

**Lösungsvorschläge zu Lineare Algebra für Informatiker und Statistiker**

**Blatt 4**

**Zu Aufgabe 13:**

Für eine Gruppe  $(G, \circ)$  und  $\emptyset \neq U \subset G$  ist zu zeigen:

$$\underbrace{(\forall a, b \in U : a \circ b^{-1} \in U)}_{(\star)} \implies U \text{ Untergruppe von } G$$

Beweis:

Wir werden die im Tutorium bewiesene Aussage:  $\forall x \in G : (x^{-1})^{-1} = x$  ( $\clubsuit$ ) verwenden. Nach Vorlesung (1.9) gilt:

$$\emptyset \neq U \subset G \text{ Untergruppe von } G \iff \begin{cases} \textcircled{i} & \forall a, b \in U : a \circ b \in U \\ \textcircled{ii} & \forall a \in U : a^{-1} \in U \end{cases}$$

Wir müssen also  $\textcircled{i}$  und  $\textcircled{ii}$  aus der Voraussetzung  $(\star)$  herleiten.

- Wir zeigen zunächst, daß das neutrale Element  $e \in G$  in  $U$  liegt:

$$U \neq \emptyset \implies \exists u \in U \implies \text{mit } a := u \in U \text{ und } b := u \in U \text{ folgt aus } (\star) : e = u \circ u^{-1} \in U$$

- Damit folgt  $\forall a \in U : e \in U \wedge a \in U \xRightarrow{(\star)} a^{-1} \stackrel{e}{\underset{\text{neutral}}{=}} e \circ a^{-1} \in U$ ,

d.h.  $\textcircled{ii}$  ist gezeigt.

- Damit folgt  $\forall a, b \in U : b \in U \xRightarrow{\text{s.o.}} b^{-1} \in U$ , also  $a, b^{-1} \in U \xRightarrow{(\star)} a \circ (b^{-1})^{-1} \in U \implies a \circ b \stackrel{(\clubsuit)}{=} a \circ (b^{-1})^{-1} \in U$ ,

d.h. es gilt  $\textcircled{i}$ .

**Zu Aufgabe 14:** Sei  $(G, \circ)$  eine Gruppe und  $a \in G$ .

Wir verwenden wieder die im Tutorium bewiesenen Aussagen

$$(\clubsuit) \quad \forall x \in G : (x^{-1})^{-1} = x$$

$$(\clubsuit\clubsuit) \quad \forall a, b \in G : (a \circ b)^{-1} = b^{-1} \circ a^{-1}$$

$$\text{ad (a)} : \quad \forall n \in \mathbb{N} : (a^{-1})^n = (a^n)^{-1}$$

Beweis:

Es wird behauptet, daß das (eindeutig bestimmte !) Inverse zu  $a^n$  gleich  $(a^{-1})^n$  ist. Nach der Bemerkung in (1.2)/Vorl. reicht es dafür zu zeigen, daß  $(a^{-1})^n$  rechtsinvers zu  $a^n$  ist, d.h. daß gilt:

$$\forall n \in \mathbb{N} : a^n \circ (a^{-1})^n = e.$$

Beweis durch Induktion nach  $n$  :

Induktionsanfang:  $n = 1$   $a^1 \circ (a^{-1})^1 \stackrel{\text{Def.}}{=} a \circ a^{-1} = e$ .

Induktionsschritt  $n \mapsto n + 1$  : Es gelte für ein  $n \in \mathbb{N}$  :  $a^n \circ (a^{-1})^n = e$  (IV)

