M 7. Abgeschlossene Operatoren.

Entscheiden Sie, welche der angegebenen Mengen bezüglich der jeweils angegebenen Operationen abgeschlossen sind:

	$\frac{1}{(\dots)}$	$\sqrt{\dots}$	5% von ...	200% von ...	$2^{(\dots)}$
$\mathbb{N}$					
$\mathbb{Z} - \{0\}$					
$\mathbb{Q}$					
$\mathbb{R}$					
$\mathbb{R}^+$					
$\mathbb{C}$					

	$\frac{1}{(\dots)}$	$\sqrt{(\dots)}$	5% von ...	200% von ...	$2^{(\dots)}$
$\mathbb{N}$	$\frac{1}{2} \notin \mathbb{N}$	$\sqrt{2} \notin \mathbb{N}$	$5\% \notin \mathbb{N}$	$200\% \cdot \mathbb{N} \subset \mathbb{N}$	$2^{\mathbb{N}} \subset \mathbb{N}$
$\mathbb{Z}\setminus\{0\}$	$\frac{1}{2} \notin \mathbb{Z}\setminus\{0\}$	$\sqrt{2} \notin \mathbb{Z}\setminus\{0\}$	$5\% \notin \mathbb{Z}\setminus\{0\}$	$200\% \mathbb{Z}\setminus\{0\} \subset \mathbb{Z}\setminus\{0\}$	$2^{-1} \notin \mathbb{Z}\setminus\{0\}$
$\mathbb{Q}$	$\frac{1}{0}$ n. def.	$\sqrt{2} \notin \mathbb{Q}$	$5\% \mathbb{Q} \subset \mathbb{Q}$	$200\% \mathbb{Q} \subset \mathbb{Q}$	$2^{\frac{1}{2}} \notin \mathbb{Q}$
$\mathbb{R}$	$\frac{1}{0}$ n. def.	$\sqrt{-1} \notin \mathbb{R}$	$5\% \mathbb{R} \subset \mathbb{R}$	$200\% \mathbb{R} \subset \mathbb{R}$	$2^{\mathbb{R}} \subset \mathbb{R}$
$\mathbb{R}^+$	$\frac{1}{\mathbb{R}^+} \subset \mathbb{R}^+$	$\sqrt{\mathbb{R}^+} \subset \mathbb{R}^+$	$5\% \mathbb{R}^+ \subset \mathbb{R}^+$	$200\% \mathbb{R}^+ \subset \mathbb{R}^+$	$2^{\mathbb{R}^+} \subset \mathbb{R}^+$
$\mathbb{C}$	$\frac{1}{0}$ n. def.	$\sqrt{\mathbb{C}} \subset \mathbb{C}$	$5\% \mathbb{C} \subset \mathbb{C}$	$200\% \mathbb{C} \subset \mathbb{C}$	$2^{\mathbb{C}} \subset \mathbb{C}$

M 8. Wer wird Millionär mit Gruppenaxiomen.

Sei $(G, \circ)$ eine Gruppe mit neutralem Element $e \in G$. Das zu $g \in G$ inverse Element werde mit g^{-1} bezeichnet. Welche der folgenden Aussagen sind für alle Gruppen richtig ?

☐ $\exists h \in G \; \forall g \in G : \; h \circ g = e$

☐ $\forall g \in G \; \forall f \in G : \; g \circ f \circ g^{-1} = f$

☐ $\forall g, f, h, k \in G : \; (g \circ f) \circ (h \circ k) = g \circ ((f \circ h) \circ k)$

☐ $\exists h \in G \; \forall g \in G : \; h \circ g = h$

☐ $\forall g \in G \; \exists h \in G : \; h \circ g = e$

<u>Aus Vorlesung:</u>

(0) Für alle $a, b \in G \Rightarrow a \circ b \in G$ (abgeschlossen)

(i) Es gibt ein $e \in G$ mit $e \circ g = g$ für alle $g \in G$ (neutrales El.)

(ii) Für alle $g \in G$ existiert $g^{-1} \in G$ mit $g^{-1} \circ g = e$ (inverses El. zu g)

(iii) Für alle $g_1, g_2, g_3 \in G$ gilt: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ (assoziativ)

<u>Bem:</u> Dann gilt auch $g \circ e = e \circ g = g$ und e ist eindeutig sowie $g \circ g^{-1} = g^{-1} \circ g = e$ und g^{-1} existiert eindeutig zu g.

