LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley

Wintersemester 2019/20

# Algebraische Zahlentheorie
# Übungsblatt 8 Lösung

**Aufgabe 1**
Berechnen Sie die ersten 3 Koeffizienten in der 5-adischen Entwicklung von $1/3$.

Es gilt

$$\begin{aligned} & \frac{1}{3} \equiv a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 \pmod{5^3\mathbb{Z}_p} \\ \iff \quad & 3(a_0 + a_1 \cdot 5 + a_2 \cdot 5^2) \equiv 1 \pmod{5^3\mathbb{Z}_p} \\ \iff \quad & 3(a_0 + a_1 \cdot 5 + a_2 \cdot 5^2) \equiv 1 \pmod{5^3\,\mathbb{Z}} \\ \iff \quad & a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 \equiv 42 \pmod{5^3\,\mathbb{Z}}. \end{aligned}$$

Man beachte dazu $\mathbb{Z}\,/\,p^n\,\mathbb{Z} \simeq \mathbb{Z}_p\,/\,p^n\mathbb{Z}_p$ und $3^{-1} = 42$ in $\mathbb{Z}\,/125\,\mathbb{Z}$. Die 5-adische Entwicklung von 42 liefert die Ziffern $a_0 = 2, a_1 = 3, a_2 = 1$.

**Aufgabe 2**
Sei $n$ eine zur Primzahl $p$ teilerfremde natürliche Zahl. Zeige, dass die Menge

$$\{a \in \mathbb{Z} \mid a > 0 \text{ und } a \equiv 1 \pmod{n}\}$$

dicht in $\mathbb{Z}_p$ ist.

Sei $\alpha = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p$ und $k \in \mathbb{N}$. Wegen $(n, p) = 1$ gibt es nach dem chinesischen Restsatz ein $\alpha_k \in \mathbb{Z}_{>0}$ mit

$$\begin{aligned} \alpha_k &\equiv 1 \pmod{n}, \\ \alpha_k &\equiv \sum_{\nu=0}^{k-1} a_\nu p^\nu \pmod{p^k}. \end{aligned}$$

Dann gilt $v_p(\alpha_n - \alpha) \geq k \longrightarrow \infty$ für $k \longrightarrow \infty$, d.h., die Folge der $\alpha_k$ konvergiert gegen $\alpha$.

**Aufgabe 3**
Seien $\mathbb{F}_p$ der endliche Körper mit $p$ Elementen, $R = \mathbb{F}_p[T]$ und $K = \mathbb{F}_p(T)$ der Quotientenkörper.

a) Definieren Sie zu jedem Primideal $\mathfrak{p}$ von $R$, $\mathfrak{p} \neq (0)$, eine $\mathfrak{p}$-adische Bewertung. Beschreiben Sie den Zusammenhang zur Null- bzw. Polstellenordung bei $T = \alpha$, falls $\mathfrak{p} = (T - \alpha)$.

b) Zeigen Sie: Durch $v_\infty(\frac{f(T)}{g(T)}) = \deg(g(T)) - \deg(f(T))$ wird ebenfalls eine Bewertung auf $K$ definiert. Interpretieren Sie dies als Null- bzw. Polstellenordnung in einem unendlich fernen Punkt $\infty$.

c) Seien $\mathfrak{p} = (p(T))$ mit irreduziblem $p(T)$, $F_\mathfrak{p}$ die durch $p(T)$ definierte Körperweiterung und $f_\mathfrak{p} = [F_\mathfrak{p} : \mathbb{F}_p]$. Definiere

$$|h(T)|_\mathfrak{p} := q^{-f_\mathfrak{p} v_\mathfrak{p}(h(T))} \text{ für } h(T) \in K \text{ und } |h(T)|_\infty := q^{-v_\infty(h(T))}, \text{ mit } q \in \mathbb{R}_{>1}\,.$$

Zeigen Sie die Geschlossenheitsrelation, i.e. für jedes $h(T) \in K^\times$ gilt:

$$|h(T)|_\infty \cdot \prod_{\mathfrak{p} \neq (0)} |h(T)|_\mathfrak{p} = 1.$$

a) R ist ein Hauptidealring, also ist jedes Primideal $\mathfrak{p}$ von $R$ von der Form $(p(T))$ für ein normiertes irreduzibles Polynom $p(T) \in R$. Eine Bewertung defineren wir wie folgt: Sei $f(T) = \frac{g(T)}{h(T)}$ mit $g(T), h(T) \in R$ nicht das Nullelement. Dann können wir

