# Lösung Übungsblatt 2

**A1**, (ii) $\Rightarrow$ (i): ✓

(i) $\Rightarrow$ (ii): • Zunächst zeigen wir die Aussage für $a$ nicht prim. Die Menge aller $p \in \mathbb{P}$ mit $p \equiv a \ (b)$ ist eine nichtleere Teilmenge von $\mathbb{N}$.

Annahme: Diese Menge ist endlich. Dann gibt es eine maximale Primzahl $p_0$ mit $p_0 \equiv a \ (b)$.

Unter allen Primzahlen existiert eine Primzahl $q$ mit $q > a$, $q > p_0$, denn $\#\mathbb{P} = \infty$.

Es ist $ggT(q, a) = 1$ (denn da $ggT \mid q$, aber $q$ ist kein Primteiler von $a$, da $q > a$),

und mit $ggT(b, a) = 1$ folgt $ggT(b \cdot q, a) = 1$.

Nach Voraussetzung existiert eine Primzahl $p_1 \equiv a \ (b \cdot q)$,

also $p_1 = a + k \cdot bq$ für ein $k \in \mathbb{N}_0$, denn für $k < 0$ ist $a + k \cdot bq < 0$.

Da aber $a$ nicht prim ist $k \geq 1$ und damit

$p_1 \geq q > p_0$.

Modulo $b$ gilt $p_1 \equiv a \ (b)$, was mit $p_1 > p_0$ einen Widerspruch darstellt.

• Sei nun $a$ prim. Wir betrachten $a \cdot (b+1) = a \cdot b + a$.

Es ist $ggT(a \cdot b + a, b) = ggT(a, b) = 1$.

Da $a \cdot (b+1)$ nicht prim ist ($a \in \mathbb{P}$, $b + 1 \geq 2$) existieren unendlich viele Primzahlen $p \equiv a \cdot (b+1) \ (b)$.

Für all diese $p$ gilt $p = a \cdot (b+1) + k \cdot b$ für ein $k \in \mathbb{Z}$

$\equiv a \ (b)$.

Also gibt es unendlich viele Primzahlen $p \equiv a \ (b)$.

A2 a) • M ist nicht assoziativ, z.B. $(1-1)-1 = -1 \neq 1 = 1-(1-1)$.

• Ein linksneutrales Element e erfüllt insbesondere $e-1 = 1$, also $e=2$.
Andererseits muss auch $e-2=2$, also $e=4$ gelten.
Folglich kann es kein linksneutrales Element geben.

• Ein rechtsneutrales Element erfüllt insbesondere $1-e=1$, also $e=0$, und wegen $z-0=z \ \forall z \in \mathbb{Z}$ ist $e=0$ der einzige ~~Null~~ rechtsneutrale Element.

• Wäre M kommutativ, so wäre jedes rechtsneutrale Element auch linksneutral und andersrum.
Also ist M nicht kommutativ.
(Da hätten wir auch mit einem konkreten z

b) Jeder EZS besitzt mindestens ein Element.

• $\{1\}$ ist ein EZS und dann also eines mit der minimalen Anzahl a Elementen. Zz ist also $\langle 1 \rangle \overset{(!)}{=} \mathbb{Z}$.
Wegen $(1-1)-1 = -1$ ist $-1 \in \langle 1 \rangle$.
Für $n \in \mathbb{N}$ gilt dann $n = (\underbrace{(1-(-1))-(-1))-1 \ldots}_{n-1 \text{ Subtraktionen von } -1 \in \langle 1 \rangle} \in \langle 1 \rangle$,

für $z \in \mathbb{Z} \setminus \mathbb{N}$ gilt $z = (\underbrace{(1-1)-1)-1 \ldots}_{-z+1 \text{ Subtraktionen}} \in \langle 1 \rangle$.

$\Rightarrow \{1\}$ ist EZS.

• Wegen $1 = (-1-(-1))-(-1) \in \langle -1 \rangle$ ist auch $1, -1 \in \langle -1 \rangle$, also wie oben $\langle -1 \rangle = \mathbb{Z}$,
also $\{-1\}$ ein weiterer EZS mit minimaler Elementanzahl.

- Für $m \in \mathbb{Z}$, $m \neq 1, m \neq -1$ ist $\{m\}$ kein $\in \mathcal{Z}S$, denn alle $a \in \langle m \rangle$ sind Vielfache von $m$, also $\cancel{a=1} \notin \langle m \rangle$.

  $\{1\}, \{-1\}$ sind die einzigen $\in \mathcal{Z}S$ mit minimale Elementzahl.

- $\{2,3\}$ ist $\in \mathcal{Z}S$ wegen $3-2=1 \in \langle 2,3 \rangle$, also $\mathbb{Z} = \langle 1 \rangle \subseteq \langle 2,3 \rangle$.
  Wegen $\langle 2 \rangle \neq \mathbb{Z}$, $\langle 3 \rangle \neq \mathbb{Z}$ ~~kann~~ umfasst $\{2,3\}$ kein kleineres $\in \mathcal{Z}S$.

c) Wir definieren $\varphi: \mathbb{Z} \longrightarrow End(M)$

$$x \longmapsto \varphi_x : M \longrightarrow M$$
$$a \longmapsto x \cdot a$$

zz: $\varphi$ ist ein Homomorphismus.

