

**Lösungen**

- 1.) i) Die 1 ist neutrales Element der Multiplikation.  $(M, \circ)$  ist damit keine Gruppe, denn es gibt keine inversen Elemente für  $a \circ x = 1$  (zum Beispiel  $5 \cdot x = 1$ ). Dies müsste ja  $1/a \in \mathbb{Q} \notin \mathbb{Z}$  sein.  
ii)  $(\mathbb{R}, \circ)$  ist eine Gruppe.  
iii) Die Menge  $M$  ist leer und damit ist  $(M, \circ)$  keine Gruppe.
- 2.) Ja, es handelt sich um eine Gruppentafel. Das neutrale Element ist  $a$ . In jeder Zeile / Spalte kommt jedes Element genau einmal vor. Die jeweils inversen Elemente sowie die Abgeschlossenheit liest man ebenfalls ab. Die Gruppe ist kommutativ (Symmetrie zur Hauptdiagonalen). Die Gruppe ist isomorph zur  $\mathbb{Z}_3$ .  
! Die Assoziativität kann man nicht in der Gruppentafel ablesen, diese müsste für jeweils 3 von allen Elementen geprüft werden.
- 3.) Gruppenaxiome nachweisen.
- 4.) Ja,  $(\mathbb{Z}, +)$  ist Untergruppe von  $(\mathbb{Q}, +)$ .
- 5.) Beweisen Sie: Der Durchschnitt zweier Untergruppen  $H$  und  $K$  der Gruppe  $G$  ist eine Untergruppe der Gruppe  $G$ .

Zu zeigen sind die Untergruppenkriterien:

1.  $U = H \cap K \subseteq G$  und  $U = H \cap K \neq \emptyset$
2. Für alle  $u_1, u_2 \in U$  gilt  $u_1 \circ u_2^{-1} \in U$

Beweis:

$e \in H$ . Denn da  $H$  nicht leer ist ( $H$  ist ja Untergruppe), gibt es ein Element  $h \in H$ . Doch dann enthält  $H$  auch  $h \circ h^{-1} = e$  (Untergruppenkriterium), die Identität von  $G$ . Analog folgt  $e \in K$ . Damit ist  $e \in H \cap K$  und  $H \cap K \neq \emptyset$ .

Sind  $u_1, u_2 \in H \cap K$ , dann  $u_1, u_2 \in H$  und  $u_1 \circ u_2^{-1} \in H$  (da ja  $H$  Untergruppe) und auch  $u_1 \circ u_2^{-1} \in K$  (da auch  $K$  Untergruppe). Damit ist  $u_1 \circ u_2^{-1} \in H \cap K$  und  $U = H \cap K$  ist eine Untergruppe von  $G$

6.) Gegeben sind für  $x \in \mathbb{R} \setminus \{0\}$  die 4 Funktionen

$$f_0(x) = x, f_1(x) = \frac{1}{x}, f_2(x) = -x, f_3(x) = -\frac{1}{x}$$

Hier müssen wie üblich die Gruppenaxiome geprüft werden.

- Assoziativität: Die Verkettung von Abbildungen ist stets assoziativ.
- Existenz des Neutralen Elementes:  
Die Identität  $\text{id} = f_0(x)$  stellt selbstverständlich bei der Komposition von Abbildungen das neutrale Element dar. Es gilt:

$$f_0 \circ f_0 = f_0(f_0(x)) = x = f_0 \circ f_0 = f_0.$$

$$f_1 \circ f_0 = f_1(f_0(x)) = \frac{1}{x} = f_0 \circ f_1 = f_0(f_1(x)) = f_1.$$

$$f_2 \circ f_0 = f_2(f_0(x)) = -x = f_0 \circ f_2 = f_0(f_2(x)) = f_2.$$

$$f_3 \circ f_0 = f_3(f_0(x)) = -\frac{1}{x} = f_0 \circ f_3 = f_0(f_3(x)) = f_3.$$

