Seminar zu Elliptischen Kurven

Dozenten: Prof. Dr. Böckle und Dr. Ludwig
Wintersemester 20/21

Formalitäten

Bitte erstellen Sie begleitend zu Ihrem Vortrag ein Handout für die Seminarteilnehmer. Dieses Dokument sollte die wichtigsten Definitionen und Resultate aus ihrem Vortrag beinhalten. Gerne können Sie dort auch Details von Rechnungen und Beispielen erklären, für die im Vortrag keine Zeit bleibt. Denken Sie sich außerdem ein Quiz mit drei Fragen zu Ihrem Vortrag für die anderen Teilnehmer aus. Jeder Vortrag sollte mindestens ein Beispiel enthalten.

Beginnen Sie rechtzeitig (ca. 4 Wochen vorher) mit der Vorbereitung Ihres Vortrages. Kommen Sie zwei Wochen vor Ihrem Vortrag zur einer Vorbesprechung. Der Termin zur Vorbesprechung ist dann am entsprechenden Dienstag um 9:30 Uhr. Bringen Sie einen Entwurf des Handouts zur Vorbesprechung mit.

Bitte schicken Sie das fertige Handout sowie die Quizfragen spätestens am Montag Vormittag vor Ihrem Vortrag per Email an Frau Ludwig, damit die Materialien den anderen Seminarteilnehmern vorab zu Verfügung gestellt werden können.

Vorträge

1. Grundlagen der Algebraischen Geometrie

1) Algebraische Varietäten (03.11.)
Referenz: [Si] Kapitel I.
Definieren und erklären Sie folgende Begriffe: Affine und projektive Varietäten, rationale Punkte, Dimension, glatte Varietäten, Morphismen von Varietäten. Illustrieren Sie die Konzepte an Beispielen.

2) Algebraische Kurven (10.11.)
Referenz: [Si] Abschnitte II.1 und II.2.
Definieren Sie den Begriff einer Kurve. Erklären Sie das Konzept der Ordnung einer

Funktion in einem Punkt einer Kurve, sowie Polstellen und den Begriff des Funktionenkörpers. Erklären Sie die wichtigsten Resultate zu Morphismen von Kurven (2.1, 2.3, 2.4), und definieren Sie den Grad einer Abbildung sowie den Verzweigungsindex. Erklären Sie, wie die beiden zusammenhängen. Diskutieren Sie die Frobeniusabbildung.

3) Der Satz von Riemann–Roch (17.11.)
Referenz: [Si] Abschnitte II.3–II.5.
Erklären Sie das Konzept der Divisoren und ihre wichtigsten Eigenschaften (3.1, 3.6). Definieren Sie Differentialformen und die kanonische Divisorenklasse. Erklären Sie, was effektive Divisoren sind und definieren Sie die Größe $l(D)$ (s. Definition vor 5.2) und einige Eigenschaften (5.2). Erklären Sie nun nach diesen Vorbereitungen den Satz von Riemann–Roch (5.4) sowie die Hurwitz–Formel (5.9). Wenden Sie die Sätze auf Beispiele an.

2. Elliptische Kurven über algebraisch abgeschlossenen Körpern

4) Weierstraß Gleichungen und das Gruppengesetz (24.11.)
Referenz: [Si] Abschnitte III.1 und III.2.
Erklären Sie die Weierstraß-Gleichungen und die Umformungen in die einfache Form $y^2 = x^3 + ax + b$ über Körpern deren Charakteristik von 2 und 3 verschieden ist. Definieren Sie die Diskriminante und die j-Invariante. Beweisen Sie Proposition 1.4. Diskutieren sie kurz die Legendre Form. Erklären Sie dann die Gruppenoperation und beweisen Sie, dass die Punkte einer elliptischen Kurve eine abelsche Gruppe bilden. Berechnen Sie Beispiele.[1]

5) Elliptische Kurven (01.12.)
Referenz: [Si] Abschnitt III.3.
Definieren Sie den Begriff einer elliptischen Kurve. Zeigen Sie, dass jede elliptische Kurve eine Weierstraß-Gleichung besitzt (3.1). Studieren Sie Divisoren auf elliptischen Kurven und beweisen Sie Proposition 3.4. Beweisen Sie Theorem 3.6, also dass die Gruppenoperationen auf einer elliptischen Kurve Morphismen definieren.

6) Isogenien (08.12.)
Referenz: [Si] Abschnitte III.4-III.6.
Definieren und erklären Sie den Begriff einer Isogenie sowie deren Grad. Diskutieren

[1] Die Anwendung Elliptic Curve Plotter ist hilfreich für Visualisierungen.