Induktionsbeweis:

$$\begin{aligned}
 a^{n+1} \circ (a^{-1})^{n+1} &\stackrel{\text{Def. der Potenz}}{=} \underbrace{(a \circ a \circ \dots \circ a)}_{n+1 \text{ mal}} \circ \underbrace{(a^{-1} \circ a^{-1} \circ \dots \circ a^{-1})}_{n+1 \text{ mal}} \\
 &\stackrel{\text{assoz.}}{=} \left[ \underbrace{(a \circ \dots \circ a)}_{n \text{ mal}} \circ a \right] \circ \left[ a^{-1} \circ \underbrace{(a^{-1} \circ \dots \circ a^{-1})}_{n \text{ mal}} \right] \\
 &\stackrel{\text{Def.}}{=} [a^n \circ a] \circ [a^{-1} \circ (a^{-1})^n] \\
 &\stackrel{\text{assoz.}}{=} a^n \circ ((a \circ a^{-1}) \circ (a^{-1})^n) \\
 &= a^n \circ (e \circ (a^{-1})^n) \\
 &= a^n \circ (a^{-1})^n \\
 &\stackrel{\text{IV}}{=} e
 \end{aligned}$$

**ad (b) :**  $\forall m, n \in \mathbb{Z} : a^{m+n} = a^m \circ a^n$

Beweis:

**1. Möglichkeit:** Wir testen alle Kombinationen für  $m$  und  $n$  in  $\mathbb{Z}$  unter Benutzung der Definitionen der Vorlesung:

$$a^0 := e \quad \wedge \quad \left[ \forall n \in \mathbb{N} : a^n = \underbrace{a \circ \dots \circ a}_{n \text{ mal}} \quad \wedge \quad a^{-n} = (a^{-1})^n = \underbrace{a^{-1} \circ \dots \circ a^{-1}}_{n \text{ mal}} \right]$$

• **Fall 1  $m, n > 0$  :**  $a^{m+n} \stackrel{\text{assoz.}}{=} \underbrace{a \circ \dots \circ a}_{m+n \text{ mal}} = \underbrace{(a \circ \dots \circ a)}_{m \text{ mal}} \circ \underbrace{(a \circ \dots \circ a)}_{n \text{ mal}} \stackrel{\text{Def.}}{=} a^m \circ a^n$

• **Fall 2  $m > 0 \wedge n = 0$  :**  $a^{m+0} = a^m = a^m \circ e \stackrel{\text{Def.}}{=} a^m \circ a^0$

• **Fall 3  $m > 0 \wedge n < 0$  :**

**3.1 :**  $m > |n| : m - |n| > 0 \implies$

$$\begin{aligned}
 a^{m+n} &= a^{m-|n|} = a^{m-|n|} \circ e \\
 &= a^{m-|n|} \circ \left( a^{|n|} \circ (a^{|n|})^{-1} \right) \\
 &\stackrel{\text{assoz.}}{=} \left( a^{m-|n|} \circ a^{|n|} \right) \circ (a^{|n|})^{-1} \\
 &\stackrel{\text{1. Fall}}{=} a^{(m-|n|)+|n|} \circ (a^{|n|})^{-1} \\
 &\stackrel{\text{Teil (a)}}{=} a^m \circ (a^{-1})^{|n|} \\
 &\stackrel{\text{Def.}}{=} a^m \circ a^{-|n|} \\
 &\stackrel{n=-|n|}{=} a^m \circ a^n
 \end{aligned}$$

**3.2 :**  $m = |n| \implies m + n = 0$ , d.h.  $n = -m$  :

$$a^{m+n} = a^0 = e = a^m \circ (a^m)^{-1} \stackrel{\text{Teil (a)}}{=} a^m \circ (a^{-1})^m \stackrel{\text{Def.}}{=} a^m \circ a^{-m} = a^m \circ a^n$$

**3.3 :**  $m < |n|$ , d.h.  $m + n < 0$  :

$$\begin{aligned}
a^{m+n} &= a^{m-|n|} = a^{-(|n|-m)} \stackrel{\text{Def.}}{=}_{|n|-m>0} (a^{-1})^{|n|-m} \\
&\stackrel{\text{Teil (a)}}{=}_{|n|>m} (a^{|n|-m})^{-1} \\
&\stackrel{\text{Fall 3.1}}{=}_{n>m=|-m|} (a^{|n|} \circ a^{-m})^{-1} \\
&\stackrel{(\clubsuit\clubsuit)}{=} (a^{-m})^{-1} \circ (a^{|n|})^{-1} \\
&\stackrel{\text{Teil (a)}}{=}_{m>0} ((a^m)^{-1})^{-1} \circ (a^{|n|})^{-1} \\
&\stackrel{\text{Def.}}{=}_{(\clubsuit)} a^m \circ a^n
\end{aligned}$$

