Lineare Algebra Blatt 5

Lukas Beichert, Jannis Schnitzer Tutor: Philipp Schill

14.10.11

1	2	3	4	Σ
3	4	3	4	14

Aufgabe 1

a)

gegeben: $n = a_r \cdot 10^r + \dots + a_1 \cdot 10 + a_0$, $a_i \in \{0, \dots, 9\}$

Zz: $(a_r + \dots + a_1 + a_0) \bmod 9 \equiv 0$

$\Rightarrow (a_r \cdot 10^r + \dots + a_1 \cdot 10 + a_0) \bmod 9 = 0$

-1 zB: $\Leftrightarrow$

Bew.:

$(a_r + \dots + a_1 + a_0) \bmod 9 = 0$

$\Leftrightarrow a_r \bmod 9 + \dots + a_1 \bmod 9 + a_0 \bmod 9 = 0$

$\Leftrightarrow (a_r \cdot 1) \bmod 9 + \dots + (a_1 \cdot 1) \bmod 9 + a_0 \bmod 9 = 0$

$\Rightarrow (a_r) \bmod 9 \cdot (1) \bmod 9 + \dots + (a_1) \bmod 9 \cdot (1) \bmod 9 + a_0 \bmod 9 = 0$

(da $(1) \bmod 9 = (9+1) \bmod 9 = (9+1)^r \bmod 9$)

$\Rightarrow (a_r) \bmod 9 \cdot (9+1)^r \bmod 9 + \dots + (a_1) \bmod 9 \cdot (9+1) \bmod 9 + a_0 \bmod 9 = 0$

$\Rightarrow (a_r \cdot 10^r + \dots + a_1 \cdot 10 + a_0) \bmod 9 = 0$ ✓

Da durch 9 teilbar auch durch 3 teilbar. // Aber nicht jede Zahl, die durch 3 teilbar ist, ist auch durch 9 teilbar. -1

b)

Zz: $\left((-1)^r a_r + (-1)^{r-1} a_{r-1} + \dots - a_1 + a_0\right) \bmod 11 = 0$

$\Rightarrow (a_r \cdot 10^r + \dots + a_1 \cdot 10 + a_0) \bmod 11 = 0$

-1 zB: $\Leftrightarrow$

Bew.:

$\left((-1)^r a_r + (-1)^{r-1} a_{r-1} + \dots - a_1 + a_0\right) \bmod 11 = 0$

Da $(-1)^r \bmod 11 = (10)^r \bmod 11$

$\Rightarrow (a_r) \bmod 11 \cdot (10)^r \bmod 11 + (a_{r-1}) \bmod 11 \cdot (10^{r-1}) \bmod 11 + \dots$

$+ a_1 \bmod 11 \cdot (10) \bmod 11 + (a_0) \bmod 11 = 0$

$\Rightarrow (a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_1 \cdot 10 + a_0) \bmod 11 = 0$ ✓

Schreibweise zum Rechnen in Restklassen:

$\bar{a} = \bar{b}$ oder $[a] = [b]$ oder $a \equiv b \pmod c$

3/6

1

Aufl. 2

geg. $G = (G, +, 0)$, kommut.

$\alpha, \beta \in End(G)$

$\alpha + \beta : G \to G, \quad g \mapsto \alpha(g) + \beta(g)$

$0 : G \to G, \quad g \mapsto 0$

a)

ZZ: $\alpha + \beta$ ist Gruppenhomomorphismus

d.h. $(\alpha + \beta)(g + g') = (\alpha + \beta)(g) + (\alpha + \beta)(g')$

$g, g' \in G$

Bew.:

(1) $(\alpha + \beta)(g + g') = \alpha(g + g') + \beta(g + g')$

(da α, β Endomorphismen)

$\Rightarrow \alpha(g) + \alpha(g') + \beta(g) + \beta(g') = \alpha(g) + \beta(g) + \alpha(g') + \beta(g')$

(2) $(\alpha + \beta)(g) + (\alpha + \beta)(g') = \alpha(g) + \beta(g) + \alpha(g') + \beta(g')$

$= (1)$ ✓ (da G abelsch) □

b)

ZZ: $(End(G), +, \circ, 0, id)$ ist unitärer Ring

Bew.: $\alpha, \beta, \gamma \in End(G)$ $g, g' \in G$

ist kommut. Gruppe: R1) G1) $\alpha(g) + (\beta(g) + \gamma(g)) = \alpha(g) + ((\beta + \gamma)(g))$

$= (\alpha + \beta + \gamma)(g) = (\alpha + \beta)(g) + \gamma(g) = (\alpha(g) + \beta(g)) + \gamma(g)$ □

$\uparrow$ da $\alpha(g), \beta(g), \gamma(g) \in G$, G ist Gruppe.

