# Algebra I, WiSe 2011\2012 – Lösung Blatt 1

**1.1.** (a) $m \circ n = m^n$

- Assoziativität: Nein

$$m \circ (n \circ p) = m \circ (n^p) = m^{(n^p)}$$

$$(m \circ n) \circ p = (m^n) \circ p = (m^n)^p = m^{n \cdot p}$$

Im Allgemeinen ist $n^p \neq n \cdot p$

$$\left( \text{z.B. } \begin{aligned} 2 \circ (2 \circ 3) &= 2 \circ 2^3 = 2 \circ 8 = 2^8 \\ (2 \circ 2) \circ 3 &= 2^2 \circ 3 = (2^2)^3 = 2^6 \end{aligned} \right)$$

- Kommutativität: Nein

z.B. $2 \circ 3 = 2^3 = 8 \neq 9 = 3^2 = 3 \circ 2$

- Neutrales Element: Nein.

Es gilt stets: $m \circ 1 = m^1 = m \quad \forall m \in \mathbb{N}$

$\Rightarrow$ 1 ist rechtsneutrales Element

$\lightning$ $\exists$ neutrales Element $e \in \mathbb{N}$. $\overset{\text{insb.}}{\Rightarrow}$ $e$ ist linksneutral

$\Rightarrow e = 1 \qquad \left(\text{denn: } 1 \underset{e \text{ l.n.}}{=} e \cdot 1 \underset{1 \text{ r.n.}}{=} e \right)$

$\Rightarrow$ 1 ist linksneutrales Element.

Aber: $1 \circ 2 = 1^2 = 1 \neq 2 \qquad \lightning$

Also: $\nexists$ neutrales Element.

(b) $m \circ n = m + n + mn$

- Assoziativität: Ja

$$m \circ (n \circ p) = m \circ (n + p + np) = m + n + p + np + mn + mp + mnp$$

$$(m \circ n) \circ p = (m + n + mn) \circ p = m + n + mn + p + mp + np + mnp$$

- Kommutativität: Ja

$$m \circ n = m + n + mn \underset{\substack{+,\cdot \text{ in } \mathbb{N} \\ \text{Kommutativ}}}{=} n + m + nm = n \circ m$$

- Neutrales Element: Nein (Achtung: $0 \notin \mathbb{N}$ bei Schlickewei)

  Dehne Verknüpfung auf $\mathbb{N}_0$ aus. Dann:

$$\left.\begin{aligned} m \circ 0 &= m + 0 + m \cdot 0 = m \\ 0 \circ m &\underset{\circ \text{ Komm.}}{=} m \circ 0 = m \end{aligned}\right\} \Rightarrow 0 \text{ ist neutrales Element}$$

$\Rightarrow$ Ist $e \in \mathbb{N}$ neutral, so folgt $e = 0 \notin \mathbb{N}$ ...

(Alternative: Direkt. $m \circ n = m \quad \forall m \in \mathbb{N}$

$$\begin{aligned} &\Leftrightarrow m + n + mn = m \quad \forall m \\ &\Leftrightarrow n + mn = 0 \quad \forall m \\ &\Leftrightarrow n \underbrace{(1+m)}_{\neq 0} = 0 \quad \forall m \\ &\Leftrightarrow n = 0 \end{aligned}$$
)

(c) $m \circ n = ggT(m,n)$.

Sei $P \subset \mathbb{N}$ die Menge aller Primzahlen.

Bekannt: Jedes $n \in \mathbb{N}$ besitzt eindeutige Zerlegung in Primzahlen, d.h. $\forall n \in \mathbb{N} \; \exists$ eindeutige $v_p(n)$ für alle $p \in P$ mit $v_p(n) \geq 0$, $v_p(n) = 0$ für fast alle $p \in P$ und

$$n = \prod_{p \in P} p^{v_p(n)}.$$

Für $m, n \in \mathbb{N}$ ist offenbar $ggT(m,n) = \prod_{p \in P} p^{\min\{v_p(m), v_p(n)\}}$

- Assoziativität: Ja.