• **Fall 4**  $m = 0 \wedge n \in \mathbb{Z}$  :  $a^{0+n} = a^n = e \circ a^n = a^0 \circ a^n$

• **Fall 5**  $m < 0 \wedge n > 0$  :  $a^{m+n} = a^{-|m|+n}$

**5.1**  $|m| > n$  :

$$\begin{aligned}
a^{m+n} &= a^{-|m|+n} = a^{-(|m|-n)} \\
&\stackrel{\text{Def.}}{=}_{|m|-n>0} (a^{-1})^{|m|-n} \\
&\stackrel{\text{Fall 3.1}}{=}_{|m|>|-n|=n} (a^{-1})^{|m|} \circ (a^{-1})^{-n} \\
&\stackrel{\text{Def.}}{=}_{n>0} a^{-|m|} \circ ((a^{-1})^{-1})^n \\
&\stackrel{(\clubsuit)}{=}_{-|m|=m} a^m \circ a^n
\end{aligned}$$

**5.2**  $|m| = n \iff -m = n$  :

$$a^{m+n} = a^0 = e = (a^n)^{-1} \circ a^n \stackrel{\text{Teil (a)}}{=}_{n>0} (a^{-1})^n \circ a^n \stackrel{\text{Def.}}{=} a^{-n} \circ a^n = a^m \circ a^n$$

**5.3**  $|m| < n$  :

$$\begin{aligned}
a^{m+n} &= a^{-|m|+n} \stackrel{(\clubsuit)}{=} ((a^{-1})^{-1})^{-|m|+n} \\
&= (a^{-1})^{-(n-|m|)} = (a^{-1})^{|m|-n} \\
&\stackrel{\text{Fall 3.3}}{=} (a^{-1})^{|m|} \circ (a^{-1})^{-n} \\
&\stackrel{\text{Def.}}{=}_{n>0} a^{-|m|} \circ ((a^{-1})^{-1})^n \\
&\stackrel{(\clubsuit)}{=} a^m \circ a^n
\end{aligned}$$

• **Fall 6**  $m < 0 \wedge n = 0$  :  $a^{m+n} = a^m = a^m \circ e \stackrel{\text{Def.}}{=} a^m \circ a^0$

• **Fall 7**  $m < 0 \wedge n < 0$  :

$$\begin{aligned}
a^{m+n} &= a^{-|m|-|n|} = a^{-(|m|+|n|)} \\
&\stackrel{\text{Def.}}{=} (a^{-1})^{|m|+|n|} \\
&\stackrel{\text{Fall 1}}{=} (a^{-1})^{|m|} \circ (a^{-1})^{|n|} \\
&\stackrel{\text{Def.}}{=} a^{-|m|} \circ a^{-|n|} \\
&= a^m \circ a^n
\end{aligned}$$

**2.Möglichkeit:** Wir suchen einen kürzeren Lösungsweg, bei dem wir nicht alle Fälle testen müssen. Dazu beweisen wir zunächst:

$$(\clubsuit\clubsuit\clubsuit) \quad \forall l \in \mathbb{Z} : a^{-l} = (a^{-1})^l = (a^l)^{-1}$$

(Beweis:

Für  $l > 0$  ist dies die Behauptung aus Teil (a).

Für  $l = 0$  :  $a^{-0} = a^0 = e = (a^{-1})^0 = e = e^{-1} = (a^0)^{-1}$ .

