

Lösung 5

Aufgabe 1.

- (1) Es ist $\{x \in \mathbf{F}_5 : x^2 - 2 = 0\} = \emptyset$. Daher existiert erst recht keine Lösung in $\mathbf{Z}_5$ oder in $\mathbf{Z}_{(5)}$.
- (2) Da $X^2 - 2 \in \mathbf{Q}[X]$ irreduzibel ist, existiert erst recht keine Lösung in $\mathbf{Z}_{(7)}$. Es wird $\{x \in \mathbf{F}_7 : x^2 - 2 = 0\} = \{\pm 3\}$. Es ist $f'(X) = 2X$, insbesondere hat $f'(\pm 3) = \mp 1$ die Bewertung 0 bei 7. Das Newton-Hensel-Verfahren liefert die Cauchyfolgen

$$\{x \in \mathbf{Z}_7 : x^2 - 2 = 0\} = \{\pm(3, 10, 108, -235, \dots)\}.$$

Dies sind alle Lösungen, da eine Gleichung 2-ten Grades über dem Körper $\mathbf{Q}_7$ maximal 2 Lösungen haben kann.

- (3) Da $X^3 - 2 \in \mathbf{Q}[X]$ irreduzibel ist, existiert erst recht keine Lösung in $\mathbf{Z}_{(5)}$. Es wird $\{x \in \mathbf{F}_5 : x^3 - 2 = 0\} = \{3\}$. Es ist $f'(X) = 3X^2$, insbesondere hat $f'(3) = 27$ die Bewertung 0 bei 5. Das Newton-Hensel-Verfahren liefert die Cauchyfolge

$$\{x \in \mathbf{Z}_5 : x^3 - 2 = 0\} = \{(3, 3, 53, 303, \dots)\}.$$

Bleibt zu zeigen, daß dies die einzige Lösung darstellt. Gäbe es eine weitere, so würde $X^3 - 2$ über $\mathbf{Z}_5$ in 3 Linearfaktoren zerfallen, und dito über $\mathbf{F}_5$. Aber $X^3 - 2 \equiv_5 (X - 3)(X^2 - 2X - 1)$, und letzterer Faktor ist irreduzibel über $\mathbf{F}_5$.

- (4) Wir haben zunächst $\{x \in \mathbf{Z}_{(2)} : x^3 - 1 = 0\} = \{1\}$. Es wird $\{x \in \mathbf{F}_7 : x^3 - 1 = 0\} = \{1, 2, 4\}$. Es ist $f'(X) = 3X^2$, insbesondere haben $f'(1) = 3$, $f'(2) = 24$ und $f'(4) = 192$ die Bewertung 0 bei 7. Das Newton-Hensel-Verfahren liefert die Cauchyfolgen

$$\{x \in \mathbf{Z}_7 : x^3 - 1 = 0\} = \{(1, 1, 1, 1, \dots), (2, 30, 324, 1353, \dots), (4, 18, 18, 1047, \dots)\}.$$

Dies sind alle Lösungen, da eine Gleichung 3-ten Grades über dem Körper $\mathbf{Q}_7$ maximal 3 Lösungen haben kann.

- (5) Zunächst haben wir keine Lösungen über $\mathbf{Z}_{(3)}$. Es wird $\{x \in \mathbf{F}_3 : x^2 - 3x - 27 = 0\} = \{0\}$. Es ist $f'(X) = 2X - 3$, insbesondere $f'(0) = -3$, von Bewertung 1. Da aber $f(0) = -27$ Bewertung $3 > 2 \cdot 1$ hat, liefert eine Betrachtung modulo 9 zusammen mit Newton-Hensel die Cauchyfolgen

$$\{x \in \mathbf{Z}_3 : x^2 - 3x - 27 = 0\} = \{(0, 0, 18, 18, 99, 342, \dots), (0, 3, 12, 66, 147, 390, \dots)\}.$$

Dies sind alle Lösungen, da eine Gleichung 2-ten Grades über dem Körper $\mathbf{Q}_3$ maximal 2 Lösungen haben kann.