  Seien $m, n, q \in \mathbb{N}$. Haben Zerlegungen in Primzahlen:

$$ggT(m,n) = \prod_{p \in P} p^{\min\{v_p(m), v_p(n)\}}, \quad ggT(n,q) = \prod_{p \in P} p^{\min\{v_p(n), v_p(q)\}}$$

Damit:

$$
\begin{aligned}
(m \circ n) \circ q &= ggT(ggT(m,n), q) \\
&= \prod_{p \in P} p^{\min\{\min\{v_p(m), v_p(n)\}, v_p(q)\}} \\
&= \prod_{p \in P} p^{\min\{v_p(m), v_p(n), v_p(q)\}} \\
&= \prod_{p \in P} p^{\min\{v_p(m), \min\{v_p(n), v_p(q)\}\}} \\
&= ggT(m, ggT(n,q)) \\
&= m \circ (n \circ q).
\end{aligned}
$$

- Kommutativität: Ja

$$
m \circ n = ggT(m,n) = \prod_{p \in P} p^{\min\{v_p(m), v_p(n)\}} = \prod_{p \in P} p^{\min\{v_p(n), v_p(m)\}}
$$

$$
= ggT(n,m) = n \circ m
$$

- Neutrales Element: Nein (wieder, da $0 \notin \mathbb{N}$...)

$\lightning$ $e \in \mathbb{N}$ ist neutrales Element.

$$\Rightarrow \quad ggT(m,e) = m \circ e = m \quad \forall m \in \mathbb{N}.$$

Also: $e \underset{\text{direkt}}{=} ggT(2e, e) \underset{\text{s.o.}}{=} 2e \quad \lightning$ (da $e \neq 0$)

$\blacksquare$

**1.2.** Es ist

$$\prod_{g \in G} g^2 \overset{G\text{ abelsch}}{=} \left(\prod_{g \in G} g\right) \cdot \left(\prod_{g \in G} g\right)$$

$$= \left(\prod_{g \in G} g\right) \cdot \left(\prod_{g \in G} g^{-1}\right)$$

(Mit $g$ durchläuft auch $g^{-1}$ die gesamte Gruppe, denn: $G$ Gruppe $\Rightarrow$ $g \mapsto g^{-1}$ ist bijektiv)

$$\overset{G\text{ abelsch}}{=} \prod_{g \in G} g g^{-1}$$

$$= \prod_{g \in G} e$$

$$= e$$

$\blacksquare$

1.3. Benenne Elemente: $G = \{e, a, b, c\}$, $e$ sei neutrales Element. Klar: Wegen Neutralität von $e$ gilt stets:

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | | | |
| $b$ | $b$ | | | |
| $c$ | $c$ | | | |

Fallunterscheidung:

- Falls $a \circ a = e$, d.h.

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $\boxed{e}$ | | |
| $b$ | $b$ | | | |
| $c$ | $c$ | | | |

Da Links- und Rechtstranslation in einer Gruppe bijektiv sind, muss gelten:

$a \circ b = c = b \circ a$

$a \circ c = b = c \circ a$

Also:

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $\boxed{c}$ | $\boxed{b}$ |
| $b$ | $b$ | $\boxed{c}$ | | |
| $c$ | $c$ | $\boxed{b}$ | | |

Wegen der Bijektivität von Links- und Rechtstranslation gibt es für $b \circ b$ nur zwei Möglichkeiten:

$b \circ b = a$ $\rightsquigarrow$

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $\boxed{a}$ | |
| $c$ | $c$ | $b$ | | |

$\rightsquigarrow$

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $a$ | $\boxed{e}$ |
| $c$ | $c$ | $b$ | $\boxed{e}$ | $\boxed{a}$ |

