Aufgabe 14. Untergruppen
Gegeben seien die folgenden Gruppen und Teilmengen. Entscheiden Sie, welche der Teilmengen Untergruppen sind:

1) Für die Gruppe $(\mathbb{Z}_{12}, \bigoplus_{12})$

- ☐ $\{\}$
- ☐ $\{0, 4, 8\}$
- ☐ $\{6\}$
- ☐ $\{0, 3, 5, 8\}$

2) Für die Gruppe $(\mathbb{R}, +)$

- ☐ $\{a + b\sqrt{2} \mid a \in \mathbb{Q} \ \wedge \ b \in \mathbb{R}\}$
- ☐ $\mathbb{R} \setminus \mathbb{Q}$;
- ☐ $\{x \in \mathbb{R} \mid 5x + 1 = 0\}$
- ☐ $\{2x \mid x \in \mathbb{Z}\}$

Zusatz: Welche Elemente müsste man zu den Teilmengen, die keine Untergruppen bilden, mindestens hinzunehmen, damit sie Untergruppen werden.

LÖSUNG:

Nur die angekreuzten Mengen sind Untergruppen. Erinnerung an den Satz aus der Vorlesung:
Sei $U \subseteq G$. $(U, \circ)$ ist eine Untergruppe von $(G, \circ)$ genau dann wenn
(i) mit $a, b \in U$ ist auch $a \circ b \in U$, (ii) mit $a \in U$ ist auch $a^{-1} \in U$, (iii) $U \neq \{\}$.
Beachte: Zu $a \in U \subseteq G$ existiert $a^{-1} \in G$! In (ii) ist nur noch zu zeigen, dass dieses a^{-1} in U liegt.

1. Für die Gruppe $(\mathbb{Z}_{12}, \oplus_{12})$:
   - ☐ $\{\}$ (dies ist nicht ungleich der leeren Menge) Zusatz: $\{\} \cup \{0\} = \{0\}$
   - ☒ $\{0, 4, 8\}$
   - ☐ $\{6\}$ (bzgl. $\oplus_{12}$ nicht abgeschlossen) Zusatz: $\{6\} \cup \{0\} = \{0, 6\}$
   - ☐ $\{0, 3, 5, 8\}$ (bzgl. $\oplus_{12}$ nicht abgeschlossen) Zusatz: $\{0, 3, 5, 8\} \cup \{2, 1, 4, 6, 7, 9, 10, 11\} = \mathbb{Z}_{12}$
2. Für die Gruppe $(\mathbb{R}, +)$:
   - ☒ $\{a + b\sqrt{2} \mid a \in \mathbb{Q}, b \in \mathbb{R}\} = \mathbb{R}$
   - ☐ $\mathbb{R}\setminus\mathbb{Q}$ (besitzt kein neutrales Element) Zusatz: $(\mathbb{R}\setminus\mathbb{Q}) \cup \mathbb{Q} = \mathbb{R}$, siehe Bemerkung
   - ☐ $\{x \in \mathbb{R} \mid 5x + 1 = 0\} = \{-\frac{1}{5}\}$ Zusatz: $\{-\frac{1}{5}\} \cup \{n * \frac{1}{5} | n \in \mathbb{Z}\setminus\{-1\}\} = \{\frac{x}{5} \mid x \in \mathbb{Z}\}$
   - ☒ $\{2x \mid x \in \mathbb{Z}\}$

Bemerkung: Für $x \in \mathbb{R}\setminus\mathbb{Q}$ und $q \in \mathbb{Q}$ gilt $x + q \in \mathbb{R}\setminus\mathbb{Q}$.
Widerspruchsbeweis: Annahme $x + q \in \mathbb{Q} \Rightarrow \exists m, n \in \mathbb{Z}$ so, dass $x + q = \frac{m}{n}$, also $x = \frac{m}{n} - q \in \mathbb{Q}$ im Widerspruch zur Voraussetzung.
Folgerung: Damit $(\mathbb{R}\setminus\mathbb{Q}, +)$ zu einer Gruppe wird, muss zu zwei Elementen $x, x + q \in \mathbb{R}\setminus\mathbb{Q}$ auch deren Differenz $(x + q) - x = q$, also ganz $\mathbb{Q}$, in der gesuchten Teilmenge liegen.