Für  $l < 0$  :

$$a^{-l} = a^{|l|} \stackrel{(\clubsuit)}{=} \left( (a^{|l|})^{-1} \right)^{-1} \stackrel{|l| \geq 0}{\stackrel{\text{Teil (a)}}{=}} \left( (a^{-1})^{|l|} \right)^{-1} \begin{cases} \stackrel{\text{Def.}}{=} (a^{-|l|})^{-1} = (a^l)^{-1} \\ \stackrel{\text{Teil (a)}}{=} (a^{-1})^{-|l|} = (a^{-1})^{-l} \end{cases}$$

q.e.d.

$$(1) \quad \forall m \in \mathbb{N}_0 : a^{m+1} = a^m \circ a$$

denn:

Für  $m = 0$  :  $a^{0+1} = a^1 = a = e \circ a = a^0 \circ a$

Für  $m \geq 1$  :  $a^{m+1} \stackrel{\text{Def.}}{=} \underbrace{a \circ \dots \circ a}_{(m+1) \text{ mal}} = \underbrace{(a \circ \dots \circ a)}_{m \text{ mal}} \circ a \stackrel{\text{Def.}}{=} a^m \circ a \quad \text{q.e.d.}$

$$(2) \quad \forall m \in \mathbb{N} : a^{-m+1} = a^{-m} \circ a$$

denn:

$$\begin{aligned} a^{-m+1} &= a^{-(m-1)} \stackrel{m-1 \geq 0}{\stackrel{(\clubsuit\clubsuit\clubsuit)}{=}} (a^{-1})^{m-1} = (a^{-1})^{m-1} \circ e = (a^{-1})^{m-1} \circ (a^{-1} \circ a) \stackrel{\text{assoz.}}{=} \\ &= \left( (a^{-1})^{m-1} \circ a^{-1} \right) \circ a \stackrel{m-1 \geq 0}{\stackrel{\text{①}}{=}} (a^{-1})^{(m-1)+1} \circ a = \\ &= (a^{-1})^m \circ a \stackrel{(\clubsuit\clubsuit\clubsuit)}{=} a^{-m} \circ a \end{aligned}$$

$$(3) \quad \forall m \in \mathbb{Z} : \left[ \forall n \in \mathbb{N}_0 : a^{m+n} = a^m \circ a^n \right]$$

Induktion nach  $n \in \mathbb{N}_0$  :

Induktionsanfang:  $n = 0$  :  $a^{m+0} = a^m = a^m \circ e = a^m \circ a^0$

Induktionsschritt:  $n \mapsto n+1$  : Es sei für ein  $n \in \mathbb{N}_0$  wahr:  $a^{m+n} = a^m \circ a^n$  (IV).

Dann folgt:

$$a^{m+(n+1)} = a^{(m+n)+1} \stackrel{\text{①}}{=} a^{m+n} \circ a \stackrel{\text{(IV)}}{=} (a^m \circ a^n) \circ a \stackrel{\text{assoz.}}{=} a^m \circ (a^n \circ a) \stackrel{\text{①}}{=} a^m \circ a^{n+1}$$

$$(4) \quad \forall m \in \mathbb{Z} \forall n < 0 : a^{m+n} = a^m \circ a^n$$

Denn

$$a^{m+n} = a^{m-|n|} \stackrel{(\clubsuit\clubsuit\clubsuit)}{=} (a^{-1})^{-m+|n|} \stackrel{\text{③}}{=} (a^{-1})^{-m} \circ (a^{-1})^{|n|} \stackrel{(\clubsuit\clubsuit\clubsuit)}{=} a^{-(-m)} \circ a^{-|n|} = a^m \circ a^n \quad \text{q.e.d.}$$

**ad (c):**  $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$  ist eine Untergruppe von  $G$ ,  
(die sogenannte „von  $a$  erzeugte zyklische Untergruppe von  $G$ “).

Wir müssen das in Aufgabe (13) bewiesene Untergruppenkriterien überprüfen:

$$\forall x, y \in U : x \circ y^{-1} \in U \implies U \text{ ist Untergruppe}$$

Seien also  $x, y \in \langle a \rangle \implies \exists k, l \in \mathbb{Z} : x = a^k \wedge y = a^l$ .

