

H25T2A4 geg:  $f \in \mathbb{Z}[x]$  mit  $f(1) = 1$  und  
 $f(2) = 2$

In Teil (a) wurde gezeigt, dass  $f(a) \equiv 1 \pmod{a-1}$   
und  $f(a) \equiv 2 \pmod{a-2}$  für alle  $a \in \mathbb{Z}$  mit  $a \geq 3$   
gilt.

zu (b) Voraussetzung:  $f(10) > 10$  z.zg:  $f(10) \geq 82$

Nach Teil (a), angewendet auf  $a=10$ , gilt

$$f(10) \equiv 1 \pmod{9} \text{ und } f(10) \equiv 2 \pmod{8}.$$

$\Rightarrow f(10)$  ist Lösung des Kongruenzsystems

$$x \equiv 1 \pmod{9}, x \equiv 2 \pmod{8}. \text{ Wegen } \text{ggT}(9, 8) =$$

$x \equiv 1 \pmod{9}$ ,  $x \equiv 2 \pmod{8}$ . Wegen  $\text{ggT}(9, 8) =$

1 ist der Chin. Restsatz (für Kongruenzen) anwendbar. Demnach existiert ein eind. bestimmtes  $c \in \{0, 1, \dots, 71\}$ , das das System löst. Wegen  $10 \equiv 1 \pmod{9}$  und  $10 \equiv 2 \pmod{8}$  ist  $c = 10 \Rightarrow$   
 $f(10) \equiv 10 \pmod{72} \Rightarrow \exists k \in \mathbb{Z}$  mit  $f(10) = 10 + 72k$ . Wegen  $f(10) > 10$  ist  $k \geq 1 \Rightarrow$   
 $f(10) = 10 + 72k \geq 10 + 72 \cdot 1 = 82$ .  $\square$

## F24T3A2 (Übung: H23T3A4)

(a) Bestimmen Sie die Anzahl der Lösungen von  
 $x^5 = a$  in  $\mathbb{Z}/8\mathbb{Z}$ ; für  $a \in \{0, 1, 2, 3\}$ .

(Erinnerung: In  $\mathbb{Z}/8\mathbb{Z}$  gilt  $1^2 = 3^2 = 5^2 = 7^2 = 1$ .)

$a=0$  Jede Lösung  $\bar{c}$  von  $x^2 = 0$  muss durch eine gerade Zahl repräsentiert werden. Einsetzen zeigt, dass  $0, 2, 4, 6$  Lösungen sind.

$a=1$  Der Repräsentant von jeder Lsg. muss ungerade sein.

Für jedes  $\bar{c} \in \mathbb{Z}/8\mathbb{Z}$  mit  $\bar{c} \in \{1, 3, 5, 7\}$  gilt

$$\bar{c}^5 = (\bar{c}^2)^2 \cdot \bar{c} = 1^2 \cdot \bar{c} = \bar{c} \Rightarrow \text{einzige Lösung: } 1$$

$$\bar{c}^5 = (\bar{c}^2)^2 \cdot \bar{c} = \bar{1}^2 \cdot \bar{c} = \bar{c} \Rightarrow \text{einzige Lösung: } \bar{1}$$

$a = \bar{2}$ : Für  $\bar{c} \in \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$  gilt  $\bar{c}^5 = \bar{0}$   
 $\Rightarrow x^2 = \bar{2}$  hat keine Lösung

$a = \bar{3}$ : Wegen  $\bar{c}^5 = \bar{c} \forall \bar{c} \in \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$   
ist  $\bar{3}$  die einzige Lösung.

(b) Bestimmen Sie die Anzahl der Lösungen

von  $x^5 = a$ ,  $a \in \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  in  $R = \mathbb{Z}/2024\mathbb{Z}$ .