Aufgabe 15. Division mit Rest

1. Berechnen Sie (möglichst ohne großen Aufwand) die Zahlen
$$(17+13) \mod 3, \quad (17\cdot 6) \mod 11, \quad 5^9 \mod 7\,.$$
2. Bestimmen Sie einen größten gemeinsamen Teiler (ggT) der Zahlen $a = 4620$ und $b = 225$, und finden Sie Zahlen $m, n \in \mathbb{Z}$ mit $ggT(a,b) = ma + nb$.
3. Bestimmen Sie einen größten gemeinsamen Teiler (ggT) der Polynome
$f(X) = X^5 + X^4 - 2X^2 - 9X - 22$ und $g(X) = X^3 + X^2 - 3X - 6$.
4. Geben Sie zwei ganze Zahlen $a, b < 1000$ an, so dass sich bei Division von a und b mit einem Taschenrechner der Näherungswert $2,3088235$ einstellt.

LÖSUNG:

1. Die Berechnungen kann man vereinfachen, indem man in jedem Schritt modulo (Division mit Rest) rechnet, und damit die "Zahlen klein hält".

   Klappt bei Addition...
   $$(17+13) \mod 3 = (15+2)+(12+1) \mod 3 = (2+1) \mod 3 = 0,$$
   genauso bei Multiplikation
   $$(17\cdot 6) \mod 11 = (11+6)\cdot 6 \mod 11 = (6\cdot 6) \mod 11 = (33+3) \mod 11 = 3.$$
   Hohe Potenzen kann man aufspalten, z.B. sukzessive in Quadrate. Dabei gilt:
   $$(a^m)\cdot(a^n) = a^{m+n}, \quad (a^m)^n = a^{m\cdot n} \text{ und } \quad a^b \mod c = (a \mod c)^b \mod c.$$
   $$5^9 \mod 7 = \left(\left((5^2)^2\right)^2\cdot 5\right) \mod 7 = \left(\left((21+4)^2\right)^2\cdot 5\right) \mod 7 = \left((4^2)^2\cdot 5\right) \mod 7$$
   $$= \left((14+2)^2\cdot 5\right) \mod 7 = (4\cdot 5) \mod 7 = (14+6) \mod 7 = 6.$$
   Alternativ: Nach dem kleinen Satz von Fermat gilt: $a^p \mod p = a$, wenn p eine Primzahl ist.
   $5^9 \mod 7 = (5^7\cdot 5^2) \mod 7 = (5\cdot 25) \mod 7 = 5\cdot(21+4) \mod 7 = (5\cdot 4) \mod 7 = 6.$

2. Der euklidische Algorithmus liefert für $a_1 := a = 4620 \geq 225 = b =: a_2$:

$$\begin{aligned}
a_1 = q_1a_2 + a_3,\ 0 \leq |a_3| \leq |a_2|, \quad 4620 &= 20\cdot 225 + 120 \quad \Leftrightarrow \quad a_3 = 120 = a + (-20)\cdot b\\
a_2 = q_2a_3 + a_4,\ 0 \leq |a_4| \leq |a_3|, \quad 225 &= 1\cdot 120 + 105 \quad \Leftrightarrow \quad a_4 = 105 = b + (-1)\cdot a_3\\
a_3 = q_3a_4 + a_5,\ 0 \leq |a_5| \leq |a_4|, \quad 120 &= 1\cdot 105 + 15 \quad \Leftrightarrow \quad a_5 = 15 = a_3 + (-1)\cdot a_4\\
a_4 = q_4a_5 + a_6,\ 0 \leq |a_6| \leq |a_5|, \quad 105 &= 7\cdot 15 + 0 \quad \Leftrightarrow \quad a_6 = 0 \Rightarrow ggT(a,b) = a_5 = 15.
\end{aligned}$$