Da nach Teil (b) gilt:  $a^m \circ a^{-m} = a^{m+(-m)} = a^0 = e$  folgt aus der Eindeutigkeit des Inversen in der Gruppe  $G$ , daß für jedes  $m \in \mathbb{Z} : (a^m)^{-1} = a^{-m}$ , also:

$$x \circ y^{-1} = a^k \circ (a^l)^{-1} = a^k \circ a^{-l} \stackrel{\text{Teil (b)}}{=} a^{k-l} \in \langle a \rangle, \text{ da } k-l \in \mathbb{Z} \implies \langle a \rangle \text{ ist Untergruppe.}$$

### Zu Aufgabe 15:

Es ist die Verknüpfungstafel für die Gruppe  $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$  zu erstellen, und es sind alle deren zyklischen Untergruppen zu bestimmen.

Die Verknüpfungstafel ergibt sich zu:

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Dabei ist die Verknüpfungsreihenfolge folgendermaßen definiert:

$\circ$	$\dots$	$b$
$\vdots$	$\dots$	$\dots$
$a$	$\dots$	$a \circ b$

### Zyklische Untergruppen:

Wir benutzen:

(■)  $\forall k \in \mathbb{Z} \exists q \in \mathbb{Z} : k = q \cdot 6 + r$  mit  $0 \leq r < 6$  (nach Vorlesung Satz (0.11))

(■■)  $\forall m, n \in \mathbb{Z} : (a^m)^n = a^{mn}$  (nach Tutorium)

(■■■)  $G$  (abelsche) Gruppe und  $n = |G| \implies \forall x \in G : x^n = e$  (Satz von Fermat, Vorl. Satz 1.7)

Zunächst gilt mit (■) in jeder (abelschen) Gruppe  $G$  mit  $|G| = n$  :

$\forall k \in \mathbb{Z} : k = q \cdot n + r$  für geeignete  $q, r \in \mathbb{Z}$  mit  $0 \leq r < n$

$$\implies \forall a \in G : a^k = a^{qn+r} \stackrel{\text{Aufg. 14(b)}}{=} a^{qn} \circ a^r \stackrel{(\text{■■})}{=} (a^n)^q \circ a^r \stackrel{(\text{■■■})}{=} e^q \circ a^r = e \circ a^r = a^r$$

Also folgt:  $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = \{a^r \mid r \in \mathbb{N}_0 \wedge 0 \leq r < n\}$  (♥).

Damit ( da  $|\mathbb{Z}_7 \setminus \{0\}| = 6$  ) :

- $\langle \bar{1} \rangle = \{\bar{1}^k \mid k \in \mathbb{Z}\} = \{\bar{1}\}$
- $\langle \bar{2} \rangle = \{\bar{2}^r \mid 0 \leq r < 6\} = \{\bar{2}^0, \bar{2}^1, \bar{2}^2, \bar{2}^3, \bar{2}^4, \bar{2}^5\} = \{\bar{1}, \bar{2}, \bar{4}, \bar{1}, \bar{2}, \bar{4}\} = \{\bar{1}, \bar{2}, \bar{4}\}$ .
- $\langle \bar{3} \rangle = \{\bar{3}^r \mid 0 \leq r < 6\} = \{\bar{3}^0, \bar{3}^1, \bar{3}^2, \bar{3}^3, \bar{3}^4, \bar{3}^5\} = \{\bar{1}, \bar{3}, \bar{2}, \bar{6}, \bar{4}, \bar{5}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \mathbb{Z}_7 \setminus \{0\}$
- $\langle \bar{4} \rangle = \{\bar{4}^r \mid 0 \leq r < 6\} = \{\bar{4}^0, \bar{4}^1, \bar{4}^2, \bar{4}^3, \bar{4}^4, \bar{4}^5\} = \{\bar{1}, \bar{4}, \bar{2}, \bar{1}, \bar{4}, \bar{2}\} = \{\bar{1}, \bar{2}, \bar{4}\}$
- $\langle \bar{5} \rangle = \{\bar{5}^r \mid 0 \leq r < 6\} = \{\bar{5}^0, \bar{5}^1, \bar{5}^2, \bar{5}^3, \bar{5}^4, \bar{5}^5\} = \{\bar{1}, \bar{5}, \bar{4}, \bar{6}, \bar{2}, \bar{3}\} = \mathbb{Z}_7 \setminus \{0\}$
- $\langle \bar{6} \rangle = \{\bar{6}^r \mid 0 \leq r < 6\} = \{\bar{6}^0, \bar{6}^1, \bar{6}^2, \bar{6}^3, \bar{6}^4, \bar{6}^5\} = \{\bar{1}, \bar{6}, \bar{1}, \bar{6}, \bar{1}, \bar{6}\} = \{\bar{1}, \bar{6}\}$

