Prof. Otmar Venjakob
Dr. Andreas Riedel

Seminar

Rationale Punkte auf Quadriken und elliptischen Kurven

Wintersemester 2014/15

Ort: HS 4 **Zeit**: 14 Uhr c.t. **Begin**: 16.10.2014

Vortragsliste zum Seminar: Im folgenden beziehen sich alle Angaben (bis auf bei Vortrag 7) auf das Buch [1]. Eventuell werden wir Vorträge 6 und 7 weglassen (d.h. das quadratische Reziprozitätgesetz als "Black-Box" benutzen), falls sich nicht genügend Vortragende finden.

1. Elliptische Kurven (S. 18-24): Definition elliptischer Kurven; Beispiele über $\mathbb{R}$; Lemma 1.3: Beweis durch Lemma 1.4 und Lemma 1.5; Definition der Höhe; Beweis von Proposition 1.2; Lemma 1.7 nur im Fall $k = 2$.

2. Gruppenstruktur auf $E(\mathbb{Q})$ (S. 25-30): Definition der Menge der rationalen Punkte $E(K)$; Gruppenstruktur auf $E(\mathbb{Q})$; Projektive Ebene, Bedeuting des neutralen Elements; Beispiele; Fermat's Methode mit Referenz zum 1. Vortrag.

3. Satz von Mordell I (S. 30-34): $E(\mathbb{Q})$ ist e.e. abelsche Gruppe: Beweis von Proposition 1.13; Beweis von (I) durch Beweis von Proposition 1.14 (1), (2) und (3); Bemerkung 1.6.

4. Satz von Mordell II (S. 35-36, 40-42): Beweis von (IIB)(1); Beweis von Lemma 1.16.

5. Satz von Mordell III (S. 36-40): Beweis von (IIB)(2); Beweis von Lemma 1.17 und Lemma 1.18.

6. Quadriken (S. 45-51): Definition/Wiederholung Quadriken; Rationale Punkte auf $ax^2 + by^2 = c$; Kongruenzen; Proposition 2.1; Struktur von $\mathbb{F}_p^\times$.

7. Quadratisches Reziprozitätsgesetz: Beweis des "goldenen Theorems" (eine passende Referenz wird noch hinzugefügt).

8. Das Hilbert-Symbol (S. 53-57): Definition des Hilbert-Symbols; Definition von $\mathbb{Z}_{(p)}$, Produktformel für das Hilbert-Symbol; Beispiele.

9. p-adische Zahlen (S. 58-65): Definition von $\mathbb{Z}_p$, Bewertungen, Metriken, $\mathbb{Q}_p$ als Vervollständigung von $\mathbb{Q}$ bzgl. der p-adischen Bewertung.

10. Alternative Beschreibung von $\mathbb{Q}_p$ (S. 65-69): Definition des inversen Limes, $\mathbb{Q}_p$ via der Reihendarstellung.

11. Struktur von $\mathbb{Q}_p$ (S. 69-74): Definition der Exponential- und Logarithmusfunktion auf $\mathbb{Q}_p$; Struktur von $\mathbb{Q}_p^\times$; Quadrate in $\mathbb{Q}_p$.

12. Rationale Punkte auf Quadriken (S. 74-77): Das Hasse-Prinzip (auch Lokal/Global-Prinzip genannt); Beweis über die Existenz von rationalen Punkten auf Quadriken via p-adische Zahlen.

(bitte wenden)

Kontakt:
Andreas Riedel
INF 288, Zimmer 104c
email: ariedel@mathi.uni-heidelberg.de

Literatur: [1] K. Kato, N. Kurokawa, T. Saito, *Number Theory 1, Fermat's Dream*, 1996,
[2] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, 1992,
[3] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, 2007.