(i) zz $\varphi$ ist wohldefiniert, d.h. $\forall x$ ist $\varphi_x \overset{(!)}{\in} End(M)$.

Klar: $\varphi_x \in Abb(M,M)$ und für $a,b \in \mathbb{Z}$ gilt:

$$\varphi_x(a-b) = x \cdot (a-b) = xa - xb = \varphi_x(a) - \varphi_x(b),$$

also $\varphi_x \in End(M)$.

(ii) zz. $\varphi$ ist homomorph, d.h. es ist $\varphi(x \cdot y) \overset{(!)}{=} \varphi(x) \circ \varphi(y)$ für alle $x,y \in \mathbb{Z}$ und $\varphi(1) = id$.

Für $a \in M$ beliebig ist

- $\varphi(x \cdot y)(a) = (x \cdot y) \cdot a = x \cdot (y \cdot a) = \varphi_x(y \cdot a)$
  $= \varphi_x(\varphi_y(a)) = (\varphi_x \circ \varphi_y)(a)$.
- $\varphi(1)(a) = 1 \cdot a = a \Rightarrow \varphi(1)$ neutral in $End(M)$.

(iii) zz $\varphi$ ist injektiv. Sei $\varphi(x) = \varphi(y)$ für $x,y \in \mathbb{Z}$.
Dann ist $x = x \cdot 1 = \varphi(x)(1) = \varphi(y)(1) = y \cdot 1 = y$.

(iv) zz $\Psi$ ist surjektiv, d.h. für $\chi \in End(M)$ beliebig existiert $x \in \mathbb{Z}$ mit $\Psi(x) = \chi$.

Es muss gelten $\chi(1) = \Psi(x)(1) = x \cdot 1 = x$.

Beh: $\chi \overset{(!)}{=} \Psi(\chi(1))$.

Da $\chi, \Psi(\chi(1)) \in End(M)$ auf dem Erzeugendensystem $\{1\}$ übereinstimmen, sind wir schon fertig.

AB a) o.E. $M \neq \emptyset$, sonst sind wir fertig.

$M \neq \emptyset \Rightarrow k := \min(M \setminus \{0\})$ existiert.

Setze $J = \{j \in \{0, \dots, k-1\} \mid \exists m \in M \; m \equiv j(k)\}$.

Setze $k_0 = k$ und für $j \in J \setminus \{0\}$ $k_j = \min\{m \in M \mid m \equiv j(k)\}$.

Beh: $\{k_j\}_{j \in J}$ erzeugt $M$.

Wav: $\langle k_j \rangle_{j \in J} \subseteq M$.

Sei $t \in M$, $t \neq 0$ beliebig $\Rightarrow t \equiv j(k)$ für ein $j \in J$ und $t \geq k_j$ nach Wahl von $k_j$.

$\Rightarrow t - k_j \equiv 0(k)$ und $t - k_j \geq 0$,

also $t - k_j = \ell \cdot k$ für ein $\ell \in \mathbb{N}_0$

$\Rightarrow t = k_j + \underbrace{k + \dots + k}_{\ell\text{-mal}} = k_j + k_0 + \dots + k_0 \in \langle k_j \rangle_{j \in J}$.

b) Betrachte $N = \langle \{k, k+1, \dots, 2k-1\} \rangle$.

Für $n \in \mathbb{N} \setminus \{0\}$ gilt: $n$ ist endliche Summe von Elementen der Form $k+i$, $i \in \{0, \dots, k-1\} \Rightarrow n \geq k$.

Sei nun $T$ ein $\in \mathcal{P}$ von $N$, $0 \notin T$.

Für alle $i \in \{0, \dots, k-1\}$ gilt:

$k+i \in N \Rightarrow k+i \in \langle T \rangle \Rightarrow k+i = \sum_{j=1}^{r} t_j \geq r \cdot k$

mit $t_j \in T$.

$\Rightarrow r = 1 \Rightarrow k+i = t_1 \in T$.

$\Rightarrow \# T \geq k$.

