A1.9.4: Sei $(G,\cdot)$ eine Gruppe mit neutralen Element e. Für alle $a \in G$ und alle $n \in \mathbb{N}^\times$ sind die Potenzen von a erklärt durch $a^0 := e$, $a^n := a \cdot a^{n-1}$ sowie $a^{-n} := (a^{-1})^n$.

(a) Beweise die Rechenregel $a^n a^m = a^{n+m}$ für alle $n,m \in \mathbb{Z}$.

Anmerkung zu Aufgabe 1.9.4 (a): Erstens: Laut Angabe gilt die Eigenschaft $a^n = a \cdot a^{n-1}$ für alle natürliche Zahlen n. Es könnte hilfreich sein, diese Eigenschaft für alle ganzen Zahlen n zu beweisen. Zweitens: Wann immer Sie das Assoziativgesetz $(x \cdot y)\cdot z = x \cdot (y \cdot z)$ verwenden, geben Sie an, auf welche Werte für x, y, z Sie das Assoziativgesetz anwenden.

Beweis: Um zu zeigen, dass $a^n = a a^{n-1}$ auch für ganze Zahlen gilt, zeigen wir, dass es für $-n < 0$ gilt, also $a^{-n} = a^{-n-1}$:

$$a^{-n} = (-a)^n = a \cdot (-a)^1 \cdot (-a)^n = a(a^{-1})^{n+1} = a a^{-(n+1)} = a a^{-n-1}.$$

Die Rechenregel kann mit vollständiger Induktion bewiesen werden:

- Induktionsanfang: $a^0 a^m = a^{0+m} \Leftrightarrow e a^m = a^m$
- Induktionsschritt $(n \Rightarrow n+1)$: Laut Definition wissen wir:

$a^{n+1} = a a^{n+1-1} = a a^n \wedge a^{n+1+m} = a a^{n+1+m-1} = a a^{n+m}$.

Wir wollen folgendes zeigen: $a^{n+m} = a^n a^m \Rightarrow a^{n+1} a^m = a^{n+1+m}$.

Wir substituieren und bekommen: $\Leftrightarrow a a^n a^m = a a^{n+m} \Leftrightarrow$
$a^n a^m = a^{n+m}$.

- Induktionsschritt $(n \Rightarrow n-1)$: —"— :

$a^n = a a^{n-1} \Leftrightarrow a^{-1} a^n = a^{n-1}$. Wir wollen folgendes zeigen:
$a^{n+m} = a^n a^m \Rightarrow a^{n-1+m} = a^{n-1} a^m$. Wir substituieren und bekommen:
$\Leftrightarrow a^{n-1+m} = a^{-1} a^n a^m \Leftrightarrow a a^{n-1+m} = a^n a^m$. Weil aber laut Definition $a^{(n-1+m)+1} = a a^{n-1+m}$, gilt $a^{(n-1+m)+1} = a^n a^m$, also $a^{n+m} = a^n a^m$. $\square$

A 1.9.5 Sei G eine Gruppe. Beweise:

(a) Ist $(U_i)_{i \in I}$ eine nicht leere Familie von Untergruppen von G, so ist $\bigcap_{i \in I} U_i$ wieder eine Untergruppe von G.

(b) Sind U_1 und U_2 Untergruppen von G, so ist $U_1 \cup U_2$ genau dann eine Untergruppe von G, wenn $U_1 \subset U_2$ oder $U_2 \subset U_1$ gilt.

Beweis (a): $\bigcap_{i \in I} U_i \neq \emptyset$, da $\bigwedge_{i \in I} U_i \ni e$.

Seien $x, y \in \bigcap_{i \in I} U_i$ beliebig, aber fest, dann folgt $\forall i \in I: x, y \in U_i$ und (insbesondere) $x, y \in U_i$, wobei U_i beliebig ist. Weil U_i tatsächlich eine Untergruppe ist, folgt $xy^{-1} \in U_i$. Das gilt aber für alle U_i und somit auch $xy^{-1} \in \bigcap_{i \in I} U_i$. $\square$

[Untergruppenaxiome: 1. $U \neq \emptyset \wedge$ 2. $xy^{-1} \in U$ für alle $x, y \in U$.]

Beweis (b): Wir zeigen $U_1 \cup U_2 \subset G \Leftrightarrow U_1 \subset U_2 \vee U_2 \subset U_1$.