- Existenz des Inversen Elementes zu jedem Element:

$$f_0 \circ f_0 = f_0(f_0(x)) = x = f_0.$$

$$f_1 \circ f_1 = f_1(f_1(x)) = \frac{1}{\frac{1}{x}} = x = f_0.$$

$$f_2 \circ f_2 = f_2(f_2(x)) = -(-x) = x = f_0$$

$$f_3 \circ f_3 = f_3(f_3(x)) = -\frac{1}{-\frac{1}{x}} = x = f_0.$$

- Abgeschlossenheit, dazu müssen alle Verknüpfungen strategisch berechnet werden. Die Gruppentafel ergibt sich wie folgt:

| $\circ$ | $f_0$ | $f_1$ | $f_2$ | $f_3$ |
|---------|-------|-------|-------|-------|
| $f_0$   | $f_0$ | $f_1$ | $f_2$ | $f_3$ |
| $f_1$   | $f_1$ | $f_0$ | $f_3$ | $f_2$ |
| $f_2$   | $f_2$ | $f_3$ | $f_0$ | $f_1$ |
| $f_3$   | $f_3$ | $f_2$ | $f_1$ | $f_0$ |

Es sind also alle Elemente selbstinvers. Die Gruppe ist isomorph zur Kleinschen Vierergruppe (Deckabbildungen des unregulären Rechtecks).

7.) Man beweise: Ist  $G$  eine endliche Gruppe der Ordnung  $n$ , so ist  $a^n = e$  für jedes  $a \in G$ .

Beweis: Nach Satz (siehe unten) ist die Ordnung  $m$  eines Elementes  $a \in G$  Teiler der Gruppenordnung  $n$ , es gilt also  $m \cdot t = n$  mit  $t \in \mathbb{N}$ . Damit folgt  $a^n = (a^m)^t = e^t = e$ .

Info: Zunächst gilt der Satz, dass jedes Element einer Gruppe eine zyklische Untergruppe erzeugt. Hier ist  $H = \langle a^2 \rangle$  eine Untergruppe von  $G$  durch  $\{a^2\}$  erzeugt. Dies musste aber nicht gezeigt werden.

Definition „Ordnung eines Elementes“:

Ist  $a$  ein Element der Gruppe  $G$  und  $m$  der kleinste Exponent mit  $a^m = e$ , so nennt man  $m$  die Ordnung von  $a$ .

Satz: In endlichen Gruppen ist die Ordnung eines Elementes stets Teiler der Gruppenordnung.

Beweis:

Da die Potenzen von  $a$  eine zyklische Untergruppe der Ordnung  $m$  bilden und die Ordnung jeder Untergruppe Teiler der Gruppenordnung ist (Satz von Lagrange).

8.) Zu zeigen ist die Assoziativität, also  $A \cdot (B \cdot C) = (A \cdot B) \cdot C$  für alle  $A, B, C \in \mathbb{R}^{2 \times 2}$ .

Dies zeigt man durch Ausrechnen und Gleichheit der linken und rechten Seite, unter Verwendung der gewöhnlichen Matrizenmultiplikation. (Indexschlacht)

Linke Seite:

$$A \cdot (B \cdot C) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \left[ \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \right] = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 \cdot c_1 + b_2 \cdot c_3 & b_1 \cdot c_2 + b_2 \cdot c_4 \\ b_3 \cdot c_1 + b_4 \cdot c_3 & b_3 \cdot c_2 + b_4 \cdot c_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 \cdot (b_1 \cdot c_1 + b_2 \cdot c_3) + a_2 \cdot (b_3 \cdot c_1 + b_4 \cdot c_3) & a_1 \cdot (b_1 \cdot c_2 + b_2 \cdot c_4) + a_2 \cdot (b_3 \cdot c_2 + b_4 \cdot c_4) \\ a_3 \cdot (b_1 \cdot c_1 + b_2 \cdot c_3) + a_4 \cdot (b_3 \cdot c_1 + b_4 \cdot c_3) & a_3 \cdot (b_1 \cdot c_2 + b_2 \cdot c_4) + a_4 \cdot (b_3 \cdot c_2 + b_4 \cdot c_4) \end{pmatrix}$$