Ergänzung: Beweis zu (■) :

Sei  $m \in \mathbb{Z}$  fest, aber beliebig. Dann gilt:  $\forall n \in \mathbb{N}_0 : (a^m)^n = a^{mn} \quad (\star)$

Beweis durch Induktion nach  $n$  :

Induktionsanfang  $n = 0$  :  $(a^m)^0 = e = a^0 = a^{m \cdot 0}$

Induktionsschritt  $n \mapsto n + 1$  : Es gelte für ein  $n \in \mathbb{N}_0$  :  $(a^m)^n = a^{mn} \quad (\text{IV})$

Induktionsbeweis:  $(a^m)^{n+1} \stackrel{\text{Aufg. 14(b)}}{=} (a^m)^n \circ a^m \stackrel{\text{IV)}}{=} a^{mn} \circ a^m \stackrel{\text{Aufg. 14(b)}}{=} a^{mn+m} = a^{m \cdot (n+1)} \quad \text{q.e.d.}$

Bleibt noch zu zeigen: Für beliebiges  $m \in \mathbb{Z}$  :  $n < 0 \implies (a^m)^n = a^{mn}$ .

Sei also  $m \in \mathbb{Z}$  beliebig und  $n < 0$ . Dann gilt:

$$(a^m)^n = (a^m)^{-|n|} \stackrel{\text{Def.}}{=} \left[ (a^m)^{-1} \right]^{|n|} \stackrel{\text{14(a)}}{=} \left[ (a^m)^{|n|} \right]^{-1} \stackrel{\text{s.o.}}{=} \left[ a^{m \cdot |n|} \right]^{-1}$$

$$\bullet \text{ falls } m > 0 : mn < 0 \stackrel{\text{Aufg. 14(a)}}{\implies} (a^{m \cdot |n|})^{-1} = (a^{-1})^{m|n|} \stackrel{\text{Def.}}{=} a^{-m|n|} \stackrel{n=-|n|}{=} a^{m \cdot n}$$

$$\bullet \text{ falls } m = 0 : mn = 0 \implies (a^{m \cdot |n|})^{-1} = a^0 = e = a^{0 \cdot n}$$

$$\begin{aligned} \bullet \text{ falls } m < 0 : mn > 0 &\implies (a^{m \cdot |n|})^{-1} = (a^{-|m||n|})^{-1} \stackrel{\text{Aufg. 14(a)}}{=} \\ &= \left( (a^{|m||n|})^{-1} \right)^{-1} \stackrel{(\clubsuit)}{=} \\ &= a^{|m||n|} \\ &= a^{(-|m|) \cdot (-|n|)} \\ &= a^{m \cdot n} \end{aligned}$$

### Zu Aufgabe 16:

**Ad (a) :** Es seien  $(G, \circ)$  und  $(H, *)$  Gruppen. Dann ist auch  $G \times H$  mit der Verknüpfung

$$\diamond : (G \times H) \times (G \times H) \rightarrow G \times H, (g_1, h_1) \diamond (g_2, h_2) := (g_1 \circ g_2, h_1 * h_2)$$

eine Gruppe.