- (6) Zunächst haben wir keine Lösungen über $\mathbf{Z}_{(3)}$. Es wird $\{x \in \mathbf{F}_3 : x^2 - 3x - 9 = 0\} = \{0\}$. Es ist $f'(X) = 2X - 3$, insbesondere $f'(0) = -3$, von Bewertung 1. Da aber $f(0) = -9$ Bewertung $2 = 2 \cdot 1$ hat, können wir Newton-Hensel nicht anwenden. Es werden aber

$$\begin{aligned} f(0) &\equiv_{27} f(3) \equiv_{27} f(9) \equiv_{27} f(12) \equiv_{27} f(18) \equiv_{27} f(21) \equiv_{27} -9 \\ f(6) &\equiv_{27} f(15) \equiv_{27} f(24) \equiv_{27} 9. \end{aligned}$$

Modulo 27 gibt es somit keine Lösung, und folglich auch nicht über $\mathbf{Z}_3$.

- (7) In $\mathbf{F}_p$ lautet die Lösungsmenge $\mathbf{F}_p^*$. Da $p-1$ gerade ist, ist in $\mathbf{Z}_{(p)}$ die Lösungsmenge gegeben durch $\{-1, +1\}$.

Betrachten wir $\mathbf{Z}_p$. Wir behaupten, daß $\xi(j) := (j, j^p, j^{p^2}, \dots)$ für $j \in [1, p-1]$ in $\mathbf{Z}_p$ liegt. In der Tat ist für $k \geq 0$

$$j^{p^k} - j^{p^{k+1}} = j^{p^k} - (j^p)^{p^k} \equiv_{p^{k+1}} (j^{p^k} - (j^p)^{p^k}) \equiv_{p^{p^k}} 0,$$

wobei wir die Kongruenz $\equiv_{p^{k+1}}$ mit folgedem Lemma begründen wollen.

Lemma. In $\mathbf{Z}[X, Y]$ ist

$$(X + pY)^{p^k} \equiv_{p^{k+1}} X^{p^k}.$$

Beweis. Da $\binom{p^k}{j} = \frac{p^k}{j} \binom{p^k-1}{j-1}$ für $j \geq 1$, ist $v_p\left(\binom{p^k}{j} p^j\right) \geq j + k - v_p(j) \geq k + 1$, verschwinden außer X^{p^k} alle Terme der Binomialentwicklung modulo p^k .

Mit dem Lemma folgt aus $j^p = j + ap$ für ein $a \in \mathbf{Z}$, daß $j^{p^{k+1}} = (j + ap)^{p^k} \equiv_{p^{k+1}} j^{p^k}$.

Nun ist $\xi(j)$ eine Nullstelle von $X^p - X$, und ungleich 0, also eine Nullstelle von $X^{p-1} - 1$. Damit ist $\{x \in \mathbf{Z}_p : x^{p-1} = 1\} = \{\xi(j) : j \in [1, p-1]\}$.

Aufgabe 2.

Die Zerlegungen in Primideale in R und in $\hat{R}$ stimmen jeweils überein, da $R/pR \simeq \hat{R}/p\hat{R}$. Nur zerfällt $\hat{R}$ gemäß der Primidealzerlegung in ringdirekte Faktoren, R jedoch nicht, da $R \subseteq \mathbf{C}$ Teilring.

(1)

$p = 2$ Es ist $\mu_{i, \mathbf{Q}}(X) = X^2 + 1 \equiv_2 (X + 1)^2$, also $(2) = (1 + i)^2$. In $\hat{R}/2\hat{R}$, wie dann auch in $\hat{R}$, ist $e_1 = 1$ bereits ein primitives Idempotent. Also $\hat{R} = \hat{R}e_1 = \mathbf{Z}_2[i]$.

$p = 3$ Es ist $X^2 + 1 \equiv_3 (X^2 + 1)$, also bleibt (3) prim. In $\hat{R}$ ist $e_1 = 1$ bereits ein primitives Idempotent. Also $\hat{R} = \hat{R}e_1 = \mathbf{Z}_3[i]$.

$p = 5$ Es ist $X^2 + 1 \equiv_5 (X + 2)(X - 2)$, und somit $(5) = (2 + i)(2 - i)$. Wir haben in

$$\hat{R}/5\hat{R} \simeq \mathbf{F}_5[X]/(X + 2) \times \mathbf{F}_5[X]/(X - 2)$$

die zu diesen beiden ringdirekten Faktoren gehörenden primitiven Idempotenten. Diese werden wie folgt ermittelt. Es ist $(-1) \cdot (X + 2) + 1 \cdot (X - 2) \equiv_5 1$. Also geht $\bar{e}_1 = 1 \cdot (i - 2) = i - 2 \in \hat{R}/5\hat{R}$ auf $(1, 0)$ und entsprechend $\bar{e}_2 = (-1) \cdot (i + 2) = -i - 2 \in \hat{R}/5\hat{R}$ auf $(0, 1)$. Sei also $e_{1,1} = i - 2 \in \hat{R}$ der Ansatz einer Cauchyfolge. Mit $e_{1,k+1} \equiv_{5^{k+1}} 3e_{1,k}^2 - 2e_{1,k}^3$ erhalten wir $e_1 =$

$(i-2, 13+16i, 63+91i, 313+91i, \dots)$, und entsprechend eine (die!) orthogonale Zerlegung

$$1 = \underbrace{(i-2, 13-9i, 63-34i, 313+91i, \dots)}_{= e_1} + \underbrace{(-i-2, 13+9i, 63+34i, 313-91i, \dots)}_{= 1-e_1 = e_2}$$

in primitive Idempotente in $\hat{R}$.

Um $\hat{R}e_1$ als Erweiterung von $\mathbf{Z}_p$ zu berechnen, genügt es hier zu bemerken, daß die Abbildung $\mathbf{Z}_p \rightarrow \hat{R}e_1$, $x \mapsto xe_1$, modulo 5 einen Isomorphismus $\mathbf{F}_5 \xrightarrow{\sim} \mathbf{F}_5[X]/(X+2)$ gibt, und mit Nakayama somit selbst ein Isomorphismus ist. Also $\hat{R}e_1 \simeq \mathbf{Z}_5$, und genauso $\hat{R}e_2 \simeq \mathbf{Z}_5$, insgesamt mithin

$$\mathbf{Z}_5[i] \simeq \mathbf{Z}_5 \times \mathbf{Z}_5.$$

Liftet man die Zerlegung $X^2 + 1 \equiv_5 (X+2)(X-2)$, so erhält man übrigens mit Newton-Hensel

$$X^2 + 1 = (X + (2, 7, 57, 182, \dots))(X - (2, 7, 57, 182, \dots)).$$

(2) Wir schreiben $\theta := \sqrt[3]{2}$.

$p = 2$ Es ist $\mu_{\theta, \mathbf{Q}}(X) = X^3 - 2 \equiv_2 X^3$, also $(2) = (\theta)^3$. In $\hat{R}/2\hat{R}$, wie dann auch in $\hat{R}$, ist $e_1 = 1$ bereits ein primitives Idempotent. Also $\hat{R} = \hat{R}e_1 = \mathbf{Z}_2[\theta]$.

$p = 3$ Es ist $X^3 - 2 \equiv_3 (X+1)^3$, also $(3) = (1+\theta)^3$. In $\hat{R}/3\hat{R}$, wie dann auch in $\hat{R}$, ist $e_1 = 1$ bereits ein primitives Idempotent. Also $\hat{R} = \hat{R}e_1 = \mathbf{Z}_3[\theta]$.

$p = 5$ Es ist $X^3 - 2 \equiv_5 (X+2)(X^2 - 2X - 1)$, also $(5) = (2+\theta)(1+2\theta-\theta^2)$. Wir haben in

$$\hat{R}/5\hat{R} \simeq \mathbf{F}_5[X]/(X+2) \times \mathbf{F}_5[X]/(X^2 - 2X - 1)$$

die zu diesen beiden ringdirekten Faktoren gehörenden primitiven Idempotente. Diese werden wie folgt ermittelt. Es ist $(2X+2) \cdot (X+2) + (-2) \cdot (X^2 - 2X - 1) \equiv_5 1$. Also geht $\bar{e}_1 = (-2) \cdot (\theta^2 - 2\theta - 1) = 2 - \theta - 2\theta^2 \in \hat{R}/5\hat{R}$ auf $(1, 0)$ und entsprechend $\bar{e}_2 = (2\theta + 2) \cdot (\theta + 2) = -1 + \theta + 2\theta^2 \in \hat{R}/5\hat{R}$ auf $(0, 1)$. Heben von Idempotenten liefert die Zerlegung

$$1 = \underbrace{(-2\theta^2 - \theta + 2, -12\theta^2 - 11\theta - 8, -12\theta^2 - 11\theta + 42, 363\theta^2 - 11\theta + 417, \dots)}_{= e_1} + \underbrace{(-1 + \theta + 2\theta^2, 12\theta^2 + 11\theta + 9, 12\theta^2 + 11\theta - 41, -363\theta^2 + 11\theta - 416, \dots)}_{= 1-e_1 = e_2}$$

in primitive Idempotente in $\hat{R}$.