$$f(T) = p(T)^m \frac{G(T)}{H(T)}$$

für ein $m \in \mathbb{Z}$ und $G(T)$, $H(T)$ nicht teilbar durch $p(T)$ schreiben und wir setzen nun

$$v_\mathfrak{p}(f(T)) := m \text{ und } v_\mathfrak{p}(0) := \infty.$$

Es ist nun einfach zu prüfen, dass die Funktion

$$v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$$

die folgenden Eigenschaften erfüllt und somit eine Bewertung ist:

i) $v_\mathfrak{p}(f(T)) = \infty$ genau dann, wenn $f(T) = 0$,

ii) $v_\mathfrak{p}(f(T) \cdot g(T)) = v_\mathfrak{p}(f(T)) + v_\mathfrak{p}(g(T))$,

iii) $v_\mathfrak{p}(f(T) + g(T)) \geq \min\{v_\mathfrak{p}(f(T)), v_\mathfrak{p}(g(T))\}$

Im Fall $p(T) = T - \alpha$ ist die Bewertung $v_\mathfrak{p}(f(T))$ per Definition die Ordnung der Nullstelle bzw. des Pols, der Funktion $f(T)$ bei $T = \alpha$.

b) Einfache Rechnungen zeigen nun, dass auch die angegebene Abbildung $v_\infty$ eine Bewertung ist. Nun beschreibt $v_\infty(h(T))$ die Ordnung der Nullstelle bzw. des Pols der Funktion $h(1/T)$ bei $T = 0$.

c) Für ein normiertes irreduzibles Polynom $p(T) \in R$ gilt nun $\deg(p(T)) = f_\mathfrak{p}$ mit $\mathfrak{p} = (p(T))$, da $\{\overline{1}, \overline{T}, \ldots, \overline{T^{\deg(p(T))-1}}\}$ eine $\mathbb{F}_p$-Basis von $R/\mathfrak{p}$ ist. Sei nun $h(T) = f(T)/g(T)$. Dann gilt

$$\begin{aligned}
v_\infty(h(T)) &= \deg(g(T)) - \deg(f(T)) \\
&= \deg(\prod_{p(T)} p(T)^{v_\mathfrak{p}(g(T))}) - \deg(\prod_{p(T)} p(T)^{v_\mathfrak{p}(f(T))}) \\
&= \sum_{p(T)} v_\mathfrak{p}(g(T)) \cdot \deg(p(T)) - \sum_{p(T)} v_\mathfrak{p}(f(T)) \cdot \deg(p(T)) \\
&= -\sum_{p(T)} \deg(p(T)) v_\mathfrak{p}(h(T)) \\
&= -\sum_{p(T)} f_\mathfrak{p} v_\mathfrak{p}(h(T)).
\end{aligned}$$

Also gilt

$$|h(T)|_\infty \cdot \prod_\mathfrak{p} |h(T)|_\mathfrak{p} = q^{\sum_{p(T)} f_\mathfrak{p} v_\mathfrak{p}(h(T))} \cdot \prod_\mathfrak{p} q^{-f_\mathfrak{p} \cdot v_\mathfrak{p}(h(T))} = 1.$$

**Aufgabe 4**

Sei $\varepsilon \in 1 + p\mathbb{Z}_p$ und $\alpha = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p$ und sei $s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu$ die Folge der Partialsummen.

a) Zeigen Sie, dass für $b \in \{0, \ldots, p-1\}$, $i \in \{1, \ldots, bp^n - 1\}$ und $n \in \mathbb{N}$ gilt:

$$v_p\left(\binom{b \cdot p^n}{i}\right) = n - v_p(i).$$

b) Zeigen Sie, dass die Folge $\varepsilon^{s_n}$ gegen eine Zahl $\varepsilon^\alpha$ in $1 + p\mathbb{Z}_p$ konvergiert.
*Hinweis: Reduzieren Sie das Problem darauf zu zeigen, dass $\{\varepsilon^{s_n}\}_n$ eine Cauchyfolge ist und schreiben Sie $\varepsilon$ dann in der Form $\varepsilon = 1 + p\beta \in 1 + p\mathbb{Z}_p$.*

c) Zeigen Sie weiter, dass dadurch $1 + p\mathbb{Z}_p$ zu einem $\mathbb{Z}_p$-Modul wird.

a) Zuerst sehen wir ein, dass

$$v_p(bp^n - i) = v_p(i) \text{ und } i!\binom{bp^n}{i} = (bp^n) \cdot \ldots \cdot (bp^n - i + 1) \text{ gilt.}$$