Rechte Seite:

$$(A \cdot B) \cdot C = \left[ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \right] \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} = \begin{pmatrix} a_1 \cdot b_1 + a_2 \cdot b_3 & a_1 \cdot b_2 + a_2 \cdot b_4 \\ a_3 \cdot b_1 + a_4 \cdot b_3 & a_3 \cdot b_2 + a_4 \cdot b_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$

$$= \begin{pmatrix} (a_1 \cdot b_1 + a_2 \cdot b_3) \cdot c_1 + (a_1 \cdot b_2 + a_2 \cdot b_4) \cdot c_3 & (a_1 \cdot b_1 + a_2 \cdot b_3) \cdot c_2 + (a_1 \cdot b_2 + a_2 \cdot b_4) \cdot c_4 \\ (a_3 \cdot b_1 + a_4 \cdot b_3) \cdot c_1 + (a_3 \cdot b_2 + a_4 \cdot b_4) \cdot c_3 & (a_3 \cdot b_1 + a_4 \cdot b_3) \cdot c_2 + (a_3 \cdot b_2 + a_4 \cdot b_4) \cdot c_4 \end{pmatrix}$$

Man sieht die beiden Seiten sind gleich (sonst weiter umformen...).

9.) Zeigen Sie: In jeder Gruppe  $G$  gilt:  $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$  für alle  $a, b \in G$

Es sei  $x = (a \circ b)^{-1}$  gesetzt. Beweis mit folgender Schlusskette:

$$x = (a \circ b)^{-1} \Rightarrow x \circ (a \circ b) = e \Rightarrow (x \circ (a \circ b)) \circ b^{-1} = e \circ b^{-1} \Rightarrow x \circ ((a \circ b) \circ b^{-1}) = e \circ b^{-1}$$

$$\Rightarrow x \circ (a \circ (b \circ b^{-1})) = e \circ b^{-1} \Rightarrow x \circ (a \circ e) = e \circ b^{-1} \Rightarrow x \circ a = b^{-1}$$

$$\Rightarrow (x \circ a) \circ a^{-1} = b^{-1} \circ a^{-1} \Rightarrow x \circ (a \circ a^{-1}) = b^{-1} \circ a^{-1} \Rightarrow x \circ e = b^{-1} \circ a^{-1}$$

$$\Rightarrow x = b^{-1} \circ a^{-1}. \text{ Damit also } (a \circ b)^{-1} = b^{-1} \circ a^{-1} \text{ für alle } a, b \in G.$$

(Übrigens: nur in kommutativen Gruppen gilt also  $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$ ).

- 10.) Sei  $G$  die zyklische Gruppe der Ordnung 4 durch  $\{a\}$  erzeugt, also  $G = \langle a \rangle$ .  
 Sei  $H = \langle a^2 \rangle$  eine Untergruppe von  $G$ . Bestimmen Sie alle rechten Nebenklassen von  $H$  in  $G$ .

Es ergeben sich die verschiedenen Nebenklassen:

$$H \circ e = \{e; a^2\} = H$$

$$H \circ a = \{a; a^3\} = Ha.$$

$$H \circ a^2 = \{a^2; a^4\} = \{e; a^2\} = H$$

$$H \circ a^3 = \{a^3; a^5\} = \{a^3; a\} = Ha.$$

Die verschiedenen Nebenklassen von  $H$  in  $G$  sind damit  $H$  und  $Ha$ . Man sieht auch hier je zwei Nebenklassen sind disjunkt:  $H \cap Ha = \emptyset$  und die Vereinigung aller Nebenklassen ist  $G$ :  $H \cup Ha = \{e; a^2; a; a^3\} = G$ .

- 11.) Richtig oder falsch?

- Zu jeder natürlichen Zahl  $n$  gibt es mindestens eine Gruppe der Ordnung  $n$ .  
(wahr, die zyklische Gruppe der Ordnung  $n$ )
- Zu jeder natürlichen Zahl  $n$  gibt es genau eine Gruppe der Ordnung  $n$ .  
(falsch, Gegenbeispiel: Kleinsche Vierergruppe und Zyklische Gruppe der Ordnung 4 sind nicht isomorph.)
- Jede Gruppe hat eine Untergruppe.  
(wahr: die trivialen Untergruppen)
- Jede Gruppe besitzt eine nichttriviale Untergruppe.  
(falsch, die Gruppen der Ordnung  $p$ =prim besitzen nach dem Satz von Lagrange nur die trivialen Untergruppen)
- Die Menge der  $2 \times 2$  Matrizen mit reellen Einträgen und der Matrizenmultiplikation als Verknüpfung ist eine Gruppe.  
(wahr, Gruppeneigenschaften sind in der Übung nachgewiesen worden.)
- Zyklische Gruppen sind abelsch.  
(wahr, in der Vorlesung bewiesen worden)
- 1 ist das einzige Element aus der Menge der ganzen Zahlen  $\mathbb{Z}$ , das die zyklische Gruppe  $(\mathbb{Z}, +)$  erzeugt.  
(falsch, auch  $-1$  ist erzeugendes Element)
- Jede Gruppe der Ordnung  $p$  mit  $p$  Primzahl besitzt genau 2 Untergruppen.  
(richtig, die beiden trivialen Untergruppen)