#### Beweis:

Weil für alle  $g_1, g_2 \in G$  und  $h_1, h_2 \in H$  mit der Abgeschlossenheit der Gruppenoperationen in  $G$  bzw.  $H$  auch  $g_1 \circ g_2 \in G$  sowie  $h_1 * h_2 \in H$ , gilt  $(g_1, g_2) \diamond (h_1, h_2) = (g_1 \circ g_2, h_1 * h_2) \in G \times H$ .

Zu den Gruppenaxiomen:

- **assoziativ:** Es seien  $g_1, g_2, g_3 \in G$  und  $h_1, h_2, h_3 \in H$ . Dann:

$$\begin{aligned} (g_1, h_1) \diamond ((g_2, h_2) \diamond (g_3, h_3)) &\stackrel{\text{Def.}}{=} (g_1, h_1) \diamond (g_2 \circ g_3, h_2 * h_3) \\ &\stackrel{\text{Def.}}{=} (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3)) \\ &\stackrel{\text{Assoz. von } \circ, *}{=} ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) \\ &\stackrel{\text{Def.}}{=} (g_1 \circ g_2, h_1 * h_2) \diamond (g_3, h_3) \\ &\stackrel{\text{Def.}}{=} ((g_1, h_1) \diamond (g_2, h_2)) \diamond (g_3, h_3) \end{aligned}$$

- **Existenz des neutralen Elements:**

Es sei  $e$  neutral in  $G$  und  $f$  neutrales Element in  $H$ . Dann gilt:

$$\forall g \in G \forall h \in H : (g, h) \diamond (e, f) \stackrel{\text{Def.}}{=} (g \circ e, h * f) \stackrel{\text{Def.}}{=} (g, h)$$

Damit ist  $(e, f)$  rechtsneutral in  $G \times H$ , nach Vorlesung (1.2) damit auch neutrales Element in  $(G \times H, \diamond)$ .

- **Existenz inverser Elemente:**

Es seien  $g \in G$  und  $h \in H$ . Dann folgt mit  $g^{-1}$  das inverse Element zu  $g$  in  $G$  und  $h^{-1}$  das inverse Element zu  $h$  in  $H$ :

$$(g, h) \diamond (g^{-1}, h^{-1}) \stackrel{\text{Def.}}{=} (g \circ g^{-1}, h * h^{-1}) \stackrel{e, f}{\underset{\text{neutral}}{=}} (e, f)$$

Damit ist  $(g^{-1}, h^{-1})$  rechtsinvers zu  $(g, h)$  in  $G \times H$ , und damit auch inverses Element von  $(g, h)$ .

**Ad (b) :** Die Gruppe  $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$  ist isomorph zu  $(\mathbb{Z}_6, +)$ .

#### Beweis:

Weil in der zyklischen Gruppe  $(\mathbb{Z}_6, +)$  das Element  $\bar{1}$  erzeugendes Element ist, d.h.

$$\langle \bar{1} \rangle = \{k \cdot \bar{1} \mid k \in \mathbb{Z}\} \stackrel{\text{Def.}}{=} \{\overline{k \cdot 1} \mid k \in \mathbb{Z}\} = \{\bar{k} \mid k \in \mathbb{Z}\} \ni \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} \implies \langle \bar{1} \rangle = \mathbb{Z}_6$$

suchen wir auch in der Gruppe  $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$  nach einem erzeugenden Element; dabei berücksichtigen wir, daß  $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$  6 Elemente hat und benutzen (♥) aus Aufgabe 15:

$$\begin{aligned} \langle (\bar{1}, \bar{1}) \rangle &= \{0 \cdot (\bar{1}, \bar{1}), 1 \cdot (\bar{1}, \bar{1}), 2 \cdot (\bar{1}, \bar{1}), 3 \cdot (\bar{1}, \bar{1}), 4 \cdot (\bar{1}, \bar{1}), 5 \cdot (\bar{1}, \bar{1})\} \\ &= \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{2})\} = \mathbb{Z}_6 \end{aligned}$$

Mit der Vorschrift aus Teil (a) ist  $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$  eine Gruppe.