Es ist $\hat{R}e_1 \simeq \mathbf{Z}_5$. Um $\hat{R}e_2$ zu berechnen, heben wir die Zerlegung

$$X^3 - 2 \equiv_5 (X+2)(X^2 - 2X - 1)$$

nach $\mathbf{Z}_5$. Dazu verwenden wir Urbilder $\hat{e}_{1,n}$ resp. $\hat{e}_{2,n}$ der die Idempotenten definierenden Folge $e_{1,n}$ resp. $e_{2,n}$ in $(\mathbf{Z}/5^n\mathbf{Z})[X]$ und bilden dort den ggT mit f , mit Leitkoeffizient 1. Dies ist möglich, da die Leitkoeffizienten dieser Urbilder in $\mathbf{Z}/5^n\mathbf{Z}$ invertierbar sind. Da als Ideale in $(\mathbf{Z}/5^n\mathbf{Z})[X]$ gilt, daß $(f, e_{1,n})(f, e_{2,n}) = (f^2, fe_{1,n}, fe_{2,n}, e_{1,n}e_{2,n}) = (f)$ (letzte Gleichheit: $\subseteq$ wegen

$e_{1,n}e_{2,n} \equiv_f 0$, $\supseteq$ wegen $f = fe_{1,n} + fe_{2,n}$, ist das Produkt der beiden via ggT gewählten Idealerzeuger in der Tat gleich f . Wir erhalten

$$f = g \cdot h \in \mathbf{Z}_5[X],$$

wobei g und h durch die Cauchyfolgen

$$\begin{aligned} g &:= (X + 2, X - 3, X + 72, X + 322, \dots) \\ h &:= (X^2 - 2X - 1, X^2 + 3X + 9, X^2 + 53X + 59, X^2 + 303X + 559, \dots) \end{aligned}$$

in $\mathbf{Z}_5[X]$ definiert sind.

Alternativ hätte man auch mit Newton-Hensel die Nullstelle $(-2, 3, 53, 303, \dots)$ berechnen können und den entsprechenden Linearfaktor abspalten.

Jedenfalls wird $\hat{R}e_2 \simeq \mathbf{Z}_5[X]/(h)$, und insgesamt

$$\mathbf{Z}_5[\sqrt[3]{2}] \simeq \mathbf{Z}_5 \times \mathbf{Z}_5[X] / \left((X^2 - 2X - 1, X^2 + 3X + 9, X^2 + 53X + 59, \dots) \right).$$

$p = 31$ Es ist $X^3 - 2 \equiv_{31} (X + 11)(X - 7)(X - 4)$, also $(31) = (11 + \theta)(7 - \theta)(4 - \theta)$. Wir haben in

$$\hat{R}/31\hat{R} \simeq \mathbf{F}_{31}[X]/(X + 11) \times \mathbf{F}_{31}[X]/(X - 7) \times \mathbf{F}_{31}[X]/(X - 4)$$

die zu diesen ringdirekten Faktoren gehörenden primitiven Idempotente. Diese werden wie folgt ermittelt.

Es ist $(7X + 1) \cdot (X + 11) + (-7) \cdot (X - 7)(X - 4) \equiv_{31} 1$. Also geht $\bar{e}_1 = (-7) \cdot (\theta - 7)(\theta - 4) = -7\theta^2 + 15\theta - 10 \in \hat{R}/31\hat{R}$ auf $(1, 0, 0)$.

Es ist $(4X - 6) \cdot (X - 7) + (-4) \cdot (X + 11)(X - 4) \equiv_{31} 1$. Also geht $\bar{e}_2 = (-4) \cdot (\theta + 11)(\theta - 4) = -4\theta^2 + 3\theta - 10 \in \hat{R}/31\hat{R}$ auf $(0, 1, 0)$.

Es ist $(-11X + 5) \cdot (X - 4) + 11 \cdot (X + 11)(X - 7) \equiv_{31} 1$. Also geht $\bar{e}_3 = 11 \cdot (\theta + 11)(\theta - 7) = 11\theta^2 + 13\theta - 10 \in \hat{R}/31\hat{R}$ auf $(0, 0, 1)$.

Liften der Idempotente via $e \rightsquigarrow 3e^2 - 2e^3$ gibt nun

$$\begin{aligned} e_1 &= (-7\theta^2 + 15\theta - 10, 365\theta^2 + 759\theta + 641, 24390\theta^2 + 2681\theta + 19861, \\ &\quad 54181\theta^2 + 92054\theta + 615681, \dots) \\ e_2 &= (-4\theta^2 + 3\theta - 10, 709\theta^2 + 468\theta + 641, 29539\theta^2 + 23532\theta + 19861, \\ &\quad 59330\theta^2 + 291651\theta + 615681, \dots) \\ e_3 &= (-11\theta^2 + 13\theta - 10, 848\theta^2 + 659\theta + 641, 5653\theta^2 + 3578\theta + 19861, \\ &\quad 810010\theta^2 + 539816\theta + 615681, \dots), \end{aligned}$$

und so eine orthogonale Zerlegung $1 = e_1 + e_2 + e_3$ in primitive Idempotente. Es ist

$$\mathbf{Z}_{31}[\sqrt[3]{2}] \simeq \mathbf{Z}_{31} \times \mathbf{Z}_{31} \times \mathbf{Z}_{31}.$$

Liften der 3 Nullstellen von $X^3 - 2$ in $\mathbf{F}_{31}$ mit Newton-Hensel gibt übrigens die drei Nullstellen

$$\begin{aligned} &(-11, 268, -2615, 325086, \dots) \\ &(7, 410, -1512, 355980, \dots) \\ &(4, 283, 4127, 242455, \dots) \end{aligned}$$

von $X^3 - 2$ in $\mathbf{Z}_{31}$.

(3) Wir schreiben $\zeta := \zeta_5$.

$p = 5$ Es ist $\mu_{\zeta, \mathbf{Q}}(X) = \Phi_5(X) = X^4 + X^3 + X^2 + X + 1 \equiv_5 (X-1)^4$, also $(5) = (\zeta-1)^4$.
In $\hat{R}/5\hat{R}$, wie dann auch in $\hat{R}$, ist $e_1 = 1$ bereits ein primitives Idempotent.
Also $\hat{R} = \hat{R}e_1 = \mathbf{Z}_5[\zeta_5]$.

$p = 11$ Es ist $\Phi_5(X) \equiv_{11} (X-3)(X-4)(X-5)(X-9)$, also $(11) = (\zeta-3)(\zeta-4)(\zeta-5)(\zeta-9)$. Wir haben in

$$\hat{R}/11\hat{R} \simeq \mathbf{F}_{11}[X]/(X-3) \times \mathbf{F}_{11}[X]/(X-4) \times \mathbf{F}_{11}[X]/(X-5) \times \mathbf{F}_{11}[X]/(X-9)$$

die zu diesen ringdirekten Faktoren gehörenden primitiven Idempotenten. Diese werden wie folgt ermittelt.

Es ist $(X^2 + 7X + 1) \cdot (X-3) - 1 \cdot (X-4)(X-5)(X-9) \equiv_{11} 1$. Also geht $\bar{e}_1 = -(\zeta-4)(\zeta-5)(\zeta-9) = -\zeta^3 - 4\zeta^2 - 2\zeta + 4 \in \hat{R}/11\hat{R}$ auf $(1, 0, 0, 0)$.

Es ist $(2X^2 + 7X + 4) \cdot (X-4) - 2 \cdot (X-3)(X-5)(X-9) \equiv_{11} 1$. Also geht $\bar{e}_2 = -2(\zeta-3)(\zeta-5)(\zeta-9) = -2\zeta^3 + \zeta^2 + 2\zeta + 6 \in \hat{R}/11\hat{R}$ auf $(0, 1, 0, 0)$.

Es ist $(-4X^2 - 3) \cdot (X-5) + 4 \cdot (X-3)(X-4)(X-9) \equiv_{11} 1$. Also geht $\bar{e}_3 = 4(\zeta-3)(\zeta-4)(\zeta-9) = 4\zeta^3 + 2\zeta^2 + 3\zeta - 3 \in \hat{R}/11\hat{R}$ auf $(0, 0, 1, 0)$.

Es ist $(X^2 - 3X - 2) \cdot (X-9) - 1 \cdot (X-3)(X-4)(X-5) \equiv_{11} 1$. Also geht $\bar{e}_4 = -(\zeta-3)(\zeta-4)(\zeta-5) = -\zeta^3 + \zeta^2 - 3\zeta + 5 \in \hat{R}/11\hat{R}$ auf $(0, 0, 0, 1)$.

Liften der Idempotenten via $e \rightsquigarrow 3e^2 - 2e^3$ gibt nun

$$\begin{aligned} e_1 &= (-\zeta^3 - 4\zeta^2 - 2\zeta + 4, 98\zeta^3 + 29\zeta^2 + 64\zeta + 48, \\ &\quad 1187\zeta^3 + 634\zeta^2 + 1274\zeta + 774, 14497\zeta^3 + 8620\zeta^2 + 3936\zeta + 14084, \dots) \\ e_2 &= (-2\zeta^3 + \zeta^2 + 2\zeta + 6, 86\zeta^3 + 34\zeta^2 + 57\zeta + 105, \\ &\quad 691\zeta^3 + 1244\zeta^2 + 57\zeta + 831, 4684\zeta^3 + 10561\zeta^2 + 10705\zeta + 10148, \dots) \\ e_3 &= (4\zeta^3 + 2\zeta^2 + 3\zeta - 3, 92\zeta^3 + 35\zeta^2 + 69\zeta + 19, \\ &\quad 697\zeta^3 + 640\zeta^2 + 553\zeta + 140, 6021\zeta^3 + 9957\zeta^2 + 5877\zeta + 5464, \dots) \\ e_4 &= (-\zeta^3 + \zeta^2 - 3\zeta + 5, 87\zeta^3 + 23\zeta^2 + 52\zeta + 71, \\ &\quad 87\zeta^3 + 144\zeta^2 + 778\zeta + 918, 4080\zeta^3 + 144\zeta^2 + 8764\zeta + 14228, \dots) \end{aligned}$$

und so eine orthogonale Zerlegung $1 = e_1 + e_2 + e_3 + e_4$ in primitive Idempotenten.

Es ist

$$\mathbf{Z}_{11}[\zeta_5] \simeq \mathbf{Z}_{11} \times \mathbf{Z}_{11} \times \mathbf{Z}_{11} \times \mathbf{Z}_{11}.$$

Liften der 4 Nullstellen von $\Phi_5(X)$ in $\mathbf{F}_{11}$ gibt übrigens die 4 Nullstellen

$$\begin{aligned} &(3, 3^{11}, 3^{11^2}, \dots) \\ &(4, 4^{11}, 4^{11^2}, \dots) \\ &(5, 5^{11}, 5^{11^2}, \dots) \\ &(9, 9^{11}, 9^{11^2}, \dots) \end{aligned}$$

von $\Phi_5(X)$ in $\mathbf{Z}_{11}$.

$p = 19$ Es ist $\Phi_5(X) \equiv_{19} (X^2 + 5X + 1)(X^2 - 4X + 1)$, also $(19) = (\zeta^2 + 5\zeta + 1)(\zeta^2 - 4\zeta + 1)$.
Wir haben in

$$\hat{R}/19\hat{R} \simeq \mathbf{F}_{19}[X]/(X^2 + 5X + 1) \times \mathbf{F}_{19}[X]/(X^2 - 4X + 1)$$

die zu diesen ringdirekten Faktoren gehörenden primitiven Idempotente. Diese werden wie folgt ermittelt.

Es ist $(2X + 11) \cdot (X^2 + 5X + 1) - (2X + 10) \cdot (X^2 - 4X + 1) \equiv_{19} 1$. Also geht $\bar{e}_1 = -(2\zeta + 10) \cdot (\zeta^2 - 4\zeta + 1) = 2\zeta^3 + 2\zeta^2 - 8 \in \hat{R}/19\hat{R}$ auf $(1, 0)$ und $\bar{e}_2 = (2\zeta + 11) \cdot (\zeta^2 + 5\zeta + 1) = -2\zeta^3 - 2\zeta^2 + 9 \in \hat{R}/19\hat{R}$ auf $(0, 1)$.

Liften der Idempotente via $e \rightsquigarrow 3e^2 - 2e^3$ gibt nun

$$\begin{aligned} e_1 &= (-2\zeta^3 - 2\zeta^2 + 9, 17\zeta^3 + 17\zeta^2 + 9, 1461\zeta^3 + 1461\zeta^2 + 731, \\ &\quad -12257\zeta^3 - 12257\zeta^2 - 6128, \dots) \\ e_2 &= (2\zeta^3 + 2\zeta^2 - 8, -17\zeta^3 - 17\zeta^2 - 8, -1461\zeta^3 - 1461\zeta^2 - 730, \\ &\quad 12257\zeta^3 + 12257\zeta^2 + 6129, \dots) . \end{aligned}$$

Liften der Zerlegung $\Phi_5(X) \equiv_{19} (X^2 + 5X + 1)(X^2 - 4X + 1)$ durch Bilden der ggT in $(\mathbf{Z}/19^n\mathbf{Z})[X]$ von Φ und $e_{1,n}$ resp. $e_{2,n}$ gibt

$$\Phi_5(X) = g \cdot h \in \mathbf{Z}_{19}[X] ,$$

wobei

$$\begin{aligned} g &= (X^2 - 4X + 1, X^2 - 42X + 1, X^2 + 3207X + 1, X^2 + 30643X + 1, \dots) \\ h &= (X^2 + 5X + 1, X^2 + 43X + 1, X^2 - 3206X + 1, X^2 - 30642X + 1, \dots) \end{aligned}$$

in $\mathbf{Z}_{19}[X]$. Insgesamt wird

$$\begin{aligned} \mathbf{Z}_{19}[\zeta_5] &\simeq \mathbf{Z}_{19}[X] \Big/ \left((X^2 - 4X + 1, X^2 - 42X + 1, X^2 + 3207X + 1, \dots) \right) \\ &\quad \times \mathbf{Z}_{19}[X] \Big/ \left((X^2 + 5X + 1, X^2 + 43X + 1, X^2 - 3206X + 1, \dots) \right) . \end{aligned}$$

Aufgabe 3. Die Voraussetzung $R \subseteq \mathbf{C}$ kann auch entfallen, sie stand nur zwecks besserer Orientierung dabei.

(1) $\implies$ Sei S ein diskreter Bewertungsring mit maximalem Ideal erzeugt von s . Schreiben wir $rS = s^e S$, so ist $e \mid l$ nach der Indexformel, hier $l = ef$, mit $f = \dim_{R/rR} S/sS$. Insbesondere ist $s^l \equiv_r 0$, und damit $(R/rR)[X]/(X^l) \xrightarrow{\bar{\varphi}} S/rS$, $X \mapsto s$ wohldefiniert. Dieser Ringmorphismus ist surjektiv, da $S = R[s]$. Da Quelle und Ziel Vektorräume über R/rR der Dimension l sind – letzterer, da Basis $(s^0, \dots, s^{l-1})$ vorliegt –, ist $\bar{\varphi}$ vollends ein Isomorphismus. Speziell ist $e = l$ und $v_r = lv_s$ auf R . Da $\mu_{s,K}(X)$ auch im Kern von $\bar{\varphi}$ liegt, ist nun X^l in $(R/rR)[X]$ ein Teiler von $\mu_{s,K}(X)$. Da die beiden Polynome denselben Grad aufweisen, folgt $\mu_{s,K}(X) \equiv_r X^l$. Schreibe $\mu_{s,K}(X) = X^l + \sum_{j \in [0, l-1]} a_j X^j$ mit $a_j \in R$. Es bleibt zu zeigen, daß $a_0 = \mu_{s,K}(0) \not\equiv_{r^2} 0$. Die Bewertung bei s von s^l ist gleich l , also genauso die Bewertung von $-\sum_{j \in [0, l-1]} a_j s^j$. Diese Summanden haben alle verschiedene Bewertungen bei s , wie eine Betrachtung dieser Bewertungen modulo l lehrt. Die Bewertung dieser Summe ist also gleich der minimalen Bewertung ihrer Summanden. Nun hat aber nur $a_0 s^0$ eine durch l teilbare Bewertung. Somit folgt $v_s(a_0) = v_s(s^l) = l$, d.h. $v_r(a_0) = 1$. (Dieses Argument zeigt auch abermals, daß $v_r(a_j) \geq 1$ für $j \in [0, l-1]$).

($\Leftarrow$) Sei nun umgekehrt $\mu_{s,K}(X)$ ein Eisensteinpolynom. Wir behaupten, daß $R[s]$ ein diskreter Bewertungsring mit maximalem Ideal $(s) = sR[s]$ ist.

