Lösung zu (21)

(a) Für alle $z \in \mathbb{R}$ ist $z = sd + r$ mit $s = \lfloor \frac{z}{d} \rfloor$ und $r = z - s \cdot d$.
Dabei ist (per Def. von $\lfloor\ \rfloor$) $s \in \mathbb{Z}$ und es gilt $s \le \frac{z}{d} < s+1$.
Daraus folgt $sd \le z < sd + d$ und $0 \le z - sd < d$. Letzteres besagt: $r \in [0, d)$.
Falls mit $s, s' \in \mathbb{Z}$ und $r, r' \in [0,d)$ gilt: $z = sd + r = s'd + r'$, dann folgt: $|(s-s')d| = |r' - r| < d$. Da $s - s' \in \mathbb{Z}$ und $d \in \mathbb{N}_+$, folgt $r' = r$, $s' = s$.

(b) Mit $z \in \mathbb{R}$ und $\lambda \in \mathbb{Z}$ ist $\rho_d(z + \lambda d) = z + \lambda d - \lfloor \frac{z + \lambda d}{d} \rfloor d$
$= z + \lambda d - \left(\lfloor \frac{z}{d} \rfloor + \lambda \right) d = z - \lfloor \frac{z}{d} \rfloor d = \rho_d(z)$. Diese Eigenschaft entspricht 2.3 (b). Nun zu (c): Für alle $r \in [0,d)$ ist $\lfloor \frac{r}{d} \rfloor = 0$ und somit $\rho_d(r) = r$. (d) ergibt sich wie folgt: Für alle $z, z' \in \mathbb{Z}$ gilt:
$\rho_d(z+z') = z + z' - \lfloor \frac{z+z'}{d} \rfloor d = z + z' - \left(\lfloor \frac{z}{d} \rfloor + \lfloor \frac{z'}{d} \rfloor + e \right) d$ mit einem geeigneten $e \in \mathbb{Z}$. Mit Hilfe von (b) und (c) folgt jetzt:

$$\rho_d(z+z') \overset{(c)}{=} \rho_d(\rho_d(z+z')) \overset{(b)}{=} \rho_d\left(z + z' - \left(\lfloor \tfrac{z}{d} \rfloor + \lfloor \tfrac{z}{d} \rfloor \right) d\right)$$
$$= \rho_d(\rho_d(z) + \rho_d(z'))$$

(c) Mit den Parametern $d = 1$, $z = \frac{3}{2}$, $z' = \frac{2}{3}$ erhält man ein Gegenbeispiel, denn es ist dann $0 = \rho_1(1) = \rho_1\left(\frac{3}{2} \cdot \frac{2}{3}\right) \ne \rho_1\left(\rho_1\left(\frac{3}{2}\right) \cdot \rho_1\left(\frac{2}{3}\right)\right) = \rho_1\left(\frac{1}{2} \cdot \frac{2}{3}\right) = \frac{1}{3}$.

Lösung zu (23):

(a) Man berechnet zunächst $L=\{0_2, E_2, A, E_2+A\}$. Dabei ist $E_2+A=\begin{bmatrix}1&1\\1&0\end{bmatrix}=A^2$ und $A^3=E_2$. Offensichtlich ist $|L|=4$. Da $E_2\in L$ gilt (a) aus Definition 1.13; (b) und (d) gelten, da L ein $\mathbb{Z}_2$-Untervektorraum ist. Schließlich gilt auch (c), wie ein Blick auf die folgende Tafel zeigt:

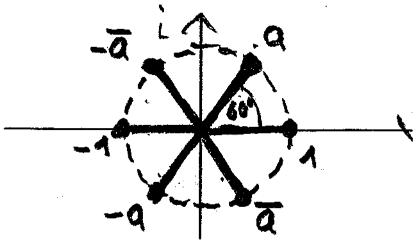
	0	E	A	A^2
0	0	0	0	0
E	0	E	A	A^2
A	0	A	A^2	E
A^2	0	A^2	E	A

(b) An der vorigen Tabelle erkennt man auch dass L ein Körper ist und dass $A^4=A$, $(A^2)^4=A^2$. Trivialerweise ist $E^4=E$, $0^4=0$.

