ [Mum, 1, (1)].

Jede elliptische Kurve ist ein komplexer Torus [Mum, 1, (2)]. Surjektivität der Multiplikation mit n [Mum, 1, (3)].

Die Weierstraßsche φ -Funktion, ihre Ableitung [HC, II, 1, §6] und ihre Funktionalgleichung [HC, II, 1, §7, Satz 3].

Weierstraßgleichung [Har, Thm. 4.12 B] und Isomorphismus

$$\varphi : \mathbb{C}/\Lambda \cong X = \{(x, y) \mid y^2 = 4x^3 - g_2x - g_3\} \subset \mathbb{P}^2.$$

Siehe dazu auch [HC, II, 5, §1].

Jede (nichtsinguläre) Weierstraßgleichung definiert eine elliptische Kurve [Har, Thm. 4.14 B], [HC, II, 4, §4] (der fehlende Teil, dass $\Delta \neq 0$ äquivalent zur Glattheit der Hyperfläche X ist, muss selber erbracht werden).

Ohne Beweis: Geschlecht einer Riemannschen Fläche/Topologische Klassifikation von Flächen. Charakterisierung einer elliptischen Kurve als kompakte Riemannsche Fläche vom Geschlecht 1 mit ausgezeichnetem Punkt.

3) Parametrisierung und Endomorphismenring

Parametrisierung von elliptischen Kurven durch die obere Halbebene. Operation von $SL_2(\mathbb{Z})$ auf der oberen Halbebene. Fundamentalbereich und Stabilisatoren [Ser, VII, §1].

Parametrisierung via j -Invariante. Zusammenhang zur ersten Parametrisierung, [Har, Thm 4.15 B], [HC, II, 4, §3].

Komplexe Multiplikation und Endomorphismenring einer elliptischen Kurve [Har, Prop. 4.18, Thm. 4.19].

Wenn es die Zeit erlaubt, kann man noch darauf eingehen, dass es keine *universelle* elliptische Kurve über dem affinen Raum gibt, der durch die j -Invariante definiert wird [Har, Exc. 4.22].

ZWEITER TEIL: ALGEBRAISCHE THEORIE

Für die algebraische Theorie folgen wir im wesentlichen dem Buch von Silverman [Sil]. Auch in diesem Teil gilt, dass wir versuchen wollen die modernere Sprache wie z.B. in [Har] zu benutzen. An einigen Stellen müssen einige Sätze ohne Beweis benutzt werden, die im Laufe der Vorlesung über algebraische Geometrie bewiesen werden.

4) Elliptische Kurven

Kurze Erinnerung an algebraische Kurven. Glattheit algebraischer Kurven [Sil, II, §1]. Abbildung zwischen Kurven [Sil, II, §2]. Grad einer Abbildung, Verzweigungsindizes. Faktorisierung in einen separablen Anteil und eine Potenz des Frobenius [Sil, II, Cor. 2.12]

Definition einer elliptischen Kurve via Weierstraßgleichung [Sil, III, §1] (ohne das invariante Differential). Glattheit, Degenerationen und j -Invariante [Sil, III, Prop. 1.4]. Legendreform [Sil, Iii, Prop. 1.7].

5) Divisoren und Differentiale

Divisoren und Divisorenklassengruppe [Sil, II, §3], siehe auch [Har, II, 6] (wir brauchen den Teil über Weil-divisoren).

Hauptdivisoren (und Zusammenhang mit Null- und Polstellen der zugehörigen Abbildung $X \rightarrow \mathbb{P}^1$) [Sil, p. 32, Definition, Prop. 3.1]. Hauptdivisoren haben Grad 0 [Har, II, Cor. 6.10].

Induzierte Abbildungen auf Divisoren [Sil, II, Prop. 3.6], [Har, p. 137].

Differentiale und Divisor eines Differentials. Kanonischer Divisor. [Sil, II, §4], siehe auch [Har, II, 8 p. 172 ff.]. Vorsicht: Bei Silverman werden meromorphe Differentials definiert.

