# Blatt 3

① a) Alle irred. Polynome vom Grad $\leq 4$ in $\mathbb{Z}_2[t]$ sind:

$t, \; t + [1]_2$

$t^2 + t + [1]_2$

$t^3 + t^2 + [1]_2, \quad t^3 + t + [1]_2$

$t^4 + t + [1]_2, \quad t^4 + t^3 + [1]_2,$

$t^4 + t^3 + t^2 + t + [1]_2$

Beweis: • Polynome vom Grad 1 sind über einem Körper immer irred.

• Polynome vom Grad 2, 3 sind über einem Körper genau dann irred., wenn sie keine Nullstelle haben (→ Test durch Einsetzen von $[0]_2$ und $[1]_2$)

• Da $\mathbb{Z}_2[t]$ faktoriell ist und es nur ein irred. Polynom vom Grad 2 gibt, ist ein Polynom vom Grad 4 genau dann irred., wenn es keine Nullstelle hat und nicht gleich ist zu

$$(t^2 + t + [1]_2)^2 = t^4 + t^2 + [1]_2$$

1 b) $K = \{0, 1, 2, t, t+1, t+2, 2t, 2t+1, 2t+2\}$

Beh: $t$ erzeugt $K^*$

Bew: Berechnung der Potenzen von $t$

$$t^2 = \underbrace{(t^2+t+2)}_{\in I} + 2t+1 = 2t+1 \mod I$$

$$t^3 = t \cdot t^2 = 2t^2+t = 2(2t+1)+t$$
$$= 2t+2 \mod I$$

$$t^4 = t \cdot t^3 = 2t^2+2t = 2(2t+1)+2t$$
$$= 2 \mod I$$

$$t^5 = t \cdot t^4 = 2t \mod I$$

$$t^6 = t \cdot t^5 = 2t^2 = 2(2t+1) = t+2 \mod I$$

$$t^7 = t \cdot t^6 = t^2+2t = 2t+1+2t$$
$$= t+1 \mod I$$

$$t^8 = t \cdot t^7 = t^2+t = 2t+1+t = 1 \mod I$$

Somit ist $t$ ein erzeugendes Element der multiplikativen Gruppe $K^*$

② a) $x \equiv 2 \mod 5$
$x \equiv 5 \mod 8$
$x \equiv 3 \mod 7$

wird genau von allen $x \in \mathbb{Z}$ der Form $x = 157 + k \cdot 280$, $k \in \mathbb{Z}$, gelöst.

Lösungsverfahren anwenden:

$5$, $7 \cdot 8 = 56$

$56 - 11 \cdot 5 = 1$

$8$, $5 \cdot 7 = 35$

$3 \cdot 35 - 13 \cdot 8 = 1$

$7$, $5 \cdot 8 = 40$

$3 \cdot 40 - 17 \cdot 7 = 1$

$\Rightarrow x \equiv 2 \cdot 56 + 5 \cdot 105 + 3 \cdot 120$
$= 997 \equiv 157 \mod 280$

b) Gesucht ist $a \in \mathbb{Z}$ mit $0 \leq a < 210$

und $a \equiv 2 \mod 5$
$a \equiv 2 \mod 7$
$a \equiv 5 \mod 6$

Lösen wie in a):

$17 \cdot 5 - 2 \cdot 42 = 1$
$13 \cdot 7 - 3 \cdot 30 = 1$
$6 \cdot 6 - 35 = 1$

$a \equiv 2 \cdot (-84) + 2 \cdot (-90) + 5 \cdot (-35)$
$= -523 \equiv 107 \mod 210$

$\Rightarrow \varphi([107]_{210}) = ([7]_5, [2]_7, [5]_6)$

(2) c) Sei $x$ die Anzahl der Tage mit dem 15. März

Ansatz $x \equiv 0 \mod 5$

$x \equiv 0 \mod 11$

$x \equiv 1 \mod 7$

$\Rightarrow x \equiv 0 \mod 55$

$8 \cdot 7 - 55 = 1$

$\Rightarrow x \equiv -55 \mod 385 = 5 \cdot 11 \cdot 7$

$\Rightarrow x = 330$ kleinste positive Lösung

330 Tage mit dem 15. März ergibt

den 7. Februar

③ Wir zeigen a) und b) zusammen, indem wir zeigen:

i) $m, n$ teilerfremd $\Rightarrow \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ als Ringe

ii) $m, n$ nicht teilerfremd $\Rightarrow \mathbb{Z}_{mn} \not\cong \mathbb{Z}_m \times \mathbb{Z}_n$ als abelsche Gruppen

Da ein Ringisomorphismus immer auch ein Gruppenisomorphismus ist, ist mit i), ii) alles gezeigt.

<u>zu i)</u> Das ist der chinesische Restsatz 5.1.25 mit $R = \mathbb{Z}$, $a_1 = m$, $a_2 = n$

<u>zu ii)</u> $s := \text{kgV}(m, n) < m \cdot n$ da $m, n$ nicht teilerfremd sind

$x = ([a]_m, [b]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$

$\Rightarrow s \cdot x = ([0]_m, [0]_n)$

$\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ ist nicht zyklisch

$\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ ist nicht zu der zyklischen Gruppe $\mathbb{Z}_{mn}$ isomorph

④ a) $\mathrm{Kern}(\Psi_1) = (9)_{\mathbb{Z}}$

b) $\mathrm{Kern}(\Psi_2) = (3)_{\mathbb{Z}}$

c) $\mathrm{Ker}(\Psi_3) = ((t-2)(t-1))_{\mathbb{R}[t]}$

d) $\mathrm{Ker}(\Psi_4) = (t-3)_{\mathbb{R}[t]}$

Bew: a) $n \in \mathrm{Ker}(\Psi_1) \Leftrightarrow \rho_n = 0$

$\Leftrightarrow [na]_9 = [0]_9$ für alle $a \in \{0, \dots, 8\}$

$\Leftrightarrow 9 \mid n$

$\Leftrightarrow n \in (9)_{\mathbb{Z}}$

b) $n \in \mathrm{Ker}(\Psi_2) \Leftrightarrow \rho_n = 0$

$\Leftrightarrow ([na]_3, [nb]_3) = ([0]_3, [0]_3)$

für alle $a, b \in \{1, 0, 2\}$

$\Leftrightarrow 3 \mid n \Leftrightarrow n \in (3)_{\mathbb{Z}}$

c) $f \in \mathrm{Ker}(\Psi_3) \Leftrightarrow f(\varphi_A) = 0$

$\Leftrightarrow f(A) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\chi_A = (t-2)(t-1)$

$$\Rightarrow \chi_A(A) = (A - 2E_2)(A - E_2)$$

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

Sei $\ker(\varphi_3) = (\mu_A)_{\mathbb{R}[t]}$

mit einem $\mu_A \in \mathbb{R}[t]$

($\mu_A$ existiert, da $\mathbb{R}[t]$ ein Hauptidealring ist und $\ker(\varphi_3)$ also ein Hauptideal sein muss)

$$\Rightarrow \mu_A \mid (t-1)(t-2)$$

$$f \in \{t-1, t-2\} \Rightarrow f(A) \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow \mu_A = (t-1)(t-2) = \chi_A$$

$$\Rightarrow \ker(\varphi_3) = ((t-1)(t-2))_{\mathbb{R}[t]}$$

d) Analog zu c), hier gilt aber

$$B - 3 \cdot E_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow f(B) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ mit } f = t-3$$

(wogegen $\chi_B = (t-3)^2$ ist!)

$$\Rightarrow \ker(\varphi_4) = (t-3)_{\mathbb{R}[t]}$$