$\exists$ ... Existenzquantor, $\forall$ ... Allquantor, : ... es gilt

☐ $\exists h \in G$, so dass $\forall g \in G$ gilt: $h \circ g = e$ nur bei einelementigen Gruppen
(Begr. Speziell für $g = e$ folgt $\underline{e} = h \circ e = \underline{h}$ und damit $e = h \circ g = e \circ g = g \;\; \forall g \in G$)

☐ $\forall g \in G$ und $\forall f \in G$ gilt: $g \circ f \circ g^{-1} = f$ nur bei kommutativen Gruppen
(Begr. Aus $g \circ f \circ g^{-1} = f$ folgt: $f \circ g = (g \circ f \circ g^{-1}) \circ g = (g \circ f) \circ (g^{-1} \circ g) = g \circ f \;\; \forall g, f \in G$)

☒ $\forall g, f, h, k \in G$ gilt: $(g \circ f) \circ (h \circ k) = g \circ ((f \circ h) \circ k)$ Assoziativgesetz
(Begr. $(g \circ f) \circ (h \circ k) = g \circ (f \circ (h \circ k)) = g \circ ((f \circ h) \circ k)$)

☐ $\exists h \in G$, so dass $\forall g \in G$ gilt: $h \circ g = h$ nur bei einelementigen Gruppen
(Begr. Wegen Eindeutigkeit des neutralen Elements folgt $g = e \;\; \forall g \in G$)

☒ $\forall g \in G \;\; \exists h \in G$, so dass: $h \circ g = e$ ✓ (etwa $h = g^{-1}$ inverses El. zu g)

P 9. Sei $\mathbb{Q}[x] := \left\{ \sum_{i=0}^{n} q_i x^i \mid n \in \mathbb{N}\ ,\ q_i \in \mathbb{Q} \right\}$ die Menge der Polynome in x mit rationalen Koeffizienten.

1. Zeigen Sie, dass $\mathbb{Q}[\sqrt{7}] = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$ gilt.
2. Zeigen Sie, dass $(\mathbb{Q}[\sqrt{7}], +)$ und $(\mathbb{Q}[\sqrt{7}] \setminus \{0\}, \cdot)$ bezüglich der Addition bzw. Multiplikation in $\mathbb{R}$ Gruppen sind.

1) Wir sortieren die Summe nach Gliedern mit geraden Potenzen $(i=2k)$ bzw. ungeraden Potenzen $(i=2k+1, k\in\mathbb{N})$ und erhalten für $n=2m$, $m\in\mathbb{N}$ mit $m':=m-1$ bzw. für $n=2m+1$, $m\in\mathbb{N}$ mit $m'=m$

$$\sum_{i=0}^{n} q_i (\sqrt{7})^i = \sum_{k=0}^{m} q_{2k} (\sqrt{7})^{2k} + \sum_{k=0}^{m'} q_{2k+1} (\sqrt{7})^{2k+1} =$$

$$= \underbrace{\left(\sum_{k=0}^{m} q_{2k}\, 7^k\right)}_{=:\,a\,\in\,\mathbb{Q}} + \underbrace{\left(\sum_{k=0}^{m'} q_{2k+1}\, 7^k\right)}_{=:\,b\,\in\,\mathbb{Q}} \cdot \sqrt{7} = a + b\sqrt{7} \overset{\text{umgekehrt}}{\in} \mathbb{Q}[x=\sqrt{7}]$$

für $q_0 = a$, $q_1 = b$ und $q_i = 0$, $i \geq 2$

2) a) Wir zeigen $(\mathbb{Q}[\sqrt{7}], +)$ ist eine Gruppe

(i) <u>abgeschlossen:</u> $\forall x = a_1 + b_1\sqrt{7}$, $y = a_2 + b_2\sqrt{7} \in \mathbb{Q}[\sqrt{7}]$:

$$x + y = (a_1 + b_1\sqrt{7}) + (a_2 + b_2\sqrt{7}) = \underbrace{(a_1 + a_2)}_{\in\mathbb{Q}} + \underbrace{(b_1 + b_2)}_{\in\mathbb{Q}}\sqrt{7} \in \mathbb{Q}[\sqrt{7}]$$