- 12.) Es erweist sich als sinnvoll, für  $1 - x$  eine Abkürzung einzuführen. Für  $x \in \mathbb{R}$  sei  $\underline{x} := 1 - x$ . Die folgenden, unmittelbar einsichtigen Gesetze kann man beim Nachweis der Gruppeneigenschaften benutzen.

$$1. \quad x = y \Leftrightarrow \underline{x} = \underline{y}$$

$$2. \quad \underline{x \oplus y} = 1 - (x + y - xy) = (1 - x)(1 - y) = \underline{x} \underline{y}$$

Nun folgt der Beweis der Gruppeneigenschaften für  $(\mathbb{R} \setminus \{1\}, \oplus)$ :

(1) Abgeschlossenheit:

$$x \neq 1 \wedge y \neq 1 \Leftrightarrow \underline{x} \neq 0 \wedge \underline{y} \neq 0 \Leftrightarrow \underline{x} \underline{y} \neq 0$$

Nach 2. heißt das  $\underline{x \oplus y} \neq 0$ , also  $x \oplus y \neq 1$ .

(2) Assoziativität:

Für alle  $x, y, z \in \mathbb{R}$  gilt  $(\underline{x \oplus y}) \underline{z} = \underline{x} (\underline{y \oplus z})$ : Mittels 2. und dann 1. folgt weiter:

$$(\underline{x \oplus y}) \underline{z} = \underline{x} (\underline{y \oplus z}) \Rightarrow (\underline{x \oplus y}) \oplus z = \underline{x} \oplus (\underline{y \oplus z}) \Rightarrow (x \oplus y) \oplus z = x \oplus (y \oplus z).$$

(3) Kommutativität:

$$x \oplus y = x + y - xy = y + x - yx = y \oplus x.$$

(4) 0 ist neutrales Element

$$x \oplus 0 = x + 0 - x0 = x = 0 \oplus x \text{ (wegen der Kommutativität)}$$

(5) Existenz inverser Elemente

Für  $x \in \mathbb{R} \setminus \{1\}$  gilt auch  $x / (x-1) \in \mathbb{R} \setminus \{1\}$  und man rechnet nach, dass  $x / (x-1)$  das inverse Element für jedes  $x \in \mathbb{R} \setminus \{1\}$  ist.

- 13.) Gilt für jedes Element  $x \in G$  die Gleichung  $x + x = e$ , so gilt insbesondere auch  $(x + y) + (x + y) = e$ . Aus  $(x + y) + (x + y) = e$  folgt nun durch Addition von  $y$  von rechts und unter Ausnutzung der Assoziativität in der Gruppe  $G$ :  $x + y + x = y$ . Addiert man nun noch  $x$  von rechts, so folgt  $x + y = y + x$ , und das war zu zeigen.
- 14.) Die Ordnung der Gruppe  $G$  ist  $p=17$  prim. Damit besitzt sie nach dem Satz von Lagrange nur die beiden trivialen Untergruppen  $G$  und  $\{e\}$ .
- 15.) In jeder Nebenklasse liegt genau ein Element der Gruppe, die Anzahl der Nebenklassen entspricht also der Ordnung der Gruppe  $G$ .
- 16.) Zeigen Sie: Die Gruppe  $S_7$  besitzt keine Untergruppe der Ordnung 11.

Beweis:  $|S_7| = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 7 \cdot 5 \cdot 3^2 \cdot 2^4$ . Wäre  $H$  Untergruppe von  $S_7$  der Ordnung 11, dann müsste 11 nach dem Satz von Lagrange  $|S_7|$  teilen. In der Primzahlzerlegung von  $|S_7|$  kommt jedoch 11 nicht vor, also gibt es keine Untergruppe der Ordnung 11. q.e.d.