Sie Multiplikation mit ganzen Zahlen auf elliptischen Kurven, komplexe Multiplikation und Frobenius-Abbildungen. Beweisen Sie Theorem 4.8. Erklären Sie den Zusammenhang von Isogenien und der Galoistheorie der Funktionenkörper (Theorem III.4.10). Zeigen Sie, dass der Quotient einer elliptischen Kurve nach einer endlichen Untergruppe wieder eine elliptische Kurve ist (4.12). Diskutieren Sie schließlich das invariante Differential sowie Konstruktion und Eigenschaften der dualen Isogenie.

7) Der Tate-Modul und die Weil-Paarung (15.12.)
Referenz: [Si] Abschnitte III.7-III.10.
Geben Sie die Definition und Eigenschaften des Tate-Moduls einer elliptischen Kurve. Erklären Sie wie der Tate-Modul mit Isogenien zusammenhängt (Theorem 7.4). Erklären Sie ohne Beweis das Isogenie-Theorem 7.7 und Theorem 7.9. Konstruieren Sie die Weil-Paarung (III.8). Geben Sie einen kurzen Überblick (ohne Beweise) über die Strukturaussagen zum Endomorphismenring (Korollar 9.4). Erklären Sie wie die Automorphismengruppe einer elliptischen Kurve aussieht (Theorem 10.1).

3. Elliptische Kurven über endlichen Körpern

8) Elliptische Kurven über endlichen Körpern (12.01.)
Referenz: [Si] Kapitel V.
Beweisen Sie den Satz von Hasse-Weil über rationale Punkte auf elliptischen Kurven über endlichen Körpern (Theorem 1.1). Definieren Sie die Zeta-Funktion einer Varietät über einem endlichen Körper und formulieren Sie die Weil-Vermutungen. Beweisen Sie diese für elliptische Kurven. Definieren Sie den Begriff einer supersingulären und einer gewöhnlichen elliptischen Kurve und geben Sie einen Überblick über die Resultate aus V.4 (ohne Beweise).

4. Elliptische Kurven über $\mathbb{C}$

9) Elliptische Kurven über $\mathbb{C}$ (19.01.)
Referenz: [Si] Kapitel VI.
Ziel des Vortrags ist es den Uniformisierungssatz (Theorem 5.1, Korollar 5.1.1 und Theorem 5.3), also insbesondere die Beschreibung von elliptischen Kurven über $\mathbb{C}$ durch Gitter $\Lambda \subset \mathbb{C}$ zu erklären. Bereiten Sie dieses Theorem vor, indem Sie zunächst elliptische Integrale und anschließend elliptische Funktionen, sowie deren Konstruktion, erklären. Formulieren Sie dann die Hauptresultate. Beweisen Sie anschließend Proposition 5.4, sowie Theorem 5.5.

5. Elliptische Kurven über lokalen Körpern

10) Elliptische Kurven über lokalen Körpern (26.01.)
Referenz: [Si] Kapitel VII.
Erklären Sie das Konzept einer minimalen Weierstraß-Gleichung und der Reduktion modulo eines uniformisierenden Elementes. Diskutieren Sie die kurze exakte Sequenz aus Proposition 2.1. Erklären Sie Proposition 3.1, sowie die Anwendung 3.2 und geben Sie ein Beispiel. Beweisen Sie Proposition 4.1. Studieren Sie nun die verschiedene Reduktionstypen von elliptischen Kurven (Propositionen 5.1, 5.4 und 5.5.). Formulieren Sie das Kriterium von Néron–Ogg–Shafarevich (Theorem 7.1) und beweisen Sie die Korollare 7.2 und 7.3. (Resultate aus Kapitel IV dürfen ohne Beweise verwendet werden.)

6. Elliptische Kurven über $\mathbb{Q}$

11) Das schwache Mordell–Weil Theorem (02.02.)
Referenz: [Si] Abschnitte VIII.1–VIII.2.
Formulieren Sie den Satz von Mordell–Weil. Formulieren und beweisen Sie das schwache Mordell–Weil Theorem.

12) Das Mordell-Weil Theorem über $\mathbb{Q}$ (09.02.)
Referenz: [Si] Abschnitt VIII.4.
Beweisen Sie den Satz von Mordell-Weil über $\mathbb{Q}$ (VIII.4.1). Diskutieren Sie zum Abschluss des Seminars Resultate bzgl. Torsionspunkte aus III.7 (ohne Beweise) und Vermutungen aus III.10.

Literatur

[Si] Silverman, Joseph H., *The Arithmetic of Elliptic Curves*, Springer Graduate Texts in Mathematics (106), 2nd Edition, 2010.