(c) Das charakteristische Polynom von A ist $q=x^2+x+1$, und es ist $q(A)=0$. Also ist $q\cdot\mathbb{Z}_2[x]\subseteq \operatorname{Kern}\pi_A$. Zu einem $p\in\operatorname{Kern}\pi_A$ gibt es $s,r\in\mathbb{Z}_2[x]$ so, dass $p=sq+r$, wobei $r=0$ oder $\deg r<\deg q=2$ gilt. Sei etwa $r=ax+b$ mit $a,b\in\mathbb{Z}_2$. Wenn $r(A)=a\cdot A+bE=0$, dann folgt sofort $a=b=0$. Aus $0=p(A)=s(A)q(A)+r(A)=r(A)$ folgt also $r=0$ und somit $p\in q\cdot\mathbb{Z}_2[x]$. Insgesamt ergibt sich: $\operatorname{Kern}\pi_A=q\,\mathbb{Z}_2[x]$.

Lösung zu (24)

(a) Man berechnet $a^2 = -\bar{a}$ und entsprechend $a^3 = -\bar{a}a = -1$, $a^4 = -a$, $a^5 = \bar{a}$, $a^6 = 1$. Dies führt zu folgender Skizze:



und der Inklusion $\{1, a, -\bar{a}, -1, -a, \bar{a}\} \subseteq S$.

Da $a^6 = 1$, folgt $a^{6s} = 1$ für alle $s \in \mathbb{Z}$ und daher auch $a^z = a^{\rho_6(z)}$ für alle $z \in \mathbb{Z}$. Es folgt: $S = \{1, a, \dots, a^5\}$.

(b) Es gilt: $z \in \varphi^{-1}(1) \iff a^z = 1 \iff a^{\rho_6(z)} = 1 \iff \rho_6(z) = 0$

Daher ist $\varphi^{-1}(1) = 6\mathbb{Z}$.

(c) Ich definiere für $r, r' \in \mathbb{Z}_d$: $a^r \boxplus a^{r'} = a^{r+r'}$ und $a^r \boxdot a^{r'} = a^{r \cdot r'}$. Mit diesen Verknüpfungen gilt für alle $r, r', r'' \in \mathbb{Z}_d$ (und damit in der Form $a^r, a^{r'}, a^{r''}$ für beliebige Zahlen aus S):

$$a^r \boxdot (a^{r'} \boxplus a^{r''}) = a^r \boxdot (a^{r'+r''}) = a^{r\cdot(r'+r'')} = a^{r\cdot r' + r \cdot r''}$$
$$= a^r \boxdot a^{r'} \boxplus a^r \boxdot a^{r''}$$

(d) Offensichtlich gilt jetzt für alle $z, z' \in \mathbb{Z}$:

$$\varphi(z+z') = a^{z+z'} = a^{\rho_6(z)+\rho_6(z')} = a^{\rho_6(z)} \boxplus a^{\rho_6(z')} = a^z \boxplus a^{z'}$$

und

$$\varphi(z \cdot z') = a^{z\cdot z'} = a^{\rho_6(z)\cdot\rho_6(z')} = a^{\rho_6(z)} \boxdot a^{\rho_6(z')} = a^z \boxdot a^{z'}.$$

und $\varphi(1) = a$. Beachte dabei: $a^r \boxdot a^1 = a^{r\cdot 1} = a^r$ für $\in \mathbb{Z}_6$.

(e) $\varphi|_{\mathbb{Z}_6}$ ist bijektiv, $\varphi(1) = a$ und für alle $r, r' \in \mathbb{Z}_6$ gilt

$$\varphi(r \underset{\odot}{\oplus} r') = a^{\rho_6(r \underset{\cdot}{+} r')} = a^{r \underset{\cdot}{+} r'} = a^r \underset{\boxdot}{\boxplus} a^{r'}.$$