   Allgemein: $a_i = q_ia_{i+1} + a_{i+2}, \quad 0 \leq |a_{i+2}| \leq |a_{i+1}|, \quad i = 1,2,3,\ldots$

   Durch Rückwärts oder Vorwärtseinsetzen finden wir $n, m \in \mathbb{Z}$ mit $15 = m\cdot 4620 + n\cdot 225$:
   Rückwärtseinsetzen
$$\begin{aligned}
15 = a_5 &= a_3 + (-1)\cdot a_4\\
&= a_3 + (-1)\cdot(b + (-1)\cdot a_3) = 2\cdot a_3 + (-1)\cdot b\\
&= 2\cdot(a + (-20)\cdot b) + (-1)\cdot b = 2\cdot a + (-41)\cdot b = 2\cdot 4620 + (-41)\cdot 225
\end{aligned}$$
   Somit ist $m = 2$ und $n = -41$.

Vorwärtseinsetzen

$$\begin{aligned} a_3 &= a - 20 \cdot b \\ a_4 &= b - a_3 = b - (a - 20 \cdot b) = -a + 21 \cdot b \\ 15 = a_5 &= a_3 - a_4 = (a - 20 \cdot b) - (-a + 21 \cdot b) = 2 \cdot a + (-41) \cdot b \end{aligned}$$

Somit ist $m = 2$ und $n = -41$.

3. Mit Hilfe der Polynomdivision mit Rest erhält man für $a_1 = f(X)$ und $a_2 = g(X)$

$$\begin{array}{l} (X^5 + X^4 \qquad - 2X^2 - 9X - 22) \;\; : (X^3 + X^2 - 3X - 6) = X^2 + 3 = q_1 \\ \underline{X^5 + X^4 - 3X^3 - 6X^2} \\ \qquad\qquad 3X^3 + 4X^2 \\ \qquad\qquad \underline{3X^3 + 3X^2 - 9X - 18} \\ \qquad\qquad\qquad X^2 \qquad - 4 \quad = a_3 \end{array}$$ (Rest) und

$$\begin{array}{l} (X^3 + X^2 - 3X - 6) \;\; : (X^2 - 4) = X + 1 = q_2 \\ \underline{X^3 \qquad - 4X} \\ \qquad X^2 \; + \; X \\ \qquad \underline{X^2 \qquad - 4} \\ \qquad\qquad X - 2 \quad = a_4 = ggT(f(X), g(X)) \end{array}$$ (Rest), da

$(X^2 - 4) : (X - 2) = X + 2$ mit Rest 0 ist.

Bemerkung: Hier nimmt der Grad der Polynome ab, d.h. $0 \leq grad(a_{i+1}) \leq grad(a_i)$.

Man erhält also folgendes Schema des euklidischen Algorithmus:

$$\begin{aligned} X^5 + X^4 - 2X^2 - 9X - 22 &= (X^2 + 3) \cdot (X^3 + X^2 - 3X - 6) + (X^2 - 4) \\ X^3 + X^2 - 3X - 6 &= (X + 1) \cdot (X^2 - 4) + (X - 2) \\ X^2 - 4 &= (X + 2) \cdot (X - 2) + 0 \end{aligned}$$

Somit gilt $ggT(X^5 + X^4 - 2X^2 - 9X - 22 \;\; , \;\; X^3 + X^2 - 3X - 6) = X - 2$.

4. Kettenbruchdarstellung von $x = 2,3088235$ nach Vorlesung: $x = p_0 + \frac{1}{p_1 + \frac{1}{p_2 + \frac{1}{p_3 + \cdots}}}$. Es gilt:

$$x = 2,3088235 = 2 + 0,3088235 = 2 + \frac{1}{\frac{1}{0,3088235}} \approx 2 + \frac{1}{3,2380955} = 2 + \frac{1}{3 + 0,2380955}$$

$$= 2 + \frac{1}{3 + \frac{1}{\frac{1}{0,2380955}}} \approx 2 + \frac{1}{3 + \frac{1}{4,1999953}} = 2 + \frac{1}{3 + \frac{1}{4 + 0,1999953}} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{\frac{1}{0,1999953}}}}$$

$$\approx 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5,0001175}}} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5 + 0,0001175}}}$$

Abruch, da im nächsten Schritt $p_4 = 8510$, d.h. $a, b \geq 1000$ wäre. Wir erhalten also:

$$2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5}}} = 2 + \frac{1}{3 + \frac{5}{21}} = 2 + \frac{21}{68} = \frac{157}{68} \approx 2,3088235$$

P 16. Bestimmen Sie alle Untergruppen von $(\mathbb{Z}, +)$.