$2024 = 8 \cdot 11 \cdot 23 = 2^3 \cdot 11 \cdot 23$ . Da die drei Faktoren 8, 11, 23 paarweise teilerfremd sind, existiert auf Grund des Chines. Restsatzes ein Isomorphismus von Ringen

$$\Phi: \mathbb{Z}/2024\mathbb{Z} \rightarrow \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}, c + 2024\mathbb{Z} \mapsto (c + 8\mathbb{Z}, c + 11\mathbb{Z}, c + 23\mathbb{Z})$$

Sei  $\bar{a} = a + 2024\mathbb{Z}$ , mit  $a \in \{0, 1, 2, 3\}$

Sei  $\mathcal{L} \subseteq \mathbb{Z}/2024\mathbb{Z}$  die Menge der Lösungen  
von  $x^5 = \bar{a}$  in  $\mathbb{Z}/2024\mathbb{Z}$ , und sei  $\mathcal{L}_m$  für  
 $m \in \{8, 11, 23\}$  jeweils die Menge der  
Lösungen von  $x^5 = a + m\mathbb{Z}$  in  $\mathbb{Z}/m\mathbb{Z}$

Beh:  $\bar{\Phi}(\mathcal{L}) = \mathcal{L}_8 \times \mathcal{L}_{11} \times \mathcal{L}_{23}$

denn: Sei  $c \in \mathbb{Z}$  und  $(\bar{u}, \bar{v}, \bar{w}) = \bar{\Phi}(c)$

Dann gilt die Äquivalenz

$$(\bar{u}, \bar{v}, \bar{w}) \in \bar{\Phi}(\mathcal{L}) \iff \bar{\Phi}(c + 2024\mathbb{Z}) \in \bar{\Phi}(\mathcal{L})$$

$\bar{\Phi}$  bij  $c + 2024\mathbb{Z} \in \mathcal{L} \iff (c + 2024\mathbb{Z})^2 = a + 2024\mathbb{Z}$

$\bar{\Phi}$  Kon  $\bar{\Phi}(c + 2024\mathbb{Z})^5 = (a + 8\mathbb{Z}, a + 11\mathbb{Z}, a + 23\mathbb{Z})$

$$\Leftrightarrow (\bar{u}, \bar{v}, \bar{w})^5 = (a+8\mathbb{Z}, a+11\mathbb{Z}, a+23\mathbb{Z})$$

$$\Leftrightarrow (\bar{u}^5, \bar{v}^5, \bar{w}^5) = (a+8\mathbb{Z}, a+11\mathbb{Z}, a+23\mathbb{Z})$$

$$\Leftrightarrow \bar{u}^5 = a+8\mathbb{Z}, \bar{v}^5 = a+11\mathbb{Z}, \bar{w}^5 = a+23\mathbb{Z}$$

$$\Leftrightarrow (\bar{u}, \bar{v}, \bar{w}) \in \mathbb{L}_8 \times \mathbb{L}_{11} \times \mathbb{L}_{23} \quad (\Rightarrow \text{Beh.})$$

Aus der Beh. folgt  $|\mathbb{L}| = |\mathbb{L}_8| \cdot |\mathbb{L}_{11}| \cdot |\mathbb{L}_{23}|$

Im Fall  $a=2$  ist  $\mathbb{L}_8 = \emptyset$  nach Teil (a)

$$\Rightarrow |\mathbb{L}_8| = 0 \Rightarrow |\mathbb{L}| = 0$$

Fall  $a=0$ : Da 11 und 23 Primzahlen sind, sind  $\mathbb{Z}/11\mathbb{Z}$  und  $\mathbb{Z}/23\mathbb{Z}$  Körper. In jedem Körper  $K$  hat die Gleichung  $x^5 = 0_K$  nur eine Lösung, nämlich  $x = 0_K$ .  $\Rightarrow |\mathbb{L}_{11}| = |\mathbb{L}_{23}| = 1$ .

$$\text{Teil (a)} \Rightarrow |\mathbb{L}_8| = 4 \Rightarrow |\mathbb{L}| = 4 \cdot 1 \cdot 1 = 4$$

2) Fall  $a=1$ . Für  $p \in \{11, 23\}$  sind die

Lösungen von  $x^5 = T$  in  $\mathbb{F}_p$  jeweils in  $\mathbb{F}_p^\times$  enthalten. Es handelt sich um die Elemente der Ordnung 1 oder 5 in  $\mathbb{F}_p^\times$ .