$-0{,}5$ α, β, γ sind nicht in G

G2)

$e = 0, \quad 0 : G \to G, \quad g \mapsto 0$

$(0 + \alpha)(g) = 0(g) + \alpha(g) = 0 + \alpha(g) = \alpha(g)$ ✓ □

G3)

$\alpha(g) + \beta(g) \stackrel{!}{=} 0$ da $\alpha(g), \beta(g) \in G$ und G ist Gruppe

$\to$ zu jedem $\alpha(g)$ ex. ein $\beta(g)$ mit $\alpha(g) + \beta(g) = 0$ ✓ □

2

14.12.11

(G4) $(\alpha+\beta)(g) = \alpha(g)+\beta(g) = \beta(g)+\alpha(g) = (\beta+\alpha)(g)$

↑ da $\alpha(g), \beta(g) \in G$ und G ist kommut. Gruppe.

- R2) ZZ: $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$

Sei: $g \in G$

$\alpha(g) \in G$, als kann $\alpha(g)$ nicht mit $\circ$ verknüpft werden. −1

Beweis: $\Rightarrow$ $\alpha(g) \circ (\beta(g) \circ \gamma(g)) = \alpha(g) \circ (\beta(\gamma(g))) = \alpha(\beta(\gamma(g)))$

$\Leftarrow$ $(\alpha(g) \circ \beta(g)) \circ \gamma(g) = \alpha(\beta(g)) \circ \gamma(g) = \alpha(\beta(\gamma(g)))$ □

- R3) ZZ (i): $\alpha \circ (\beta+\gamma) = (\alpha \circ \beta) + (\alpha \circ \gamma)$

Beweis: $\alpha(g) \circ (\beta(g)+\gamma(g)) = \alpha(g) \circ ((\beta+\gamma)(g))$

$= \alpha((\beta+\gamma)(g)) = \alpha(\beta(g)) + \alpha(\gamma(g)) = (\alpha \circ \beta)(g) + (\alpha \circ \gamma)(g)$ (L) □

↑ α Homomorph. $\alpha(\beta(g)+\gamma(g))$ −0,5

ZZ (ii): $(\alpha+\beta) \circ \gamma = (\alpha \circ \gamma) + (\beta \circ \gamma)$

Beweis:

$(\alpha(g)+\beta(g)) \circ \gamma(g) = (\alpha+\beta)(g) \circ \gamma(g) = (\alpha+\beta)(\gamma(g))$

$= \alpha(\gamma(g)) + \beta(\gamma(g)) = (\alpha \circ \gamma)(g) + (\beta \circ \gamma)(g)$ (L) □

- R4) ZZ: $id \circ \alpha = \alpha = \alpha \circ id$ $\quad \alpha, \beta \in End(G)$ $g \in G$

Beweis: ~~$id \circ \alpha(g) = id(\alpha(g)) = \alpha(g) = \alpha(id(g)) = \alpha \circ id$~~

~~$id(\beta \circ \alpha(g))$~~

$id(g) \circ \alpha(g) = id(\alpha(g)) = \alpha(g) = \alpha(id(g)) = \alpha(g) \circ id(g)$ (L) □

↑ da $id(g) = g$

4/6

14.11.11

Aufg 3

geg: $\alpha: \{1,2,\dots,n\} \to G$, $G = (G, *, e)$

$\sigma_g : \{1,2,\dots,n\} \to \{1,2,\dots,n\}$, $i \mapsto \alpha^{-1}(g * \alpha(i))$

a)

zz: Es gilt $\sigma_g \in S_n$

$S_n := \{ f \in Abb(\{1,2,\dots,n\}, \{1,2,\dots,n\}) \mid f \text{ ist bijektiv} \}$

Also zz: σ_g ist bijektiv

Es gilt: σ_g ist bijektiv $\Leftrightarrow$ es ex. σ_g^{-1} mit $\sigma_g \circ \sigma_g^{-1} = id$

und dann $\sigma_g^{-1} \circ \sigma_g = id$! →

σ_g^{-1} lässt sich leicht finden: $\sigma_g^{-1} : \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ $j \mapsto \alpha^{-1}(\alpha(j) * g^{-1})$

Das ist nicht die Umkehrabbildung. Die ist nämlich $j \mapsto \alpha^{-1}(g^{-1} * \alpha(j))$