Vorbemerkung: Sei $(G, \circ)$ eine Gruppe. Um zu zeigen, dass $U \subset G$ bzgl. $\circ$ eine Gruppe (Untergruppe von G) ist, genügt das Untergruppenkriterium zu zeigen:

(i) $U \neq \{\}$ (nicht leer)

(ii) $\forall a, b \in U \Rightarrow a \circ b \in U$ (abgeschlossen)

(iii) Zu jedem $a \in U$ $\exists\, a^{-1} \in U$ (Inverses Element in U)

1. Behauptung: $n \cdot \mathbb{Z} := \{n \cdot k \mid k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ ist $\forall n \in \mathbb{N}$ bzgl Addition eine Untergruppe von $(\mathbb{Z}, +)$.

Beweis mit Untergruppenkriterium

(i) $n \cdot \mathbb{Z} \neq \{\}$

(ii) $a, b \in n\mathbb{Z} \Rightarrow \exists p, q \in \mathbb{Z}: a = p \cdot n,\ b = q \cdot n \Rightarrow a + b = (p+q) \cdot n \Rightarrow a + b \in n \cdot \mathbb{Z}$

(iii) Zu $a = p \cdot n \in n \cdot \mathbb{Z}$ ist $a^{-1} = (-p) \cdot n \in n \cdot \mathbb{Z}$ das Inverse $(a + a^{-1} = 0)$

Bemerkung: Für $n = 1$ bzw $n = 0$ erhält man die trivialen Untergruppen $(\mathbb{Z}, +)$ und $(\{0\}, +)$ von $(\mathbb{Z}, +)$

2. Behauptung: $(n \cdot \mathbb{Z}, +)$ mit $n \in \mathbb{N}$ sind alle Untergruppen von $(\mathbb{Z}, +)$

Beweis: Sei $(U \neq \{0\}, +)$ eine nichttriviale Untergruppe von $(\mathbb{Z}, +)$ und $a := \min\{u \in U \mid 0 < u\}$ (*)

1. Schritt: Dann ist $a \cdot \mathbb{Z} \subset U$ denn

- mit a und $p \in \mathbb{N}$ ist auch $a \cdot p = \underbrace{a + \cdots + a}_{p\text{-fache Summe}} \in U$
- mit a ist auch $-a \in U$

$\Rightarrow a \cdot z \in U \quad \forall z \in \mathbb{Z} \Rightarrow a \cdot \mathbb{Z} \subset U$

2. Schritt: Annahme $\exists\, b \in U \setminus a \cdot \mathbb{Z} \Rightarrow -b \in U \Rightarrow$ o.E. $b > 0$

$\overset{(*)}{\Rightarrow} 0 < a < b \Rightarrow b - a,\ b - 2a, \ldots, b - q \cdot a \in U$

Division mit Rest: $\exists\, q \in \mathbb{N}$: $b = q \cdot a + r$ mit $0 < r < a$

$\Rightarrow b - q \cdot a = r \in U \not\Rightarrow$ (*) wegen $r < a$!