(ii) <u>neutrales Element</u> der Addition (Nullelement)

Wähle in (i) $a_1 = b_1 = 0 \in \mathbb{Q} \Rightarrow x = 0 + 0\cdot\sqrt{7} = 0$ und

$x + y = (0 + 0\cdot\sqrt{7}) + (a_2 + b_2\sqrt{7}) = a_2 + b_2\sqrt{7} = y \Rightarrow x = 0$ ist Nullelement in $\mathbb{Q}[\sqrt{7}]$

(iii) <u>inverses Element</u> der Addition (negatives Element)

Wähle in (i) $a_1 = -a_2 \in \mathbb{Q}$ und $b_1 = -b_2 \in \mathbb{Q}$ (negative Elemente in $\mathbb{Q}$)

$\Rightarrow x + y = (-a_2 - b_2\sqrt{7}) + (a_2 + b_2\sqrt{7}) = (-a_2 + a_2) + (-b_2 + b_2)\sqrt{7} = 0 + 0\sqrt{7} = 0$

$\Rightarrow$ Zu $y = a_2 + b_2\sqrt{7}$ ist $-y = -a_2 - b_2\sqrt{7}$ das negative Element

(iv) <u>assoziativ</u> Wegen $\mathbb{Q}[\sqrt{7}] \subset \mathbb{R}$ erbt $\mathbb{Q}[\sqrt{7}]$ die Assoziativität von $(\mathbb{R}, +)$.

ausführlich: $\forall x = a_1 + b_1\sqrt{7}$, $y = a_2 + b_2\sqrt{7}$, $z = a_3 + b_3\sqrt{7} \in \mathbb{Q}[\sqrt{7}]$:

$(x+y)+z = [(a_1 + b_1\sqrt{7}) + (a_2 + b_2\sqrt{7})] + (a_3 + b_3\sqrt{7}) =$

$= [(a_1 + a_2) + (b_1 + b_2)\sqrt{7}] + (a_3 + b_3\sqrt{7}) = [(a_1 + a_2) + a_3] + [(b_1 + b_2) + b_3]\sqrt{7} \overset{(\mathbb{Q}\text{ assoziativ})}{=}$

$= [a_1 + (a_2 + a_3)] + [b_1 + (b_2 + b_3)]\sqrt{7} = (a_1 + b_1\sqrt{7}) + [(a_2 + a_3) + (b_2 + b_3)\sqrt{7}] =$

$= (a_1 + b_1\sqrt{7}) + [(a_2 + b_2\sqrt{7}) + (a_3 + b_3\sqrt{7})] = x + (y + z)$

<u>Bemerkung:</u> $(\mathbb{Q}[\sqrt{7}], +)$ erbt auch die Kommutativität von $(\mathbb{R}, +)$, d.h.

$x + y = (a_1 + b_1\sqrt{7}) + (a_2 + b_2\sqrt{7}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{7} = (a_2 + a_1) + (b_2 + b_1)\sqrt{7} = (a_2 + b_2\sqrt{7}) + (a_1 + b_1\sqrt{7}) = y + x$

2) b) Wir zeigen $(\mathbb{Q}[\sqrt{7}]\setminus\{0\},\cdot)$ ist eine Gruppe (fast „analog" zu a))

(i) <u>abgeschlossen</u> $\forall\, x=a_1+b_1\sqrt{7},\ y=a_2+b_2\sqrt{7}\in\mathbb{Q}[\sqrt{7}]\setminus\{0\}$:

$$x\cdot y=(a_1+b_1\sqrt{7})\cdot(a_2+b_2\sqrt{7})=\underbrace{(a_1a_2+7b_1b_2)}_{\in\mathbb{Q}}+\underbrace{(a_1b_2+b_1a_2)}_{\in\mathbb{Q}}\sqrt{7}\in\mathbb{Q}[\sqrt{7}]\setminus\{0\}$$

<u>Bem</u>: $x\neq0,\ y\neq0\Rightarrow x\cdot y\neq0$ wird wegen $\mathbb{Q}[\sqrt{7}]\subset\mathbb{R}$ von $(\mathbb{R}\setminus\{0\},\cdot)$ geerbt.