Probe: $\sigma_g^{-1} \circ \sigma_g(j) = \alpha^{-1}\left(\alpha\left[\alpha^{-1}(g * \alpha(j))\right] * g^{-1}\right)$

$= \alpha^{-1}\left(g * \alpha(j) * g^{-1}\right)$ nur wenn G abelsch! →

$= \alpha^{-1}(\alpha(j)) = j$ ✓

Folglich ist σ_g bijektiv, also gilt $\sigma_g \in S_n$

σ_g wohldef fehlt →

b)

Abb $\beta: G \to S_n$, $g \mapsto \sigma_n$

zz: β ist injektiver Gruppenhomomorphismus.

(1) zz: β ist injektiv d.h. $\beta(g) = \beta(h) \Rightarrow g = h$, $g, h \in G$

Ber: ~~$\beta(g) = \beta(h)$~~ $\Rightarrow \beta(g)(i) = \beta(h)(i)$

$\Rightarrow \alpha^{-1}(g * \alpha(i)) = \alpha^{-1}(h * \alpha(i))$ da α^{-1} injektiv

$\Rightarrow g * \alpha(i) = h * \alpha(i)$ kürzen

$\Rightarrow g = h$ ✓

2) zz: β ist Gruppenhom

d.h. $\beta(g * h) \overset{!}{=} \beta(g) \circ \beta(h)$ | Da $*_{G_1}$ = "o"

Bew: $\beta(g*h)(i) = \alpha^{-1}((g*h) * \alpha(i))$

$\beta(g) \circ \beta(h) = \alpha^{-1}\left(g * \alpha(\alpha^{-1}(h * \alpha(i)))\right)$

$= \alpha^{-1}(g * h * \alpha(i))$

$= \alpha^{-1}((g*h) * \alpha(i)) = \beta(g*h)(i)$ ✓ □

3/6

4

14.11.11

Aufg. 4

a) geg: $G = (G, *, e)$ mit $\#G = 4$

Sei $G = \{e, f, g, h\}$

auch geg: $g * g = e$ für jedes $g \in G$

die einzig mögliche Verknüpfung ist dann: ✓

$*$:

$*$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

denn 1.) ~~jedes~~ $g' * g' = e$ für jedes $g' \in G$

2.) $f * g = h = g * h$ $g * f$?

denn: - $f * g \neq e$, da $g \neq f^{-1} = f$ ist.

- $f * g \neq f$, da $g \neq e$ ist.

- $f * g \neq g$, da $f \neq e$ ist.

3.) $f * h = g = h * f$

analog zu 2.)

4.) $g * h = f = h * g$

analog zu 2.)

Wir def. in $\mathbb{Z}/2\mathbb{Z}$ die Verknüpfung "+" mit

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

und in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mit ~~$+ : (x,y) + (x',y')$~~

$$+ : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (x,y) + (x',y') \longrightarrow (x+x', y+y')$$

Also:

$+$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$

Offensichtlich lässt sich eine Abb. f definieren mit ✓

$f: (\bar{0},\bar{0}) \longrightarrow e$

$(\bar{0},\bar{1}) \longrightarrow f$

$(\bar{1},\bar{0}) \longrightarrow g$

$(\bar{1},\bar{1}) \longrightarrow h$

~~Für diese gilt:~~

16

Entsprechend lässt sich f^{-1}, die Umkehrfunktion, definieren:

f^{-1}: $e \to (\bar{0}, \bar{0})$
$f \to (\bar{0}, \bar{1})$
$g \to (\bar{1}, \bar{0})$
$h \to (\bar{1}, \bar{1})$

Für diese Abbildungen gilt

$f(x+y) = f(x) * f(y) \quad | \; x, y \in \mathbb{Z}_{2\mathbb{Z}} \times \mathbb{Z}_{2\mathbb{Z}}$

und $f^{-1}(j * k) = f^{-1}(j) * f^{-1}(k) \quad | \; j, k \in G$

f ist also ein Gruppenisomorphismus. ✓

b)

gog: $f * f \neq e$; $g * g = e$ das ist keine gegebene Voraussetzung. g^{-1} ✓

dann gibt es nur eine mögliche Verknüpfung auf G: ✓

*	e	f	g	h
e	e	f	g	h
f	f	g	h	e
g	g	h	e	f
h	h	e	f	g

denn:

1.) $g * f = h = f * g$ das ist keine Voraussetzung.