$|\mathbb{F}_{11}^\times| = 10$ . Die multiplikative Gruppe eines endl. Körpers ist zyklisch.  $\Rightarrow \mathbb{F}_{11}^\times$  ist eine zykl. Gruppe der Ordnung 10 und enthält wegen  $5|10$  genau eine (zykl.) Untgr. der Ordnung 5. In dieser gibt es genau  $\varphi(5) = 4$  Elemente der Ordnung 5, also genau 5 Elemente der Ordnung 1 oder 5.  $\Rightarrow |\mathbb{Z}_{11}| = 5$

$|\mathbb{F}_{23}^\times| = 22$ ,  $5 \nmid 22 \Rightarrow \mathbb{F}_{23}^\times$  hat keine Elemente der Ordnung 5, und  $T$  ist einziges Ele-

ment sind,  
jedem Körper  
Lösung,

= 1

= 4



ment der Ordnung 1  $\Rightarrow |\mathbb{Z}_{23}| = 1$

$$\text{Ter}(a) \Rightarrow |\mathbb{Z}_8| = 1 \Rightarrow |\mathbb{Z}| = 1 \cdot 5 \cdot 1 = 5$$

Fall  $a=3$  Einsetzen zeigt, dass  $x^5 = \bar{3}$  in  $\mathbb{F}_{11}$   
keine Lösung hat  $\Rightarrow |\mathbb{Z}| = |\mathbb{Z}_8| \cdot 0 \cdot |\mathbb{Z}_{23}| = 0$ .

zu (c) Bestimmen Sie die Anzahl der 5-ten  
Potenzen in  $\mathbb{Z}/2024\mathbb{Z}$

Sei  $P$  die Menge der 5-ten Potenzen in  
 $\mathbb{Z}/2024\mathbb{Z}$  und  $P_m$  die Menge der 5-ten  
Potenzen in  $\mathbb{Z}/m\mathbb{Z}$ , für  $m \in \{8, 11, 23\}$

$$\in \Phi(\mathbb{Z}) \quad \text{Beh.: } \Phi(P) = P_8 \times P_{11} \times P_{23}$$

$$\mathbb{Z}^2 = a + 2024\mathbb{Z}$$

Beweis: Übung



Bestimmung von  $|P_8|$ :  $c^5 = \bar{0}$  für  
 $c \in \{0, 2, 4, 6\}$ ,  $c^5 = c$  für  $c \in \{1, 3, 5, 7\}$   
 $\Rightarrow P_8 = \{0, 1, 3, 5, 7\}$   
 $\Rightarrow |P_8| = 5$

Bestimmung von  $|P_{11}|$ :

$$\bar{0}^5 = \bar{0} \Rightarrow \bar{0} \in P_{11}$$

Für jedes  $c \in \mathbb{F}_{11}^\times$  gilt  $(c^5)^2 = c^{10} = 1$   
wegen  $|\mathbb{F}_{11}^\times| = 10 \Rightarrow$  Die fünften Potenzen  
in  $\mathbb{F}_{11}^\times$  sind Lösungen von  $x^2 = 1$ . Da  $\mathbb{F}_{11}$

ein Körper ungerader Char. ist, sind  $\{ \pm \bar{1} \}$  die einzigen beiden Lösungen dieser Gleichung

$$\bar{1}^5 = \bar{1}, (-\bar{1})^5 = -\bar{1} \Rightarrow P_n = \{ \bar{0}, \bar{1}, -\bar{1} \} \\ \rightarrow |P_n| = 3$$

Bestimmung von  $|P_{23}|$ :  $\bar{0}^5 = \bar{0} \Rightarrow \bar{0} \in P_{23}$

Da  $\mathbb{F}_{23}^\times$  zyklisch ist, existiert ein  $c \in \mathbb{F}_{23}^\times$   
mit  $\mathbb{F}_{23}^\times = \langle c \rangle$   $\text{ord}(c) = |\mathbb{F}_{23}^\times| = 22$ ,  
 $\text{ggT}(5, 22) = 1 \Rightarrow \text{ord}(c^5) = 22$

$$\langle c^5 \rangle \subseteq \mathbb{F}_{23}^\times, |\langle c^5 \rangle| = 22 = |\mathbb{F}_{23}^\times| \Rightarrow \mathbb{F}_{23}^\times =$$

$$\langle c^5 \rangle = \{ (c^5)^k \mid k \in \mathbb{Z} \} = \{ (c^k)^5 \mid k \in \mathbb{Z} \}.$$

$\Rightarrow$  Alle Elemente von  $F_{23}^\times$  sind 5-te Potenzen

$$\Rightarrow P_{23} = F_{23}^\times \Rightarrow |P_{23}| = 23$$

$$\text{insgesamt: } |P| = |P_8| \cdot |P_4| \cdot |P_{23}| = 5 \cdot 3 \cdot 23 \\ = 15 \cdot 23 = 345$$