(ii) <u>neutrales Element</u> der Multiplikation (Einselement)

Wähle in (i) $a_1=1,\ b_1=0\in\mathbb{Q}\Rightarrow x=1+0\cdot\sqrt{7}=1$ und

$x\cdot y=(1+0\cdot\sqrt{7})\cdot(a_2+b_2\sqrt{7})=a_2+b_2\sqrt{7}=y\Rightarrow x=1$ ist Einselement in $\mathbb{Q}[7]\setminus\{0\}$

(iii) <u>inverses Element</u> der Multiplikation (inverses Element)

Suche in (i) zu $y=a_2+b_2\sqrt{7}\neq0$ ein $x=a_1+b_1\sqrt{7}$: $x\cdot y=1\Leftrightarrow$ LGS:

① $a_1a_2+7b_1b_2=1$ (LGS für a_1,b_1)

② $a_1b_2+b_1a_2=0\Leftrightarrow a_1b_2=-b_1a_2$. Wähle $a_1=\lambda a_2\wedge b_1=-\lambda b_2,\ \lambda\in\mathbb{Q}$.

Mit ① $\Rightarrow \lambda a_2^2-\lambda 7b_2^2=1\Leftrightarrow\lambda\underbrace{(a_2^2-7b_2^2)}_{\neq0}=1\Leftrightarrow\lambda=\frac{1}{a_2^2-7b_2^2}\in\mathbb{Q}$

$\neq0$ da $a_2,b_2\in\mathbb{Q}$ aber $\sqrt{7}\notin\mathbb{Q}$! und $(a_2,b_2)\neq(0,0)$

$$\Rightarrow x=y^{-1}=\overbrace{\frac{a_2}{a_2^2-7b_2^2}}^{\in\mathbb{Q}}+\overbrace{\frac{-b_2}{a_2^2-7b_2^2}}^{\in\mathbb{Q}}\sqrt{7}\in\mathbb{Q}[\sqrt{7}]\setminus\{0\}$$

(Probe $x\cdot y=1$)

<u>Bemerkung</u>: Man kann formal auch $\frac{1}{y}=\frac{1}{a_2+b_2\sqrt{7}}$ betrachten und den „Nenner rational" machen wie folgt:

$$\frac{1}{y}=\frac{1}{a_2+b_2\sqrt{7}}=\frac{1}{a_2+b_2\sqrt{7}}\cdot\frac{a_2-b_2\sqrt{7}}{a_2-b_2\sqrt{7}}=\frac{a_2-b_2\sqrt{7}}{a_2^2-7b_2^2}=y^{-1}\in\mathbb{Q}[\sqrt{7}]\setminus\{0\}$$

(iv) <u>assoziativ</u> Wegen $\mathbb{Q}[\sqrt{7}]\setminus\{0\}\subset\mathbb{R}\setminus\{0\}$ erbt $\mathbb{Q}[\sqrt{7}]$ die Assoziativität von $(\mathbb{R}\setminus\{0\},\cdot)$

ausführlich: $\forall\, x=a_1+b_1\sqrt{7},\ y=a_2+b_2\sqrt{7},\ z=a_3+b_3\sqrt{7}\in\mathbb{Q}[\sqrt{7}]\setminus\{0\}$:

- $(x\cdot y)\cdot z=[(a_1+b_1\sqrt{7})(a_2+b_2\sqrt{7})]\cdot(a_3+b_3\sqrt{7})=[(a_1a_2+7b_1b_2)+(a_1b_2+b_1a_2)\sqrt{7}]\cdot(a_3+b_3\sqrt{7})=$
  $=[(a_1a_2+7b_1b_2)a_3+7(a_1b_2+b_1a_2)b_3]+[(a_1a_2+7b_1b_2)b_3+(a_1b_2+b_1a_2)a_3]\sqrt{7}$ (∗)
- $x\cdot(y\cdot z)=(a_1+b_1\sqrt{7})[(a_2+b_2\sqrt{7})(a_3+b_3\sqrt{7})]=[a_1+b_1\sqrt{7}][(a_2a_3+7b_2b_3)+(a_2b_3+b_2a_3)\sqrt{7}]$
  $=[a_1(a_2a_3+7b_2b_3)+7b_1(a_2b_3+b_2a_3)]+[a_1(a_2b_3+b_2a_3)+b_1(a_2a_3+7b_2b_3)]\sqrt{7}$ (∗∗)