„Zyklische Gruppe der Ordnung 4"
(1)

oder

$b \circ b = e$ $\rightsquigarrow$

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $\boxed{e}$ | |
| $c$ | $c$ | $b$ | | |

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $\boxed{a}$ |
| $c$ | $c$ | $b$ | $\boxed{a}$ | $\boxed{e}$ |

„Kleinsche Vierergruppe"
(2)

- Falls $a \circ a \neq e$ sei OE $a \circ a = b$ (sonst: Benenne b und c um)

$$\begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & & \\ b & b & & & \\ c & c & & & \end{array}$$

Mit dem gleichen Argument wie zuvor (Bijektivität..) folgt sukzessive:

$$\begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & \boxed{c} & \boxed{e} \\ b & b & \boxed{c} & & \\ c & c & \boxed{e} & & \end{array} \rightsquigarrow \begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & & \\ c & c & e & & \boxed{b} \end{array} \rightsquigarrow \begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & \boxed{e} & \boxed{a} \\ c & c & e & \boxed{a} & b \end{array} \quad (3)$$

$\blacksquare$

Bemerkungen:

- (1), (2) und (3) sind tatsächlich Gruppen.
- (1) und (3) definieren dieselbe Gruppe (Elemente sind nur verschieden benannt;

$$(3) \quad \begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array} \quad \underset{\text{schreiben}}{\overset{\text{Um-}}{\rightsquigarrow}} \quad \begin{array}{c|cccc} \circ & e & b & a & c \\ \hline e & e & b & a & c \\ a & a & c & b & e \\ b & b & e & c & a \\ c & c & a & e & b \end{array} \quad \underset{\text{schreiben}}{\overset{\text{Um-}}{\rightsquigarrow}} \quad \begin{array}{c|cccc} \circ & e & b & a & c \\ \hline e & e & b & a & c \\ b & b & e & c & a \\ a & a & c & b & e \\ c & c & a & e & b \end{array}$$

$$\underset{\text{a und b um}}{\overset{\text{Benenne}}{\rightsquigarrow}} \quad \begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & a & e \\ c & c & b & e & a \end{array} \quad (1)$$

- Dagegen unterscheiden sich die Gruppen (1) und (2) wesentlich.

  In (2) gilt $\forall x \in G: x \circ x = e$

  In (1) ist z.B. für $b \in G$: $b \circ b = a \neq e$.

1.4. (1) Identifiziere neutrales Element $e$:

- $e \neq a$ denn $a \circ y = c \quad (\neq y)$
- $e \neq b$ denn $b \circ b = x$
- $e \neq c$ denn $c \circ b = y$
- $e \neq y$ denn: $\nearrow\, e = y$. Tafel: $c \circ b = y \Rightarrow b = c^{-1} \Rightarrow b \circ c = c^{-1} \circ c = y$
  Aber (Tafel): $b \circ c = z$ ↯
- $e \neq z$ denn: $z \circ b = a$

$\Rightarrow$ $x$ ist das neutrale Element von $G$.

$\rightsquigarrow$

| $\circ$ | $a$ | $b$ | $c$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|
| $a$ | | | | $a$ | $c$ | $b$ |
| $b$ | | $x$ | $z$ | $b$ | | |
| $c$ | | $y$ | | $c$ | | |
| $x$ | $a$ | $b$ | $c$ | $x$ | $y$ | $z$ |
| $y$ | | | | $y$ | | |
| $z$ | | $a$ | | $z$ | $x$ | |

(2) $a \circ b = ?$

$$\left.\begin{array}{l} l_a \text{ bijektiv} \Rightarrow a \circ b \notin \{a, b, c\} \\ r_b \text{ bijektiv} \Rightarrow a \circ b \notin \{a, b, x, y\} \end{array}\right\} \Rightarrow a \circ b = z$$

(3) $r_b$ bijektiv $\Rightarrow$ $y \circ b = c$ (d.h. Spalte zu $b$ vollständig)