($\Rightarrow$): Sei $x \in U_1$ und $y \in U_2$. $U_1, U_2 \subset G$, also $x^{-1} \in U_1$ und $y^{-1} \in U_2$. Außerdem sind $x, y \in U_1 \cup U_2$, und weil $U_1 \cup U_2 \subset G$ ist $xy \in U_1 \cup U_2$, also $xy \in U_1 \vee xy \in U_2$:

1. Fall: $xy \in U_1$: $\wedge\ x^{-1} \in U_1 \Rightarrow x^{-1}xy \in U_1 \Rightarrow y \in U_1$

Weil wir gesagt haben, dass $y \in U_2$ und $y \in U_1$ folgt ist $U_2 \subset U_1$.

2. Fall: $xy \in U_2$: $\wedge\ y^{-1} \in U_2 \Rightarrow xyy^{-1} \in U_2 \Rightarrow x \in U_2$

—"— $x \in U_1$ und $x \in U_2$ folgt ist $U_1 \subset U_2$. $\square$

1.9.8 Überprüfe, ob durch die folgenden Vorschriften (kommutative) Gruppen $(G,*)$ festgelegt werden. Gib dabei in jedem Fall an, ob eine kommutative Verknüpfung vorliegt, welche Gruppenaxiome gelten und welche nicht gelten:

(γ) $G = \{WAHR, FALSCH\}$, $a * b := a \Leftrightarrow b$.

(δ) $G = \{WAHR, FALSCH\}$, $a * b := a \wedge b$.

(ι) $G = \mathbb{R} \setminus \{-1\}$, $a * b := ab + a + b$.

Bei (γ) gilt:

- Neutrales Element: $= W$, weil $(F \Leftrightarrow W) \Leftrightarrow F$ und $(W \Leftrightarrow W) \Leftrightarrow W$.
- Assoziativität: Gilt, weil $((a \Leftrightarrow b) \Leftrightarrow c) \Leftrightarrow (a \Leftrightarrow (b \Leftrightarrow c))$.

W	W	W	W	W	W	W	W
W	W	W	F	F	W	F	F
W	F	F	F	W	W	F	F
W	F	F	W	F	W	W	W
F	F	W	F	W	W	F	W
F	F	W	W	F	W	W	F
F	W	F	W	W	W	W	F
F	W	F	F	F	W	F	W

- Inverses Element:

  Für W ist es W

  $(W \Leftrightarrow W) \Leftrightarrow W$

  Für F ist es F

  $(F \Leftrightarrow F) \Leftrightarrow W$
- Kommutativität: Gilt, weil $(a \Leftrightarrow b) \Leftrightarrow (b \Leftrightarrow a)$

Bei (δ) gilt:

- Neutrales Element: $= W$, weil $(F \wedge W) \Leftrightarrow F$ und $(W \wedge W) \Leftrightarrow W$.
- Assoziativität: Gilt, weil $(a \wedge b) \wedge c \Leftrightarrow a \wedge (b \wedge c)$.
- Inverses Element: nicht für F, weil $(F \wedge ?) \Leftrightarrow W$.
- Kommutativität: Gilt, weil $(a \wedge b) \Leftrightarrow (b \wedge a)$

Bei (ι) gilt:

- Neutrales Element: $= 0$, weil $a * 0 = a0 + a + 0 = a$.

- Assoziativität: Gilt, weil $(a * b) * c = a * (b * c) \Leftrightarrow$
$(ab + a + b)c + (ab + a + b) + c = a(bc + b + c) + a + (bc + b + c)$
$\Leftrightarrow abc + ac + bc + ab + a + b + c = abc + ab + ac + a + bc + b + c.$
- Inverses Element: $a = b^{-1}$, wenn $ab + a + b = 0 \Leftrightarrow$
$ab + a = -b \Leftrightarrow a(b+1) = -b \Leftrightarrow a = -\frac{b}{b+1} = b^{-1}$
- Kommutativität: Gilt, wenn $+, \cdot$ kommutativ sind, weil
$a * b = b * a \Leftrightarrow ab + a + b = ba + b + a.$

(γ), (δ), und (υ) sind in sich geschlossen, weil:
1. $\forall a, b \in \{W, F\}: a \Leftrightarrow b \in \{W, F\}$
2. $\forall a, b \in \{W, F\}: a \wedge b \in \{W, F\}$
3. $\forall a, b \in \mathbb{R} \setminus \{-1\}: ab + a + b \in \mathbb{R} \setminus \{-1\}$, weil für

$ab + a + b = -1$ immer $a = -1 \vee b = -1$ gilt:
$ab + a + b = -1 \Leftrightarrow ab + a + 1 = -b \Leftrightarrow a + 1 = -b - ab \Leftrightarrow$
$a + 1 = -b(1 + a) \Leftrightarrow \frac{a+1}{a+1} = -b \Leftrightarrow 1 = -b \Leftrightarrow b = -1$, und
$a = -1$ folgt analog. $\square$

A 1.9.9 Welche der folgenden Teilmengen sind Untergruppen der Gruppe aller Bijektionen einer Ebene $\mathcal{E}$ auf sich?

(α) $\emptyset$.

(β) $\{id_{\mathcal{E}}\}$

(γ) die Menge aller Drehungen (einschließlich der Identität).

(ϑ) die Menge aller Translationen bei denen der Abstand von Ur- und Bildpunkt einen vorgegebenen Wert ≥ 0 (z.B. 10 cm) nicht überschreitet.

$\emptyset$ ist keine Untergruppe.

Beweis: $e \notin \emptyset$. $\square$

$\{id_{\mathcal{E}}\}$ ist eine Untergruppe.

Beweis: $\{id_{\mathcal{E}}\} \neq \emptyset \wedge id_{\mathcal{E}} \circ id_{\mathcal{E}}^{-1} \in \{id_{\mathcal{E}}\}$.

Die Menge aller Drehungen ist keine Untergruppe.

Beweis: Betrachte eine Teilmenge von $\mathcal{E}$, die aus Punkten auf einer Zahlengerade besteht. Dabei ist die Funktion, die eine 180° (also π rad) Drehung durchführt definiert als

$a : x \mapsto -(x-a)+a$.

Wir wissen, dass $[-2 \circ 0](2) = -2$ und $[-2 \circ 0](1) = -3$, und $[0 \circ -2](-2) = 2$ und $[0 \circ -2](-3) = 1$. Aber es gilt auch $0(-2) = 2$ und $0(-3) = 3 \neq 1$. $\square$

Die Menge aller Translationen ist keine Untergruppe.

Beweis: Angenommen, der vorgegebene Wert ist tatsächlich 10 cm. Eine Translation t mit 8cm führt aber zu $t \circ t$ mit 16 cm. $\square$

A1.9.13: Beweise: Für jede Untergruppe U von $(\mathbb{Z}, +)$ gibt es genau eine Zahl $m \in \mathbb{N}$ derart, dass $U = \mathbb{Z}m$.

Hinweis: Für $U = \{0\}$ ist $m = 0$ offenbar die einzige Lösung. Andernfalls ist m das kleinste positive Element von U.

Beweis: Sei m das kleinste positive Element von einer beliebigen Untergruppe U. Dann sind alle anderen Elemente, sofern es diese gibt, Vielfache von m.
Gäbe es ein $n \nmid m$, dann käme durch wiederholtes Addieren von $-m$ ein kleineres positives Element heraus, $0 < \tilde{n} < m$.
Das wäre jedoch ein Widerspruch. $\square$

A 1.9.14 Beweise die folgende Variante des Untergruppenkriteriums:
Eine Teilmenge U einer Gruppe G ist genau dann eine Untergruppe, falls U die folgenden drei Eigenschaften erfüllt: (i) $U \neq \emptyset$. (ii) $xy \in U$ für alle $x, y \in U$. (iii) $x^{-1} \in U$ für alle $x \in U$.

Mit 1.9.14x ist folgende Variante der Aufgabe 1.9.14 gemeint:
Sei U eine Teilmenge der Gruppe G. Wir bezeichnen die Gruppenoperation von G mit $*$, das neutrale Element mit e, und das zu x inverse Element mit x^{-1}.
Zeigen Sie, dass die Aussage "(1) und (2)" äquivalent zur Aussage "(A) und (B) und (C)" ist, wobei:

(1) U ist nicht leer.
(2) Für alle x, y in U gilt $x * (y^{-1})$ in U.

(A) e in U
(B) Für alle u in U gilt u^{-1} in U.
(C) Für alle u, v in U gilt $u * v$ in U.

Beweis: Wir wollen zeigen, dass $(1) \wedge (2) \Leftrightarrow (A) \wedge (B) \wedge (C)$.
$(\Rightarrow)$: (2) gibt uns $\forall x, x \in U : x x^{-1} \in U$. Wegen (1) ist die Prämisse $(x \in U)$ wahr und daher (Modus Ponendo Ponens) folgt (A). Deshalb können wir $\forall e, x \in U : e x^{-1} \in U$ schreiben und es folgt (B). Deshalb können wir $\forall x, y^{-1} \in U : x (y^{-1})^{-1} \in U$ schreiben und es folgt (C).
$(\Leftarrow)$: $(A) \Rightarrow (1)$ ist trivial. Schreibe (B) als $\forall w \in U : w^{-1} \in U$ und $w^{-1} = v$. Dann kann man (C) als $\forall u, w^{-1} \in U : u w^{-1} \in U$ schreiben. Daher gilt $(B) \wedge (C) \Rightarrow (2)$. $\square$