Da $\mathbb{Q}$ ein Körper ist, gilt (∗) = (∗∗) also $(x\cdot y)\cdot z=x\cdot(y\cdot z)$

<u>Bemerkung</u>: $(\mathbb{Q}[\sqrt{7}]\setminus\{0\},\cdot)$ erbt auch die Kommutativität von $(\mathbb{R}\setminus\{0\},\cdot)$, d.h.

$x\cdot y=(a_1+b_1\sqrt{7})(a_2+b_2\sqrt{7})=(a_1a_2+7b_1b_2)+(a_1b_2+b_1a_2)\sqrt{7}=(a_2a_1+7b_2b_1)+(a_2b_1+b_1a_2)\sqrt{7}=$

$=(a_2+b_2\sqrt{7})(a_1+b_1\sqrt{7})=y\cdot x$

P 10. Sudoku und endliche Gruppen

1. Wie viele unterschiedliche Gruppen mit jeweils 1, 2, 3, 4, 5 Elementen gibt es?
2. Geben Sie die jeweiligen Gruppentafeln an.
   Der vollständige Nachweis der Assoziativität darf dabei weggelassen werden.
3. Welche dieser Gruppen $(G, \circ)$ sind kommutativ (d.h. $\forall a, b \in G : a \circ b = b \circ a$) ?

a) Einelementige Gruppen:

Ansatz $G = \{e\}$, e muss neutrales Element sein mit $e \cdot e = e \Rightarrow$

Gruppentafel (Verknüpfungstafel)

$\cdot$	e
e	e

$\Rightarrow$ G0) $G \neq \{\ \}$ und $\cdot$ abgeschlossen.

$(G, \cdot)$ ist Gruppe: G1) e ist neutrales Element

G2) inverses Element zu e ist e

G3) $(e \cdot e) \cdot e = e \cdot e = e \cdot (e \cdot e)$

$\exists_1$ einelementige Gruppe, die zudem kommutativ ist.

b) Zweielementige Gruppen

Ansatz $G = \{e, a\}$ mit neutralem Element $e \neq a \Rightarrow$ Gruppentafel

$\circ$	e	a
e	e	a
a	a	$\boxed{e}$

Annahme $a \cdot a = \boxed{a} \Rightarrow (a \cdot a) \cdot a^{-1} = a \cdot a^{-1} \Leftrightarrow a = e$ ↯

$\Rightarrow a \cdot a = \boxed{e} \Rightarrow$ G0) $G \neq \{\ \}$ und $\cdot$ abgeschlossen

$(G, \cdot)$ ist Gruppe: G1) e ist neutrales Element (vgl. 1. Zeile, 1. Spalte !)

G2) e steht in jeder Zeile & Spalte genau einmal

G3) assoziativ (Nachrechnen, nicht verlangt !)

Gruppentafel ist symmetrisch bzgl. Hauptdiagonale $\Rightarrow$

$\exists_1$ zweielementige Gruppe, die zudem kommutativ ist

(bis auf Umbenennung der Elemente !) vgl. $(\mathbb{Z}_2, \oplus_2)$

c) Dreielementige Gruppen

Ansatz $G = \{e, a, b\}$ mit neutralem Element $e \Rightarrow$ Gruppentafel

$\cdot$	e	a	b
e	e	a	b
a	a	$\boxed{?}$	?
b	b		

Für $p \in G$ gilt: $p \cdot x = p \cdot y \Rightarrow x = y$ und $x \cdot p = y \cdot p \Rightarrow x = y$ $\Big\}$ in jeder (*)

Spalte & in jeder Zeile steht jedes Element höchstens einmal

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

<u>Annahme</u> e in □ ⇒ b in ○ ⇒ ↯

⇒ b in □ und e in ○ ⇒

$(G, \cdot)$ ist Gruppe vgl. b)