(4) $a \circ c \overset{(3)}{=} a \circ (y \circ b) = (a \circ y) \circ b = c \circ b = y$

(5) $l_a$ bijektiv $\Rightarrow$ $a \circ a = x$

Zwischenstand:

| $\circ$ | $a$ | $b$ | $c$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|
| $a$ | $x$ | $z$ | $y$ | $a$ | $c$ | $b$ |
| $b$ | | $x$ | $z$ | $b$ | | |
| $c$ | | $y$ | | $c$ | | |
| $x$ | $a$ | $b$ | $c$ | $x$ | $y$ | $z$ |
| $y$ | | $c$ | | $y$ | | |
| $z$ | | $a$ | | $z$ | $x$ | |

(6) $b \circ y = ?$

$$\left.\begin{array}{l} r_y \text{ bijektiv} \Rightarrow \quad b \circ y \notin \{c, x, y\} \\ \ell_b \text{ bijektiv} \Rightarrow \quad b \circ y \notin \{b, x, z\} \end{array}\right\} \Rightarrow b \circ y = a$$

(7) $z \circ y = x \xRightarrow[\text{Element}]{x \text{ neutr.}} y = z^{-1} \Rightarrow y \circ z = x$

(8) $y \circ c = ?$

$$\left.\begin{array}{l} r_y \text{ bijektiv} \Rightarrow \quad y \circ y \neq a \\ r_a \text{ bijektiv} \Rightarrow \quad y \circ a \neq a \end{array}\right\} \xRightarrow{\ell_y \text{ bij.}} y \circ c = a$$

(9) $z \circ c = ?$

$$\left.\begin{array}{l} r_c \text{ bijektiv} \Rightarrow \quad z \circ c \notin \{c, y, z, a\} \\ \ell_z \text{ bijektiv} \Rightarrow \quad z \circ c \notin \{a, z, x\} \end{array}\right\} \Rightarrow z \circ c = b$$

(10) $r_c$ bijektiv $\Rightarrow \quad c \circ c = x$

Zwischenstand:

| $\circ$ | $a$ | $b$ | $c$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|---|---|
| $a$ | $x$ | $z$ | $y$ | $a$ | $c$ | $b$ |
| $b$ | | $x$ | $z$ | $b$ | $a$ | |
| $c$ | | $y$ | $x$ | $c$ | | |
| $x$ | $a$ | $b$ | $c$ | $x$ | $y$ | $z$ |
| $y$ | | $c$ | $a$ | $y$ | | $x$ |
| $z$ | | $a$ | $b$ | $z$ | $x$ | |

(11) $c \circ z = c \circ (b \circ c) = (c \circ b) \circ c = y \circ c = a$

(12) $z \circ z = z \circ (b \circ c) = (z \circ b) \circ c = a \circ c = y$

(13) $r_z$ bijektiv $\Rightarrow \quad b \circ z = c$

(14) $\ell_b$ bijektiv $\Rightarrow \quad b \circ a = y$

(15) $\ell_z$ bijektiv $\Rightarrow \quad z \circ a = c$

(16) $y \circ a = y \circ (z \circ b) = (y \circ z) \circ b = x \circ b = b$

(17) $l_y$ bijektiv $\Rightarrow$ $y \circ y = z$

(18) $r_a$ bijektiv $\Rightarrow$ $c \circ a = z$

(19) $r_y$ bijektiv $\Rightarrow$ $c \circ y = b$

Resultat:

| $\circ$ | a | b | c | x | y | z |
|---|---|---|---|---|---|---|
| a | x | z | y | a | c | b |
| b | y | x | z | b | a | c |
| c | z | y | x | c | b | a |
| x | a | b | c | x | y | z |
| y | b | c | a | y | z | x |
| z | c | a | b | z | x | y |

(Also: Die Gruppentafel kann <u>eindeutig</u> vervollständigt werden !)

■