

## Lösung 9

### Aufgabe 31.

Es ist  $\det F = \det \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = 8$  nicht quadratfrei. Damit allein kann man also noch nicht entscheiden, ob  $F$  in  $A_4$  primitiv ist. Die beschreibende Matrix bezüglich der Basis  $(e_1 - e_3, e_1 - e_2 + e_3 - e_4)$  von  $F$  und der Basis  $\underline{a} := (e_1 - e_2, e_2 - e_3, e_3 - e_4, e_4 - e_5)$  von  $A_4$  ist  $\begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ , und diese hat Elementarteilerform  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ . Mit Aufgabe 4 (2) ist  $F$  also primitiv in  $A_4$ .

Berechnen wir  $F^\perp$ , dargestellt in der Basis  $\underline{a}$ , als den Kern von

$$\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & -2 \\ -1 & 2 \\ 0 & -1 \end{pmatrix}$$

Vgl. Aufgabe 2 (1) für die Grammatrix bzgl.  $\underline{a}$ . Wir führen eine Elementarteilerformberechnung unter Mitführen der für die Zeilenumformungen verantwortlichen Matrix durch.

$$\left( \begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & -2 \\ 0 & 0 & 1 & 0 & -1 & 2 \\ 0 & 0 & 0 & 1 & 0 & -1 \end{array} \right) \rightsquigarrow \left( \begin{array}{cccc|cc} 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \end{array} \right) \rightsquigarrow \left( \begin{array}{cccc|cc} 1 & 0 & 1 & 4 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -2 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \end{array} \right) \rightsquigarrow \left( \begin{array}{cccc|cc} 0 & 0 & -1 & -2 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & 4 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{array} \right).$$

Der Kern  $F^\perp$  ergibt sich aus den zu den entstandenen Nullzeilen korrespondierenden Zeilen, i.e. den letzten beiden Zeilen. Er hat also z.B. als Basis, ausgedrückt in  $\underline{a}$ , die Zeilen von

$$\begin{pmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Somit ergibt sich

$$\det(F^\perp) = \det \left( \begin{pmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 4 & 0 \end{pmatrix} \right) = \det \begin{pmatrix} 28 & -4 \\ -4 & 2 \end{pmatrix} = 40.$$

Da nach der Lösung von Aufgabe 2 (2), oder, inzwischen besser, nach Beispiel nach (11.6) aus Vorlesung,  $\det A_4 = 5$ , erhalten wir mit  $c = 1$  nun in der Tat

$$\begin{aligned} (\det F)(\det A_4) &= 8 \cdot 5 \\ c^2(\det F^\perp) &= 1^2 \cdot 40. \end{aligned}$$

Es ist  $c = 1$  nun kein übergroßer Zufall, da ohnehin  $c \in \{1, 5\}$ .

### Aufgabe 32.

Zu  $\tilde{D}_n$ .

Sei  $n \geq 2$  und  $n \equiv_2 0$ . Wir behaupten, daß  $(e_2 - e_3, e_3 - e_4, \dots, e_{n-1} - e_n, 2e_n, \frac{1}{2} \sum_{i \in [1, n]} e_i)$  eine Basis von  $\tilde{D}_n$  ist. Lineare Unabhängigkeit folgt aus der oberen Dreiecksform der zugehörigen Matrix, wenn wir noch den letzten Eintrag nach vorne sortieren. Angesichts der Basis von  $D_n$  aus Aufgabe 2 (3) und der Definition  $\tilde{D}_n = D_n + \langle \frac{1}{2} \sum_{i \in [1, n]} e_i \rangle$  bleibt zu zeigen, daß  $e_1 - e_2$  im Erzeugnis der behaupteten Basis von  $\tilde{D}_n$  liegt. In der Tat ist

$$e_1 - e_2 = \left( \sum_{i \in [1, n]} e_i \right) - \left( \sum_{i \in [2, n-1]} i(e_i - e_{i+1}) \right) - (n/2)2e_n.$$

Die Grammatrix bezüglich der noch etwas modifizierten Basis

$$(e_2 - e_3, e_3 - e_4, \dots, e_{n-1} - e_n, e_{n-1} + e_n, \frac{1}{2} \sum_{i \in [1, n]} e_i)$$