denn: $\neq e$, da $f \neq g^{-1} = g$
$\neq g$, da $f \neq e$
$\neq f$, da $g \neq e$

2.) $g * h = f = h * g$

denn: $\neq e$, da $h \neq g^{-1} = g$
$\neq h$, da $g \neq e$
$\neq g$, da $h \neq e$

3.) $f * h = e = h * f$

denn: $\neq f$, da $h \neq e$
$\neq h$, da $f \neq e$
$\neq g$, da $g * f = h$

Es wäre also $f * h * f = h$
$\Rightarrow f * f = e$ ↯ WID

4.) $f * f = g$ ✗

denn: $\neq e$, da $f = h^{-1}$ und $f * h^{-1} \neq e$
$\neq f$, da $f \neq e$
$\neq h$, da $h^{-1} * h^{-1} \neq h$

14.11.17

5.) $h * h = g$

denn: $\neq e$ da $h = f^{-1}$ und $f^{-1} * f^{-1} \neq e$

$\neq f$ da $f^{-1} * f^{-1} \neq f$

$\neq h$ da $f^{-1} * f^{-1} \neq h$

In $\mathbb{Z}/4\mathbb{Z}$ ist die Verknüpfung "+" definiert mit

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Es lässt sich also eine Abb f def. mit f: $\bar{0} \longrightarrow e$ ✓

$\bar{1} \longrightarrow f$

$\bar{2} \longrightarrow g$

$\bar{3} \longrightarrow h$

Entsprechend die Umkehrfkt f^{-1}:

f^{-1}: $e \longrightarrow \bar{0}$

$f \longrightarrow \bar{1}$

$g \longrightarrow \bar{2}$

$h \longrightarrow \bar{3}$

Es gilt:

$f(x+y) = f(x) * f(y) \quad | \; x,y \in \mathbb{Z}/4\mathbb{Z}$

$f^{-1}(j*k) = f^{-1}(j) + f^{-1}(k) \quad | \; j,k \in G$

$\Rightarrow$ f ist ein Gruppenisomorphismus. ✓

c)

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

+	$\bar{0},\bar{0}$	$\bar{0},\bar{1}$	$\bar{1},\bar{0}$	$\bar{1},\bar{1}$
$\bar{0},\bar{0}$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$\bar{0},\bar{1}$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$
$\bar{1},\bar{0}$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$
$\bar{1},\bar{1}$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$

$\not\Leftrightarrow$

$\mathbb{Z}/4\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Die beiden Verknüpfungstabellen unterscheiden sich in ihrer Struktur (in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: $g * g = e \; \forall \; g \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, in $\mathbb{Z}/4\mathbb{Z}$ gilt dies nicht). Es lässt sich also keine bijektive Abb von der einen auf die andere finden. Genau!

4/4

18

Nachbesprechung

Zu 1)

a) In $\mathbb{Z}/3\mathbb{Z}$ gilt $\overline{10} = \overline{1}$

also zz: $\overline{n} = \overline{\left(\sum_{i=0}^{r} a_i\right)} = \overline{q}$

$$\overline{n} = \overline{\sum_{i=0}^{r} a_i 10^i} = \sum_{i=0}^{r} \overline{a_i 10^i} = \sum_{i=0}^{r} \overline{a_i} \cdot \overline{10}^i = \sum_{i=0}^{r} \overline{a_i} \quad \ldots$$

Regeln für Gruppenhomomorphismen

für $f: M \to N$ gilt:

1) $f(e_M) = e_N$
2) $f(g)^{-1} = f(g^{-1})$
3) f injektiv $\Leftrightarrow \ker(f) = \{e_M\}$

Bew (1) $f(e_M) = f(e_M^* * e_M) = f(e_M) * f(e_M) \overset{\text{kürzen}}{=} f(e_M)$

also $f(e_M) = e_N$

3) "$\Rightarrow$": sei f inj. Gelte $f(a) = e_N$ mit $f(e_M) = e_N$

da f inj $\Rightarrow a = e_M \Rightarrow \ker(f) = \{e_M\}$

"$\Leftarrow$": Sei $\ker(f) = \{e_M\}$

$$f(a) = f(b)$$
$$\Rightarrow f(a) * (f(b))^{-1} = e_N$$
$$\Leftrightarrow f(a) * f(b^{-1}) = e_N$$
$$\Leftrightarrow f(a * b^{-1}) = e_N$$

Aus $\ker(f) = e_M$ folgt $a * b^{-1} = e_M \quad | * b$

$a = b$

$\Rightarrow f$ ist injektiv