Kriterium für Separabilität mittels Differential [Sil, II, Prop. 4.2 (c)].

6) Elliptische Kurven als Kurven vom Geschlecht 1

Das zu einem Divisor assoziierte Geradenbündel [Har, II, Definition, Prop. 6.13]. Siehe auch [Sil, II, p. 38 Definition].

Ohne Beweis: Riemann-Roch auf glatten Kurven. [Har, IV Thm. 1.3], [Sil, II, Thm

5.4].

Geschlecht einer Kurve, Grad des kanonischen Divisors [Sil, II, Cor. 5.5]

Charakterisierung einer elliptischen Kurve als glatte projektive Kurve vom Geschlecht 1: Jede glatte projektive Kurve vom Geschlecht 1 zusammen mit einem ausgezeichneten k -rationalen Punkt erfüllt eine Weierstraßgleichung [Sil, III Prop. 3.1].

Definition des invarianten Differentials aus der Weierstraßgleichung [Sil, p. 46, 48]. Verschwinden des zugehörigen Divisors [Sil, II, Prop 1.5]. Eine elliptische Kurve hat Geschlecht 1.

7) Das Gruppengesetz auf elliptischen Kurven

Der Satz von Bezout [Har, I, Cor. 7.8] (Eventuell nur für den Fall, dass eine der Kurven eine Gerade ist).

Geometrisches Gruppengesetz auf elliptischen Kurven [Sil, III, §2] (ohne den Teil über das Gruppengesetz auf dem glatten Teil einer singulären Weierstraßgleichung), [Sil, III, Thm. 3.6].

Der Isomorphismus $E(k) \cong \text{Div}^0(E)$ [Sil, III, Prop. 3.4].

Charakterisierung einer elliptischen Kurve als glatte projektive Kurve mit Gruppenstruktur: Eine glatte Kurve mit Gruppengesetz hat trivialen kanonischen Divisor, i.e. bis auf Multiplikation mit Elementen von k^\times gibt es genau ein holomorphes Differential.

Verhalten von Differentialen unter Pullback mittels der Gruppenstruktur: Beschreibe

$$m^* : \Gamma(E, \Omega_{E,K}) \rightarrow \Gamma(E \times E, \Omega_{E \times E/k}) \cong \Gamma(E, \Omega_{E,K}) \oplus \Gamma(E, \Omega_{E,K}),$$

wobei $m : E \times E \rightarrow E$ die Gruppenaddition ist.

8) Isogenien

Definition einer Isogenie. Die Isogenie $[n]$. [Sil, III, §4]. Die Gruppe $\text{Hom}(E, E')$ ist torsionsfrei [Sil, III, Prop. 4.2].

Komplexe Multiplikation [Sil, III, Expl. 4.4]. (Relativer) Frobenius [Sil, III, Expl. 4.6].

Isogenien sind Gruppenhomomorphismen [Sil, III, Thm. 4.8], [Har, IV Lemma 4.9].

Grad und Kern einer Isogenie, Eigenschaften [Sil, III, Thm. 4.10].

Isogenien und das invariante Differential [Sil, III, Thm. 5.2, Cor. 5.3, Cor. 5.4].

(Den Beweis von Thm. 5.2 ersetzen wir durch ein besseres Argument. Da wir schon wissen, wie sich das Differential unter Pullback mit der Gruppenstruktur verhält, muss man noch berechnen, wie sich Differentiale unter Einschränken auf die Diagonale verhalten.)

9) Duale elliptische Kurve und duale Isogenie

Definition der Jacobischen einer Kurve [Har, IV, 4, p. 323 ff.]. Autodualität von elliptischen Kurven [Har, IV, Thm.4.11] (die Aussage über Kohomologie und Basiswechsel darf ohne Beweis verwendet werden).