$\Rightarrow \nexists\, b \in U \setminus a \cdot \mathbb{Z} \Rightarrow$ **$U = a \cdot \mathbb{Z}$ mit $a \in \mathbb{N}$.**

P 17. Kern und Bild

Gegeben sei die Abbildung $f : \mathbb{R}^3 \to \mathbb{R}^3,\ (x, y, z) \mapsto (x - 3y + z, -x + 2y, y - z)$

1. Bestimmen Sie $Kern(f)$ und $Bild(f)$.
2. Ist f ein Homomorphismus? Ist dieser injektiv oder surjektiv ?

aus Vorlesung: $(G,\circ)$, $(H,\bullet)$ seien Gruppen und $f: G \to H$ eine Abbildung

$Kern(f) := \{ g \in G \mid f(g) = e_H \}$

$Bild(f) := \{ f(g) \in H \mid g \in G \} = \{ h \in H \mid \exists g \in G : f(g) = h \}$ (beachte unterschiedliche Sichtweise!)

f Homomorphismus $\Leftrightarrow \forall g_1, g_2 \in G : f(g_1 \circ g_2) = f(g_1) \bullet f(g_2)$

f injektiv $\Leftrightarrow (\forall x, y \in G$ mit $f(x) = f(y) \Rightarrow x = y)$

f surjektiv $\Leftrightarrow \forall y \in H\ \exists x \in G : f(x) = y \Leftrightarrow Bild(f) = H$,

---

Hier $G = H = \mathbb{R}^3$, Gruppe $(\mathbb{R}^3, +)$

Abbildung $f : (x, y, z) \mapsto (x - 3y + z, -x + 2y, y - z)$

1.) Kern(f): Suche $(x, y, z) \in \mathbb{R}^3$ mit $f(x, y, z) = (0, 0, 0) \Leftrightarrow$ LGS

$$\begin{array}{lll} x - 3y + z = 0 & & x - 3y + z = 0 \\ -x + 2y = 0 & \Leftrightarrow & -y + z = 0 \\ y - z = 0 & & 0 = 0 \end{array}$$

Wähle z.B. $z = \lambda \in \mathbb{R} \Rightarrow y = \lambda$ und $x = 3 \cdot y - z = 2\lambda$, d.h. $(x, y, z) = (2\lambda, \lambda, \lambda)$ mit $\lambda \in \mathbb{R}$.

$\Rightarrow$ $Kern(f) = \{ (2\lambda, \lambda, \lambda) \in \mathbb{R}^3 \mid \lambda \in \mathbb{R} \}$ (geom. Deutung: Gerade mit Richt. (2,1,1))

Bild(f): Suche alle $(a, b, c) \in \mathbb{R}^3$, zu denen es ein $(x, y, z) \in \mathbb{R}^3$ mit $f(x, y, z) = (a, b, c)$ gibt $\Leftrightarrow$ LGS (nicht notwendig eindeutig!)

$$\begin{array}{lll} x - 3y + z = a & & x - 3y + z = a \\ -x + 2y = b & \Leftrightarrow & -y + z = a + b \\ y - z = c & & 0 = a + b + c \end{array}$$

$\Rightarrow$ lösbar $\Leftrightarrow a + b + c = 0$

$\Rightarrow$ $Bild(f) = \{ (a, b, c) \in \mathbb{R}^3 \mid a + b + c = 0 \}$ (geom. Deutung: Ebene in $\mathbb{R}^3$)

2.) f homomorph: $f((x_1, y_1, z_1) + (x_2, y_2, z_2)) = f(x_1 + x_2, y_1 + y_2, z_1 + z_2) =$

$= (x_1 + x_2 - 3y_1 - 3y_2 + z_1 + z_2, -x_1 - x_2 + 2y_1 + 2y_2, y_1 + y_2 - z_1 - z_2) =$

$= (x_1 - 3y_1 + z_1, -x_1 + 2y_1, y_1 - z_1) + (x_2 - 3y_2 + z_2, -x_2 + 2y_2, y_2 - z_2) =$

$= f(x_1, y_1, z_1) + f(x_2, y_2, z_2)$

f nicht injektiv, da $|Kern(f)| > 1$, z.B. $f(0,0,0) = (0,0,0) = f(2,1,1)$

f nicht surjektiv, da $Bild(f) \subset \mathbb{R}^3$, z.B. $\nexists (x, y, z)$ mit $f(x, y, z) = (1, 1, 1)$.

Bem. Man kann zeigen: Ein Homomorphismus f ist injektiv $\Leftrightarrow Kern(f) = \{e_G\}$