Prof. Dr. Werner Bley Wintersemester 2019/20

Algebraische Zahlentheorie
Übungsblatt 8 Lösung

Aufgabe 1
Zeigen Sie, dass die Gleichung $x^2 = 2$ in $\mathbb{Z}_7$ eine Lösung hat.

Lösung: Wir suchen Lösungen der Gleichung $x^2 = 2$ in $\mathbb{Z}_7$, d.h. wir wollen eine Prozedur angeben, um eine unendliche Folge von Repräsentanten $a_i \in \{0, \dots, 6\}$ zu bekommen für die gilt

$$\left(a_0 + a_1 7 + a_2 + \dots + a_{n-1} 7^{n-1}\right)^2 \equiv 2 \bmod 7^n$$

für alle $n \geq 1$. Für $n = 1$ erhalten wir die Kongruenz $a_0^2 \equiv 2 \bmod 7$, also können wir $a_0 = 3$ oder $a_0 = 4$ setzen. Ohne Einschränkung setzen wir $a_0 = 3$. Dann erhalten wir für $n = 2$ die Kongruenz $a_0^2 + 2a_1 7 \equiv 2 \bmod 7^2$, was äquivalent zu $\frac{a_0^2 - 2}{7} + a_1 \equiv 0 \bmod 7$ ist, was eine eindeutige Lösung im Repräsentantensystem hat und zu beachten ist, dass $\frac{a_0^2-2}{7}$ wegen der ersten Kongruenz ein ganze Zahl ist. Wenn wir $a_0, a_1, \dots, a_{n-1}$ gefunden haben, nutzen wir die Kongruenz

$$(a_0 + a_1 7 + a_2 + \dots + a_n 7^n)^2 \equiv 2 \bmod 7^{n+1},$$

um

$$\frac{(a_0 + a_1 7 + \dots + a_{n-1} 7^{n-1})^2 - 2}{7} + 2a_n \equiv 0 \bmod 7$$

zu erhalten, was uns wiederum eine eindeutige Lösung für a_n im Repräsentantensystem liefert, wobei der Term ganz links wegen der vorigen Kongruenz wieder ganzzahlig ist. Also haben wir eine Prozedur gefunden, die uns eine Lösung in $\mathbb{Z}_7$ liefert.

Aufgabe 2
Zeigen Sie: Die Folge $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \dots$ konvergiert fur keine Primzahl p in $\mathbb{Q}_p$.

Lösung: Man betrachte für $m \geq n$

$$\frac{1}{10^n} - \frac{1}{10^m} = \frac{10^{m-n} - 1}{10^m}.$$

Für $p \neq 2, 5$ ist $\overline{10} \in (\mathbb{Z}/p\,\mathbb{Z})^\times$. Sei t die Ordnung von $\overline{10}$. Dann gilt für alle $m \geq n$ mit $m \not\equiv n \pmod t$

$$v_p\left(\frac{1}{10^n} - \frac{1}{10^m}\right) = 0 \not\longrightarrow \infty.$$

Also ist $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \dots$ keine Cauchyfolge.

Ebenso:

$$v_2\left(\frac{1}{10^n} - \frac{1}{10^m}\right) = v_5\left(\frac{1}{10^n} - \frac{1}{10^m}\right) = -m \not\longrightarrow \infty.$$

Aufgabe 3
Sei $K/\mathbb{Q}$ ein Zahlkörper und $\alpha \in K^\times$. Sei $\mathcal{P}$ die Menge der Primideale $\neq 0$ von $\mathcal{O}_K$ und $\mathcal{P}_\infty := \{\rho_1, \dots, \rho_r, \sigma_1, \dots, \sigma_s\}$ die Menge der reellen Einbettungen und "der Hälfte der komplexen Einbettungen". Für eine reelle Einbettung ρ definieren wir $|\alpha|_\rho := |\rho(\alpha)|_\mathbb{R}$, wobei $|\ |_\mathbb{R}$ den gewöhnlichen Betrag auf $\mathbb{R}$ bezeichnet. Für eine komplexe Einbettung σ definieren wir $|\alpha|_\sigma := |\sigma(\alpha)|_\mathbb{C}^2$, wobei $|\ |_\mathbb{C}$ den gewöhnlichen Betrag auf $\mathbb{C}$ bezeichnet. Man zeige:

$$\prod_{\mathfrak{p} \in \mathcal{P} \cup \mathcal{P}_\infty} |\alpha|_\mathfrak{p} = 1.$$