Jedes maximale Ideal $\mathfrak{m} \subseteq R[s]$ enthält r , da sonst $\mathfrak{m} \cap R = 0$ sein müßte, was der Ganzheit von $R[s]|R$ widerspricht (betrachte konstanten Koeffizienten des Minimalpolynoms über K eines Elementes aus $\mathfrak{m} \setminus \{0\}$). Da $R[s]/rR[s] \simeq (R/rR)[X]/(\mu_{s,K}(X)) \simeq (R/rR)[X]/(X^l)$, ist $R[s]$ lokal mit maximalem Ideal (s, r) . Nun ist aber $r \in (s)$, da $a_0 \in (s)$, wie man von $\mu_{s,K}(s) = 0$ abliest, und da a_0/r eine Einheit in R ist. Also ist das maximale Ideal $(s) \subseteq R[s]$.

Wir behaupten, daß s^l/r eine Einheit in $R[s]$ ist. Wegen $s^l = -\sum_{j \in [0, l-1]} a_j s^j$ ist s^l durch r teilbar. Da $\sum_{j \in [1, l-1]} (a_j/r) s^j \in (s)$ liegt und a_0/r als Einheit (in R , also auch in $R[s]$) nicht in (s) liegen kann, kann auch s^l/r nicht in (s) liegen. In einem lokalen Ring ist nun jedes Element außerhalb des maximalen Ideals eine Einheit, da das von ihm erzeugte Ideal in *keinem* maximalen Ideal enthalten ist.

Sei $x = \sum_{j \in [0, l-1]} b_j s^j \in R[s] \setminus \{0\}$ vorgegeben, $b_j \in R$. Sei $c \in [0, l-1]$ minimal unter den $j \in [0, l-1]$, für die $v_r(b_j)$ den minimalen Wert annimmt. Speziell ist $b_c \neq 0$. Schreibe $d := v_r(b_c)$. Dann ist $s^{-c} r^{-d} (b_c s^c)$ nicht in (s) , während $s^{-c} r^{-d} (b_j s^j)$ in (s) liegt für $j \in [0, l-1] \setminus \{c\}$. Damit ist $s^{-c} r^{-d} x$ nicht in (s) , und mithin eine Einheit. Da auch s^l/r eine Einheit ist, ist damit auch $s^{-c-dl} x$ eine Einheit.

Jedes Ideal $\mathfrak{a} \neq 0$ von $R[s]$ ist somit von der Form $\mathfrak{a} = (s^v)$ für ein $v \geq 0$, namentlich mit $v = \min\{w \geq 0 \mid \text{es gibt ein } x \in \mathfrak{a} \text{ mit } x/s^w \text{ Einheit}\}$. Folglich ist $R[s]$ ein lokaler Hauptidealbereich, d.h. ein diskreter Bewertungsring.

- (2) In (1, $\Rightarrow$) haben wir $e = l$ gesehen, d.h. $rS = s^l S$. Das wiederum impliziert wegen $l = ef$, daß $f = 1$, i.e. $R/rR \xrightarrow{\sim} S/sS$, $x \mapsto x$.
- (3) Im Falle $R = \mathbf{Z}_{(p)}$, $r = p$, $s = \zeta_p - 1$ ist sowohl $R[s] = \mathbf{Z}_{(p)}[\zeta_p]$ ein diskreter Bewertungsring mit maximalem Ideal erzeugt von $s = \zeta_p - 1$ (cf. Blatt 1, Lösung zu Aufgabe 2 (a)), als auch

$$\mu_{\zeta_p-1, \mathbf{Q}}(X) = \Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \sum_{j \in [0, p-1]} \binom{p}{j+1} X^j$$

ein Eisensteinpolynom.

- (4) Im Falle $R = \mathbf{Z}_{(p)}[\zeta_p]$, $r = \zeta_p - 1$, $s = \zeta_{p^2} - 1$ ist sowohl $R[s] = \mathbf{Z}_{(p)}[\zeta_{p^2}]$ ein diskreter Bewertungsring mit maximalem Ideal erzeugt von $s = \zeta_{p^2} - 1$ (cf. Blatt 4, Lösung zu Aufgabe 2 (b)), als auch

$$\mu_{\zeta_{p^2}-1, \mathbf{Q}(\zeta_p)}(X) = \mu_{\zeta_{p^2}, \mathbf{Q}(\zeta_p)}(X+1) = (X+1)^p - \zeta_p = \left(\sum_{j \in [1, p]} \binom{p}{j} X^j \right) - (\zeta_p - 1)$$

ein Eisensteinpolynom (wobei wir $\zeta_{p^2}^p = \zeta_p$ vereinbart haben).