ulm university universität
uulm

Prof. Dr. Irene Bouw
Christian Steck
Sommersemester 2014

# Übungsblatt 9

**Elliptische Kurven**

Die Besprechung erfolgt am Mittwoch, dem 16.7.2014,
um 12:00 Uhr in He18 - E60.

**Aufgabe 1** (*Einführung in die l-adischen ganzen Zahlen*) (2+2+1+2+3)
Es sei $K$ separabel und $l \neq \operatorname{char} K$ eine Primzahl. In der Vorlesung wurde $\mathbb{Z}_l(1)$ definiert als der projektive Limes $\varprojlim_n \mu_{l^n}(\overline{K})$. Man hat Gruppenisomorphismen $\mu_{l^n}(\overline{K}) \to \mathbb{Z}/l^n\mathbb{Z}$ durch $\zeta_{l^n}^i \mapsto i$, wobei $\zeta_{l^n}$ ein kompatibles System von Einheitswurzeln ist, d.h. es gilt $\zeta_{l^{n+1}}^l = \zeta_{l^n}$. Man hat also ein Diagramm der folgenden Form:

$$\begin{array}{ccc} \mu_{l^{n+1}} & \longrightarrow & \mathbb{Z}/l^{n+1}\mathbb{Z} \\ \downarrow{\scriptstyle (\cdot)^l} & & \downarrow{\scriptstyle \varphi} \\ \mu_{l^n} & \longrightarrow & \mathbb{Z}/l^n\mathbb{Z} \end{array}$$

(a) Zeigen Sie, dass die Abbildung $\varphi$ die kanonische Reduktion ist.

Dadurch lässt sich nun auch der projektive Limes $\mathbb{Z}_l \coloneqq \varprojlim_n \mathbb{Z}/l^n\mathbb{Z}$ bilden und man kann zeigen, dass dieser Limes gegeben ist durch die Menge

$$\mathbb{Z}_l \coloneqq \left\{ (x_k)_{k\in\mathbb{N}} \in \prod_{k=0}^{\infty} \mathbb{Z}/l^{k+1}\mathbb{Z} \;;\; x_{k+1} \equiv x_k \pmod{p^{k+1}} \right\},$$

welche mit komponentenweiser Addition und Multiplikation ein Integritätsring ist. Für die restlichen Aufgaben dürfen Sie dies als Definition von $\mathbb{Z}_l$ verwenden. Zeigen Sie:

(b) Jedes Element $x = (x_k)_{k\in\mathbb{N}} \in \mathbb{Z}_l$ lässt sich als eine formale Potenzreihe in $l$ schreiben: $x = \sum_{k=0}^{\infty} a_k l^k$ mit Koeffizienten $a_k \in \{0, \ldots, l-1\}$.

(c) Die Abbildung $\varepsilon_l : \mathbb{Z} \to \mathbb{Z}_l$, $x \mapsto (\overline{x})_{k\in\mathbb{N}} = (\overline{x}, \overline{x}, \overline{x}, \ldots)$ ist injektiv.

(d) Es ist $\mathbb{Z}_l^\times = \mathbb{Z}_l \backslash l\mathbb{Z}_l$, d.h. $x = \sum_{k=0}^{\infty} a_k l^k$ ist genau dann invertierbar, wenn $a_0 \neq 0$.

(e) Zeigen Sie, dass $\frac{1}{2}$, $\frac{5}{3}$ und $\frac{5}{6}$ Elemente in $\mathbb{Z}_7$ sind und berechnen Sie jeweils die ersten drei Koeffizienten $a_0$, $a_1$ und $a_2$.

*Bemerkung*: Vergleichen Sie hierzu auch Kapitel 13 im Buch *Elementare und algebraische Zahlentheorie – Stefan Müller-Stach, Jens Piotkowski.*

*Bemerkung*: Im Gegensatz zu der in obiger Bemerkung angegebenen Literatur verwenden wir die Bezeichnung $l$-adische Zahlen, da $p$ in unserer Vorlesung bereits die Charakteristik des Grundkörpers bezeichnet.

**Bitte wenden!**

**Aufgabe 2** (*Der Tate-Modul $T_l(E)$*) (5+5)
Seien $E$, $E_1$ und $E_2$ elliptische Kurven über einem separablen Körper $K$ und $l \neq \operatorname{char} K$ eine Primzahl. In der Vorlesung wurde $T_l(E)$ definiert als der projektive Limes $\varprojlim_n E[l^n]$.

(a) Zeigen Sie, dass eine Isogenie $\Phi : E_1 \to E_2$ eine Abbildung $\Phi_l : T_l(E_1) \to T_l(E_2)$ induziert.

(b) Zeigen Sie, dass die Abbildung

$$\operatorname{Hom}(E_1, E_2) \longrightarrow \operatorname{Hom}(T_l(E_1), T_l(E_2)), \quad \Phi \longmapsto \Phi_l$$

aus Aufgabenteil (a) injektiv ist.

*Hinweis*: Nehmen Sie $\Phi_l = 0$ an. Was lässt sicht dann über den Grad von $\Phi$ sagen?