Lösung: Sei v eine unendliche Primstelle und τ_v eine dazu korrespondierende Einbettung. Wir setzen

$$|\alpha|_v = \begin{cases} |\tau_v(\alpha)| & \text{falls } v \text{ reell ist,} \\ |\tau_v(\alpha)|^2 & \text{falls } v \text{ komplex ist.} \end{cases}$$

Wir wollen nun zeigen, dass

$$\prod_v |\alpha|_v = 1$$

gilt wobei v alle Primideale $\neq (0)$ von $\mathcal{O}_K$ durchläuft, so wie die reellen und die Hälfte der komplexen Einbettungen (diese bezeichnet man oft als archimedische Primstellen). Mit den bekannten Definitionen erhalten wir nun alle Primzahlen p:

$$\prod_{\mathfrak{p}|p} |\alpha|_{\mathfrak{p}} = \prod_{\mathfrak{p}|p} N(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)} = \prod_{\mathfrak{p}|p} p^{-f_{\mathfrak{p}} v_{\mathfrak{p}}(\alpha)}$$

und für die unendlichen Primstellen

$$\prod_{v|\infty} |\alpha|_v = \prod_{\tau: K \hookrightarrow \mathbb{C}} |\tau(\alpha)| = N(\alpha).$$

Außerdem gilt für $\alpha \mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$:

$$N((\alpha)) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{v_{\mathfrak{p}}(\alpha)} = \prod_{\mathfrak{p}} p^{f_{\mathfrak{p}} v_{\mathfrak{p}}(\alpha)}.$$

Also erhalten wir mit insgesamt

$$\prod_v |\alpha|_v = \prod_p \prod_{\mathfrak{p}|p} |\alpha|_{\mathfrak{p}} \cdot \prod_{v|\infty} |\alpha|_v = \prod_{\mathfrak{p}} p^{-f_{\mathfrak{p}} v_{\mathfrak{p}}(\alpha)} \cdot N(\alpha) = \prod_{\mathfrak{p}} p^{-f_{\mathfrak{p}} v_{\mathfrak{p}}(\alpha)} \cdot \prod_{\mathfrak{p}} p^{f_{\mathfrak{p}} v_{\mathfrak{p}}(\alpha)} = 1.$$

Aufgabe 4

Sei $a = (a_n)_{n=1}^{\infty} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ und $m \in \mathbb{Z}_{\geq 1}$.

a) Zeige: $p^m a = p^m (a_n)_{n=1}^{\infty} = (\ldots, p^m a_2 \mod p^{p+2}, p^m a_1 \mod p^{m+1}, 0, \ldots, 0)$.

b) Zeige: $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ ist nullteilerfrei.

Lösung: a) Es reicht zu zeigen:

$$p\,(a_n)_{n=1}^{\infty} = p(\ldots, a_3, a_2, a_1) \overset{!}{=} (\ldots, pa_2, pa_1, 0).$$

Der Rest ist eine einfache Induktion. Zum !: Per Definition gilt

$$p(\ldots, a_3, a_2, a_1) = (\ldots, pa_3, pa_2, pa_1).$$

Wegen $a_{n+1} \equiv a_n \pmod{p^n}$ folgt $pa_{n+1} \equiv pa_n \pmod{p^{n+1}}$ und offensichtlich gilt $pa_1 \equiv 0 \pmod{p}$. Daher ist

$$(\ldots, pa_3, pa_2, pa_1) = (\ldots, pa_2, pa_1, 0),$$

was zu beweisen war.

b) Sei $a = (s_n)_{n=1}^{\infty} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ ein Nullteiler. Statt in $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ rechnen wir für den Moment in den formalen Potenzreihen und setzen

$$a = \sum_{\nu=0}^{\infty} a_\nu p^\nu \text{ mit } 0 \leq a_\nu < p.$$

Wie üblich ist dann $s_n = \sum_{\nu=0}^{n-1}$ die n-te Partialsumme. Falls nun a ein Nullteiler ist, so gibt es

$$0 \neq b = \sum_{\mu=m_0}^{\infty} b_\mu p^\mu \text{ mit } m_0 \geq 0, 0 \leq b_\mu < p \text{ und } b_{m_0} \neq 0,$$

so dass $ab = 0$. Wir schreiben

$$b = p^{m_0} \sum_{\mu=m_0}^{\infty} b_\mu p^{\mu - m_0} = p^{m_0} c \text{ mit } c \in \mathbb{Z}_p^{\times}.$$

Aus $ab = 0$ folgt dann, da c eine Einheit ist, $p^{m_0} a = 0$. Nach a) ist also $p^{m_0} s_n \equiv 0 \pmod{p^{m_0+n}}$ für alle $n \geq 1$. Es folgt $s_n \equiv 0 \pmod{p^n}$ für alle $n \geq 1$.