□

H24T3A2 Sei  $R = \mathbb{Z}[x] / (x^3 + x)$

(a) Zeigen Sie:  $R \cong \mathbb{Z} \times \mathbb{Z}[i]$

$$x^3 + x = x(x^2 + 1) \rightarrow (x^3 + x) = (x) \cdot (x^2 + 1)$$

Die Ideale  $I = (x)$  und  $J = (x^2 + 1)$  in  $\mathbb{Z}[x]$  sind teilerfremd, denn:  $1 = (-x) \cdot x + 1 \cdot (x^2 + 1) \in I + J \Rightarrow I + J = (1)$

Nach dem Chines. Restsatz existiert somit ein Isom.

$$\Phi: R \rightarrow \mathbb{Z}[x]/I \times \mathbb{Z}[x]/J, a + (f) \mapsto (a + I, a + J),$$

wobei  $f = x^3 + x$ .

Beh.  $\mathbb{Z}[x]/I \cong \mathbb{Z}, \mathbb{Z}[x]/J \cong \mathbb{Z}[i]$

Wir wenden den Homomorphiesatz für Ringe  
auf die Einsetzungshomomorphismen

$$\rho_0: \mathbb{Z}[x] \rightarrow \mathbb{Z}, g \mapsto g(0) \text{ und}$$

$$\rho_i: \mathbb{Z}[x] \rightarrow \mathbb{Z}[i], h \mapsto h(i) \text{ an.}$$

zu überprüfen: (1)  $\rho_0, \rho_i$  sind surjektiv

$$(2) \ker(\rho_0) = I, \ker(\rho_i) = J$$

zu (1) Für jedes  $a \in \mathbb{Z}$  gilt  $\rho_0(a) = a$ .

$\Rightarrow \rho_0$  ist surjektiv.

Sei  $x \in \mathbb{Z}[i]$ .  $\Rightarrow \exists a, b \in \mathbb{Z}$  mit  $x = a + bi$ .

$$\Rightarrow \rho_i(a + bi) = a + bi = x.$$

Also ist auch  $\rho_i$  surjektiv.

zu (2) Für jedes  $f = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$  mit  $a_0, \dots, a_n \in \mathbb{Z}, n \in \mathbb{N}_0$ , gilt die Äquivalenz  
 $f \in \ker(\rho_0) \iff f(0) = 0 \iff a_0 = 0 \iff$   
 $f$  ist Vielfaches von  $x$  in  $\mathbb{Z}[x] \iff f \in (x)$ .  
 also:  $\ker(\rho_0) = (x) = \mathbb{I}$

$$\rho_i(x^2+1) = i^2+1 = (-1)+1 = 0 \implies x^2+1 \in \ker(\rho_i)$$

$$\implies \mathcal{J} = (x^2+1) \subseteq \ker(\rho_i)$$

Sei umgekehrt  $g \in \ker(\rho_i) \implies g(1) = 0$   
 $\xRightarrow{g \in \mathbb{Q}[x]}$   $g$  ist Vielfaches des Minimalpolynoms  
 $M_{i,\mathbb{Q}}$  von  $i$  über  $\mathbb{Q}$ . Bekanntlich ist  $M_{i,\mathbb{Q}} = x^2+1$   
 $\implies (x^2+1) \mid g$ . Da  $x^2+1, g \in \mathbb{Z}[x]$  gilt,  
 $x^2+1$  ein Teil von  $g$  in  $\mathbb{Q}[x]$  und  $x^2+1$  als

normiertes Polynom primitiv ist,

folgt  $(x^2+1) \mid g$  in  $\mathbb{Z}[x]$ .  $\Rightarrow$

$g$  liegt in  $\mathcal{I} = (x^2+1)$ !

Auf Grund des Homomorphiesatzes existieren

also Ringisomorphismen  $\bar{\rho}_0: \mathbb{Z}[x]/\mathcal{I} \rightarrow \mathbb{Z}$ ,

$g+\mathcal{I} \mapsto g(0)$  und  $\bar{\rho}_1: \mathbb{Z}[x]/\mathcal{I} \rightarrow \mathbb{Z}[i]$ ,  
 $h+\mathcal{I} \mapsto h(i)$

Insgesamt erhalten wir ein Isom.

$\alpha: R \rightarrow \mathbb{Z} \times \mathbb{Z}[i], g+(x^2+1)x \mapsto (g(0), g(i))$