Es bietet sich damit an, den Isomorphismus  $\varphi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$  über die Zuordnung

$$\varphi(\bar{1}) = (\bar{1}, \bar{1}) \quad \text{bzw.} \quad \varphi(r \cdot \bar{1}) = r \cdot (\bar{1}, \bar{1}) = r \cdot \varphi(\bar{1}) \quad \text{mit} \quad 0 \leq r < 6 \quad (r \in \mathbb{N}_0)$$

zu definieren.

Weil  $\mathbb{Z}_6 = \{r \cdot \bar{1} \mid r \in \mathbb{N}_0 \wedge 0 \leq r < 6\}$  (siehe (♥)) und  $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{r \cdot (\bar{1}, \bar{1}) \mid r \in \mathbb{N}_0 \wedge 0 \leq r < 6\}$  ist damit jedem Element von  $\mathbb{Z}_6$  ein Element aus  $\mathbb{Z}_2 \times \mathbb{Z}_3$  zugeordnet und umgekehrt auch jedes Element von  $\mathbb{Z}_2 \times \mathbb{Z}_3$  Bild genau eines Elements aus  $\mathbb{Z}_6$ .

Folglich ist  $\varphi$  bijektiv.

Es bleibt die Homomorphismeigenschaft nachzuweisen:

Jedes Element  $x$  von  $\mathbb{Z}_6$  hat die Gestalt  $x = r \cdot \bar{1}$  für ein  $r \in \{0, \dots, 5\}$ . Damit:

$$x, y \in \mathbb{Z}_6 \implies \exists r, s \in \{0, \dots, 5\} : x = r \cdot \bar{1} \wedge y = s \cdot \bar{1} \implies$$

$$\varphi(x + y) = \varphi(r \cdot \bar{1} + l \cdot \bar{1}) \stackrel{(\bullet)}{=} \varphi((r + s) \cdot \bar{1}) \quad (\text{ad } (\bullet) : \text{wegen Aufg. 14 (b) mit Verknüpfung } \circ = +)$$

Mit  $r + s = 6 \cdot q + l$ ,  $0 \leq l < 6$ , folgt in  $(\mathbb{Z}_6, +)$ :

$$(r + s) \cdot \bar{1} = (q6 + l) \cdot \bar{1} \stackrel{\text{Aufg. 14(b)}}{=} q \cdot \underbrace{(6 \cdot \bar{1})}_{\substack{=0 \\ (\text{nach} \\ \text{Fermat})}} + l \cdot \bar{1} = l \cdot \bar{1} \stackrel{\text{Def.}}{=} \bar{l} \implies$$

$$\varphi(x + y) = \varphi(\bar{l}) \stackrel{\text{Def. von } \varphi}{=} l \cdot (\bar{1}, \bar{1}).$$

Andererseits gilt:

$$\begin{aligned} \varphi(x) + \varphi(y) &= \varphi(r \cdot \bar{1}) + \varphi(s \cdot \bar{1}) \stackrel{\text{Def. von } \varphi}{=} r \cdot (\bar{1}, \bar{1}) + s \cdot (\bar{1}, \bar{1}) \\ &= (r + s) \cdot (\bar{1}, \bar{1}) \quad (\text{weg, Aufg. 14(b) mit Verknüpfung } \circ = + \text{ in } \mathbb{Z}_2 \times \mathbb{Z}_3) \\ &= (q6 + l) \cdot (\bar{1}, \bar{1}) \\ &\stackrel{\text{Aufg. 14(b)}}{=} q \cdot \underbrace{[6 \cdot (\bar{1}, \bar{1})]}_{\substack{=0 \\ (\text{nach Fermat})}} + l \cdot (\bar{1}, \bar{1}) \quad (\text{mit } (\blacksquare) \text{ aus Aufg. 15}) \\ &= l \cdot (\bar{1}, \bar{1}) \end{aligned}$$

Also ist  $\varphi(x + y) = \varphi(x) + \varphi(y)$  wie gewünscht.