Also bekommen wir

$$\begin{aligned} v_p(i!\binom{bp^n}{i}) &= v_p((bp^n)\cdot\ldots\cdot(bp^n-i+1)) \\ &= v_p(bp^n)+v_p(bp^n-1)+\ldots+v_p(bp^n-(i-1)) \\ &= n+v_p(1)+\ldots+v_p(i-1) \\ &= n+v_p((i-1)!) \end{aligned}$$

Somit folgt wegen $v_p(i!\binom{bp^n}{i}) = v_p(i!) + v_p(\binom{bp^n}{i})$ die Behauptung.

b) Sei $\varepsilon = 1+p\beta \in 1+p\,\mathbb{Z}_p$, $\alpha = \sum_{\nu=0}^{\infty} a_\nu p^\nu$ und $s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu$. Um die Behauptung zu zeigen, reicht es zu zeigen, dass $\{\varepsilon^{s_n}\}_n$ ein Cauchyfolge ist und wir nehmen oE an $a_n \neq 0$. Wir betrachten also

$$|\varepsilon^{s_{n+1}} - \varepsilon^{s_n}|_p = |\varepsilon^{s_n}|_p \cdot |\varepsilon^{a_n p^n} - 1|_p = |\varepsilon^{a_n p^n} - 1|_p = |(1+p\beta)^{a_n p^n} - 1|_p = \left| \sum_{i=1}^{a_n p^n} \binom{a_n p^n}{i} p^i \beta^i \right|_p$$

Mit Teilaufgabe a) gilt für alle $i$: $v_p\left(\binom{a_n p^n}{i} p^i \beta^i\right) = n - v_p(i) + i + i v_p(\beta)$. Außerdem sehen wir sofort ein, dass $v_p\left(\binom{a_n p^n}{a_n p^n} p^{a_n p^n} \beta^{a_n p^n}\right) = a_n p^n + a_n p^n v_p(\beta)$ gilt. Also ist die kleinste Bewertung bei $i = 1$. Wir erhalten also

$$v_p(\varepsilon^{a_n p^n} - 1) = v_p\left(\sum_{i=1}^{a_n p^n} \binom{a_n p^n}{i} p^i \beta^i\right) \geq n + 1 + v_p(\beta)$$

und somit auch

$$|\varepsilon^{s_{n+1}} - \varepsilon^{s_n}|_p \leq p^{-n-1-v_p(\beta)}$$

was gegen Null geht für $n \to \infty$.

c) Es ist nun einfach zu verifizieren, dass die Definition von $\varepsilon^\alpha$ die multiplikative Gruppe $1 + p\,\mathbb{Z}_p$ mit einer $\mathbb{Z}_p$-Modulstruktur ausstattet.

**Aufgabe 5**

Für eine natürliche Zahl $n$ bezeichne $\mu_n$ die Gruppe der $n$-ten Einheitswurzeln in einem algebraischen Abschluss von $\mathbb{Q}_p$. Sei nun $p$ eine ungerade Primzahl. Zeige:

$$\mu_n \subseteq \mathbb{Z}_p \iff p \equiv 1 \pmod{n}.$$

Falls $p \equiv 1 \pmod{n}$ so zerfällt das Polynom $f(x) = x^n - 1$ über $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ vollständig in paarweise verschiedene Linearfaktoren. Wegen $(f, f') = 1$ (in $\mathbb{F}_p[x]$) kann man nach der Folgerung aus dem Henselschen Lemma jede der Nullstellen zu einem Element aus $\mathbb{Z}_p$ liften.

Umgekehrt zeigen wir, dass die Abbildung $\mu_n \longrightarrow \left(\mathbb{Z}_p/p\mathbb{Z}_p\right)^\times, \varepsilon \mapsto \bar{\varepsilon}$, injektiv ist. Wegen $\#\left(\mathbb{Z}_p/p\mathbb{Z}_p\right)^\times = \#\mathbb{F}_p^\times = p-1$ folgt dann $n \mid (p-1)$. Sei also $\varepsilon \equiv 1 \pmod{p\mathbb{Z}_p}$. Dann ist $\varepsilon \in 1 + p\mathbb{Z}_p$ und der $p$-adische Logarithmus liefert einen Isomorphismus $1 + p\mathbb{Z}_p \simeq p\mathbb{Z}_p$. Da $p\mathbb{Z}_p$ torsionsfrei ist, ist auch $1 + p\mathbb{Z}_p$ torsionfrei, und es folgt $\varepsilon = 1$.