Definition der dualen Isogenie. Eigenschaften [Sil, III, Thm. 6.1, Thm. 6.2].

Hier wollen wir wieder bessere Beweise geben. Wir definieren die duale Isogenie funktoriell auf der Jacobischen. Die meisten Aussagen über die duale Isogenie folgen dann relativ formal. Schwierig ist nur die Aussage $(\varphi + \psi)^* = \varphi^* + \psi^*$. Dafür

muss man sich überlegen wie sich Geradenbündel unter Pullback mit der Gruppenaddition verhalten:

$$m^* \mathcal{L} \cong \text{pr}_1^* \mathcal{L} \otimes \text{pr}_2^* \mathcal{L},$$

wobei $m : E \times E \rightarrow E$ die Multiplikation ist und pr_i die Projektion auf den i -ten Faktor.

DRITTER TEIL: ARITHMETISCHE ASPEKTE

Im letzten Teil des Seminars wollen wir auf ein paar arithmetische Fragestellungen im Zusammenhang mit elliptischen Kurven eingehen.

10) Der Tatemodul einer elliptischen Kurve

Struktur der m -Torsion einer elliptischen Kurve [Sil, III, Cor. 6.4]. Operation der Galoisgruppe auf der m -Torsion [Sil, III, §7 p. 90].

Definition des Tatemoduls und der Galoisdarstellung ρ_ℓ [Sil, III, §7]. Tatemodule der multiplikativen Gruppe [Sil, III, Rem. 7.3].

Grad einer Isogenie, der Grad ist quadratische Form auf $\text{Hom}(E, E')$ [Sil, III, Cor. 6.3].

Einbettung der Isogenien $E \rightarrow E'$ in die Abbildungen auf dem Tatemodul [Sil, III, Thm. 7.4].

Ohne Beweis: Elliptische Kurven über endlichen Körpern oder Zahlkörpern sind isogen, falls ihre Tatemoduln isomorph sind [Sil, III, Thm. 7.7].

11) Weilpaarung und Endomorphismenring

Definition der Weilpaarung auf der m -Torsion.

Eigenschaften der Weilpaarung (hier sollen die Eigenschaften aus [Sil, III, Prop. 8.1, Prop. 8.2, Prop. 8.3] aus der funktoriellen Definition hergeleitet werden.)

Explizite Beschreibung mittels Divisoren [Sil, III, §8].

Die Weilpaarung auf dem Tatemodul.

Der Endomorphismenring einer elliptischen Kurve [Sil, III, Thm. 9.3, Cor. 9.4].

12) Elliptische Kurven in positiver Charakteristik

Der Endomorphismenring einer elliptischen Kurve in Charakteristik p [Sil, V, Thm. 3.1] (ohne die Aussagen über die formale Gruppe).

Beispiel einer supersingulären elliptischen Kurve.

Der Satz von Hasse [Sil, V, Thm. 1.1].

Je nachdem wieviel Zeit verbleibt: Zetafunktion und Weilvermutung [Sil, V, §2], [Har, Appendix C, 1,2]. Die Weilvermutung für elliptische Kurven über endlichen Körpern [Sil, V, Prop. 2.3, Thm. 2.4].

LITERATUR

- [FG] K. Fritsche, H. Grauert, *From holomorphic functions to complex manifolds*, Graduate Texts in Mathematics, Springer.
- [God] R. Godement, *Intoduction a la theorie des groupes de Lie*, Springer.
- [Har] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer.
- [HC] A. Hurwitz, R. Courant, *Vorlesungen über allgemeine Funktionentheorie und elliptische Funktionen*, *Geometrische Funktionentheorie*, Springer.
- [Huy] D. Huybrechts, *Complex Geometry, an introduction*, Springer.
- [Mum] D. Mumford, *Abelian Varieties*, Oxford University Press.
- [Ser] J.-P. Serre, *A course in Arithmetic*, Springer.
- [Sil] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer.