

## 10. MODULORECHNEN

In diesem Kapitel sind Ringe immer kommutative Ringe mit 1. Erinnerung: Ein kommutativer Ring mit 1 ist ein Modell der Ringaxiome  $RT_0 - RT_8$ , also eine  $\mathcal{L}_{RT}$ -Struktur mit Bereich  $R$ , wobei  $\mathcal{L}_{RT} = \{0, 1, +, \cdot\}$ . Wie üblich identifizieren wir einen Ring  $(R, 0, 1, +, \cdot)$  mit seinem Bereich  $R$ , oder wir schreiben  $(R, +, \cdot)$  um auch die binären Operationen hervorzuheben.

### IDEALE

Sei  $(R, 0, 1, +, \cdot)$  ein kommutativer Ring. Eine Menge  $I \subseteq R$  ist ein **Ideal** in  $R$ , falls die folgenden Bedingungen erfüllt sind:

- (I<sub>0</sub>)  $I \neq \emptyset$
- (I<sub>1</sub>)  $\forall a, b \in I (a + b \in I)$
- (I<sub>2</sub>)  $\forall x \in R \forall a \in I (x \cdot a \in I)$

Da mit  $1 \in R$  auch  $-1 \in R$  ist, folgt aus (I<sub>2</sub>), dass mit jedem  $a \in I$  auch  $(-1) \cdot a = -a$  in  $I$  ist. Mit (I<sub>0</sub>) und (I<sub>1</sub>) ist das Ideal also eine additive Untergruppe von  $R$ , d. h. eine Untergruppe der abelschen Gruppe  $(R, 0, +)$ . Ist  $1 \in I$ , so ist  $I = R$  (also ein Ring), ist aber  $1 \notin I$  und  $I \neq \{0\}$ , so ist  $I$  kein Unterring von  $R$  (nicht-triviale Unterringe von  $R$  müssen die 1 enthalten). Beachte, dass  $\{0\}$  ein Ring mit 1 ist – in  $\{0\}$  gilt  $0 = 1$ .

Jeder Ring  $R$  besitzt die beiden *trivialen* Ideale  $R$  und  $\{0\}$ ; das Ideal  $\{0\}$  heisst **Nullideal**. Wie wir später sehen werden, sind Körper dadurch charakterisiert, dass sie nur die trivialen Ideale enthalten.

*Beispiele:* (a) Für  $m \in \mathbb{Z}$  sei

$$m\mathbb{Z} := \{x \cdot m : x \in \mathbb{Z}\}.$$

Dann ist  $m\mathbb{Z}$  ein Ideal im Ring  $(\mathbb{Z}, 0, 1, +, \cdot)$ . Denn mit  $xm \in m\mathbb{Z}$  ist auch  $y \cdot (xm) = (yx) \cdot m \in m\mathbb{Z}$ , und mit  $xm, ym \in m\mathbb{Z}$  ist auch  $xm + ym = (x + y)m \in m\mathbb{Z}$ .

(b) Sei  $\mathbb{Z}[X]$  der Ring der Polynome mit Koeffizienten in  $\mathbb{Z}$  (siehe Aufgabe 11), und sei  $f \in \mathbb{Z}[X]$ , zum Beispiel  $f = 1 - X^2 + 7X^3$ . Dann ist

$$(f) := \{g \cdot f : g \in \mathbb{Z}[X]\}$$

ein Ideal in  $\mathbb{Z}[X]$ : Nach Definition sind (I<sub>0</sub>) und (I<sub>2</sub>) erfüllt, und weil  $\mathbb{Z} \subseteq \mathbb{Z}[X]$ , ist mit (I<sub>2</sub>) auch (I<sub>1</sub>) erfüllt.

Für Beispiel (a) gilt auch eine Art Umkehrung.

**PROPOSITION 10.1.** *Ist  $I \subseteq \mathbb{Z}$  ein Ideal, dann existiert ein  $m \in \mathbb{Z}$ , sodass gilt:*

$$I = m\mathbb{Z}$$

*Beweis.* Ist  $I$  das Nullideal, so ist  $I = 0\mathbb{Z}$  und wir sind fertig. Ist  $I \neq \{0\}$ , so enthält  $I$  mit (I<sub>2</sub>) positive Zahlen. Sei

$$m := \min \{n \in \mathbb{N} \setminus \{0\} : n \in I\}.$$

Wir zeigen  $I = m\mathbb{Z}$ . Für einen Widerspruch nehmen wir an, dass ein  $a \in I$  existiert mit  $a \notin m\mathbb{Z}$ . Wir dürfen annehmen, dass  $a > 0$ , denn mit  $a \in I$  ist immer auch  $-a \in I$ . Nach Definition von  $m$  ist  $m < a$ . Sei  $d := \text{ggT}(a, m)$ . Dann ist  $1 \leq d < m$ , weil  $a \notin m\mathbb{Z}$ . Mit dem vEA finden wir  $k, l \in \mathbb{Z}$  mit  $ka + lm = d$ . Aus (I<sub>2</sub>) folgt, dass sowohl  $ka$  wie auch  $lm$  in  $I$  sind, und mit (I<sub>1</sub>) ist somit auch  $ka + lm$ , also  $d < m$  in  $I$ , was aber der Definition von  $m$  widerspricht. –

## FAKTORRINGE

Sei  $R$  ein kommutativer Ring und sei  $I \subseteq R$  ein Ideal, zum Beispiel  $R = \mathbb{Z}$  und  $I = m\mathbb{Z}$  für ein  $m \in \mathbb{Z}$ . Für  $x \in R$  definieren wir die sogenannte **Restklasse** von  $x$  durch

$$\bar{x} := x + I = \{x + a : a \in I\}.$$

Weiter definieren wir auf  $R$  die binäre Relation “ $\sim$ ” durch:

$$x \sim y \iff \bar{x} = \bar{y}$$

Weil “ $=$ ” eine Äquivalenzrelation ist, ist auch “ $\sim$ ” eine Äquivalenzrelation. Gilt  $x \sim y$ , so sagen wir “ $x$  ist kongruent  $y$  modulo  $I$ ” und schreiben

$$x \equiv y \pmod{I}.$$

Sei  $R/I := \{\bar{x} : x \in R\}$  (gesprochen “ $R$  modulo  $I$ ”) die Menge der Äquivalenzklassen. Auf  $R/I$  definieren wir die beiden binären Operationen  $\oplus$  und  $\otimes$  auf Repräsentanten von Äquivalenzklassen wie folgt:

$$\bar{x} \oplus \bar{y} := \overline{x + y} \quad \text{und} \quad \bar{x} \otimes \bar{y} := \overline{x \cdot y}$$

Das folgenden Lemma zeigt, dass die Operationen  $\oplus$  und  $\otimes$  wohldefiniert (d. h. unabhängig von der Wahl der Repräsentanten) sind.

**LEMMA 10.2.** Seien  $x_0, x_1, y_0, y_1 \in R$ , sodass gilt  $\bar{x}_0 = \bar{x}_1$  und  $\bar{y}_0 = \bar{y}_1$ . Dann gilt:

$$\bar{x}_0 \oplus \bar{y}_0 = \bar{x}_1 \oplus \bar{y}_1 \quad \text{und} \quad \bar{x}_0 \otimes \bar{y}_0 = \bar{x}_1 \otimes \bar{y}_1$$

*Beweis.* Beachte, dass für alle  $x, y \in R$  gilt:

$$x \in I \Rightarrow (x + I) = I \quad \text{und} \quad x + I = y + I \iff x - y \in I$$

$\oplus$  ist wohldefiniert: Seien nun  $x_0, x_1, y_0, y_1 \in R$ , sodass gilt  $\bar{x}_0 = \bar{x}_1$  und  $\bar{y}_0 = \bar{y}_1$ . Es gilt nun:

$$\begin{aligned} \overline{x_0 + y_0} &= (x_0 + y_0) + I = (x_0 + I) + (y_0 + I) = \\ &= \left(x_0 + \underbrace{((x_1 - x_0) + I)}_{\in I}\right) + \left(y_0 + \underbrace{((y_1 - y_0) + I)}_{\in I}\right) = \\ &= (x_1 + I) + (y_1 + I) = (x_1 + y_1) + I = \overline{x_1 + y_1} \end{aligned}$$

Somit ist  $\overline{x_0 + y_0} = \overline{x_1 + y_1}$ , d. h.  $\bar{x}_0 \oplus \bar{y}_0 = \bar{x}_1 \oplus \bar{y}_1$ .

$\otimes$  ist wohldefiniert: Weil nach Voraussetzung  $\bar{x}_0 = \bar{x}_1$  und  $\bar{y}_0 = \bar{y}_1$ , gilt  $x_0 - x_1 \in I$  und  $y_0 - y_1 \in I$ . Somit haben wir

$$\left. \begin{aligned} x_0 \cdot (y_0 - y_1) &= x_0 y_0 - x_0 y_1 \in I \\ y_1 \cdot (x_0 - x_1) &= -x_1 y_1 + x_0 y_1 \in I \end{aligned} \right\} \Rightarrow (x_0 y_0 - x_1 y_1) \in I,$$

woraus folgt  $x_0 y_0 + I = x_1 y_1 + I$ , d. h.  $\overline{x_0 \cdot y_0} = \overline{x_1 \cdot y_1}$ . Somit ist  $\bar{x}_0 \otimes \bar{y}_0 = \bar{x}_1 \otimes \bar{y}_1$ .  $\dashv$

Mit Lemma 10.2 können wir die Ringstruktur vom Ring  $R$  auf  $R/I$  übertragen und erhalten, dass  $(R/I, \bar{0}, \bar{1}, \oplus, \otimes)$  ein kommutativer Ring ist (den Beweis lassen wir weg). Der Ring  $R/I$  ist ein sogenannter **Faktorring**.

DIE RINGE  $\mathbb{Z}_m$ 

In diesem Abschnitt betrachten wir den Faktorring  $\mathbb{Z}/I$ , wobei  $I \subseteq \mathbb{Z}$  ein Ideal ist, d. h.  $I = m\mathbb{Z}$  für ein  $m \in \mathbb{Z}$ . Die Elemente von  $\mathbb{Z}/I$  bezeichnen wir wieder mit  $\bar{x}, \bar{y}, \dots$ , aber anstelle von “ $\oplus$ ” und “ $\otimes$ ” schreiben wir “+” bzw. “ $\cdot$ ”, wobei wir den Multiplikationspunkt wie üblich auch manchmal weglassen. Da Ideale  $I \subseteq \mathbb{Z}$  immer von der Form  $I = m\mathbb{Z}$  sind für ein  $m \in \mathbb{Z}$ , schreiben wir  $\mathbb{Z}_m$  anstelle von  $\mathbb{Z}/m\mathbb{Z}$ .

Für  $m \geq 1$  ist somit  $\mathbb{Z}_m$  ein Ring mit den  $m - 1$  Elementen  $\bar{0}, \dots, \overline{m-1}$ , insbesondere ist  $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z}$  der Nullring  $\{\bar{0}\}$ . Weiter ist  $(\mathbb{Z}_m, \bar{0}, +)$  eine zyklische Gruppe, denn  $\mathbb{Z}_m$  wird durch 1 erzeugt, d. h.  $\mathbb{Z}_m = \langle \bar{1} \rangle$ . Andererseits ist für  $m \geq 2$ ,  $(\mathbb{Z}_m \setminus \{\bar{0}\}, \bar{1}, \cdot)$  im Allgemeinen keine Gruppe (z. B. hat  $\bar{6}$  in  $\mathbb{Z}_{15}$  kein multiplikativ Inverses). Mit der folgenden Proposition lassen sich die Elemente von  $\mathbb{Z}_m$  bestimmen, welche ein multiplikativ Inverses haben.

**PROPOSITION 10.3.** *Sei  $m \geq 2$  und sei  $\bar{a} \in \mathbb{Z}_m$ . Dann existiert genau dann ein  $\bar{b} \in \mathbb{Z}_m$  mit  $\bar{a} \cdot \bar{b} = \bar{1}$ , wenn  $\text{ggT}(a, m) = 1$ .*

*Beweis.* Sei  $d := \text{ggT}(a, m)$ . Existiert ein  $\bar{b} \in \mathbb{Z}_m$  mit  $\bar{a} \cdot \bar{b} = \bar{1}$ , so erhalten wir  $ab = ml + 1$  für ein  $l \in \mathbb{Z}$ . Aus  $d \mid a$  und  $d \mid m$  folgt dann  $d \mid (ab - ml)$ , d. h.  $d \mid 1$ . Somit muss  $d = 1$  sein.

Ist nun  $\text{ggT}(a, m) = 1$ , so finden wir mit dem vEA Zahlen  $b, l \in \mathbb{Z}$  mit  $ab + ml = 1$ . Das heisst  $ab \equiv 1 \pmod{m}$ , woraus folgt  $\overline{ab} = \bar{a} \cdot \bar{b} = \bar{1}$ . ←

Wenn wir nur die Elemente aus  $\mathbb{Z}_m \setminus \{\bar{0}\}$  betrachten, welche ein multiplikativ Inverses haben, so bilden diese Elemente bezüglich der Multiplikation eine Gruppe, die sogenannte **Einheitengruppe** des Rings  $\mathbb{Z}_m$ , welche wir mit  $\mathbb{Z}_m^*$  bezeichnen. Um zu sehen, dass  $\mathbb{Z}_m^*$  eine multiplikative Gruppe ist, genügt es zu zeigen, dass mit  $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$  auch  $\overline{ab}$  in  $\mathbb{Z}_m^*$  ist. Das folgt aber direkt aus den Eigenschaften des ggT, denn wenn  $\text{ggT}(a, m) = 1$  und  $\text{ggT}(b, m) = 1$ , dann ist auch  $\text{ggT}(ab, m) = 1$ . Die Ordnung der Gruppe  $\mathbb{Z}_m^*$  wird mit  $\varphi(m)$  bezeichnet, also  $\varphi(m) := |\mathbb{Z}_m^*|$  und  $\varphi$  heisst **Euler’sche  $\varphi$ -Funktion**. Aus Korollar 9.15 erhalten wir den folgenden Satz:

**EULER’SCHER SATZ.** *Für  $m \geq 2$  und  $\text{ggT}(a, m) = 1$  gilt:*

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \text{bzw.} \quad m \mid a^{\varphi(m)} - 1$$

*Beweis.* Ist  $\text{ggT}(a, m) = 1$ , so ist  $\bar{a} \in \mathbb{Z}_m^*$ . Weil nun  $|\mathbb{Z}_m^*| = \varphi(m)$ , erhalten wir mit Korollar 9.15,  $\overline{a^{\varphi(m)}} = \bar{1}$ . Somit ist  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . ←

Als Spezialfall des Euler’schen Satzes erhalten wir den folgenden Satz:

**KLEINER SATZ VON FERMAT.** *Für  $p$  prim und  $\text{ggT}(a, p) = 1$  gilt:*

$$a^p - a \equiv 0 \pmod{p}$$

*Beweis.* Ist  $p$  prim, so ist  $\mathbb{Z}_p^* = \{\bar{1}, \dots, \overline{p-1}\}$ , also  $\varphi(p) = p - 1$ . Ist  $\text{ggT}(a, m) = 1$ , was gleichbedeutend ist mit  $\bar{a} \neq \bar{0}$ , so gilt mit dem Euler’schen Satz

$$a^{p-1} \equiv 1 \pmod{p}.$$

Weil nun  $a \cdot a^{p-1} = a^p$ , gilt somit

$$a^p \equiv a \pmod{p}$$

was zu zeigen war. ←

## DER CHINESISCHE RESTSATZ

CHINESISCHER RESTSATZ. Seien  $m_0, \dots, m_k \in \mathbb{Z}$  positive, paarweise teilerfremde Zahlen und seien  $a_0, \dots, a_k \in \mathbb{Z}$ . Dann gibt es eine Zahl  $n \in \mathbb{Z}$ , sodass für alle  $0 \leq i \leq k$  gilt:

$$n \equiv a_i \pmod{m_i}$$

Algorithmus zur Berechnung von  $n$ . Wir illustrieren den Algorithmus zur Berechnung eines solchen  $n$  an einem Beispiel, in dem wir die kleinste positive solche Zahl  $n$  berechnen: Seien  $m_0 = 7$ ,  $m_1 = 10$ ,  $m_2 = 13$ , und seien  $a_0 = 5$ ,  $a_1 = 7$ ,  $a_2 = 10$ . Es ist also eine Zahl  $n$  zu finden, für die gilt:

$$\begin{aligned} n &\equiv 5 \pmod{7} \\ n &\equiv 7 \pmod{10} \\ n &\equiv 10 \pmod{13} \end{aligned}$$

Wir betrachten zuerst die ersten beiden Bedingungen. Für  $n$  muss gelten:  $n = k \cdot 7 + 5$  und  $n = l \cdot 10 + 7$ , d. h.

$$k \cdot 7 + 5 = l \cdot 10 + 7 \iff k \cdot 7 = l \cdot 10 + 2 \iff k \cdot 7 - l \cdot 10 = 2$$

Wir suchen zuerst Zahlen  $k'$  und  $l'$  mit  $k' \cdot 7 - l' \cdot 10 = 1$ . Mit dem vEA erhalten wir:

$$\begin{aligned} 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

		1	2	3
<b>0</b>	<b>1</b>	1	3	10
<b>1</b>	<b>0</b>	1	2	7

Somit ist  $k' = 3$  und  $l' = 2$ , also  $k = 2 \cdot k' = 6$  und  $l = 2 \cdot l' = 4$ , und wir erhalten  $n = 6 \cdot 7 + 5 = 47$ . Für jede Zahl  $n = s \cdot 70 + 47$  ist  $n \equiv 5 \pmod{7}$  und  $n \equiv 7 \pmod{10}$ . Damit die dritte Bedingung erfüllt ist, muss gelten  $n = t \cdot 13 + 10$ , d. h.

$$s \cdot 70 + 47 = t \cdot 13 + 10 \iff s \cdot 70 + 37 = t \cdot 13 \iff t \cdot 13 - s \cdot 70 = 37.$$

Wir suchen wieder zuerst Zahlen  $s'$  und  $t'$  mit  $t' \cdot 13 - s' \cdot 70 = 1$ , welche wir wieder mit dem vEA erhalten:

$$\begin{aligned} 70 &= 5 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

		5	2	1	1	2
<b>0</b>	<b>1</b>	5	11	16	27	70
<b>1</b>	<b>0</b>	1	2	3	5	13

Somit ist  $t' = 27$  und  $s' = 5$ , also  $t = 37 \cdot t' = 999$  und  $s = 37 \cdot s' = 185$ , und wir erhalten, dass die Zahl  $t \cdot 13 + 10 = 12997$  alle drei Bedingungen erfüllt.

Da nun für jedes  $k \in \mathbb{Z}$ , die Zahl  $12997 + k \cdot \text{kgV}(7, 10, 13) = 12997 + k \cdot (7 \cdot 10 \cdot 13) = 12997 + k \cdot 910$  ebenfalls alle drei Bedingungen erfüllt, und alle Lösungen  $n$  von dieser Form sind, haben wir alle Lösungen gefunden. Zum Beispiel ist die kleinste positive Zahl, welche alle drei Bedingungen erfüllt:  $n = 257$ . ◄

DIE KÖRPER  $\mathbb{F}_p$ 

Für  $m \geq 2$  ist der Ring  $(\mathbb{Z}_m, \bar{0}, \bar{1}, +, \cdot)$  genau dann ein Körper, wenn jedes Element aus  $\mathbb{Z}_m \setminus \{\bar{0}\}$  ein multiplikativ Inverses besitzt. Mit Proposition 10.3 ist dies genau dann der Fall, wenn für jedes  $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$  gilt  $\text{ggT}(a, m) = 1$ . Das ist genau dann erfüllt, wenn  $m$  eine Primzahl ist: Denn ist  $m$  eine Primzahl und  $1 \leq a < m$ , so ist  $\text{ggT}(a, m) = 1$ . Ist andererseits  $m$  keine Primzahl, so existiert ein  $1 < a < m$  mit  $a \mid m$ . Das heisst  $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$ ,  $\text{ggT}(a, m) > 1$  und  $\bar{a}$  hat kein multiplikativ Inverses.

Der Ring  $\mathbb{Z}_m$  ist also genau dann ein Körper (engl. *field*), wenn  $m$  eine Primzahl ist. Die Körper  $\mathbb{Z}_p$  für  $p$  prim werden mit  $\mathbb{F}_p$  bezeichnet.

Etwas allgemeiner erhalten wir für Ringe  $R$ , dass  $R/I$  genau dann ein Körper ist, wenn das Ideal  $I$  maximal ist, wobei ein Ideal  $I$  ein **maximales Ideal** ist, wenn  $I \neq R$  und  $I$  in keinem echten Ideal  $J \subsetneq R$  echt enthalten ist.

**PROPOSITION 10.4.** *Sei  $R$  ein Ring und sei  $I \neq R$  ein Ideal von  $R$ . Dann ist  $R/I$  genau dann ein Körper, wenn  $I$  ein maximales Ideal ist.*

*Beweis.* ( $\Leftarrow$ ): Wir zeigen diese Richtung mit Kontraposition. Sei  $I \subsetneq R$  ein Ideal und sei  $R/I$  kein Körper. Dann existiert ein  $a_0 \in R \setminus I$  (d. h.  $\bar{a}_0 \neq \bar{0}$ ), sodass für alle  $x \in R$  gilt  $\bar{a}_0 \cdot \bar{x} \neq \bar{1}$ . Sei

$$J_0 := \{x \cdot a_0 + y \cdot b : x, y \in R \wedge b \in I\}.$$

Dann ist  $J_0 \subseteq R$  ein Ideal mit  $a_0 \in J_0$  und  $1 \notin J_0$ . Um  $1 \notin J_0$  zu sehen, beachte, dass aus  $x \cdot a_0 + y \cdot b = 1$  mit  $b \in I$  (d. h.  $\overline{y \cdot b} = \bar{0}$ ),  $\bar{x} \cdot \bar{a}_0 = \bar{1}$  folgt, im Widerspruch zu unserer Annahme. Es gilt somit

$$I \subsetneq_{a_0 \notin I} J_0 \subsetneq_{1 \notin J_0} R$$

und  $I$  ist nicht maximal.

( $\Rightarrow$ ): Sei  $R/I$  ein Körper und sei  $I \subsetneq J \subseteq R$ . Weiter sei  $a_0 \in J \setminus I$ . Weil  $R/I$  ein Körper ist, existiert ein  $\bar{x}$  mit  $\bar{a}_0 \cdot \bar{x} = \bar{1}$ . Das heisst,  $a_0 \cdot x = 1 + b$  für ein  $b \in I$ . Weil  $a_0 \in J$ , ist mit  $(I_2)$  auch  $a_0 \cdot x \in J$ , und weil  $I \subseteq J$ , ist  $b \in J$ . Somit ist mit  $(I_1)$  auch  $a_0 \cdot x - b = 1 \in J$ . Weil  $1 \in J$ , haben wir  $J = R$ , und somit ist  $I$  ein maximales Ideal.  $\dashv$

Als Folgerung erhalten wir:

**KOROLLAR 10.5.** *Ein Ideal  $m\mathbb{Z} \subseteq \mathbb{Z}$  ist genau dann maximal, wenn  $m$  eine Primzahl ist.*

Zum Schluss zeigen wir, dass die multiplikative Gruppe eines Körper  $\mathbb{F}_p$  zyklisch ist.

**THEOREM 10.6.** *Die Gruppe  $(\mathbb{F}_p^*, 1, \cdot)$  ist zyklisch.*

*Beweis.* Weil  $|\mathbb{F}_p^*| = p - 1$ , ist mit Korollar 9.15 jedes  $a \in \mathbb{F}_p^*$  eine Nullstelle der Polynomfunktion  $x^{p-1} - 1$ . Allgemein gilt, dass in einem Körper die Polynomfunktion  $x^k - 1$  höchstens  $k$  verschiedene Nullstellen besitzt (Beweis durch abspalten von Nullstellen von  $x^k - 1$ ).

Sei  $\mathbb{F}_p^* = \{a_1, \dots, a_{p-1}\}$  und sei  $\mu_i := \text{ord}(a_i)$ . Weiter sei  $\mu_0 := \max\{\mu_i : 1 \leq i \leq p - 1\}$  und sei  $g \in \mathbb{F}_p^*$  so, dass  $\text{ord}(g) = \mu_0$ .

Ist  $\mu_0 = p - 1$ , so ist  $\mathbb{F}_p^* = \langle g \rangle$ , also zyklisch.

Ist  $\mu_0 < p - 1$  und gilt  $\mu_i \mid \mu_0$  für alle  $1 \leq i \leq p - 1$ , so ist jedes  $a \in \mathbb{F}_p^*$  eine Nullstelle der Polynomfunktion  $x^{\mu_0} - 1$ . Da aber  $x^{\mu_0} - 1$  höchstens  $\mu_0$  verschiedene Nullstellen besitzt, folgt  $|\mathbb{F}_p^*| \leq \mu_0 < p - 1$ , was ein Widerspruch zu  $|\mathbb{F}_p^*| = p - 1$  ist.

Ist  $\mu_0 < p - 1$  und gilt  $\mu_j \nmid \mu_0$  für ein  $1 \leq j \leq p - 1$ , so finden wir, weil  $\mu_j < \mu_0$ , ein  $d > 1$  mit  $d \mid \mu_j$  und  $\text{ggT}(d, \mu_0) = 1$ . Für  $\nu := \frac{\mu_j}{d}$  ist dann  $\text{ord}(a_j^\nu) = d$  und mit Aufgabe 38 ist dann  $\text{ord}(a_j^\nu \cdot g) = d \cdot \mu_0 > \mu_0$ , was ein Widerspruch zur Definition von  $\mu_0$  ist.  $\dashv$