**Aufgabe 33.**

- (1) Können wir zeigen, daß für  $x \in E_8$  stets  $q_b(x) = b(x, x) \equiv_2 0$  ist, so folgt  $E_8 \not\cong I_8$ , da diese Eigenschaft (ein *gerades Gitter* zu sein) für  $I_8$  nicht zutrifft und da diese Eigenschaft unter Isometrie erhalten bleibt. Wir lesen an der Grammatrixdiagonalen ab, daß  $q_b(b_i) \equiv_2 0$  für  $i \in [1, 8]$ . Es folgt  $q_b(\sum_i z_i b_i) \equiv_2 0$  für  $z_i \in \mathbf{Z}$  für  $i \in [1, 8]$ , da die gemischten Summanden in der distributiven Zerlegung ohnehin einen Faktor 2 enthalten.
- (2) Es genügt für  $E_8 \perp \langle -1 \rangle \simeq I_8 \perp \langle -1 \rangle$ , in  $E_8 \perp \langle -1 \rangle$  eine Orthogonalbasis  $(c_1, \dots, c_9)$  so anzugeben, daß  $q_b(c_i) = +1$  für  $i \in [1, 8]$  und  $q_b(c_9) = -1$ . Wir können hierzu sukzessive Vektoren  $v$  mit  $q_b(v) = 1$  orthogonal abspalten und uns auf die nachfolgende Betrachtung des jeweiligen Komplements beschränken. Bei der Angabe der Vektoren  $c_i$  werden wir Basen des jeweils aktuell zu betrachtenden Komplements verwenden. Die nach 8 solchen Schritten verbleibende Grammatrix in  $\mathbf{Z}^{1 \times 1}$  sollte dann gleich  $(-1)$  sein. (So der Prozeß überhaupt durchführbar ist, ist das dann schon wegen der Determinante der Fall.)

Bezeichne  $b_9$  einen Basisvektor von  $\langle -1 \rangle$  mit  $q_b(b_9) = -1$ .

Es hat  $E_8 \perp \langle -1 \rangle$  die Grammatrix

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Vgl. Aufgabe 32.

Es hat  $c_1 := (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ -1)$  den Wert  $q_b(c_1) = 1$ . Das orthogonale Komplement zu  $c_1$  hat das Zeilentupel von

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

als Basis, und diesbezüglich die Grammatrix

$$\begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \end{pmatrix}.$$

Es hat  $c_2 := (0\ 1\ 0\ 0\ 0\ 0\ 0\ 0)$  den Wert  $q_b(c_2) = 1$ . Das orthogonale Komplement zu  $c_2$  hat das Zeilentupel von

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

als Basis, und diesbezüglich die Grammatrix

$$\begin{pmatrix} 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \end{pmatrix}.$$

Es hat  $c_3 := (0\ 1\ 0\ 0\ 0\ 0\ 0)$  den Wert  $q_b(c_3) = 1$ . Das orthogonale Komplement zu  $c_3$  hat das Zeilentupel von

$$\begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

als Basis, und diesbezüglich die Grammatrix

$$\begin{pmatrix} 4 & 3 & -2 & 0 & 0 & 0 \\ 3 & 1 & -1 & 0 & 0 & 0 \\ -2 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & -1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Es hat  $c_4 := (0\ 1\ 0\ 0\ 0\ 0)$  den Wert  $q_b(c_4) = 1$ . Das orthogonale Komplement zu  $c_4$  hat das Zeilentupel von

$$\begin{pmatrix} 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

als Basis, und diesbezüglich die Grammatrix

$$\begin{pmatrix} 10 & 4 & -3 & -3 & 0 \\ 4 & 1 & -1 & -1 & 0 \\ -3 & -1 & 2 & 0 & 0 \\ -3 & -1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Es hat  $c_5 := (0\ 1\ 0\ 0\ 0)$  den Wert  $q_b(c_5) = 1$ . Das orthogonale Komplement zu  $c_5$  hat das Zeilentupel von

$$\begin{pmatrix} 1 & 0 & 0 & 4 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

als Basis, und diesbezüglich die Grammatrix

$$\begin{pmatrix} 18 & 5 & -8 & 4 \\ 5 & 1 & -2 & 1 \\ -8 & -2 & 4 & -1 \\ 4 & 1 & -1 & 2 \end{pmatrix}.$$

Es hat  $c_6 := (0\ 1\ 0\ 0)$  den Wert  $q_b(c_6) = 1$ . Das orthogonale Komplement zu  $c_6$  hat das Zeilentupel von

$$\begin{pmatrix} 1 & 0 & 0 & -5 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

als Basis, und diesbezüglich die Grammatrix

$$\begin{pmatrix} 28 & 6 & -15 \\ 6 & 1 & -3 \\ -15 & -3 & 8 \end{pmatrix}.$$

Es hat  $c_7 := (0\ 1\ 0)$  den Wert  $q_b(c_7) = 1$ . Das orthogonale Komplement zu  $c_7$  hat das Zeilentupel von

$$\begin{pmatrix} 1 & -6 & 0 \\ 0 & 3 & 1 \end{pmatrix}$$

als Basis, und diesbezüglich die Grammatrix

$$\begin{pmatrix} -8 & 3 \\ 3 & -1 \end{pmatrix}.$$

Es hat  $c_8 := (1\ 3)$  den Wert  $q_b(c_8) = 1$ . Das orthogonale Komplement zu  $c_8$  hat das Zeilentupel von

$$(0\ 1)$$

als Basis, und diesbezüglich die Grammatrix

$$(-1),$$

wie gewünscht.

Durchläuft man abermals die Konstruktion, so kann man auch eine Orthogonalbasis von  $E_8 \perp \langle -1 \rangle$  gewinnen, deren Elemente bezüglich der gewählten Basis dieses Gitters geschrieben sind, und die die richtigen  $q_b$ -Werte haben, i.e. achtmal  $+1$  und einmal  $-1$ . Eine solche Basis steht in den Zeilen von

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & -1 & 1 \\ 1 & 3 & 4 & 5 & 6 & 3 & 4 & -2 & 1 \\ 0 & 3 & 3 & 3 & 3 & 1 & 2 & -1 & 3 \end{pmatrix}.$$

### Aufgabe 34.

Zunächst bemerken wir, daß  $-\sum_{i \geq 0} a_i p^i = 1 + \sum_{i \geq 0} (p-1-a_i)p^i$ , wobei  $a_i \in [0, p-1]$ . Ist also  $a_0 \in [1, p-1]$ , so ist dieses Element bereits in Standarddarstellung.

Sei allgemein für  $m \in \mathbf{Z}$  teilerfremd zu  $p$  ein  $m$  mit  $p^k \equiv_m 1$  gefunden. Dies ist möglich, da  $p$  ein Element endlicher Ordnung in  $(\mathbf{Z}/m\mathbf{Z})^*$  repräsentiert.

Sei  $\xi := \sum_{i \geq 0} p^{ki} \in \mathbf{Z}_p$ . Es ist  $p^k \xi = \xi - 1$ , und also  $\xi = -(p^k - 1)^{-1}$ . Ist  $dm = p^k - 1$ , so ist  $\sum_{i \geq 0} dp^{ki} = -m^{-1}$ .

(1) Es ist  $7^1 \equiv_2 1$ , genauer,  $2 \cdot 3 = 7^1 - 1$ . Es folgt  $-2^{-1} = \sum_{i \geq 0} 3 \cdot 7^i$ , und also

$$2^{-1} = 1 + \sum_{i \geq 0} 3 \cdot 7^i = 4 \cdot 7^0 + 3 \cdot 7^1 + 3 \cdot 7^2 + 3 \cdot 7^3 + \dots$$

Zur Probe rechnen wir

$$\begin{aligned} & 8 \cdot 7^0 + 6 \cdot 7^1 + 6 \cdot 7^2 + 6 \cdot 7^3 + \dots \\ &= 1 \cdot 7^0 + 7 \cdot 7^1 + 6 \cdot 7^2 + 6 \cdot 7^3 + \dots \\ &= 1 \cdot 7^0 + 0 \cdot 7^1 + 7 \cdot 7^2 + 6 \cdot 7^3 + \dots \\ &= 1 \cdot 7^0 + 0 \cdot 7^1 + 0 \cdot 7^2 + 7 \cdot 7^3 + \dots \\ &= \dots = 1. \end{aligned}$$

(2) Es ist  $5^2 \equiv_3 1$ , genauer,  $3 \cdot 8 = 5^2 - 1$ . Es folgt

$$-3^{-1} = \sum_{i \geq 0} 8 \cdot 5^{2i} = 3 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + 1 \cdot 5^5 + 3 \cdot 5^6 + 1 \cdot 5^7 + \dots$$

Somit ist

$$3^{-1} = 2 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 + \dots$$

Zur Probe rechnen wir

$$\begin{aligned} & 6 \cdot 5^0 + 9 \cdot 5^1 + 3 \cdot 5^2 + 9 \cdot 5^3 + 3 \cdot 5^4 + 9 \cdot 5^5 + 3 \cdot 5^6 + 9 \cdot 5^7 + \dots \\ &= 1 \cdot 5^0 + 10 \cdot 5^1 + 3 \cdot 5^2 + 9 \cdot 5^3 + 3 \cdot 5^4 + 9 \cdot 5^5 + 3 \cdot 5^6 + 9 \cdot 5^7 + \dots \\ &= 1 \cdot 5^0 + 0 \cdot 5^1 + 5 \cdot 5^2 + 9 \cdot 5^3 + 3 \cdot 5^4 + 9 \cdot 5^5 + 3 \cdot 5^6 + 9 \cdot 5^7 + \dots \\ &= 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 10 \cdot 5^3 + 3 \cdot 5^4 + 9 \cdot 5^5 + 3 \cdot 5^6 + 9 \cdot 5^7 + \dots \\ &= 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 + 5 \cdot 5^4 + 9 \cdot 5^5 + 3 \cdot 5^6 + 9 \cdot 5^7 + \dots \\ &= \dots = 1. \end{aligned}$$

(3) Es ist  $5^4 \equiv_{13} 1$ , genauer  $13 \cdot 48 = 5^4 - 1$ . Es folgt

$$\begin{aligned} -13^{-1} &= \sum_{i \geq 0} 48 \cdot 5^{4i} \\ &= 3 \cdot 5^0 + 4 \cdot 5^1 + 1 \cdot 5^2 + 0 \cdot 5^3 \\ &\quad + 3 \cdot 5^4 + 4 \cdot 5^5 + 1 \cdot 5^6 + 0 \cdot 5^7 \\ &\quad + 3 \cdot 5^8 + 4 \cdot 5^9 + 1 \cdot 5^{10} + 0 \cdot 5^{11} \\ &\quad + \dots \end{aligned}$$

Somit ist

$$\begin{aligned} 13^{-1} &= 2 \cdot 5^0 + 0 \cdot 5^1 + 3 \cdot 5^2 + 4 \cdot 5^3 \\ &\quad + 1 \cdot 5^4 + 0 \cdot 5^5 + 3 \cdot 5^6 + 4 \cdot 5^7 \\ &\quad + 1 \cdot 5^8 + 0 \cdot 5^9 + 3 \cdot 5^{10} + 4 \cdot 5^{11} \\ &\quad + \dots \end{aligned}$$

Zur Probe rechnen wir

$$\begin{aligned}
 & 26 \cdot 5^0 + 0 \cdot 5^1 + 39 \cdot 5^2 + 52 \cdot 5^3 \\
 & + 13 \cdot 5^4 + 0 \cdot 5^5 + 39 \cdot 5^6 + 52 \cdot 5^7 \\
 & + 13 \cdot 5^8 + 0 \cdot 5^9 + 39 \cdot 5^{10} + 52 \cdot 5^{11} \\
 & + \dots \\
 = & 1 \cdot 5^0 + 0 \cdot 5^1 + 40 \cdot 5^2 + 52 \cdot 5^3 \\
 & + 13 \cdot 5^4 + 0 \cdot 5^5 + 39 \cdot 5^6 + 52 \cdot 5^7 \\
 & + 13 \cdot 5^8 + 0 \cdot 5^9 + 39 \cdot 5^{10} + 52 \cdot 5^{11} \\
 & + \dots \\
 = & 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 60 \cdot 5^3 \\
 & + 13 \cdot 5^4 + 0 \cdot 5^5 + 39 \cdot 5^6 + 52 \cdot 5^7 \\
 & + 13 \cdot 5^8 + 0 \cdot 5^9 + 39 \cdot 5^{10} + 52 \cdot 5^{11} \\
 & + \dots \\
 = & 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 \\
 & + 25 \cdot 5^4 + 0 \cdot 5^5 + 39 \cdot 5^6 + 52 \cdot 5^7 \\
 & + 13 \cdot 5^8 + 0 \cdot 5^9 + 39 \cdot 5^{10} + 52 \cdot 5^{11} \\
 & + \dots \\
 = & 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 \\
 & + 0 \cdot 5^4 + 0 \cdot 5^5 + 40 \cdot 5^6 + 52 \cdot 5^7 \\
 & + 13 \cdot 5^8 + 0 \cdot 5^9 + 39 \cdot 5^{10} + 52 \cdot 5^{11} \\
 & + \dots \\
 = & \dots = 1.
 \end{aligned}$$

### Aufgabe 35.

Kurze Zusammenfassung Hensel-Newton. Sei  $R$  ein vollständiger diskreter Bewertungsring mit Bewertung  $v$ . Sei  $f(X) \in R[X]$ . Taylor für Polynome, zu verifizieren für Monome, sagt, daß  $f(X + H) \equiv_{H^2} f(X) + Hf'(X)$ .

Sei  $x_0 \in R$  mit  $v(f(x_0)) - 2v(f'(x_0)) =: d_0 > 0$ . Setze  $x_{n+1} := x_n - f(x_n)/f'(x_n)$  für  $n \geq 0$ . Taylor gibt  $v(f'(x_n)) = v(f'(x_0))$ . Ferner gibt Taylor

$$v(f(x_{n+1})) - v(f(x_0)) \geq 2(v(f(x_n)) - v(f(x_0))) + d_0.$$

Das liefert mit Induktion eine untere Abschätzung

$$v(f(x_n)) \geq (2^n - 1)d_0 + v(f(x_0)).$$

Da  $v(x_{n+1} - x_{n+2}) > v(x_n - x_{n+1})$ , ist  $x_n \rightarrow \alpha$  (Cauchyfolge). Ferner ist  $f(x_n) \rightarrow 0$ . Da  $f$  Konvergenz erhält (betrachte Monome!), ist auch  $f(x_n) \rightarrow f(\alpha)$ , und insgesamt  $f(\alpha) = 0$ . Übrigens ist auch  $v(f'(x_n)) = v(f'(\alpha))$  stets.

Abermals da  $v(x_{n+2} - x_{n+1}) > v(x_{n+1} - x_n)$ , ist  $v(x_n - \alpha) = v(x_n - x_{n+1}) = v(f(x_n)) - v(f'(x_0))$ .

Merke: "Die Qualität von  $f(x_n)$  ist um genau  $v(f'(x_0))$  Stufen besser als die Qualität von  $x_n - \alpha$ ."

Als Abschätzung erhalten wir schließlich

$$v(x_n - \alpha) = v(f(x_n)) - v(f'(x_0)) \geq 2^n d_0 + v(f'(x_0)) = 2^n d_0 + v(f'(\alpha)).$$

- (1) Faktorisierung in  $\mathbf{Z}[X]$  gibt  $X^3 + X = X(X^2 + 1)$ . Dies liefert eine Nullstelle  $\alpha = 0$  in  $\mathbf{Z} \subseteq \mathbf{Z}_2$ . Wir behaupten, daß  $X^2 + 1$  keine Nullstelle in  $\mathbf{Z}_2$  hat. Dazu genügt es zu zeigen, daß modulo 4 keine Nullstelle vorliegt. Für  $x \in [0, 3]$  ist aber  $x^2 + 1 \not\equiv_4 0$ .

Beachte, daß mit  $f(X) = X^2 + 1$  und  $f'(X) = 2X$  zwar  $f(1) \equiv_2 0$ . Aber es ist genauer betrachtet  $v_2(f(1)) = 1$ , und  $v_2(f'(1)) = 1$ . Hensel-Newton findet also wegen  $v_2(f(1)) \leq 2v_2(f'(1))$  keine Anwendung.

(2) Mit  $f(X) := X^4 - X^2 + 1 \in \mathbf{Z}_{13}[X]$  ist  $f'(X) = 4X^3 - 2X$ .

Es ist  $v_{13}(f(\pm 2)) = v_{13}(13) = 1$ , und  $v_{13}(f'(\pm 2)) = v_{13}(\pm 28) = 0$ . Da  $v_{13}(f(2)) > 2 \cdot v_{13}(f'(2))$ , und da  $v_{13}(f(2)) - v_{13}(f'(2)) = 1$ , gibt es nach Newton-Hensel eine Nullstelle  $\alpha_1$  von  $f(X)$  in  $\mathbf{Z}_{13}$  mit  $\alpha_1 \equiv_{13^1} 2$ . Genauso gibt es eine Nullstelle  $\alpha_2$  von  $f(X)$  mit  $\alpha_2 \equiv_{13^1} -2$ .

Es ist  $v_{13}(f(\pm 6)) = v_{13}(1261) = 1$ , und  $v_{13}(f'(\pm 6)) = v_{13}(\pm 852) = 0$ . Da  $v_{13}(f(6)) > 2 \cdot v_{13}(f'(6))$ , und da  $v_{13}(f(6)) - v_{13}(f'(6)) = 1$ , gibt es nach Newton-Hensel eine Nullstelle  $\alpha_3$  von  $f(X)$  in  $\mathbf{Z}_{13}$  mit  $\alpha_3 \equiv_{13^1} 6$ . Genauso gibt es eine Nullstelle  $\alpha_4$  von  $f(X)$  mit  $\alpha_4 \equiv_{13^1} -6$ .

Da  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  modulo 5 paarweise verschieden sind, sind sie es auch in  $\mathbf{Z}_{13}$ . Ferner folgt durch eine Betrachtung modulo 5, daß  $\alpha_2 = -\alpha_1$  und  $\alpha_4 = -\alpha_3$ , da ja  $f(X) \in \mathbf{Z}_{13}[X^2]$ , und daher mit jeder Nullstelle auch ihr Negatives wieder eine Nullstelle ist.

Da  $\deg f = 4$  und da  $\mathbf{Z}_{13}$  ein Integritätsbereich ist, gibt es keine weiteren Nullstellen.

Zu den Näherungen. Sei  $x_0 \in \{2, 6\}$ . Es ist  $d_0 = 1$ , es ist  $v_{13}(f'(x_0)) = 0$ , und also

$$v_{13}(x_n - \alpha_i) \geq 2^n$$

Es genügt also,  $x_3$  zu betrachten.

Ist  $x_0 = 2$ , so wird  $x_3 \equiv_{13^7} 24995687$ .

Ist  $x_0 = 6$ , so wird  $x_3 \equiv_{13^7} 30926512$ .

Insgesamt werden

$$\begin{aligned} \alpha_1 &= 2 + 6 \cdot 13 + 2 \cdot 13^2 + 2 \cdot 13^3 + 4 \cdot 13^4 + 2 \cdot 13^5 + 5 \cdot 13^6 + \dots \\ \alpha_2 &= -\alpha_1 \\ \alpha_3 &= 6 + 1 \cdot 13 + 9 \cdot 13^2 + 10 \cdot 13^3 + 3 \cdot 13^4 + 5 \cdot 13^5 + 6 \cdot 13^6 + \dots \\ \alpha_4 &= -\alpha_3 \end{aligned}$$

(3) Mit  $f(X) := X^3 + 2X^2 - 2X + 4 \in \mathbf{Z}_2[X]$  ist  $f'(X) = 3X^2 + 4X - 2$ .

Es ist  $v_2(f(2)) = v_2(16) = 4$ , und  $v_2(f'(2)) = v_2(18) = 1$ . Da  $v_2(f(2)) > 2 \cdot v_2(f'(2))$ , und da  $v_2(f(2)) - v_2(f'(2)) = 3$ , gibt es nach Newton-Hensel eine Nullstelle  $\alpha$  von  $f(X)$  in  $\mathbf{Z}_2$  mit  $\alpha \equiv_{2^3} 2$ .

Um zu zeigen, daß es keine weitere Nullstelle gibt, spalten wir den Linearfaktor  $(X - \alpha)$  ab und erhalten

$$f(X)/(X - \alpha) = X^2 + (\alpha + 2)X + (\alpha^2 + 2\alpha - 2) =: h(X) \in \mathbf{Z}_2[X].$$

Mit  $x_0 = 2$  wissen wir, daß  $v_2(\alpha - 2) \geq v_2(f(x_0)) - v_2(f'(x_0)) = 3$ . Daher ist auch  $h(x) \equiv_8 x^2 + 4x + 6$ . Hätte  $f(X)$  eine weitere Nullstelle, so hätte  $h(X)$  eine Nullstelle  $\beta \in \mathbf{Z}_2$ , und also wäre  $0 = h(\beta) \equiv_8 \beta^2 + 4\beta + 6$ . Wir können hingegen (auch ohne Durchlaufen aller Elemente) ausschließen, daß  $X^2 + 4X + 6$  eine Nullstelle in  $\mathbf{Z}/8\mathbf{Z}$  hat. Denn diese läge notwendig in  $2\mathbf{Z}/8\mathbf{Z}$ . Dann aber liegt der Wert von  $X^2 + 4X$  in  $4\mathbf{Z}/8\mathbf{Z}$ , nicht aber 6.

Es hat  $f(X)$  also genau eine Nullstelle in  $\mathbf{Z}_2$ .

Zur Näherung. Sei  $x_0 = 2$ . Es ist  $d_0 = 2$ , es ist  $v_2(f'(x_0)) = 1$ , und also

$$v_2(x_n - \alpha) \geq 2^{n+1} + 1.$$

Es genügt also,  $x_2$  zu betrachten. Es wird  $x_2 \equiv_{2^7} 58$ . Also ist

$$\alpha = 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + \dots$$