Arithmetik Elliptischer Kurven

Universität Frankfurt
Institut für Mathematik
Marius Leonhardt

Blatt 05
Wintersemester 2024/25
Besprechung am 22.01.2025

Aufgabe 1 (Formale Potenzreihen I) Es sei R ein (kommutativer) Ring und $R[[T]]$ der Ring der formalen Potenzreihen mit Koeffizienten in R. Zeige, dass $f = a_0 + a_1T + a_2T^2 + \cdots \in R[[T]]$ genau dann eine Einheit in $R[[T]]$ ist, wenn $a_0 \in R^\times$.

Aufgabe 2 (Formale Potenzreihen II) Es sei R ein (kommutativer) Ring und $f(T) = a_0 + a_1T + \cdots \in R[[T]]$.

(a) Überlege, warum für $g(T) = b_0 + b_1T + b_2T^2 + \cdots \in R[[T]]$ der Ausdruck $f(g(T))$ nur dann eine sinnvolle formale Potenzreihe ergibt, wenn $b_0 = 0$ gilt.

(b) Es sei nun $a_0 = 0$ und $a_1 \in R^\times$. Zeige, dass es eine eindeutige Potenzreihe $g(T) = a_1^{-1}T + b_2T^2 + \cdots \in R[[T]]$ gibt mit $f(g(T)) = T$. Zeige, dass dann ebenfalls $g(f(T)) = T$ gilt.

(c) Wer möchte, kann über folgende präzisere Version von (b) nachdenken: Es sei R ein nullteilerfreier Ring mit $\mathrm{char}(R) = 0$ und K sein Quotientenkörper. Angenommen, die Potenzreihen $f(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n$ und $g(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!} T^n$ aus $K[[T]]$ erfüllen $f(g(T)) = g(f(T)) = T$. Zeige, dass falls $a_1 \in R^\times$ und $a_n \in R$ für alle $n \in \mathbb{N}$, dann auch $b_n \in R$ für alle $n \in \mathbb{N}$. (*Hinweis*: Leite $f(g(T)) = T$ wieder und wieder ab und setze $T = 0$.)

Aufgabe 3 (Formale Multiplikation mit m) Es sei F eine Formale Gruppe über R.

(a) Zeige, dass die Eigenschaften (i) bis (iii) aus Definition 5.10 schon Eigenschaft (iv) implizieren, d.h. dass es eine eindeutig bestimmte Potenzreihe $\iota(X) \in R[[X]]$ gibt mit $F(X, \iota(X)) = 0$.

(b) Für $m \in \mathbb{Z}$ definiere $[m](T) \in R[[T]]$ induktiv durch

$$[0](T) = 0, \quad [m+1](T) = F([m]T, T), \quad [m-1](T) = F([m]T, \iota(T)).$$

Zeige

(i) $[m](T) \equiv mT \pmod{T^2}$.

(ii) $[m]\colon F \to F$ ist ein Morphismus Formaler Gruppen.

(iii) Falls $m \in R^\times$, so ist $[m]\colon F \to F$ ein Isomorphismus Formaler Gruppen.

(c) Es sei nun R vollständig bzgl. des Ideals I. Zeige, dass die Multiplikation mit m auf der Gruppe $F(I)$ gegeben ist durch Auswerten der Potenzreihe $[m](T)$, d.h.

$$x \oplus_F x \oplus_F \cdots \oplus_F x = [m](x), \quad x \in I.$$

Aufgabe 4 (p^n-Torsion) Wir betrachten[1] die p^n-Torsionsuntergruppe von $\widehat{\mathbb{G}}_m$ über $\mathbb{Z}_p$.

(a) Zeige, dass $[n]\colon \widehat{\mathbb{G}}_m \to \widehat{\mathbb{G}}_m$ gegeben ist durch $[n](T) = (1+T)^n - 1$.

(b) Es sei

$$\widehat{\mathbb{G}}_m[p^n] := \{z \in \overline{\mathbb{Q}}_p \colon |z|_p < 1 \text{ und } [p^n](z) = 0\}$$

Zeige, dass $\widehat{\mathbb{G}}_m[p^n]$ eine Gruppe ist bzgl. $\oplus_{\widehat{\mathbb{G}}_m}$. Zeige weiter, dass $z \mapsto z - 1$ ein Gruppenisomorphismus zwischen $\widehat{\mathbb{G}}_m[p^n]$ und den p^n-ten Einheitswurzeln μ_{p^n} ist. Insbesondere ist $\widehat{\mathbb{G}}_m[p^n] \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$.

(c) Es sei $L_n := \mathbb{Q}_p(\widehat{\mathbb{G}}_m[p^n])$. Zeige, dass $L_n/\mathbb{Q}_p$ galoissch ist, und finde einen Isomorphismus

$$\mathrm{Gal}(L_n/\mathbb{Q}_p) \xrightarrow{\sim} (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times.$$

---

[1] Diese Aufgabe ist der Ausgangspunkt der sogenannten Lubin–Tate-Theorie. Grob gesagt lassen sich alle rein verzweigten abelschen Erweiterungen eines lokalen Körpers mit Hilfe der p^n-Torsionspunkte geeigneter Formaler Gruppen konstruieren.