Gruppentafel ist symmetrisch bzgl. Hauptdiagonale ⇒

$\exists_1$ dreielementige Gruppe, die zudem kommutativ ist

(bis auf Umbenennung der Elemente!) vgl. $(\mathbb{Z}_3, \oplus_3)$

d) <u>Vierelementige Gruppen</u>

<u>Ansatz</u> $G = \{e, a, b, c\}$ mit neutralem Element e ⇒ Gruppentafeln

<u>1. Fall</u>

$\exists x \in \{a, b, c\}$ mit $x \cdot x \neq e$

⇒ o.E. $a \cdot a = b$ (sonst umben.)

$\cdot$	e	a	b	c	
e	e	a	b	c	← klar
a	a	$\boxed{b}$	c	e	Rest mit
b	b	c	e	a	(*)
c	c	e	a	b	aus c)

↑ klar

<u>2. Fall</u>

$a^2 = b^2 = c^2 = e$

$\cdot$	e	a	b	c	
e	e	a	b	c	← klar
a	a	$\boxed{e}$	c	b	Rest mit
b	b	c	$\boxed{e}$	a	(*)
c	c	b	a	$\boxed{e}$	aus c)

↑ klar

G erfüllt mit beiden Verknüpfungstabellen die Gruppenaxiome, vgl. b). Beide Gruppentafeln sind symmetrisch bzgl. Hauptdiagonale ⇒

$\exists_2$ vierelementige Gruppen, die zudem kommutativ sind.

(bis auf Umbenennung der Elemente!)

Fall 1: z.B. $(\mathbb{Z}_4, \oplus_4)$ zyklisch

Fall 2: z.B. Kleinsche Vierergruppe.

e) <u>Fünfelementige Gruppen</u>

Ansatz $G = \{e, a, b, c, d\}$ mit neutralem Element e ⇒

Fallunterscheidung:

1. Fall $a^2=b^2=c^2=d^2=\boxed{e}$

$\cdot$	e	a	b	c	d	
e	e	a	b	c	d	← klar
a	a	$\boxed{e}$	c	d	b	
b	b	d	$\boxed{e}$	a	c	Rest mit (*) aus c)
c	c	b	d	$\boxed{e}$	a	
d	d	c	a	b	$\boxed{e}$	
	↑ klar					

o.E. $a\cdot b = c$ sonst umbenennen.

G erfüllt mit dieser Verknüpfungstabelle zwar G0) – G2) aber nicht G3)! denn

$(a\cdot b)\cdot d = c\cdot d = a$ ↯

$a\cdot(b\cdot d) = a\cdot c = d$

<u>Bem:</u> Dieses Beispiel zeigt, dass man G3) tatsächlich nachrechnen müsste!

2. Fall $\exists\, x \in \{a, b, c, d\}$ mit $x\cdot x \neq e \Rightarrow$ o.E. $a\cdot a = \boxed{b}$

$\cdot$	e	a	b	c	d	
e	e	a	b	c	d	← klar
a	a	$\boxed{b}$	e	d	c	← nach (*)
b	b	e		↯		← c, d passen nicht
c	c					
d	d					
	↑ klar					

Fall 2.1

<u>Annahme</u> $a\cdot b = e = b\cdot a$

da a, b zueinander invers

$\Rightarrow a\cdot b \neq e$

$\cdot$	e	a	b	c	d	
e	e	a	b	c	d	← klar
a	a	$\boxed{b}$	c	d	$\underline{e}$	← nach (*)
b	b	c	d	e	a	Rest mit (*) aus c)
c	c	d	e	a	b	
d	d	$\underline{e}$	a	b	c	
	↑ klar					

Fall 2.2

o.E. $a\cdot b = c$ sonst umbenennen

→ $a\cdot d = \underline{e} = d\cdot a$

da a, d zueinander invers

G erfüllt mit dieser Verknüpfungstabelle die Gruppenaxiome. Da die Gruppentafel symmetrisch bzgl. Hauptdiagonale $\Rightarrow$ $\exists_1$ fünfelementige Gruppe, die zudem kommutativ ist. (bis auf Umbenennung der Elemente!) vgl. $(\mathbb{Z}_5, \oplus_5)$ zyklisch