## A4

$$(*)\quad \begin{pmatrix} a & 0 & c \\ b & 0 & b \\ c & 0 & a \end{pmatrix} \cdot \begin{pmatrix} a' & 0 & c' \\ b' & 0 & b' \\ c' & 0 & a' \end{pmatrix} = \begin{pmatrix} aa'+cc' & 0 & cb+ca' \\ (a'+c')\,b & 0 & (a+c')\,b \\ a'c+c'a & 0 & aa'+cc' \end{pmatrix}$$

a) Wegen (*) gilt: $(H,\cdot)$ abg., wenn für alle $a,b,c,$ $a',b',c' \in \mathbb{Q}$ mit $a \neq \pm c$, $a' \neq \pm c'$ gilt, dass
$$a'c + c'a \overset{(!)}{\neq} \pm(aa' + cc').$$

Annahme: $a'c + c'a = \pm(aa' + cc')$

$\Leftrightarrow a'c + c'a \mp aa' \mp cc' = 0$

$a'(c \mp a) + c'(a \mp c) = \underbrace{(a' \mp c')}_{\neq 0} \cdot \underbrace{(c \mp a)}_{\neq 0}$

$\Rightarrow$ $(H,\cdot)$ Magma und mit Matrixmultiplikation allgemein assoziativ, ist $(H,\cdot)$ sogar eine Halbgruppe.

b) Ansatz: $E = \begin{pmatrix} a' & 0 & c' \\ b' & 0 & b' \\ c' & 0 & a' \end{pmatrix} \in H$.

$E$ rechtsneutral $\Leftrightarrow \forall A \in H: A \cdot E = A$

$\overset{(*)}{\Leftrightarrow}$ $\forall a,b,c,\ a \neq \pm c$ gilt:

$$\left.\begin{aligned} aa' + cc' &= a \\ (a' + c')\,b &= b \\ a'c + c'a &= c \end{aligned}\right\} \; L$$

$\overset{(!)}{\Leftrightarrow}$ $a' = 1,\ c' = 0,\ b'$ beliebig.

denn

"$\Leftarrow$" einsetzen

"$\Rightarrow$" $L$ muss insbesondere für $a=1, c=0$ erfüllt sein.

<u>erste Gleichg</u> $\Rightarrow a'=1$.

<u>einsetzen in dritte Gleichg</u> $\Rightarrow c'=0$

c) Sei $E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H$ bzl. neutrales Element

und $A = \begin{pmatrix} a' & 0 & c' \\ b' & 0 & b' \\ c' & 0 & a' \end{pmatrix} \in H$ bzl.

<u>zz</u> $\exists!\ \hat{A} = \begin{pmatrix} a & 0 & c \\ b & 0 & b \\ c & 0 & a \end{pmatrix} \in H$ mit $\hat{A}A \overset{(!)}{=} E$.

$$\hat{A}A = E \overset{(*)}{\Leftrightarrow} \begin{aligned} aa' + cc' &= 1 \\ (a'+c')\,b &= 0 \\ a'c + ac' &= 0 \end{aligned}$$

$$\Leftrightarrow \underbrace{\begin{pmatrix} a' & 0 & c' \\ 0 & (a'+c') & 0 \\ c' & 0 & a' \end{pmatrix}}_{=:Q} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\det(Q) = \underbrace{(a'+c')}_{\neq 0} \cdot \underbrace{(a'^2 - c'^2)}_{\neq 0 \text{ da } A \in H} \neq 0,$$

also $\exists!\ (a,b,c)$, die das LGS lösen.

noch zu zeigen: $\hat{A} = \begin{pmatrix} a & 0 & c \\ b & 0 & b \\ c & 0 & a \end{pmatrix} \overset{(1)}{\in} H$, d.h. $c \neq \pm a$.

Es ist $c'a + a'c = 0$

$\Rightarrow |c'| \cdot |a| = |c'a| = |a'c| = |a'| \, |c|$

und wegen $|c'| \neq |a'| \Rightarrow |c| \neq |a|$.

d) Seien $A = \begin{pmatrix} a & 0 & c \\ b & 0 & b \\ c & 0 & a \end{pmatrix} \in H$ bel. und

$E = \begin{pmatrix} 1 & 0 & 0 \\ \tilde{5} & 0 & \tilde{5} \\ 0 & 0 & 1 \end{pmatrix} \in H$ rechtsneutral. Dann gilt:

$\exists \, \hat{A} \in H$ mit $A\hat{A} = E \iff \exists a', b', c' \in \mathbb{Q}, a' \neq \pm c'$

mit

$aa' + cc' = 1$

$b(a' + c') = \tilde{5}$

$ac' + c'a = 0$

$\iff \exists \, a', b', c' \in \mathbb{Q}, a' \neq \pm c'$ mit

$$\underbrace{\begin{pmatrix} a & c \\ c & a \end{pmatrix}}_{=: Q} \cdot \begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad (i)$$

und $b \cdot (a' + c') = \tilde{5}$ (ii)

Wegen $\det(Q) = a^2 - c^2 \neq 0$, ex. eind. Lsg $a', c'$ des (GS), wie in c) gilt $a' \neq \pm c'$.

Die letzte Bedingung ist genau dann lösbar, wenn $\tilde{b} = b \cdot (a' + c')$ für das eindeutige Paar $(a', c')$ gilt. Also gibt es immer ein $\tilde{b}$, so dass $A\tilde{A} = E$ lösbar ist.

Dann löst jedes $(a', b', c')$ mit eindeutigem $a', c'$ und $b' \neq 0$, also gibt es unendlich viele Matrizen $\tilde{A}$ mit $A\tilde{A} = E$.